Paris Security Incident Management

Last updated: June 17, 2021
# Table of Contents

## Security Operations

- Understanding Security Operations ........................................................................................................... 7  
- The Security Operations suite of applications ............................................................................................... 9  
- Security Operations and the ServiceNow Store ............................................................................................ 17  
  - Download an application from the ServiceNow Store for the first time .................................................. 18  
  - Install a Security Operations integration .................................................................................................... 24  
  - Update an application previously downloaded from the ServiceNow Store .......................................... 28  
  - Upgrade your instance to the next family release ....................................................................................... 29  

## Security Incident Response

- Understanding Security Incident Response .................................................................................................... 30  
- Security Incident Response setup .................................................................................................................. 41  
- Security incident creation .............................................................................................................................. 139  
- Manage Predictive Intelligence for User Reported Phishing ...................................................................... 187  
- Configure Predictive Intelligence for User Reported Phishing .................................................................. 194  
- Assigning security analysts ............................................................................................................................ 196  
- Managing security incidents and inbound requests ...................................................................................... 201  
- Manage security threats using the Security Analyst Workspace ............................................................... 282  
- Playbook Resources ........................................................................................................................................ 313  
- Security Incident Response reporting ........................................................................................................... 357  
- Security Incident Response integrations ......................................................................................................... 371  
- Mobile Experience for Security Incident Response ..................................................................................... 1324  
- Security Incident Response Orchestration .................................................................................................... 1387  
- Security Incident Response flow templates .................................................................................................. 1429  

## Vulnerability Response

- Understanding the Vulnerability Response application .................................................................................. 1452  
- Vulnerability Response implementation ........................................................................................................ 1528  
- Installation of Vulnerability Response and supported applications ......................................................... 1536  
- Vulnerability Response remediation overview ............................................................................................ 1712
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Response integrations</td>
<td>1841</td>
</tr>
<tr>
<td>Mobile experience for Vulnerability Response</td>
<td>2010</td>
</tr>
<tr>
<td>Vulnerability Response Orchestration</td>
<td>2043</td>
</tr>
<tr>
<td>Application Vulnerability Response</td>
<td>2050</td>
</tr>
<tr>
<td>Configure Application Vulnerability Response</td>
<td>2056</td>
</tr>
<tr>
<td>Application Vulnerability Response remediation progress monitoring</td>
<td>2103</td>
</tr>
<tr>
<td>Application Vulnerability Response integrations</td>
<td>2114</td>
</tr>
<tr>
<td>Configuration Compliance</td>
<td>2128</td>
</tr>
<tr>
<td>Understanding Configuration Compliance</td>
<td>2129</td>
</tr>
<tr>
<td>Configuration Compliance setup</td>
<td>2168</td>
</tr>
<tr>
<td>Configuration Compliance discovery</td>
<td>2210</td>
</tr>
<tr>
<td>Configuration Compliance correlation</td>
<td>2220</td>
</tr>
<tr>
<td>Configuration Compliance reporting</td>
<td>2229</td>
</tr>
<tr>
<td>Configuration Compliance remediation</td>
<td>2234</td>
</tr>
<tr>
<td>Configuration Compliance integrations</td>
<td>2252</td>
</tr>
<tr>
<td>Threat Intelligence</td>
<td>2298</td>
</tr>
<tr>
<td>Understanding Threat Intelligence</td>
<td>2299</td>
</tr>
<tr>
<td>Set up Threat Intelligence</td>
<td>2305</td>
</tr>
<tr>
<td>IoC Repository</td>
<td>2327</td>
</tr>
<tr>
<td>MITRE-ATT&amp;CK™ framework overview</td>
<td>2398</td>
</tr>
<tr>
<td>Threat Intelligence administration</td>
<td>2452</td>
</tr>
<tr>
<td>Threat Intelligence integrations</td>
<td>2454</td>
</tr>
<tr>
<td>Threat Intelligence Orchestration</td>
<td>2474</td>
</tr>
<tr>
<td>Security Case Management</td>
<td>2479</td>
</tr>
<tr>
<td>Trusted Security Circles</td>
<td>2512</td>
</tr>
<tr>
<td>Trusted Security Circles overview</td>
<td>2513</td>
</tr>
<tr>
<td>Trusted Security Circles and Threat Intelligence sharing guidelines</td>
<td>2517</td>
</tr>
<tr>
<td>Trusted Security Circles messages</td>
<td>2519</td>
</tr>
<tr>
<td>Domain separation and Trusted Security Circle</td>
<td>2521</td>
</tr>
<tr>
<td>Set up Trusted Security Circle</td>
<td>2527</td>
</tr>
<tr>
<td>Trusted Security Circles threat data sharing</td>
<td>2532</td>
</tr>
</tbody>
</table>
Create a security incident from shared observables ........................................ 2540
Components installed with Threat Intelligence Sharing ................................... 2540
Security Operations common functionality ..................................................... 2542
Create and define filter groups in Security Operations .................................... 2546
Shared data transformation ............................................................................. 2548
Security Operations email processing ............................................................. 2552
Security Operations field mapping .................................................................. 2565
Security Operations field value transforms .................................................... 2570
Security Operations enrichment data mapping ................................................. 2571
Security Operations user-defined escalation .................................................. 2574
Create domain-separated property overrides ................................................. 2576
Create an operating system group ................................................................. 2578
Set up security tag groups and tags ............................................................... 2579
Security annotations ...................................................................................... 2584
Components installed with Security Support Common .................................... 2587
Search Security Operations ............................................................................ 2587
Security Operations Integration Reference .................................................... 2588
Security Operations workflow triggers ......................................................... 2755
Security Operations Orchestration ................................................................. 2758

Index ................................................................................................................. a
Security Operations

ServiceNow® Security Operations brings incident data from your security tools into a structured response engine that uses intelligent workflows, automation, and a deep connection with IT to prioritize and resolve threats based on the impact they pose to your organization.

Automate all your security tools and work seamlessly with IT

With Security Operations, realize the full value of your Now Platform® solution. Many organizations struggle with identifying security threats and vulnerabilities, prioritizing them, and coordinating with IT to remediate them. Using Security Operations, security analysts and vulnerability managers can seamlessly automate their security tools and communicate with IT by working in a unified platform.

View and download the full infocard for a highlight of Security Operations features.

<table>
<thead>
<tr>
<th>Identify, prioritize, and remediate vulnerabilities in software, operating systems, and assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>The ServiceNow® Vulnerability Response application helps organizations identify and respond quickly and efficiently to vulnerabilities. Scan data from leading vendors to give your teams a single platform for response that can be shared between security and IT to resolve vulnerabilities.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Identify, prioritize, and remediate critical security incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>The ServiceNow® Security Incident Response application simplifies the process of identifying critical incidents by applying</td>
</tr>
</tbody>
</table>
### Identify, prioritize, and remediate misconfigured assets

The ServiceNow® Configuration Compliance application prioritizes and remediates misconfigured assets using data gathered from third-party security configuration assessment scans.

### Access your company’s Structured Threat Information Expression (STIX) data

The ServiceNow® Threat Intelligence application helps incident responders find Indicators of Compromise (IoC) and hunt for low-lying attacks and threats. The results are reported directly to security incidents.

### Access Security Operations with your mobile device

Access the Vulnerability Response and Security Incident Response applications on your Now Platform instance with your Android or iOS mobile device. As a remediation owner or security analyst, manage security incidents and vulnerability groups so that you can begin remediation without being tied to your desktop.

---

### Identify, prioritize, and remediate vulnerabilities in software, operating systems, and assets

![Diagram of vulnerability management process]

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.

Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
The Vulnerability Response application imports and automatically groups vulnerable items according to group rules enabling you to remediate vulnerabilities quickly. Vulnerability data is pulled from internal and external sources, such as the National Vulnerability Database (NVD) or third-party integrations. Compare vulnerability data pulled from internal and external sources. For any vulnerable items, create change requests and security incidents using vulnerability groups to remediate issues and mitigate risk.

**Identify, prioritize, and remediate critical security incidents**

With the Security Incident Response (SIR) application, integrate your existing Security Information and Event Manager (SIEM) tools with Security Operations applications to import threat data (via APIs or email alerts), and automatically create prioritized security incidents. Manage the life cycle of your security incidents from initial analysis to containment, eradication, and recovery. The Security Incident Response application enables you to get a comprehensive understanding of incident response procedures performed by your analysts, and understand trends and bottlenecks in those procedures with analytic-driven dashboards and reporting.
Identify, prioritize, and remediate misconfigured assets

With the Configuration Compliance application, use test results obtained from third-party Strong Customer Authentication (SCA) integrations to verify compliance with security or corporate policies. This application uses the assets listed on the ServiceNow® Configuration Management Database (CMDB) to determine which items are most critical. Workflows and automation enable quick action against individual assets or groups for bulk changes. Identify and remediate non-compliant configuration items. Automatically import policies, tests, authoritative sources, and technologies and assign test results to groups or individuals for remediation.
Access your company’s Structured Threat Information Expression (STIX) data.

Use the Threat Intelligence application to automatically search threat feeds for relevant information when an IoC is connected to a security incident and can send IoCs to third-party sources for additional analysis. The Threat Intelligence application uses Structured Threat Information Expression (STIX) as a language to describe cyber threat information in a standardized and structured manner.
Mobile experience for Security Operations

1. Tap ServiceNow Agent Mobile App to open the app
2. Add a Now platform instance with Vulnerability Response (VR) installed
3. Log in to Now platform instance

Vulnerability Response

- Vulnerability Groups (VGs)
  - Assigned to My Groups 56
  - Assigned to Me 27

- Search (VGs)
  - Search VGs

VR mobile landing page

Access the Vulnerability Response and Security Incident Response applications on your Now Platform instance with your Android or iOS mobile device.
Get started

- For an overview about Security Operations in your Now Platform instance, see Understanding Security Operations.

- For information about all the Security Operations applications available for download from the ServiceNow Store, see Security Operations and the ServiceNow Store.

Applications and features

- Vulnerability Response
- Security Incident Response
- Configuration Compliance
- Threat Intelligence

Understanding Security Operations

Security Operations brings incident data from your security tools into a structured response engine that uses intelligent workflows, automation, and a deep connection with IT to prioritize and resolve threats based on the impact they pose to your organization.

Security Operations in a nutshell

The Security Operations ecosystem can be configured in any number of ways, depending on the needs of your company and the Security Operations products you license. The following diagram provides the flow of a basic Security Operations system.
1. The first step is to use the ServiceNow application to find applications and devices on your network, and then update the ServiceNow Configuration Management Database (CMDB).

2. Integrate your existing Security Information and Event Manager (SIEM) tools with Security Operations applications to import threat data (via APIs or email alerts), and automatically create prioritized security incidents.

3. Use workflows and the Vulnerability Response application to instantly prioritize events, security incidents and vulnerabilities.

4. Enrich data using the Threat Intelligence application, as well as other machine learning or artificial intelligence operations capabilities.

5. Use Risk Management and other Governance, Risk, and Compliance applications to identify, assess, respond to, and continuously monitor Enterprise and IT risks that may negatively impact business operations.

6. Workflows built into all Security Operations applications take the guesswork and the busywork out of remediation.

7. Instantly see detailed information about your security posture using dashboards.

Connecting security with IT

Using Security Operations, security analysts and vulnerability managers can seamlessly communicate with IT by working in a unified platform. You can hand off patching and other tasks to IT while still maintaining visibility into the tasks. Skills-based routing assigns tasks to the correct responders, and service level agreements ensure the work is performed on time.

The Now Platform facilitates faster collaboration between security and IT personnel; however, sensitive security data is still protected by user roles. This means that access to security data can be restricted from users with the admin role unless they also have a security role.
Visually tracking your security
Security Operations offers role-based dashboards and reports you can customize to show the status of your security. All security incidents and vulnerabilities, with enriched context, visually show how your critical business services are being affected by threats. Dashboards enhanced with the ServiceNow Performance Analytics product shows the status of your security performance over time, so you can track how your security posture is improving.

Tracking your security posture in one convenient view

The Security Operations suite of applications
Using the power of the Now Platform, Security Operations applications allow you to scale your security solution to the needs of your business and the types of cyber threats you face.
How the Security Operations pieces fit together
As shown, Security Operations appears to be a puzzle. But when the pieces are fit together and you reveal the picture, the power and flexibility of the Now Platform becomes apparent. Each application and the other application that each touches are described in the subsequent sections.

**Note:** The Governance, Risk, and Compliance (GRC) applications are not included in the Security Operations application suite. However, they integrate and share data with Security Operations, so are included in the following descriptions and diagrams.

The Security Operations suite (click image to enlarge)

The Security Incident Response application
At the heart of the Security Operations ecosystem is the Security Incident Response (SIR) application. Security Incident Response simplifies the process of identifying critical incidents by applying powerful workflow and automation tools that speed up remediation. Integrate your existing Security Information and Event Manager (SIEM) tools with Security Operations applications to import threat data (via APIs or email alerts), and automatically create prioritized security incidents.

There are many avenues within the Security Operations ecosystem for automatically and manually creating security incidents, as illustrated.
How Security Incident Response works with other Security Operations applications (click image to enlarge)
You can easily view and track response tasks. Using SLA thresholds, Security Incident Response notifies analysts assigned to tasks if they are not completed on time, or the tasks are automatically escalated, depending on how the system is configured. So no tasks are skipped, and no decisions are ignored. Additionally, analysts can proactively keep stakeholders in the loop from within the Now Platform via conference calls or using the Connect chat feature.

Security Incident Response automates basic tasks, such as approval requests, malware scans, or threat data enrichment when SIR is integrated with the ServiceNow Threat Intelligence application. This type of automation speeds up incident response and allows the security team to spend more time hunting complex and critical threats. Orchestration packs for integrated security products automate often-repeated actions, such as firewall block requests, from within Security Operations. Playbooks allow you to resolve certain types of security threats in a step-by-step manner. For example, you can resolve phishing attacks and threats caused by malicious code activity using playbooks.

All incident activities, from analysis and investigation, to containment and remediation, are tracked in the platform. When an incident is closed, a post-incident review is distributed to all team members to create a historical audit record for future reference.

Note: For more information, see Understanding Security Incident Response.

The Vulnerability Response application

The Vulnerability Response application aids in prioritizing your vulnerable assets and adds context to help you determine when business-critical systems are threatened. Using the CMDB, Vulnerability Response can also easily identify cross-system dependencies and quickly assess the business impact of changes or downtimes. You can view all vulnerabilities affecting a given service, as well as the current state of all vulnerabilities affecting your organization.

Response teams can also leverage the workflow and automation tools in the Now Platform to remediate vulnerabilities faster. When critical vulnerabilities are found, a workflow can automatically initiate an emergency patch approval request. Once approved, orchestration tools can apply the patch and trigger an additional vulnerability scan to ensure the issue has been resolved.

For non-urgent patches, simply click a button to create a change request and send the relevant information to IT. This results in a coordinated remediation strategy for vulnerabilities across services and assets that can address the most critical items quickly.
How Vulnerability Response works with other Security Operations applications

The Threat Intelligence application

Security Operations includes a threat intelligence application to help incident responders find Indicators of Compromise (IoC) and hunt for low-lying attacks and threats. It automatically searches threat feeds for relevant information when an IoC is connected to a security incident and can send IoCs to third-party sources for additional analysis. The results are reported directly in the security incident record for the analyst to review, saving valuable time. ServiceNow

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
supports multiple threat feeds, as well as STIX and TAXII, to incorporate threat intelligence data from a variety of sources.

How Threat Intelligence works with other Security Operations applications

Security Analyst - Manually define Observables, IOCs, Threat Sources

Security Analyst - 3rd party integration - define Observables, IOCs, Threat Sources

KEY

Threat Intelligence

Security Incident Response

3rd Party Integrations

Threat Intelligence (additional information to help remEDIATE-threats)

Create case for high impact threats (higher level SI)

Security Incident

Note: For more information, see .Understanding Threat Intelligence.

The Configuration Compliance application

Improperly configured software puts organizations at risk of compromise. Configuration Compliance prioritizes and remediates misconfigured assets using data gathered from third-party security configuration assessment scans. It leverages the CMDB to determine which items are most critical. Workflows and automation enable quick action against individual assets or groups for bulk changes.

Easily coordinate with IT in a single platform to address changes and updates. In addition, Configuration Compliance data can be fed into the continuous monitoring feature of ServiceNow Governance, Risk, and Compliance to further mitigate risk.
How Configuration Compliance works with other Security Operations applications

![Diagram showing the process of Configuration Compliance]

**Policy and Compliance**
- Compliance Manager sets Control Objectives with defined configurations

**KEY**
- GRC
- Configuration Compliance
- 3rd Party Integrations

**Configuration Compliance**
- Continuous monitoring of Policies and Controls

**Change Request**

**Note:** For more information, see Understanding Configuration Compliance.

**The Trusted Security Circle application**

Share threat intelligence data with industry peers, suppliers, or a global circle of ServiceNow customers with Trusted Security Circle. Send an anonymous query containing security observables to other users and receive a sightings count automatically. With this data, security analysts can determine whether suspicious activity may be part of a larger attack.

Users can set sightings count thresholds to automatically create a security incident if the observable count limit is exceeded. Participating in Trusted Security Circle can serve as an early warning of attacks targeted at common groups.
How Trusted Security Circle works with other Security Operations applications

Manually shared threat information (Observables, IOCs, Threat Sources, etc.)

KEY
- Trusted Security Circles
- Security Incident Response

Trusted Security Circles
Sightings Search (Circle Admin)

Security Incident

Note: For more information, see Trusted Security Circles overview.

The Governance, Risk, and Compliance applications
The ServiceNow Governance, Risk, and Compliance (GRC) applications help transform inefficient processes across your extended enterprise into an integrated risk program. Through continuous monitoring and automation, ServiceNow delivers a real-time view of compliance and risk, improves decision making, and increases performance across your organization and with vendors. Only ServiceNow can connect the business, security, and IT with an integrated risk framework that transforms manual, siloed, and inefficient processes into a unified program built on a single platform.

- Risk Management—Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise, and respond to critical changes in risk posture.

- Policy and Compliance Management—Automate best practice lifecycles, unify compliance processes, and provide assurances around their effectiveness.

- Audit Management—Scope and prioritize audit engagements using risk data and profile information to eliminate recurring audit findings, enhance audit assurance, and optimize resources around internal audits.

- Vendor Risk Management—Institute a standardized and transparent process to manage the lifecycle for risks assessments, due diligence, and risk response with business partners and vendors.
How the Governance, Risk, and Compliance applications work with Security Operations applications (click image to enlarge)

Note: For more information, see .

Security Operations and the ServiceNow Store

Starting with Madrid, all Security Operations applications and supported integrations are available for download from the ServiceNow Store. This allows you to obtain new and updated features more rapidly. Before you can use any Security Operations applications, you must verify that you have entitlement to them (that is, you have valid licenses to use them), download them from the ServiceNow Store, and activate them.

The ever-growing list of Security Operations applications available for download includes:
• Security Incident Response (and supported integrations)
• Vulnerability Response (and supported integrations)
• Threat Intelligence (and supported integrations)
• Configuration Compliance
• Trusted Security Circle

Watch this five-minute video to learn about downloading Security Operations and GRC applications from the ServiceNow Store. This 5-minute video describes how to download Security Operations and GRC applications from the ServiceNow Store.

The process you use to obtain Security Operations applications and integrations depends on whether you are downloading an application for the first time, updating an application that you previously downloaded from the ServiceNow Store, or upgrading from one family release to the next one.

**Download an application from the ServiceNow Store for the first time**

Downloading an application from the ServiceNow Store for the first time involves a number of easy steps. Some of the steps are performed on the ServiceNow Store and some in your instance.

**Before you begin**
Role required: admin

**About this task**
The ServiceNow Store allows you to download core products and applications. A product contains one or more applications that are licensed as a group. For example, Security Incident Response is a product. The process involves these steps:

• In the ServiceNow Store, you must ensure that you have entitlements (or licenses) to the application and its dependent applications.

  📘 **Note:** This process applies only to applications downloaded to production instances. If you’re downloading applications to sub-production or development instances, it’s not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

• Finally, you can activate the application and run it on your instance.
Note: Starting with Orlando, dependency plugins are automatically activated when you activate a core application. For example, when you activate the Vulnerability Response application, the Vulnerability Response Dependencies plugin is also activated. For more information, see Activate a ServiceNow Store application.

Get entitlement for a Security Operations product or application

The first step in installing a Security Operations application is to verify that the application or the product and its associated applications have valid ServiceNow entitlements.

Before you begin
Role required: admin
Individuals performing entitlement must have a Now Support account and have permission to request applications for the instances under consideration.

Note: This process applies only to applications downloaded to production instances. If you are downloading applications to sub-production or development instances, it is not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Procedure

1. Navigate to the ServiceNow Store.

2. Click Login and log in using your HI credentials.

3. Click the ServiceNow Products tab to view all available ServiceNow products. Integrations and other types of content are shown on the Certified Apps tab.
Note: For the sake of this example, assume you are acquiring entitlement for the Security Incident Response product.

4. Click the plus (+) sign next to the product name you are getting entitlement to. All applications associated with the product you are entitling are listed. When you have obtained entitlement to the core product, the applications listed under it are also entitled.

Note: You can also click the product name to view more information about the product and its associated applications.
5. Click **Opt-in** to verify that you have entitlement to the product and the applications listed. You are prompted to read and accept the ServiceNow terms and conditions.

![ServiceNow Products](image)

I agree to the ServiceNow Product Terms and Conditions.

[Cancel] [Accept]

6. Select the check box and click **Accept**.

7. Notice that a check mark appears next to the product name and the Manage Entitlements button appears.

![Security Incident Response](image)

![Unsubscribe] [Manage Entitlement]

The check mark indicates that you have subscribed to the product and its associated applications. It is time to manage your entitlements. This is a one-time process for this product and any other products you want to install in the future.

8. Optionally, you can click **Manage Entitlements** to change the instances affected by the applications to which you are entitled.

![Manage Entitlements for Security Incident Response](image)

Entitlement Type

- [ ] Remove all existing entitlements
- [ ] Entitle all Instances
- [ ] Entitle selected Instances

[Cancel] [OK]

9. After you have agreed to the ServiceNow Terms and Conditions and managed entitlements, you can entitle other products with a single click.
**Activate a ServiceNow Store application**

After an application has been given entitlement, you must activate its dependencies plugin and activate the application. This process also applies to applications downloaded to sub-production instances.

**Before you begin**

Role required: admin

**Procedure**

1. Navigate to **System Applications > All Available Applications > All.**
Note: Starting with Orlando, dependency plugins are automatically activated when you activate a core application. For example, when you activate the Vulnerability Response application, the Vulnerability Response Dependencies plugin is also activated. Hence, steps 2 through 5 are optional.

2. Search for the dependencies plugin for the application you want to activate. For example, if you are activating Security Incident Response, locate the Security Incident Response Dependencies plugin.

3. Click Install. The Activate Plugin dialog box appears.
4. In the **Activate Plugin** dialog box, click **Activate**.

5. When the activation is complete, click **Close & Reload Form**.

6. Now locate the core product you are activating, click the **Install with demo data** check box if you want to load demo data, and click **Install**. Your application is automatically installed on your instance.

   **Note:** If you do not select the **Install with demo data** check box, demo data is not available to install from the **Application Manager** later. For information on how to install or reinstall demo data after the initial installation, see the Work around to install demo data if application is already installed [KB0722909] article in the HI Knowledge Base.

**Install a Security Operations integration**

All ServiceNow integrations are available on the ServiceNow Store. Core applications, such as Security Incident Response, are visible in the **ServiceNow Products** tab on the store. Integration add-ons are visible in the **Certified Apps** tab.

**Before you begin**

Role required: admin

Store installations require a Now Support account and permission to request applications for the instances under consideration.
Procedure

1. Navigate to **Security Operations > Integrations > Integration Configurations**.
   Configuration tiles for the integrations appear.
Notice that the two Email Parser tiles (McAfee and HP) show a **Configure** button. Email parser integrations are included in the base system and do not need to be installed from the ServiceNow Store.

2. Locate the integration you want to install and click **Open Page**. The selected integration is shown in the ServiceNow Store.

3. Click **View Dependencies** and review the app dependencies listed.
4. If the integration has any core application dependencies, such as Security Incident Response, to which your company is not yet entitled:

   a. Follow these instructions to obtain entitlements, download dependency plugins, and activate the applications.
   
   b. Return to this procedure.
   
   c. Click Continue.

5. Click Get. The ServiceNow Terms and Conditions appear.

6. Click Continue. A Purchase screen similar to the following opens.
7. Identify which instances you want the integration to be available on, manage your notifications, and select the **ServiceNow Store Addendum** check box.

8. Click **Get**.

   **Note:** If you are downloading an application for purchase, click **Buy**. If you are downloading an application that requires you to get prior approval from the vendor, click **Request App**.

9. Enter the instance name and a reason for the request, then click **Request**. You are sent an email with detailed installation instructions.

10. Navigate to **System Applications > All Available Applications > All**. A list of applications available for installation is displayed.

11. Locate the application, select it, and click **Install**. Your integration is automatically installed on your instance.

**Update an application previously downloaded from the ServiceNow Store**

If you have previously downloaded an application from the ServiceNow Store and a new version is available, you can update it in your instance.

**Before you begin**

Role required: admin
Procedure

1. Navigate to System Applications > All Available Applications > All.

2. Search for the application you want to update.

3. Select the version you want to upgrade to and click Update. Your application is automatically installed on your instance.

Upgrade your instance to the next family release

If you are currently running a family release (London for example) and want to upgrade to the next release, it is not necessary to acquire the applications from the ServiceNow Store. The application is automatically updated when the platform is updated to the minimum required version.

Security Incident Response

The ServiceNow® Security Incident Response application tracks the progress of security incidents from discovery and initial analysis, through containment, eradication, and recovery, and into the final post incident review, knowledge base article creation, and closure.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release
notes information for all released apps, see the ServiceNow Store version history release notes.

<table>
<thead>
<tr>
<th>Explore</th>
<th>Set up</th>
<th>Administer</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Upgrade to Paris.</td>
<td>• Install and configure Security Incident Response</td>
<td>• Other optional Security Incident Response setup tasks</td>
</tr>
<tr>
<td>• Understanding Security Incident Response</td>
<td>• Understanding Security Incident Response process definition</td>
<td>• Security Incident Response reporting</td>
</tr>
<tr>
<td>• Domain separation and Security Incident Response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Security UI (video)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use</th>
<th>Develop</th>
<th>Integrate</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Managing security incidents and inbound requests</td>
<td>• Developer training</td>
<td>• Security Incident Response integrations</td>
</tr>
<tr>
<td>• Manage lookups and scans</td>
<td>• Developer documentation</td>
<td>• ServiceNow Security Operations integrations development guidelines</td>
</tr>
<tr>
<td>• Manage post incident activities</td>
<td>• Find components installed with an application</td>
<td>• Tips for writing integrations</td>
</tr>
<tr>
<td>• Mobile Experience for Security Incident Response</td>
<td>• Security Incident Response Orchestration</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Troubleshoot and get help</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Ask or answer questions in the Security Operations community</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Search the Known Error Portal for known error articles</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Contact Customer Service and Support</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Request a Security Operations app on Store
If you are a new Security Operations customer on London Patch 6 or later, visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store.

Understanding Security Incident Response
With Security Incident Response (SIR), manage the life cycle of your security incidents from initial analysis to containment, eradication, and recovery. Security Incident Response enables you to get a comprehensive understanding of
incident response procedures performed by your analysts, and understand trends and bottlenecks in those procedures with analytic-driven dashboards and reporting.

Built in integrations with third-party cyber security solutions and partner-developed integrations from the ServiceNow Store enable security automation and orchestration for efficient and accurate incident response.

Watch this nine-minute video to learn about the SIR process, using Security Incident Response to thwart attacks and viewing security activity in the Security Incident Response Explorer. An introduction to Security Incident Response, showing how to get started using the application.

To protect your investigations and keep security incidents private, Security Incident Response provides the means to restrict access to the system to specific security-related roles and ACLs. Non-security administrators can be restricted from access, unless you expressly allow them entry.

**Note:** IT System Administrators [admin] can impersonate ServiceNow users. However, when impersonating a user with an application admin role for Security Incident Response, an admin cannot access features granted by that role, including security incidents and profile information. Access to modules and applications in the navigation bar is also restricted. Also, admin cannot change the password of any user with an application admin role for Security Incident Response.

**SIR information flow**

Security Incident Response employs the following flow of information, from integration through investigation, and then on to resolution and review.
Discovery
Security incidents can be logged or created in the following ways.

- From the Security Incident form
- From events that are spawned internally, or created by external monitoring or vulnerability tracking systems via alert rules, or manually
- From external monitoring or tracking systems
- From the service catalog

Analysis
Depending on the selected view, you are using (default, Non-IT Security, Security ITIL, and so on), the Security Incident form can show any combination of vulnerabilities, incidents, changes, problems, tasks on the affected CI and affected CI groups. The system can identify malware, viruses, and other areas of vulnerability by cross-referencing the National Institute of Standards and Technology (NIST) database, or other third-party detection software. As security incidents are resolved, you can use any incident to create a security knowledge base article for future reference.

Perform further analysis using a business service map to locate other affected systems or business services that can be infected.

Containment, Eradication, and Recovery
As you monitor and analyze vulnerabilities, you can create and assign tasks to other departments. You can use a business service map to create tasks, problems, or changes for all affected systems, documents, activities, SMS messages, bridge calls, and so forth.

Review
After the incident is resolved, other steps can take place before closure. You can perform a post incident review. Creating knowledge base articles can help with future similar incidents. Significant incidents may require a post-incident resolution review. This review can take several forms. For example:

- Conduct a meeting to discuss the incident and gather responses.
- Write and distribute to those teams who worked on an incident a list of resolution review questions designed for each category or priority of incident.
- Incident managers can write the report and gather information on their own.

An incident resolution review report can be automatically generated that includes:
• a summary of what was done
• the time line
• the type of security incident encountered
• all related incidents, changes, problems, tasks, CI groups
• the details of the resolution

In addition, an automated security incident resolution review survey system is available. It gathers the names of all users assigned to a security incident, and sends out a customized survey to gather data about the handling of the incident. This data can then be made available in a generated security incident review report, which you can edit into a final draft. Similar data can be added to a knowledge base article to contain lessons learned and the steps to take to resolve similar issues in the future.

Request apps on the Store
Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Security Incident Response Terminology
The following terms are used in Security Incident Response.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Any security incident not in the closed or cancelled state.</td>
</tr>
<tr>
<td>Administrator lockdown</td>
<td>The ability to restrict Security Incident Response access to personnel with security-related roles and ACLs.</td>
</tr>
<tr>
<td>Inbound security requests</td>
<td>Requests submitted for low-impact security demands, such as requesting a new electronic badge.</td>
</tr>
<tr>
<td>Manage post incident activities</td>
<td>A review of the origins and handling of a security incident. The final product is a post incident report, which documents all actions performed and the reasons for doing them.</td>
</tr>
<tr>
<td>Response tasks</td>
<td>Tasks assigned to a security incident for tracking actions in response to the threat.</td>
</tr>
<tr>
<td>Understanding security</td>
<td>Calculators used to update record values when pre-configured conditions are met.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>incident calculators</td>
<td>Chart type that hierarchically shows security incident data in the form of nested rectangles.</td>
</tr>
<tr>
<td>Security incident treemaps</td>
<td>A request submitted from the security incident catalog for scanning files, URLs, and IP addresses for malware.</td>
</tr>
<tr>
<td>Threat lookup</td>
<td>A request initiated from the Security Incident form for scanning affected resources (servers, computers, and other configuration items) for vulnerabilities.</td>
</tr>
</tbody>
</table>

**Domain separation and Security Incident Response**

This is an overview of domain separation and Security Incident Response. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can then control several aspects of this separation, including which users can see and access data.

**Support level: Standard**

- Includes **Basic** level support.
- Business logic: Processes can be created or modified per customer by the service provider (SP). The use cases reflect proper use of the application by multiple SP customers in a single instance.
- The owner of the instance needs to be able to configure the minimum viable product (MVP) business logic and data parameters per tenant as expected for the specific application.

Use case: An admin needs to be able to make comments mandatory when a record closes for one tenant, but not for another.

**Overview**

In the Security Incident Response application, domain separation enables service providers (SPs) to standardize SOC (Security Operations Center) and Security Incident Response (SIR) procedures across the customer base they serve with lowered operational costs and a higher quality of service. Separate customer workspaces for workflows, dashboards, reports, and so forth, ensures that customer data is separated and never exposed to other clients.
## Domain separation support in Security Incident Response by version releases

<table>
<thead>
<tr>
<th>Release</th>
<th>Support level</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geneva, Helsinki</td>
<td>No support</td>
<td>Initiation of data-level domain separation</td>
</tr>
<tr>
<td>Istanbul</td>
<td>Data only</td>
<td></td>
</tr>
<tr>
<td>Jakarta</td>
<td>Level 2 (Data, Requestor, Fulfiller)</td>
<td><strong>New features:</strong> 3rd-party Integrations support with Level 2 domain separation under a single instance of integration, including Threat Intelligence integrations</td>
</tr>
<tr>
<td>Kingston</td>
<td>Level 2 (Data, Requestor, Fulfiller)</td>
<td><strong>New features:</strong> Sighting Search integration for SIR is enabled with multiple instances, but all instances still live under a single domain. Example: If there are two instances of a Splunk integration configured (SplunkCLOUD and SplunkCORP), both are still leveraged for incident response activities in a single domain, where the implementation was originally configured.</td>
</tr>
<tr>
<td>London</td>
<td>Level 2 (Data, Requestor, Fulfiller)</td>
<td><strong>New features:</strong> All integrations reside across multiple domains</td>
</tr>
<tr>
<td>Madrid</td>
<td>Level 2 (Data, Requestor, Fulfiller)</td>
<td>All integrations can now reside across multiple domains. In the above example, SplunkCloud can be domain1 and SplunkCORP domain2.</td>
</tr>
</tbody>
</table>
Domain separation support in Security Incident Response by version releases (continued)

<table>
<thead>
<tr>
<th>Release</th>
<th>Support level</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>New York</td>
<td>Level 2 (Data, Requestor, Fulfiller)</td>
<td>All integrations reside across multiple domains.</td>
</tr>
<tr>
<td>Orlando</td>
<td>Standard</td>
<td>All integrations reside across multiple domains.</td>
</tr>
<tr>
<td>Paris</td>
<td>Standard</td>
<td>All integrations reside across multiple domains.</td>
</tr>
</tbody>
</table>

Domain separation for the Security Incident Response application covers the following product functionality:

- Security alerts are directed to the appropriate domain of the user whose ID/credential/scope generates the incident and is registered as a Security Incident.
- Alerts generate “observables,” which represent stateful properties or measurable events.
  - Observables extracted from the alert are stored in the domain of the security incident.
- Security workflows in the domain of the security incident are used to orchestrate the response.
- Integrations are configured in the domain of the security incident for response automation.
- Capabilities are configured in the domain of the security incident for response automation. These capabilities (as of the Kingston release) include:
  - Threat Lookup
  - Enrich Observable
  - Enrich Configuration item
  - Get Running Process
  - Get Network Statistics
  - Block Request
  - Isolate Host
  - Sighting Search
  - Email Search and Delete
  - Publish to Watchlist
• Results from Response Automation (such as Threat Lookup or Sighting Search) are stored in the domain of the security incident.

• Other security incidents are cross-referenced in the same domain of the security incident based on a shared set of observables.

• Other users are cross-referenced in the domain of the security incident.

• Configuration Items are cross-referenced in the same domain as the security incident.

• Manual response tasks are added to the domain of the security incident.

• Knowledge base articles and run books are referenced in the domain of the security incident.

• Security Incident Response metrics pertinent to incidents in the domain are displayed on dashboards as well as in reporting.

Note: In the preceding cases, the overarching principles of visibility in separated domains in the NOW Platform apply. As always, an incident in the parent domain can reference artifacts in the child domain, but not the other way around.

How domain separation works in Security Incident Response

The Security Incident Response application manages the life cycle of a security incident end to end. The following use cases are domain-separation aware:

• Ingestion of events and alerts to create security incidents for the analyst in the customer SOC or the MSP to respond:
  ◦ Email parsers (platform based, user-reported phishing, custom)
  ◦ De-duplication events/alerts prior to incident creation
  ◦ Auto extraction of observables
  ◦ Applications in third-party SIEM store

• Enrichment of artifacts involved in the incidents (IP, URLs, domains, file hashes):
  ◦ Asset enrichment (CMDB)
  ◦ Users (Platform)
  ◦ Automation: Observable enrichment (Ex: WhoIs)

• Investigate the incidents with the help of the artifacts and their reputation or association with known threats
Orchestrate: Playbooks and knowledge base articles

Automation: Threat Lookup (Ex: VirusTotal), Sighting Search (Ex: Splunk), Get Running Processes (Ex: Carbon Black)

- **Eradicate** the threat-related artifacts involved in the incident based on the investigation performed
  - Orchestrate: Playbooks and knowledge base articles
  - Automation: Email search and delete (Ex: Microsoft Exchange), Block IP (Ex: Palo Alto Firewall)

- **Measure** the efficiency or Incident response operations
  - Performance Analytics Dashboards: Productivity and incident trends
  - Reconstruction of incident investigation steps from work notes
  - Post-incident review

**Domain separation setup**

Setting up domain separation for Security Incident Response does not require any additional steps. All Security Incident Response tables acquire the Domain column after the instance is domain separated.

**Domain-separated data**

Data can be domain-separated, which means:

- Security incidents in one domain cannot be viewed from other domains.
- Observables extracted from the security incident are placed in the same domain and cannot be viewed from other domains.
- Up to the Kingston release, configured third-party integrations exist in the global domain and are accessible to all other domains in the instance.
- In the Madrid release, third-party integrations can be configured and activated on a per-domain basis. This means that the integration activated and configured in one domain cannot be leveraged in another domain.
- Automations that run on the observables using third-party integrations (for Threat Investigation, Containment, or Eradication), place their results in the domain of the security incident and the results cannot be viewed from another domain.
- Orchestration workflows created in one domain are not visible in another domain.
- Capabilities (as delineated in the preceding capabilities function list) that are invoked stay generic across domains with domain-specific implementation
of the capability being called. For example, a Sighting Search on an IP can invoke a Splunk implementation in one domain and a QRadar implementation in another.

**Configuration**
All aspects of product configuration are self-contained in a domain-separated environment. Setup can be tailored for individual domains.

⚠️ **Note:** Business logic and the processes in #2-5 below can be administered within the tenant domain.

The following tasks must be configured:

1. **System Administration**
   - Assign roles to users and groups of users: User roles installed with Security Incident Response
   - Install one or more third-party integration plugins to work with Security Incident Response: Security Incident Response integrations

2. **User roles installed with Security Incident Response Administration**
   - Add or review roles: Components installed with Security Incident Response
   - Configure groups and users: Create a security incident group
   - Set up incident escalations: Escalate a security incident
   - Set up security incident risk score calculators: Understanding security incident calculators
   - Set up service level agreements: Create a Security Incident Response SLA
   - Set up security incident process definitions: Understanding Security Incident Response process definition
   - Set up post-incident review processes: Manage post incident activities

3. **Security incident email settings**
   - Set the email parsing inbox: Security Operations email parsing
   - Set up email parsers for alert ingestion: Create email parsers in Security Operations
   - Set up email matching rules for user-reported phishing: Create rules to validate user-reported phishing attacks
   - Set up email inbound actions: Inbound email actions

4. **Security incident playbook settings**
• Review and set up runbook documents: Create a Security Incident Response runbook
• Set up security incident workflows: Security Operations common functionality

5. Capability configurations

• Select and configure integrations to work with these capabilities:
  ◦ Block request: Security Operations Integration - Block Request capability
  ◦ Email search and delete: Security Operations Integration - Email Search and Delete capability
  ◦ Enrich configuration item: Security Operations Integration - Enrich CI capability
  ◦ Enrich observable: Security Operations Integration - Enrich Observable capability
  ◦ Get running processes: Security Operations Integration - Get Running Processes capability
  ◦ Isolate host: Security Operations Integration - Isolate Host capability
  ◦ Publish to Watchlist: Security Operations Integration - Publish to Watchlist capability
  ◦ Sighting search: Security Operations Integration - Sightings Search capability
  ◦ Threat lookup: Security Operations Integration - Threat Lookup capability

How tenant domains manage their own application data

• Tenant domain owners create their own email parsing rules for ingesting security incidents.
• Tenant domain owners can configure specific integrations exclusively for use within the domain.
• Tenant domain owners can create their own incident response workflows.
• Tenant domain owners can create their own incident categories, incident response knowledge base articles and runbooks to be associated with incident response workflows.
• Tenant domain users create and close their own security incidents.
Business logic and processes that can be domain separated by instance owner

- Security Incident Response users and groups
- Security Incident Response integrations (starting with the Madrid release)
- Email parsing rules for incident creation
- Business rules to consolidate multiple events or alerts into a security incident
- Workflows for incident response orchestration
- Security incident risk score calculators
- Security incident escalation path
- Security incident SLAs
- Security incident process definitions
- Security incident post-incident review processes

Related information

Domain separation for service providers

Security Incident Response setup

Setup for Security Incident Response involves some mandatory steps and several optional steps, depending on your specific requirements. After you have downloaded Security Incident Response from the ServiceNow Store and installed it, you are ready to run the Setup Assistant to perform basic configuration for Security Incident Response and third-party integrations.

The Security Incident Response setup process

The following diagram illustrates the setup process. It is separated into two sub-processes, downloading and configuring the Security Incident Response application and then downloading and configuring the Security Analyst Workspace.
1. Download and install Security Incident Response

Run Setup Assistant to perform this setup:

- **System administration**
  - Define SIR users and groups
  - Activate integration plugins

- **SIR administration**
  - Define roles
  - Add roles to users and groups
  - Set up incident escalations
  - Set up calculator groups
  - Set up risk score calculators
  - Set up SLAs
  - Set up and select process definitions
  - Set up post incident review
  - Configure domain operations

- **Playbook settings**
  - Review and set up runbooks
  - Set up SIR workflows

- **Email settings**
  - Set the email parsing mailbox
  - Set up parsers for alert ingestion
  - Set up matching rules for phishing
  - Set up email inbound actions

- Configure integrations to work with data from third-party solutions

Manually configure:

- Business processes
- Assignment
- Add-ons

Optional setup steps:

- Lock down security admin
- Manage RCA
The first setup step is to download the Security Incident Response application from the ServiceNow Store. When the download is complete, several dependent applications, including the Setup Assistant, are loaded and ready for use to configure Security Incident Response.

**Setup Assistant**
The Security Incident Response Setup Assistant is a wizard-like application that guides you, step-by-step, through the setup of your base Security Incident Response instance.

The setup steps are fairly self-explanatory; however, if you require additional explanation, you can find additional assistance in the Setup Assistant reference. After you have completed the setup using the Setup Assistant, you can perform other optional setup procedures, as needed. These procedures include options for:

- Setting up the request life cycle
- Creating catalogs and requests
- Configuring notifications
- Setting up manual and auto-assignment
- Enabling the knowledge base, managed documents, and task activities

**Security Analyst Workspace**
When you have completed Security Incident Response configuration, you are ready to install and configure the Security Analyst Workspace, which simplifies security incident analysis.
First, you must download the application from the ServiceNow Store and then configure it. The configuration process includes setting up primary and secondary filters for narrowing down the list of security incidents for analysis.

After you have installed and configured the application, you can open the Security Analyst Workspace by navigating to Security Incident > Incidents (New UI).

**Install and configure Security Incident Response**

Before you run Security Incident Response in your instance, you must download it from the ServiceNow Store and complete configuration steps.

**Before you begin**

Role required: admin
Procedure

1. Follow the instructions for downloading an application from the ServiceNow Store.

2. After you have downloaded the Security Incident Response application and all of its dependency applications, navigate to Security Incident > Setup > Setup Assistant.

3. Follow the instructions on the forms to configure the Security Incident Response base system. For additional information on some of the more complicated setup tasks, see Setup Assistant reference, as needed.

Download and install the Security Analyst Workspace

Before you run the Security Incident Response new UI in your instance, you must download it from the ServiceNow Store and install it.
**Before you begin**
To ensure a smooth installation, verify that you have the required ServiceNow roles for your instance. The following roles are required for installation, configuration, and verification of expected results:

- If not already assigned, the System Administrator [admin] installs the application and assigns the Security Incident Response Admin [sn_sir.admin] role.
- The Security Incident Response Admin [sn_sir.admin] oversees configuration and verifies expected results.

**Role required:** admin

**Procedure**
1. Follow the instructions for downloading an application from the ServiceNow Store and install the Security Incident Response UI application.
2. After installation is complete, you can open the Security Analyst Workspace by navigating to Security Incident > Incidents (New UI)

**Components installed with Security Incident Response**
Several types of components are installed when you download and activate the Security Incident Response application, including user roles, tables, properties, and scheduled jobs.

**Note:** The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

Demo data is available for this feature.
## Properties installed

Users with the System Administrator [admin] role can view the properties. Users with the Security Administrator [sn_si.admin] role can modify them.

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
</table>
| Default start time for all agents when no schedule is set, formatted as 08:00  sn_si.default.start.time | • **Type**: string  
• **Default value**: 08:00  
• **Location**: Security Incident > Administration > Properties |
| Default end time for all agents when no schedule is set, formatted as 17:00  sn_si.default.end.time | • **Type**: string  
• **Default value**: 17:00  
• **Location**: Security Incident > Administration > Properties |
| Include Destination type observables along with other context type observables in the security incident user and CI relationships  sn_si.link_dest_ip | Determines whether a security incident observable with a context type of Destination is displayed under the **Configuration Items** or **Affected Users** tabs. By default, observables with a Destination context type are excluded. To include the observables, choose Yes. |
| Allow customization when creating a Problem or Change Request from a Security Incident  sn_si.popup | When a problem or change is created, this property opens a pop-up window to modify the request.  
If this properties is set to **false**, the problem or change request has the same priority, short description, and description as the security incident without the option to add or edit those fields.  
• **Type**: true | false  
• **Default value**: true  
• **Location**: Security Incident > Administration > Properties |
<table>
<thead>
<tr>
<th><strong>Property</strong></th>
<th><strong>Usage</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Associate Sightings Search results with CIs in the CMDB.</td>
<td>When set to true, sightings search results include associated configuration items that are in your cmdb.</td>
</tr>
<tr>
<td><strong>sn_si.associate_ci_with_sighting_search</strong></td>
<td><strong>Type</strong>: true</td>
</tr>
<tr>
<td>Risk score in the range is highlighted green, formatted as 0 - 49</td>
<td>In the Security Incidents list, security incidents with a risk score between 0 and 49 are marked with a green dot.</td>
</tr>
<tr>
<td><strong>sn_si.risk.score.green</strong></td>
<td></td>
</tr>
<tr>
<td>Risk score in the range is highlighted orange, formatted as 50 - 79</td>
<td>In the Security Incidents list, security incidents with a risk score between 50 and 79 are marked with an orange dot.</td>
</tr>
<tr>
<td><strong>sn_si.risk.score.orange</strong></td>
<td></td>
</tr>
<tr>
<td>Risk score in the range is highlighted red, formatted as 80 - 100</td>
<td>In the Security Incidents list, security incidents with a risk score between 80 and 100 are marked with a red dot.</td>
</tr>
<tr>
<td><strong>sn_si.risk.score.red</strong></td>
<td></td>
</tr>
<tr>
<td>This parameter enables or disables Sightings Search Configurations that have implemented this feature.</td>
<td>When set to true, sightings searches can be performed on activated integrations.</td>
</tr>
<tr>
<td><strong>sn_si.enable_sighting_search</strong></td>
<td><strong>Type</strong>: true</td>
</tr>
<tr>
<td>The number of rows of raw data that are saved when a Sighting Search is performed. Range 0 - 100</td>
<td>This property defaults to 50 rows of raw data. Half of the result rows are reported from the beginning of the search time frame and half from the end of the search time frame. So, if you select 50 rows, 25 come from the start of the search time frame and 25 from the end of the search time frame.</td>
</tr>
<tr>
<td><strong>sn_si.sighting_search_raw_data_rows</strong></td>
<td></td>
</tr>
<tr>
<td>Property</td>
<td>Usage</td>
</tr>
<tr>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>Automatically advance the Incident State to Contain when a Response Task advances to Work In Progress</td>
<td>While using flows or workflows, consider setting this property to false. This enables you to control the Incident State from within flows or workflows. It also helps avoid any potential conflicts while transitioning from one incident state to another.</td>
</tr>
</tbody>
</table>
| sn_si.rollup_task_state | • **Type**: true | false  
• **Default value**: true  
• **Location**: Security Incident > Administration > Properties |

### Assignment properties for Security Incident Response

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location Weight</td>
<td>A rating used when calculating the criteria to use for auto-assigning a security analyst. If, for example, location is considered for a task, the location weight value is added to the security analyst rating.</td>
</tr>
</tbody>
</table>
| sn_si.location.weight | • **Type**: integer  
• **Default value**: 10  
• **Location**: Security Incident > Administration > Properties |

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skills Weight</td>
<td>A rating used when calculating the criteria to use for auto-assigning a security analyst. If, for example, skills are considered for a task, the skills weight value is added to the security analyst rating.</td>
</tr>
</tbody>
</table>
| sn_si.skills.weight | • **Type**: integer  
• **Default value**: 10  
• **Location**: Security Incident > Administration > Properties |

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the maximum number of security analysts to be processed by auto-assignment at a time</td>
<td>The system has an absolute limit of 300 security analysts. If you specify more than 300, it sets the value to that level. The system cannot auto-</td>
</tr>
</tbody>
</table>
| sn_si.max.agents.processed | }
<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>dispatch a task for a dispatch group</td>
<td>that contains more security analysts than the value configured.</td>
</tr>
<tr>
<td>• Type: integer</td>
<td></td>
</tr>
<tr>
<td>• Default value: 100</td>
<td></td>
</tr>
<tr>
<td>• Location: Security Incident &gt;</td>
<td>Administration &gt; Properties</td>
</tr>
<tr>
<td>Time Zone Weight</td>
<td>A rating used when calculating the criteria to use for auto-assigning a security analyst. If, for example, the security analyst time zone is considered for a task, the time zone weight value is added to the security analyst rating.</td>
</tr>
<tr>
<td>sn_si.timezone.weight</td>
<td></td>
</tr>
<tr>
<td>• Type: integer</td>
<td></td>
</tr>
<tr>
<td>• Default value: 10</td>
<td></td>
</tr>
<tr>
<td>• Location: Security Incident &gt;</td>
<td>Administration &gt; Properties</td>
</tr>
<tr>
<td>Amount of time (in minutes) to add</td>
<td>between the end of a task and the travel start of the next.</td>
</tr>
<tr>
<td>sn_si.work.spacing</td>
<td>An example of a valid time value is 10.</td>
</tr>
<tr>
<td>Specified journal fields containing</td>
<td>code tags that render content as HTML.</td>
</tr>
<tr>
<td>sn_si.journal_field.html_enabled</td>
<td></td>
</tr>
<tr>
<td>• Type: string</td>
<td></td>
</tr>
<tr>
<td>• Default value: work_notes, comments</td>
<td></td>
</tr>
<tr>
<td>• Location: Security Incident &gt;</td>
<td>Administration &gt; Properties</td>
</tr>
</tbody>
</table>
# Roles installed

<table>
<thead>
<tr>
<th>Role title [name]</th>
<th>Description</th>
<th>Contains roles</th>
</tr>
</thead>
</table>
| security admin [sn_si.admin] | Full control over all Security Incident Response data. Also administers territories and skills, as needed. | • catalog_admin  
• skill_admin  
• skill_model_admin  
• sn_si.analyst  
• sn_si.manager  
• sn_si.knowledge_admin  
• sn_si.manager  
• template_admin  
• template_editor_global  
• territory_admin  
• treemap_admin  
• user_admin |
| security basic [sn_si.basic] | Underlying role for basic Security access. Users with this role can create and update security incidents, requests, and tasks, as well as problems, | • document_management_user  
• grc_user (if the GRC: Risk plugin is activated)  
• inventory_user  
• pa_viewer  
• service_fullfiller  
• skill_user |
<table>
<thead>
<tr>
<th>Role title [name]</th>
<th>Description</th>
<th>Contains roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>ciso [sn_si.ciso]</td>
<td>View and manipulate the CISO dashboard. Also, if the Vulnerability Response plugin is activated, users with this role can add vulnerability significance definition treemaps to the dashboard.</td>
<td>• pa_reader • sn_si.read</td>
</tr>
<tr>
<td>external [sn_si.external]</td>
<td>External users can view tasks assigned to them.</td>
<td>• service_fulfiller</td>
</tr>
<tr>
<td>integration user [sn_si.integration_user]</td>
<td>External tools can provide new security incident records and update security incident records.</td>
<td>• import_transformer</td>
</tr>
<tr>
<td>knowledge admin [sn_si.knowledge_admin]</td>
<td>Manage, update, and delete the information in the Security Incident knowledge base.</td>
<td>• knowledge_admin</td>
</tr>
<tr>
<td>manager [sn_si.manager]</td>
<td>Same access as security analysts.</td>
<td>• sn_si.basic</td>
</tr>
<tr>
<td>read [sn_si.read]</td>
<td>Read security incidents.</td>
<td>• grc_compliance_reader (if the GRC: Risk plugin is activated)</td>
</tr>
<tr>
<td>Role title [name]</td>
<td>Description</td>
<td>Contains roles</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>special access</td>
<td>Provides access to specific security incidents to users outside of the Security Operations organization.</td>
<td>N/A</td>
</tr>
<tr>
<td>sn_si.special_access</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Scheduled jobs installed

<table>
<thead>
<tr>
<th>Scheduled job</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lookup Security Incident Observables</td>
<td>Performs a lookup for observables on a user-defined schedule.</td>
</tr>
</tbody>
</table>

### Tables installed

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>News Feed Configuration [sn_si_feed_configuration]</td>
<td>Configuration records used to define the content displayed in the security incident news feed.</td>
</tr>
<tr>
<td>Post Incident Review Assignment Rule [sn_si_pir_condition]</td>
<td>Automates selection of participants of a post incident review survey when a security incident is closed.</td>
</tr>
<tr>
<td>Security Incident [sn_si_incident]</td>
<td>Stores a security incident, the responses to the incident, all linked tasks, changes, problems, and incidents related to this security incident.</td>
</tr>
<tr>
<td>Security Incident Audit Log [sn_si_audit_log]</td>
<td>Stores security incident enrichment audit logs.</td>
</tr>
<tr>
<td>Security Incident Calculator [sn_si_calculator]</td>
<td>A calculator to set certain security incident fields when certain conditions are met.</td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security Incident Calculator Group</td>
<td>A grouping of security incident calculators. The order of the calculator group determines which group is evaluated first, and in each group, one calculator at most is used.</td>
</tr>
<tr>
<td>[sn_si_calculator_group]</td>
<td></td>
</tr>
<tr>
<td>Security Incident Enrichment Firewall</td>
<td>Extends from the base table (sn_sec_cmn_enrichment_data_base) and includes all enrichment records specific to Palo Alto Networks Firewall.</td>
</tr>
<tr>
<td>[sn_si_enrichment_firewall]</td>
<td></td>
</tr>
<tr>
<td>Security Incident Enrichment Malware Results</td>
<td>Extends from the base table (sn_sec_cmn_enrichment_data_base) and includes all enrichment records specific to malware.</td>
</tr>
<tr>
<td>[sn_si_enrichment_malware]</td>
<td></td>
</tr>
<tr>
<td>Security Incident Enrichment Network Statistics</td>
<td>Extends from the base table (sn_sec_cmn_enrichment_data_base) and includes all enrichment records specific to network statistics.</td>
</tr>
<tr>
<td>[sn_si_enrichment_network_statistics]</td>
<td></td>
</tr>
<tr>
<td>Security Incident Enrichment Running Processes</td>
<td>Extends from the base table (sn_sec_cmn_enrichment_data_base) and includes all enrichment records specific to running processes.</td>
</tr>
<tr>
<td>[sn_si_enrichment_running_processes]</td>
<td></td>
</tr>
<tr>
<td>Security Incident Enrichment Running Services</td>
<td>Extends from the base table (sn_sec_cmn_enrichment_data_base) and includes all enrichment records specific to running services.</td>
</tr>
<tr>
<td>[sn_si_enrichment_running_service]</td>
<td></td>
</tr>
<tr>
<td>Security Incident Email Search</td>
<td>Maps email search records to security incidents.</td>
</tr>
<tr>
<td>[sn_si_m2m_incident_email_search]</td>
<td></td>
</tr>
<tr>
<td>Security Incident Import</td>
<td>Import table for security incidents. Used to create security incidents from external systems.</td>
</tr>
<tr>
<td>[sn_si_incident_import]</td>
<td></td>
</tr>
<tr>
<td>Security Incident Process Definition</td>
<td>Stores configuration for Security Incident process flows.</td>
</tr>
<tr>
<td>[sn_si_process_definition]</td>
<td></td>
</tr>
<tr>
<td>Security Incident Process Definition Selector</td>
<td>Stores the Security Incident Process Definition to use for security incidents.</td>
</tr>
<tr>
<td>[sn_si_process_definition_selector]</td>
<td></td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Security Incident Related Customer Service Case [sn_si_m2m_incident_customerservice_case]</td>
<td>Maps customer service cases and security incidents</td>
</tr>
<tr>
<td>Security Incident Related Enrichment Data [sn_si_m2m_incident_enrichment]</td>
<td>Maps security incidents and related enrichment data records.</td>
</tr>
<tr>
<td>Security Incident Response Task [sn_si_task]</td>
<td>Manages subtasks related to handling a security incident. These tasks can be assigned to security personnel, or to people in other departments, to manage interdepartmental communication and task tracking.</td>
</tr>
<tr>
<td>Security Incident Response Task Template [sn_si_task_template]</td>
<td>Used to create a Security Incident Response task. These templates are often used in catalog entries, to automatically create a set of appropriate subtasks for a particular type of security incident.</td>
</tr>
<tr>
<td>Security Incident Template [sn_si_incident_template]</td>
<td>Used to create a security incident. These templates are often used in catalog entries to create a prebuilt security incident.</td>
</tr>
<tr>
<td>Security Request [sn_si_request]</td>
<td>A security-related request to the security team.</td>
</tr>
<tr>
<td>Security Scan Request [sn_si_scan_request]</td>
<td>A request for a threat lookup.</td>
</tr>
<tr>
<td>Severity Calculator sn_si_severity_calculator</td>
<td>Defines the severity, impact, risk, and criticality values for a security incident.</td>
</tr>
<tr>
<td>Task Affected User [sn_si_m2m_task_affected_user]</td>
<td>A many-to-many table associating security incidents with affected users.</td>
</tr>
</tbody>
</table>
Other optional Security Incident Response setup tasks

If you are an administrator in the global domain, you configure how Security Incident Response handles day-to-day operations.

Before you begin
Role required: sn_si.admin

Note:
These options are standard to many service management applications, and as such, they use service management terminology. For example, Request is used for the main task (that is, the security incident) and Task is used for subtasks or Response Tasks.

If you are an administrator in a domain lower than the global domain, you can view the Configurations screen, but cannot modify the settings.

Procedure

1. Navigate to Security Incident > Administration > Configuration.

   The options for configuring the applications are organized under these tabs:
   - The Business Process tab contains options for setting up the request life cycle, creating catalogs and requests, and configuring notifications.
   - The Assignment tab contains options for setting up manual and auto-assignment.
   - The Add-ons tab contains options for enabling the knowledge base, managed documents, and task activities.

2. Fill in the fields on the Business process tab.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lifecycle</td>
<td>Maps a capability with an evaluation script. A new subflow can be added to a template workflow to set a response task outcome rather than having an analyst manually set it.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Work notes are required to close or cancel a request or task</td>
<td>Enable this option to require the user to enter work notes before a security incident or response task can be closed or canceled.</td>
</tr>
<tr>
<td>Copy task work notes to request</td>
<td>Enable this option to synchronize response task work notes with the work notes on the security incident. So when work notes in the task are added, the same work notes appear in the parent security incident.</td>
</tr>
</tbody>
</table>

**Catalog and Request Creation**

<table>
<thead>
<tr>
<th>Create or update requests by inbound email</th>
<th>Enable this option to create or update security incidents from inbound emails.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests are created using</td>
<td>Select <strong>catalog or regular form</strong> to activate the catalog and enable automatic publishing of security incident templates to the catalog. Select <strong>regular form only</strong> to deactivate the catalog and disable automatic publishing of security incident templates to the catalog.</td>
</tr>
<tr>
<td>Templates create a dedicated catalog item</td>
<td>Enable this option to activate automatic publishing of catalog items for the application.</td>
</tr>
</tbody>
</table>

**Notifications**

<table>
<thead>
<tr>
<th>For a request or task, when the selected field changes, send notification to recipients</th>
<th>You can configure notifications to be sent to specific recipients when selected fields in security incidents and response tasks change.</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. From <strong>Table</strong>, select <strong>Request (security incident)</strong> or <strong>Task (response task)</strong>.</td>
<td></td>
</tr>
<tr>
<td>b. From <strong>Field</strong>, select the field to use for generating notifications. When a change is made to the selected field, a notification is sent to the identified recipients.</td>
<td></td>
</tr>
<tr>
<td>c. From <strong>Recipients</strong>, select one or more recipients.</td>
<td></td>
</tr>
<tr>
<td>d. If you select <strong>a specific user</strong> or <strong>a specific group</strong>, you are prompted to select a user or group.</td>
<td></td>
</tr>
</tbody>
</table>
e. To define more notifications using other fields or recipients, repeat the preceding steps for the next set of notification settings.

f. To remove a notification, click the icon to the right of the notification.

3. Click the **Assignment** tab and fill in the fields.

**Configuration screen — Assignment tab**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignment method for requests</td>
<td>Select the method for assigning security incidents:</td>
</tr>
<tr>
<td></td>
<td>• <strong>using auto-assignment</strong>: Security incidents are automatically assigned.</td>
</tr>
<tr>
<td></td>
<td>• <strong>using a workflow</strong>: Security incidents are assigned by the selected workflow.</td>
</tr>
<tr>
<td></td>
<td>• <strong>manually</strong>: Security incidents are manually assigned.</td>
</tr>
<tr>
<td>Use this workflow to assign requests</td>
<td>Select the workflow for dispatching security incidents. This field appears when <strong>using a workflow</strong> is selected from the <strong>Assignment method for requests</strong> list.</td>
</tr>
<tr>
<td>Assignment method for tasks</td>
<td>Select the method for assigning response tasks:</td>
</tr>
<tr>
<td></td>
<td>• <strong>using auto-assignment</strong>: Response tasks are automatically assigned.</td>
</tr>
<tr>
<td></td>
<td>• <strong>using a workflow</strong>: Response tasks are assigned by the selected workflow.</td>
</tr>
<tr>
<td></td>
<td>• <strong>manually</strong>: Response tasks are manually assigned.</td>
</tr>
<tr>
<td>Use this workflow to assign tasks</td>
<td>Select the workflow for assigning response tasks. This field appears when <strong>using a workflow</strong> is selected from the <strong>Assignment method for tasks</strong> list.</td>
</tr>
<tr>
<td>Assign requests or tasks based on assignment group coverage areas</td>
<td>Enable this option to limit the assignment of security incidents and response tasks to groups that cover the location of the task.</td>
</tr>
</tbody>
</table>

**Scheduling**

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-selection of agents consider time zone for tasks</td>
<td>Enable this option to consider the time zone of the agent when assigning a task. This field appears when auto-assignment is selected for security incidents or response tasks.</td>
</tr>
<tr>
<td><strong>Additional Factors</strong></td>
<td></td>
</tr>
<tr>
<td>Auto-selection of agents consider location of agents</td>
<td>Enable this option to give preference to agents who are closer to the task location, when assigning any tasks. This field appears when auto-assignment is selected for security incidents or response tasks.</td>
</tr>
<tr>
<td>Auto-selection of agents for tasks requires them to have skills</td>
<td>Select the degree to which agent skills must be matched to a task when determining auto-assignment. • Select all to require that an assigned agent must have all the skills to perform the task. An agent who lacks even one skill is eliminated. • Select some if you want agents who have most of the skills required to perform the task. • Select none if you want to auto-assign agents without taking skills into account. This field appears when auto-assignment is selected for security incidents or response tasks.</td>
</tr>
<tr>
<td>Auto-selection attempt to assign the same agent to all tasks in a request</td>
<td>Enable this option to auto-assign all response tasks for a security incident to the same agent.</td>
</tr>
</tbody>
</table>

4. Click the **Add-ons** tab and fill in the fields.

**Configuration screen — Add-ons tab**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Documentation</strong></td>
<td></td>
</tr>
<tr>
<td>Enable a dedicated knowledge base</td>
<td>Enable this option to activate the knowledge base for Security Incident Response.</td>
</tr>
<tr>
<td>Enable managed documents</td>
<td>Enable this option to add a related list to managed documents.</td>
</tr>
</tbody>
</table>
### Lock down security administration

To protect investigations and keep security incidents private, you can restrict Security Incident Response access to security-specific roles and ACLs. Non-security administrators can be restricted from access, unless you expressly allow them entry.

**Before you begin**

When the Security Incident Response application is activated, the System Administrator user is granted the sn_si.admin role by default. The System Administrator is the only administrator who can set up security groups and users. A security role is required to have access to Security Incident Response features and records.

Role required: sn_si.admin

**Procedure**

1. After the Security Incident Response plugin has been activated, a user with the admin role assigns the Scoped Admin (sn_si.admin) role to at least one user.

2. The user with the admin role changes to the Security Incident scope.

3. Navigate to **System Applications > Applications**.

4. Click **Downloads**.

5. Type **security** in the **Search applications** field.
6. Click Security Incident.

7. Scroll down to the Related Links and click Remove from the role contained by admin.

8. Log out and log back in.
   
   The admin user cannot access the Security Incident Response application.

**Related information**

**Manage Restricted Caller Access**

The Restricted Caller Access (RCA) feature enables an administrator to define cross-scope access to an application or application resource and allow or deny access requests. This feature is enabled in Security Incident Response by default so security analysts can protect sensitive security-related information.

A field called **Caller access** has been added to all tables and script includes in Security Incident Response, and the field defaults to **Caller Tracking**. This setting means that application scopes are allowed access to Security Incident Response tables and script includes. However, a tracking record is created for each record and stored in the Restricted Caller Access Privilege [sys_restricted_caller_access] table.
Take care when changing records from Caller Tracking to Caller Restricted. Records with this status cannot be accessed until an administrator manually allows access to it. The administrator must navigate to System Applications > Application Restricted Caller Access, locate the table or script include for which access has been requested, and change the Status field from Requested to Allowed.

Run quick start tests for Security Incident Response

Validate that Security Incident Response still works after you make any configuration changes, such as applying an upgrade or developing an application. Copy and customize these quick start tests to pass when using your instance-specific data.

Security Incident Response quick start tests require activating Security Incident Response plugin (com.snc.security_incident) and loading the demo data.

<table>
<thead>
<tr>
<th>Test</th>
<th>Description</th>
<th>Release version</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIR: Create Security Incident</td>
<td>Determine whether a user can successfully create a security incident from the security incident form.</td>
<td>Madrid</td>
</tr>
<tr>
<td>SIR: Create Security Incident via Security Incident Catalog</td>
<td>Determine whether a user can successfully create a security incident from the catalog.</td>
<td>Madrid</td>
</tr>
<tr>
<td>SIR: Security Incident life cycle</td>
<td>Validate the response tasks of the Policy Violation workflow.</td>
<td>Madrid</td>
</tr>
<tr>
<td>SIR: Threat Lookup</td>
<td>Validates the Threat Lookup capability.</td>
<td>Orlando</td>
</tr>
</tbody>
</table>

Quick start tests
Setup Assistant reference

The Setup Assistant walks you through the steps you need to perform to set up the Security Incident Response base system. This section provides additional information on some of the more complicated steps for which you may require more explanation.

Create a Security Incident Response process definition

You can create a process definition to define the way security incidents transition from one state to the next. Process definitions give service desks and end users help tracking the problem throughout its life cycle.

Before you begin
Role required: sn.si_admin

Procedure

1. Navigate to **Security Incident > Administration > Process Definition**.
2. Click **New**.
3. Fill in the fields, as appropriate.

Creating process definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the record which describes the process encoded in the script include file. The name is displayed as a choice in the <strong>Process Definition Selector</strong> list.</td>
</tr>
<tr>
<td>Script include</td>
<td>The name (including the sn_si. prefix) of the script include containing the definition of the process. The script must be in the Security Incident (sn_si) application scope. See Create a custom Security Incident Response process definition script include for more information. If this field does not contain a valid script include name, the default ProcessDefinition_NIST_Stateful definition is used.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Description</td>
<td>Helpful information about the script include.</td>
</tr>
<tr>
<td>Order</td>
<td>Determines the position in the process definition list.</td>
</tr>
<tr>
<td>Active</td>
<td>When checked, it makes this process definition selectable from the <strong>Process Definition Selector</strong> page.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**Related information**

**Security Incident Response Process Selection**

**Understanding Security Incident Response process definition**

Security Incident Response Process Definition replaces state flows and provides end users and service desks with the status of a problem. A process definition helps track the problem through its life cycle. Security Incident Response is a Service Management (SM) application; it has its own set of states. Invalid states are reported as part of Process Selection.

**Security Incident Response Process Definition**

The default process definition (NIST Stateful) defines the following incident states:

⚠️ **Note:** Available states vary based on the current state of the incident.

**Security Incident process definition states**

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft</td>
<td>The request initiator adds information about the security incident, but it is not yet ready to be worked on.</td>
</tr>
<tr>
<td>Analysis</td>
<td>The incident has been assigned and the issue is being analyzed.</td>
</tr>
<tr>
<td>Contain</td>
<td>The issue has been identified and the security staff is working to contain it and perform damage control. These actions can include taking servers offline, disconnecting equipment</td>
</tr>
</tbody>
</table>
Security Incident process definition states (continued)

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>from the Internet, and verifying that backups exist.</td>
</tr>
<tr>
<td>Eradicate</td>
<td>The issue has been contained and the security staff is taking steps to fix the issue.</td>
</tr>
<tr>
<td>Recover</td>
<td>The issue is resolved and the operational readiness of the affected systems is being verified.</td>
</tr>
<tr>
<td>Review</td>
<td>The security incident is complete and all systems are back to normal function, however, a post incident review is still needed.</td>
</tr>
<tr>
<td>Closed</td>
<td>The incident is complete but before a security incident can be closed, you must fill out the information on the Closure Information tab.</td>
</tr>
</tbody>
</table>

Security Incident task process definitions

The following process definitions are used for security incident tasks.

Task process definition states

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ready</td>
<td>The task is ready to be worked on once it is assigned to an agent.</td>
</tr>
<tr>
<td>Assigned</td>
<td>The task is assigned to an agent.</td>
</tr>
<tr>
<td>Work In Progress</td>
<td>The assigned agent is working on the task.</td>
</tr>
<tr>
<td>Complete</td>
<td>The task is complete.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>The task was canceled.</td>
</tr>
</tbody>
</table>

Process Definition provides the following process definitions by default:
Security Incident Response Process Selection

Process Selection lists processes with invalid states for security incidents and response tasks.

An administrator can correct the incident or task to valid states either manually or by using a script. An empty related list (no incidents; no tasks) indicates that every active task is in a valid state. Available states vary based on the current state of the incident. For more information, see Correct an invalid security incident or task state with process definition.

Select a Security Incident Response process definition

You can select the process definition to use for the appropriate states for your company security incidents and response tasks.

Before you begin
Role required: admin and sn_si.admin
About this task

Procedure

1. Navigate to **Security Incident Response > Administration > Process Selection**.
2. Click the search icon to list the available process definitions.

3. Select a process definition.
4. Click **Update**.

Create a custom **Security Incident Response** process definition script include

Create a custom Process Definition script for the appropriate states for your company security incidents and response tasks.

**Before you begin**
Role required: sn_si.admin

**About this task**
The sn_si.ProcessDefinition main script include controls process definitions. **Process Definition** determines which definition is in use (using **Process Selection**). It calls the appropriate script include file to determine the initial states and transitions for both security incidents and response tasks.

Procedure

1. Navigate to **System Definition > Script Includes**.
2. Click **New**.
3. Fill in the fields, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of this script include.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>API Name</td>
<td>Created based on the name of the script include.</td>
</tr>
<tr>
<td>Client callable</td>
<td>Makes the script include available to client scripts, list and report filters, reference qualifiers, or, if specified, as part of the URL.</td>
</tr>
<tr>
<td>Application</td>
<td>Security Incident</td>
</tr>
<tr>
<td>Accessible from</td>
<td>Choose This application scope only.</td>
</tr>
<tr>
<td>Active</td>
<td>When checked, it makes this script include selectable from the Process Definition page.</td>
</tr>
<tr>
<td>Description</td>
<td>Helpful information about the script include.</td>
</tr>
<tr>
<td>Script</td>
<td>Defines the server-side script to run when called from other scripts. The script must define a single JavaScript class or a global function. The class or function name must match the Name field. For information on script contents, see Process Definition script include.</td>
</tr>
</tbody>
</table>
4. Click **Submit**.

**Related reference**

**Process Definition script include**

The Process Definition script include provides methods for defining a process definition.

Implement the constants, attributes, arrays, and method calls described here to customize a process definition script include.

**Where to use**

Use this script include to create a process definition.

**Script include body**

The script include body is composed of three sections:

- Constants: Initial state definitions
- Security Incident and Response Task: Process definition arrays
- Method calls: Retrieving information
Constants

Constants are used to define the initial states of security incidents and response tasks.

The use of constants is optional but encouraged for readability. For example:

```javascript
INITIAL_INCIDENT_STATE: 10,
INITIAL_TASK_STATE: 1,
```

Which are later used by the following methods:

```javascript
getInitialIncidentState: function() {
  return this.INITIAL_INCIDENT_STATE;
},
getInitialTaskState: function() {
  return this.INITIAL_TASK_STATE;
},
```

The next set of constants defines the states for both security incidents and response tasks.

Each array also contains the definition of which states are available when the incident or task is in a specific state.

For example:

```javascript
TASK_STATES: [{
  state: 1, label:"Draft", choice:[1, 10],
},
{state:10, label:"Ready", choice:[10, 16]},
{state:16, label:"Assigned", choice:[16, 18]},
{state:18, label:"Work in Progress", choice:[18, 3]},
{state:3, label:"Close Complete", choice[]},
{state:7, label:"Cancelled", choice[]},
],
```

The example is an array of objects. Each object defines a state and possible transition states.

The order of the state's object determines the desired order for the flow.

When the task is in the 'Draft' state (value 1), possible states are: 1 (Draft, which is no change) and 10 (Ready, the next step in the process).

There is no limit on the number of transitions out of a state. The 'Close Complete' and 'Cancelled' state are final states and therefore have no possible state transitions.

The order of the attributes in the object is not important. If it makes the definition clearer, put the label first.
Attributes
Required attributes in a state definition object are:
• state: numerical value of the state
• label: human readable text associated with the state
• choice: an array of state values the state can transition to (determines the content of the state dropdown)

Optional attributes are:
• mandatory: list of field IDs that become mandatory in this state
• readonly: list of field IDs that become read-only in this state
• visible: list of field IDs that become visible in this state
• notmandatory: list of field IDs that become non-mandatory in this state
• notvisible: list of field IDs that would no longer be visible in this state

⚠️ Note:
If optional attributes are used, it is the author’s responsibility to ensure that fields are made visible/invisible, mandatory/non-mandatory, visible/hidden, or readonly appropriately between states.

For example, hiding a field in one state does not make it visible in another state later unless the ‘visible’ attribute is used.

Process flow definition arrays
To define the information displayed in the process flow formatter (the bar at the top of the Security Incident and Response task forms), the system requires information on what to display for each state.

For example:

```
TASK_PF: [(label:"Draft", condition:"state=1^EQ", description:"<p>Security Incident Response Task is in draft</p>")],
(label:"Ready", condition:"state=10^EQ", description:"<p>Security Incident Response Task is ready to be assigned</p>")],
(label:"Assigned", condition:"state=16^EQ", description:"<p>Security Incident Response Task is assigned</p>")],
(label:"Work in Progress", condition:"state=18^EQ", description:"<p>Work has started on this Security Incident Response Task</p>")],
(label:"Closed", condition:"state=3^ORstate=4^ORstate=7^EQ", description:"<p>Security Incident Response Task is complete</p>")],
```
The TASK_PF array is a collection of labels, conditions, and descriptions used to determine the text displayed in the process formatter bar (including order and activity).

In the example, the text 'Ready' is the second item displayed. It is highlighted when the task satisfied the condition 'state=10^EQ'.

When the pointer hovers over the text, the description 'Security Incident Response Task is ready to be assigned' is displayed.

⚠️ **Note:**

States can be combined to a single formatter state.

In the example, both the 'Close Complete' and the 'Canceled' states show up as 'Closed' in the top bar.

**Method calls**
The following methods must be present in the script include as they are used by sn_si.ProcessDefinition:

<table>
<thead>
<tr>
<th>Return type</th>
<th>Method summary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>getInitialIncidentState: function()</td>
<td>return the initial incident state numerical value</td>
</tr>
<tr>
<td>String</td>
<td>getInitialTaskState: function()</td>
<td>return the initial task state numerical value</td>
</tr>
<tr>
<td>Array of string</td>
<td>getIncidentStates: function()</td>
<td>return the incident state's array</td>
</tr>
<tr>
<td>Array of string</td>
<td>getTaskStates: function()</td>
<td>return the task state's array</td>
</tr>
<tr>
<td>Array of objects</td>
<td>getIncidentProcessFlows: function()</td>
<td>return the incident process flow definition array</td>
</tr>
<tr>
<td>Array of objects</td>
<td>getTaskProcessFlows: function()</td>
<td>return the task process flow definition array</td>
</tr>
</tbody>
</table>

The next set of methods are called whenever an incident or a task is updated and allows actions to be taken on specific change transitions.
<table>
<thead>
<tr>
<th>Return type</th>
<th>Method summary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>void</td>
<td>performIncidentStateChange: function(current, previous)</td>
<td>In the examples, this method is used to set SM-related values and ensure that an incident advances out of 'Draft' once someone is assigned to it.</td>
</tr>
<tr>
<td>void</td>
<td>performTaskStateChange: function(current, previous)</td>
<td>In the example, this method is used to update timestamps (on assignment and closing) and advance the task from 'Ready' to 'Assigned' once the assigned_to field is filled.</td>
</tr>
</tbody>
</table>

The same actions performed by these two methods can be accomplished using a business rule. By defining them in the script include, switching process definitions is made easier.

Correct an invalid security incident or task state with process definition

An administrator can correct the security incident or task to valid states, either manually or using a script. Available states vary based on the current state of the incident.

Before you begin
Role required: admin

About this task
After you have switched process definitions, the new definition may not support some of the old states. To correct the orphan incident or task states, you can change your process definition, edit your script include, or manually open each incident or task to update the state. Generally, updating the state (which can be done in bulk) is the easiest solution.

To change states in bulk, do the following:

Procedure
1. Navigate to Process Selection.
2. Highlight the State field for the incidents or tasks you want to change.
3. Double-click the State field in the first record, select the new State, and click the green check mark (✔️) to complete the change.
4. Click **Update**.

### Create a security incident group

Set up a security incident group and assign the appropriate roles and users to the group.

**Before you begin**

Roles required:

- If you have the user_admin role, you can create security incident assignment groups.
- If you have the sn_si.admin role, you can create and edit security incident assignment groups.

**About this task**

Users in a group inherit the roles of the group, so you do not have to assign roles to each user separately.

It is a good practice to create as many groups as needed in your organization.

It is also a good practice to create one group for administrators and assign the admin role to this group only.

**Procedure**

1. Navigate to **User Administration > Groups** or **Security Incident > Setup > Groups**.
2. Click **New**.
3. Fill in the fields.
4. Make sure that you select the **security incident** type for this group.
   a. If the **Type** field is not visible, configure the form to add it.
   b. Click the lock icon beside the **Type** field.
   c. Click the reference lookup icon (🔍)
   d. Search for and select the **security incident** type.
5. Right-click the form header and select **Save**.

6. In the **Roles** related list, add the roles that each member of this group receives. For example, if you are making a group for Security Incident Response team members, add sn_si.analyst. If you are making a group for Security Incident Response administrators, add sn_si.admin.

7. In the **Group Members** related list, add users to this group.

8. Click **Update**.

**Create a security incident calculator group**

Security incident calculator groups are used to group calculators.

**Before you begin**

Role required: sn_si.admin

**Procedure**

1. Navigate to **Security Incident > Setup > Security Incident Calculator Groups**.

2. Click **New**.

3. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the security incident calculator.</td>
</tr>
<tr>
<td>Application</td>
<td>The application that contains this record.</td>
</tr>
<tr>
<td>Order</td>
<td>The order in which the security incident calculator is run. A calculator with an order entry of 100 runs before a calculator with an order entry of 200.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of this calculator group.</td>
</tr>
<tr>
<td>Created by</td>
<td>Enter the name of the user who created</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**Create a security incident calculator**

Security incident calculators allow you to calculate the severity of a security incident based on pre-defined formulas. You can define your own security incident calculators, as needed.

**Before you begin**

Role required: sn_si.admin
Procedure

2. Click the name of the group for which you want to create a calculator, or you can create a calculator group.
3. Click New.
4. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the security incident calculator.</td>
</tr>
<tr>
<td>Calculator Group</td>
<td>Name of the group to which this calculator belongs.</td>
</tr>
<tr>
<td>Note</td>
<td>Creating or changing the calculator group becomes available after you have entered a Name and Table.</td>
</tr>
<tr>
<td>Table</td>
<td>Select the table to be used for this calculator.</td>
</tr>
<tr>
<td></td>
<td>When you add calculators to tables other than Vulnerability [sn_vul_vulnerability] and Vulnerable Item [sn_vul_vulnerable_item], you must add business rules and UI Actions to those tables. To see examples:</td>
</tr>
<tr>
<td></td>
<td>• Navigate to System Definition &gt; Business Rules, and locate the Calculate Severity business rule on the Vulnerable Item [sn_vul_vulnerable_item] table.</td>
</tr>
<tr>
<td></td>
<td>• Navigate to System UI &gt; UI Actions, and locate the Calculate Severity UI action on the Vulnerable Item [sn_vul_vulnerable_item] table.</td>
</tr>
<tr>
<td></td>
<td>Also, the vulnerability admin role must be granted full read, write (or save_as_template) capabilities on any table used by a calculator to properly see the values to apply to the template.</td>
</tr>
<tr>
<td>Application</td>
<td>The scoped application to which the calculator belongs.</td>
</tr>
<tr>
<td>Order</td>
<td>The order in which the security incident calculator runs.</td>
</tr>
<tr>
<td></td>
<td>A calculator with an order entry of 100 runs before a calculator with an order entry of 200.</td>
</tr>
<tr>
<td>Active</td>
<td>Turn the calculator on or off.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of this calculator.</td>
</tr>
</tbody>
</table>
5. Right-click the form header and select **Save**. Two tabs, **Conditions** and **Values to Apply**, appear.

6. Fill in the fields in the **Conditions** tab, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use filter group</td>
<td>Select this check box to use a predefined filter group or create a new filter group to define the calculator criteria.</td>
</tr>
<tr>
<td>Filter group</td>
<td>Select the filter group to use for defining a calculator. This field appears only if you selected the <strong>Use filter groups</strong> check box.</td>
</tr>
<tr>
<td>Use advanced condition</td>
<td>Select this check box to indicate that a script condition is used to determine when this calculator is applied. When you select the check box, an <strong>Advanced condition</strong> scripting field appears. If you selected the <strong>Use filter group</strong> check box, this field is hidden.</td>
</tr>
<tr>
<td>Condition</td>
<td>Defines basic filter conditions for determining whether the calculator is used. If you selected either of the <strong>Use filter group</strong> or <strong>Use advanced conditions</strong> check boxes, this field is hidden.</td>
</tr>
</tbody>
</table>

7. Click the **Values to Apply** tab and fill in the fields on the form, as appropriate. You have the choice of creating a script for defining the values to apply to the calculation or defining a template based on fields in the selected table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use script values</td>
<td>Select this check box to define field values with a script.</td>
</tr>
<tr>
<td>Script values</td>
<td>Defines what values to apply the calculations to. This field appears only if you selected the <strong>Use script values</strong> check box.</td>
</tr>
</tbody>
</table>
8. When you have completed all entries, click **Submit**.

### Understanding security incident calculators

Security incident calculators are used to update record values when predefined conditions are met. The calculators are grouped based on the criteria used to determine how the records are updated.

The Security Incident Response base system includes the following security incident calculator groups and calculators. Within each group, the first calculator that matches the conditions is run.

#### Security incident calculators in the base system

<table>
<thead>
<tr>
<th>Security Incident Calculator Group Name</th>
<th>Calculators included in group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Impact</td>
<td>Aggregate from Severity Calculators</td>
<td>This calculator delegates to the Security Criticality Calculator that determines criticality by weighing the values of other fields.</td>
</tr>
<tr>
<td>Severity</td>
<td>Business Impacted</td>
<td>This severity calculator defines its selection criteria using a simple condition builder.</td>
</tr>
<tr>
<td></td>
<td>Critical service affected</td>
<td>This severity calculator defines its selection criteria using an advanced condition. If the configuration item in the security incident is associated with a highly critical business service, the <strong>Risk score</strong>, <strong>Business Impact</strong>, and <strong>Priority</strong> fields are elevated as defined by the calculator.</td>
</tr>
<tr>
<td></td>
<td>Critical service changes</td>
<td>This severity calculator defines its selection criteria using an advanced condition.</td>
</tr>
<tr>
<td>Security Incident Calculator Group Name</td>
<td>Calculators included in group</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the security incident meets the conditions, a script runs to define what levels the fields are elevated to. If the configuration item in the security incident is associated with a most critical or somewhat critical business service, the Risk score, Business Impact, and Priority fields are elevated as defined by the calculator.</td>
</tr>
<tr>
<td>Multi-Attack Vectors</td>
<td></td>
<td>This severity calculator defines its selection criteria using a simple condition builder. If the configuration item in the security incident is associated with web, email, and impersonation attack vectors, the Risk score, Business Impact, and Priority fields are elevated as defined by the calculator.</td>
</tr>
<tr>
<td>Set priority with category and services</td>
<td></td>
<td>This severity calculator defines its selection criteria using an advanced condition builder. The security incident priority is set to 1 - Critical when the following conditions are met: • The security incident has associated affected services and one of them is critical. • The security incident category is one of the following:</td>
</tr>
</tbody>
</table>
### Security Incident Calculator Group

<table>
<thead>
<tr>
<th>Security Incident Calculator Group Name</th>
<th>Calculators included in group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>◦ Denial of Service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◦ Spear Phishing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◦ Malicious code activity</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** This calculator is available in the base system when you have the Starter Security Operation pricing tier.

#### Set priority with observables

This severity calculator defines its selection criteria using an advanced condition builder. The security incident priority is set to **1 - Critical** when the following conditions are met:

- The security incident has associated affected services and one of them is critical.
- The security incident category is one of the following:
  - Denial of Service
  - Spear Phishing
  - Malicious code activity
- One of the associated observables or indicators has a sighting count that exceeds two sightings with active indicators (that is, the observables or indicators are confirmed as being bad from multiple sources).
<table>
<thead>
<tr>
<th>Security Incident Calculator Group Name</th>
<th>Calculators included in group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get user criticality</td>
<td>Get user criticality</td>
<td>This severity calculator defines its selection criteria using a simple condition builder. This severity calculator causes user business criticality to change to 1 - Critical when the Department field is changed to Finance.</td>
</tr>
<tr>
<td>Get user group criticality</td>
<td>Get user group criticality</td>
<td>This severity calculator defines its selection criteria using an advanced condition builder. This severity calculator provides example of a calculator that runs on data in a related list.</td>
</tr>
</tbody>
</table>

### Severity calculators

When you create a security incident, the **Risk score**, **Business Impact**, and **Priority** fields contain default values. When you save the incident, a business rule automatically validates the information in the security incident against conditions defined in each of your active severity calculators. They are validated one security calculator at a time, in the order defined by the **Order** field in each calculator. If information in the security incident matches the conditions defined in one of the calculators, the severity field values are updated accordingly to the rules set up in the calculator.

For example, assume that you create a security incident for an affected CI, and the CI is highly critical. When the security incident is saved, the CI information is compared to the conditions defined in the severity calculators. When the
security incident is validated against the **Critical service affected** severity calculator, the severity fields are automatically updated, and a message similar to the following appears at the top of the security incident.

```
Severity Calculation applied: Critical service affected; Risk: High; impact: 1 - High; Priority: 1 - Critical; Severity: 1 - High
```

You can use these severity calculators as is or you can edit them to more closely meet the needs of your business. For example, if you want to identify web and email threats that are specific to the Finance business unit, you can change the conditions of the **Multi Attack Vectors** calculator:

- [Attack Vector] contains [Web]
- [Attack Vector] contains [Email]
- [Business Unit] contains [Finance]

You can also update the severity values in an existing security incident at any time by opening the record and clicking the **Calculate Severity** related link.

### Security incident risk score calculators

The **Set priority with category and services** and **Set priority with observables** calculators are used to calculate a risk score for a security incident.

### User criticality calculators

The two calculators in the **User criticality** group (**Get user criticality** and **Get user group criticality**) provide examples of how you can drive criticality based on criteria defined in a user record or based on the group to which a user belongs. They can be edited as needed, or new user criticality calculators can be created.

The **Get user criticality** calculator causes user business criticality to change to **1 - Critical** when the **Department** field is changed to **Finance**.

The **Get user group criticality** calculator causes user business criticality to change to **1 - Critical** when the user is added to the **Database** group.

> **Note:** **Get user group criticality** is an example of a calculator that runs on data in a related list. If you want to add more groups to initiate a criticality change, add a comma-separated list of group sys_ids in the first line of the script. Example: `var CRITICAL_GROUPS = [group1_sys_id, group2_sys_id, group3_sys_id].`
Security incident risk score calculations

The risk score is calculated as an arithmetic mean that represents the risk based on the priority of a security incident, the type of security incident (Denial of Service, Spear Phishing, or Malicious code activity), and the number of sources that triggered a failed reputation score on an indicator. The risk score aids in prioritizing security incident work for analysts.

The Set priority with category and services and Set priority with observables security incident calculators are used to calculate a risk score for a security incident. Additionally, the following business rules trigger automatic calculation of risk scores:

- Calculate Severity
- Update risk score
- Update SI risk score

⚠️ Note: The risk calculator available in the base system depends on your Security Operations pricing tier.

When you look at a list of security incidents in the base system, notice the Risk score column.
The risk score is calculated using weights defined in **Risk score configuration**.
For example, if a security incident has a **Business impact** set to **2-High** and a **Priority** set to **3-Moderate**, the respective weights in the Risk Score Weights table are looked up and calculated thus:

**Security Incident Business Impact** with a value of 2 = a weight of 60.

**Security Incident Priority** with a value of 3 = a weight of 40.

\[60 + 40/2 = 50\]

The position of the security incident in the security incident list is then re-ordered based on its updated risk score.

If, in the example above, the **Business impact** or **Priority** of the security incident are changed, the risk score is recalculated, and the changes are reflected in the work notes.

The work notes are updated when the following fields are changed (causing the risk score to be updated):

- **Business impact** on the Security Incident form
- **Priority** on the Security Incident form
- **Severity** on the Security Incident form (hidden by default)
- **Business impact** on the **Affected Users** related list
- **Business impact** on the **Affected Services** related list
- **Business impact** on vulnerabilities on the **Vulnerable items** related list

Additionally, the work notes are updated in the following situations:

- When an association between affected users and a security incident is created or modified
- When an association between affected services and a security incident is created or modified
- When an association between vulnerable items and a security incident is created or modified

Work notes are also updated whenever **Update All Risk Scores** and **Clear All Risk Scores** on the **Risk Score Weights** form are clicked.
**Maintain risk score weights**

The risk score weights used to calculate risk scores in security incidents can be removed or updated on an individual basis. They can also be removed or updated for all security incidents. The ability to remove them from security incidents is useful when changing weight values.

**Before you begin**

Role required: sn_sec_cmn.admin

Note: Users with the sn_si.read role can view the risk score configuration in Security Incident Response.

**Procedure**

1. Navigate to Security Incident > Setup > Risk Score configuration.

   Note: Users with the sn_si.read role can view the risk score configuration by navigating to Security Incident > Alerts & Events > Risk Score Configuration.

2. To add a new risk score weight, click **New** and enter information in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select the type of risk score you are defining.</td>
<td></td>
</tr>
<tr>
<td>Value</td>
<td>Specify the value associated with the selected type. If multiple values are available for the type, you may want to define multiple risk score weight records. Example: Security Incident Priority with a value of 1, Security Incident Priority with a value of 2, and so forth.</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>The weight associated with the selected type/value pair. Valid entries are between 0 through 100, with 0 being the lowest weight and 100 the highest.</td>
<td></td>
</tr>
</tbody>
</table>

3. Click **Submit**.

4. Perform any of these steps, as needed.
   - To clear a risk score weight record, open it from the list and click **Delete**.
   - To clear all risk score weight records, click **Clear All Risk Scores**.
   - To update all risk score weight records, click **Update All Risk Scores**.

**Create a Security Incident Response SLA**

You can define a Service Level Agreement (SLA) for the security incidents.
Before you begin
Role required: sn_si.admin

Procedure
1. Navigate to Security Incident > Setup > SLAs.
2. Click New.
   For field descriptions and detailed instructions, see Create an SLA definition.

Repair security incident SLAs
You can repair SLA records to ensure that SLA timing and duration information is accurate.

Before you begin
Role required: sn_si.basic

Procedure
1. If it is not already open, open the security incident you want to repair SLAs for.
2. Click the form header context menu and select Repair SLAs:
3. Click **OK** in the Warning confirmation box. For more information, see Repair SLAs.

**Create a Security Incident Response runbook**

A runbook is an association between a published knowledge article and a specific task. While you are performing the task, a knowledge article in the runbook automatically opens, providing information pertinent to the task.

**Before you begin**

There must be existing knowledge articles in the Security Incident Response Runbook knowledge base. When you create a security incident knowledge article, be sure to select **Security Incident Response Runbook** in the **Knowledge base** field. After you publish the article, you can click the **Create Runbook** button.

Role required: sn.si.knowledge_admin
About this task
You can use runbooks during the security incident or response task creation processes, or you can associate the knowledge base articles in a runbook with tasks in the playbook.

Procedure
2. Fill in the fields, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge article</td>
<td>Select a knowledge article to include in the runbook.</td>
</tr>
<tr>
<td>Active</td>
<td>Check the box to make the runbook available from the Filter Navigator.</td>
</tr>
<tr>
<td>Use filter group</td>
<td>Select this check box to use a predefined filter group or create a new filter group to define the runbook criteria.</td>
</tr>
<tr>
<td>Filter group</td>
<td>Select the filter group to use for defining a runbook.</td>
</tr>
<tr>
<td></td>
<td>This field appears only if the Use filter groups check box is selected.</td>
</tr>
<tr>
<td>Table</td>
<td>Select either Security Incident [sn_si_incident] or Security Incident Response Task [sn_si_task].</td>
</tr>
<tr>
<td></td>
<td>If you selected the Use filter group check box and selected a filter group, this field defaults to the table associated with the selected filter group.</td>
</tr>
<tr>
<td>Condition</td>
<td>Set the conditions that connect this runbook to the incident or task.</td>
</tr>
<tr>
<td></td>
<td>If you selected the Use filter group check box and selected a filter group, the Condition fields are not displayed.</td>
</tr>
</tbody>
</table>

3. Right-click the form header and select Save.
The Knowledge Article Details tab and a series of buttons appear.

4. To view the details of the runbook, click the Knowledge Base Details tab.
5. To see the knowledge article as it would appear to the user, click View Article.
6. To edit the details of the knowledge article, click Edit Article.

Create rules to validate user-reported phishing attacks

When your employees receive emails that appear to be phishing attacks, they can report them to you using a phishing email address. The suspicious email is validated using rules defined by your organization.

Before you begin

Before email matching rules can be used to identify potential phishing attacks, define an email address to which emails forwarded from your employees would be sent for processing. You have the following options for defining this email address (assuming your company email domain is acme.com):

- Define an email address such as acme+phishing@service-now.com. The +phishing tag is supported by SMTP to enable filtering and your instance can receive emails sent to it.
- Define an email address, such as phishing@acme.com (your Exchange mailbox), which in turn forwards it to acme+phishing@service-now.com (your instance mailbox defined through a mail forwarding rule).

Role required: sn_sec_cmn.write

About this task

When an employee encounters a suspicious email, they should forward it as an attachment to your phishing email address. If the attached email matches a rule defining a threat, a security incident is created.

Procedure

1. Navigate to Security Operations > Email Processing > User Reported Phishing.
2. Click New.
3. Fill in the fields, as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for this email matching rule. For example, User Reported Phishing.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Conditions</td>
<td>Use the condition builder to validate whether an email sent to your company phishing email address is a phishing attack. See the following example.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**Example:**
This example shows a matching rule for handling user-reported phishing.

![Matching rule example](image)

**Configure the Security Analyst Workspace**
Configure the user interface of the Incident record in the Security Analyst Workspace to specify the fields you want to display.

**Before you begin**
Role required: sn_si.analyst

**About this task**
Specify the fields to be displayed in your Incident record and the order in which the fields must appear on the Security Incident form and the Response Task form. You can also set a limit on the number of fields that you want to display.
Note: You can create rules to determine which view should be used for a specific form. Several views are included with the base system, including the Default and SIR New UI views. Several view rules are also shipped with the base system, including the All Others Response Task rule. This rule enforces the Default view on the Response Task form when the condition specified in the view rule is met. The Security Analyst Workspace uses the SIR New UI view. If the form fields displayed in the Security Analyst Workspace do not match the form fields in the Classic UI, a view rule is most likely enforced. To use the SIR New UI view for the form, you must disable the view rule. See Control when the system displays a view for details.

Procedure
1. Navigate to any security incident list (for example, Security Incident > Incidents > Show All Incidents).
2. To open the security incident record, click a security incident link.
3. To navigate to the Configuring Security Incident form page, click the menu icon and select Configure > Form Layout.
4. From the View name list, select SIR New UI.
5. In the Section field, select the appropriate section. This can be Security Incident or Security Incident Response Task.
6. Select the fields and the order in which you want them to appear in the Incident banner in the new UI.

7. Click Save.

Note:

• Certain fields are hidden by default in the Incident and Response Task banners. Change the fields that are hidden or displayed by modifying the `sn_app_secops_ui.form.excluded_fields.incident` and `sn_app_secops_ui.form.excluded_fields.response_task` properties as described in Security Analyst Workspace properties.

• Specify the number of fields that can be displayed in the Incident and Response Task banners and on the first line of the Incident banner by setting these properties:
  - `sn_app_secops_ui.task_summary.single_summary.limit.incident`
  - `sn_app_secops_ui.task_summary.single_summary.limit.response_task`
  - `sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line`
8. To configure the styles of the dotted circles that appear next to a field value in the Incident record, for example, navigate to **System UI > Field Styles** and modify or create a new style record for the specific table and field name. The property background-color in the Style field of the style record determines the color of the dotted circle.

9. To view the updated incident banner, click **Security Incidents > Incidents (New UI)** to navigate to the Incident record in the Security Analyst Workspace and refresh the page to view the updated Incident banner.

10. To configure the Response Task banner in the Incident record, navigate to **Security Incidents > Response Tasks > Show All Tasks** and repeat the steps.

11. If you are creating a new task table extending from the base Security Incident Response Task table, you must also add the SIR New UI view to the table.

   a. From the **View Name** list, select **New**.

   ![Create new section](image)

   b. Enter **SIR New UI** (case sensitive) in the Create New View window and click **OK**.

**Results**
The security incident and response task banners are updated in the Security Analyst Workspace (**Manage security threats using the Security Analyst Workspace**).

**Set up primary and secondary filters for Security Analyst Workspace**
The Security Analyst Workspace base system includes a set of primary filters for narrowing down the list of security incidents for analysis (for security incidents assigned to you, all open incidents, and so forth) and a set of quick (or secondary) filters for narrowing down the list even further (by new incidents, open incidents, only critical incidents, and so forth). You can use the Classic Ui to define additional primary and secondary filters.
Before you begin
As you define filters to be used in the Security Analyst Workspace, you can assign tags to indicate whether they can be used as primary or secondary filters. Primary filters are shown at the top of the security incident list.

Click **Edit** next to the Quick Filters option to select secondary (or quick) filters.

Role required: admin or sn_sec_cmn.write

Procedure
1. Navigate to **System Definition > Filters**.
2. Click **New** and complete the following steps.

   a. Enter a **Title**.

   b. Select **Security Incident [sn_si_incident]** from the **Table** choice list.

   c. Add your filter conditions. For example, the **Open Incidents with Priority = Critical** filter, uses these conditions.
d. Click **Submit**.

3. If the **Tags** column is not visible on the filter list, click the gear icon and personalize the view to add it.

4. Locate the filter you created and add one of the following tags to indicate how the filter should appear in the Security Analyst Workspace.

   - **SN_SI_Primary**: If this tag is selected, the filter can be selected from the primary filter slushbucket in the Security Analyst Workspace.
   - **SN_SI_Primary_OOB**: If this tag is selected, the filter appears in the **Selected** side of the primary filter slushbucket by default.
   - **SN_SI_Secondary**: If this tag is selected, the filter can be selected from the secondary (quick) filter slushbucket.
   - **SN_SI_Secondary_OOB**: If this tag is selected, the filter appears in the **Selected** side of the primary filter slushbucket by default.

**Related information**

- **Create and edit filters**

**Security Analyst Workspace properties**

These system properties are used to configure the Security Analyst Workspace.

There are two types of properties:

- Properties that are typically not modified like sys_ids and product keys.
- Properties that are modified as required like long poll intervals and user interface configurations.

**Note:** The Security Analyst Workspace properties are located at this location: **Security Incident > Analyst Workspace Setup > Analyst Workspace Properties.**
### Security Analyst Workspace properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| sn_app_secops_ui.form.excluded_fields.response_task | Fields that are hidden by default in the response task banner.  
• **Type**: string  
• **Default value**:  
  ◦ number  
  ◦ short description  
  ◦ comments  
  ◦ work_notes  
  ◦ comments_and_work_notes  
  ◦ work_notes_list  
  ◦ automation_activity |
| sn_app_secops_ui.form.excluded_fields.incident | Fields that are hidden by default in the incident banner.  
• **Type**: string  
• **Default value**:  
  ◦ number  
  ◦ short description  
  ◦ comments  
  ◦ work_notes  
  ◦ comments_and_work_notes  
  ◦ work_notes_list  
  ◦ automation_activity  
  ◦ security_tags |
| sn_app_secops_ui.form.color_coded_fields | Background color style is applied to the fields listed here.  
• **Type**: string  
• **Default value**:  
  ◦ business criticality  
  ◦ impact  
  ◦ priority  
  ◦ risk_score  
  ◦ severity |
<table>
<thead>
<tr>
<th>Property Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>If true, tables extended from the sn_si_task base response task table, will also have access to email templates created for the base response task table.</strong></td>
<td></td>
</tr>
</tbody>
</table>
| sn_app_secops_ui.extend.base.response_task.email_templates | **Type**: true | false  
**Default value**: true |

| **Sets the width of each summary field in each response task banner.** |  |
| sn_app_secops_ui.task_summary.single_summary.width.response_task | **Type**: integer  
**Default value**: 10 |

| **Sets the width of each summary field in each incident banner.** |  |
| sn_app_secops_ui.task_summary.single_summary.width.incident | **Type**: integer  
**Default value**: 15 |

| **Sets a limit on the number of summary fields allowed in the incident banner.** |  |
| sn_app_secops_ui.task_summary.single_summary.limit.incident | **Type**: integer  
**Default value**: 12 |

| **Sets a limit on the number of summary fields allowed in the response task banner.** |  |
| sn_app_secops_ui.task_summary.single_summary.limit.response_task | **Type**: integer  
**Default value**: 12 |

| **Sets a limit on the number of summary fields allowed in the first line of the incident banner.** |  |
| sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line | **Type**: integer  
**Default value**: 3 |

| **Comma separated list of fields that may have user photos.** |  |
| sn_app_secops_ui.form.user_fields | **Type**: string  
**Default value**:  
- affected_user  
- caller  
- sys_updated_by  
- sys_created_by  
- opened_by |
<table>
<thead>
<tr>
<th>Property Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>◦ closed_by</td>
<td>◦ submitted_by</td>
</tr>
<tr>
<td>Sets the width of each summary field in each incident peek view.</td>
<td>◦ <strong>Type:</strong> integer</td>
</tr>
<tr>
<td>◦ <strong>Default value:</strong> 13.5</td>
<td>◦ <strong>Type:</strong> string</td>
</tr>
<tr>
<td>◦ <strong>Default value:</strong></td>
<td>◦ opened_at</td>
</tr>
<tr>
<td>◦ <strong>Default value:</strong></td>
<td>◦ sys_created_on</td>
</tr>
<tr>
<td>◦ <strong>Default value:</strong></td>
<td>◦ sys_updated_on</td>
</tr>
<tr>
<td>Comma separated list of fields that display time.</td>
<td>◦ <strong>Type:</strong> string</td>
</tr>
<tr>
<td>◦ <strong>Default value:</strong></td>
<td>◦ opened_at</td>
</tr>
<tr>
<td>◦ <strong>Default value:</strong></td>
<td>◦ sys_created_on</td>
</tr>
<tr>
<td>◦ <strong>Default value:</strong></td>
<td>◦ sys_updated_on</td>
</tr>
<tr>
<td>Controls the frequency (in milliseconds) at which the sighting search results are refreshed.</td>
<td>◦ <strong>Type:</strong> integer</td>
</tr>
<tr>
<td>◦ <strong>Default value:</strong> 30000</td>
<td>◦ <strong>Minimum:</strong> 15000</td>
</tr>
<tr>
<td>Controls the frequency (in milliseconds) at which the count or query data is refreshed.</td>
<td>◦ <strong>Type:</strong> integer</td>
</tr>
<tr>
<td>◦ <strong>Default value:</strong> 30000</td>
<td>◦ <strong>Minimum:</strong> 15000</td>
</tr>
<tr>
<td>Controls the frequency (in milliseconds) at which the result data is refreshed (for the playbook).</td>
<td>◦ <strong>Type:</strong> integer</td>
</tr>
<tr>
<td>◦ <strong>Default value:</strong> 30000</td>
<td>◦ <strong>Minimum:</strong> 15000</td>
</tr>
<tr>
<td>ID for the Security Operations Integration - Isolate Host workflow.</td>
<td>◦ <strong>Type:</strong> string</td>
</tr>
<tr>
<td>◦ <strong>Default value:</strong> a72041f1ff203200c68c84648e94fa5e</td>
<td>◦ <strong>Type:</strong> string</td>
</tr>
<tr>
<td>ID for the Security Operations Integration - Watchlist workflow.</td>
<td>◦ <strong>Default value:</strong> 35800c0eff343200c68c84648e94fa85</td>
</tr>
<tr>
<td>Property Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| ID for the Security Operations Integration - Block Request workflow.         | • **Type:** string  
| sn_app_secops_ui.workflow.id.block_request                                    | • **Default value:** T1a6a5270b9032008f9108e3c5673a24                                         |
| ID for the sn_si_analyst user role.                                          | • **Type:** string  
| sn_app_secops_ui.roles.id.sn_si.write                                        | • **Default value:** 66878663ff123100158bfffffffff8d                                           |
| ID for the sn_si_read user role.                                            | • **Type:** string  
| sn_app_secops_ui.roles.id.sn_si.read                                         | • **Default value:** ae878663ff123100158bfffffffff8e                                             |
| ID for the sn_si_admin user role.                                           | • **Type:** string  
| sn_app_secops_ui.roles.id.sn_si.admin                                       | • **Default value:** 22878663ff123100158bfffffffff8d                                           |
| ID for the Microsoft Exchange - Perform Email Search and Delete workflow.    | • **Type:** string  
| sn_app_secops_ui.email.phishing.manual.workflow                               | • **Default value:** ed9f289cc310220031fbdccdf3d3ae82                                         |
| ID for the Add to Blacklist custom action under the Explore tab in the Security Analyst Workspace. | • **Type:** string  
| sn_app_secops_ui.explore.action.direct.id.black_list                        | • **Default value:** BLACKLIST_e9bd0ac50b632200263a089b37673a069213af011f598f4ba52bf82daa738db620bc8929f1b1e7f0a50d6f1050d8882b001e8d2b6837b2303b5c087f9108e3c5673a24 |
| ID for the Add to Whitelist custom action under the Explore tab in the Security Analyst Workspace | • **Type:** string  
| sn_app_secops_ui.explore.action.direct.id.white_list                        | • **Default value:** WHITELIST_e9bd0ac50b632200263a089b37673a069213af011f598f4ba52bf82daa738db620bc8929f1b1e7f0a50d6f1050d8882b001e8d2b6837b2303b5c087f9108e3c5673a24 |
| ID for the Run Threat Lookup UI Action.                                     | • **Type:** string  
<p>| sn_app_secops_ui.explore.action.id.run_threat_lookup                         | • <strong>Default value:</strong> da5ff4420b540300263a089b37673ae7f0a50d6f1050d8882b001e8d2b6837b2303b5c087f9108e3c5673a24 |</p>
<table>
<thead>
<tr>
<th>Property Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| ID for the Threat Lookup integration capability. | • Type: string  
• Default value: 393444d4f0b273200263a089b37673ab1 |
| ID for the Observable Enrichment custom action under the Explore tab in the Security Analyst Workspace. | • Type: string  
• Default value: OBS_ENRICHMENT_54e2f5d60b5003009f66e94685673a1e |
| ID for the Enrich Observable integration capability. | • Type: string  
• Default value: 9ad18364b01003009f66e94685673af4 |
| ID for the Publish to Watchlist UI Action. | • Type: string  
• Default value: 8ee94002ff743200c68c84648e94faf9 |
| ID for the Block Request UI Action. | • Type: string  
• Default value: 7158f6e40b2032008f9108e3c5673adf |
| ID for the Run Sightings Search UI Action. | • Type: string  
• Default value: 43f91a6f0b032200b97c67d985673a2c |
| ID for the Create Child Security Incident UI Action. | • Type: string  
• Default value: 5a6882645363530099d5ddeeff7b1272 |
| ID for the Add Security Annotation UI Action. | • Type: string  
• Default value: 1e3a3e723b5332005a9149a4d2efc4eb |
| ID for the CI Enrichment Custom Action under the Explore tab in the Security Analyst Workspace. | • Type: string  
• Default value: CI_ENRICHMENT_54e2f5d60b5003009f66e94685673a1e |
Security Analyst Workspace properties (continued)

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID for the Isolate Host UI Action.</td>
<td>sn_app_secops_ui.explore.action.id.isolate_host</td>
</tr>
<tr>
<td><strong>Type</strong>: string</td>
<td><strong>Default value</strong>: d6244e0aff203200c68c84648e94fad3</td>
</tr>
<tr>
<td>ID for the Add Multiple Observables UI Action.</td>
<td>sn_app_secops_ui.explore.action.id.multiple_observable</td>
</tr>
<tr>
<td><strong>Type</strong>: string</td>
<td><strong>Default value</strong>: f38de478d78322007a6de294de6103aa</td>
</tr>
<tr>
<td>Product key for ag-Grid-Enterprise.</td>
<td>sn_app_secops_ui.ag-grid-license</td>
</tr>
<tr>
<td><strong>Type</strong>: string</td>
<td><strong>Default value</strong>: ServiceNow_ServiceNow_5Devs2_August_2018__MTUzMzE2NDQwMDAwMA==cedabe1c76ccf28f23aec398ec32997d</td>
</tr>
</tbody>
</table>

Additional Security Analyst Workspace configuration

Configure the Security Analyst Workspace and define filters, UI actions, and related lists.

- Landing page filter configuration
- Enable UI Actions
- Form UI actions
- Related List configuration
  - Related List UI Actions
- Form configuration system properties
- Enable playbooks for analyst selection

Landing page filter configuration

You can add new filters or modify existing filters that appear in the Security Analyst Workspace (Manage security threats using the Security Analyst Workspace).

The Security Analyst Workspace has primary and secondary filters that allow you to filter the list of security incidents so you can quickly find the security incidents you want to analyze.
Create a new filter


2. Click New.

3. Enter a title for the filter, specify the filter condition and click Submit to return to the previous page.

You will see the newly added filter listed on the page.

4. Add a tag for this filter to indicate whether this is a primary or secondary filter. The following tags are available:
   - SN_SI_Primary
   - SN_SI_Secondary

Edit existing filters

You can also do the following:

- Modify existing filters: Click the Title of an existing filter. Modify the title and the filter condition and click Update.

- Modify tags: Select a filter and click the Tag column in the Landing Page Filter Configuration. You can delete the existing tag or add a new tag for the filter.

Enable UI Actions

Before you configure any UI Actions, you must perform certain steps to enable them so that they are available for configuration in the Security Analyst Workspace.
To modify the UI actions, log in as a user with the following roles:

- ui_action_admin
- ui_page_admin
- web_service_admin

There are two types of UI actions that can be configured for the Security Analyst Workspace:

- Dialog Based UI Action
- Server-side UI Action

**Dialog Based UI Action**

To enable dialog-based UI actions in the Security Analyst Workspace, make the following changes to the UI pages associated with the respective standard UI Actions.

1. **HTML section:** Modify the HTML section to include the `react` input tag. The `react` input tag value is used in the client script section to identify if the UI Page has been launched from the Security Analyst Workspace. An example is shown below:

   ```html
   <input id="react" name="react" type="hidden" value="$\{JS,HTML:sysparm_react\}" />
   ```

2. **Client script:** Additional logic needs to be written in the client script when the `react` flag is true. This is needed to handle the **Submit** and **Cancel** button events shown as part of the dialog window.

   - **a. onCancel ()** event handler needs to dispatch the ‘SIR_WORKBENCH_POPUP_CANCEL’ event from the Security Analyst Workspace
   
   - **b. onSubmit ()** event handler needs to dispatch the ‘SIR_WORKBENCH_POPUP_SUBMIT’ event from the Security Analyst Workspace

3. The execution of the processing script is skipped from the Security Analyst Workspace context as the ‘onSubmit’ action has been modified to return false when the `react` input tag value is true. The logic of the processing script needs to be handled either via a client callable script (invoked via GlideAjax API) or REST resource endpoint.

Refer the following sample UI pages for more details:
• Related List UI action example: Publish to watchlist (UI page name: publish_to_watchlist)
• Form UI action example: Create Problem (UI page name: create_prb_change_inc)

Server side UI Action
To enable server side UI actions, you must do the following:
The logic of the standard UI action script must be handled as part of a scripted REST resource.
Refer to the following sample Form UI actions for more details:
• Create Outage
• Cancel

Form UI actions
You can configure the UI actions that are displayed in the Security Analyst Workspace.

Prerequisites:
Before you configure any UI actions, you must perform certain steps to enable them so that they are available for configuration in the Security Analyst Workspace. See Enable UI Actions for details.

To configure a Form UI action for the Security Analyst Workspace, follow these steps:
2. Enter the following details:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Select an UI action from the choice list.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of action. This can be:</td>
</tr>
<tr>
<td></td>
<td>• Dialog based action: This type of action is used when user interaction or inputs are required to execute specific business logic.</td>
</tr>
<tr>
<td></td>
<td>• Server side action: This action executes the required business logic without any additional user input.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Before you configure any UI actions, you must perform certain steps to enable them so that they are available for configuration in the Security Analyst Workspace. See Enable UI Actions for details.</td>
</tr>
<tr>
<td>Application</td>
<td>The name of the application scope (Security Incident Response UI) in which the UI action is being added is displayed here.</td>
</tr>
</tbody>
</table>

**Dialog Based Action**

If you select Dialog based action in the Type field, enter the following details:

- **UI Page**
  - Select the UI page associated with the action.
- **Dialog Title**
  - Enter a title for the dialog action.
- **Dialog Width and Height**
  - Enter the height and width of the dialog in pixels.
- **Script**
  - For the selected UI Page, you can specify additional query parameters here. The template provided with the base system constructs and returns `sysparm_sys_id` parameter only. You can override this by specifying different parameters here.

**Server-side Action**

If you select Server side action in the Type field, enter the following details:

- **Scripted Rest Resource**
  - Select the Scripted Rest Resource that defines the action.

  **Note:** The SIR UI ANALYST ACL must be added to the Rest resource.

3. Click **Submit**.


5. Click on a security incident number to view the security incident record. You can see the new UI action at the top of the page.

To modify an existing Form UI action, click the Action Name to navigate to the Form UI Actions page. You can modify the Action Name, Type, and the rest of the fields based on the selected type.
Related List configuration

You can add new related lists or new related list groups, and modify existing groups or related lists that appear in the Security Analyst Workspace.

Add a Related List Group

To add a Related List Group, follow these steps:


2. Click New to add a new Related List Group. Enter the Group Name and the Order in which it should be appear on the Incidents (New UI) page.

3. Click Submit. The newly added group appears in the Related List Groups page.
Add a Related List

To add a new Related List, follow these steps:

1. Click on a Related List Group link.
2. In the Related Lists section, click Add to add a new related list.
   If you don’t see the Add button, check if you are in same application scope as the Related List Group.
3. Select the Related List to be included in the group.

   **Note:**
   - If you do not see a specific related list, do the following:
     a. Navigate to System UI > Related Lists and search for Related Lists present in the sn_si_incident table.
     b. Click on the sn_si_incident table associated with the SIR New UI view.
     c. In the Related List Entries section, click New to add the Related List to the SIR New UI view.
4. Specify the order in which it should appear and click Submit.
   The Related List that you have added will appear in the Security Analyst Workspace.

To modify an existing Related List Group, click the Group Name to navigate to the Related List Group page. You can modify the Group Name, Order, and add or delete Related Lists from the group.
Related List UI Actions

You can add new UI actions to the related lists that appear in the Security Analyst Workspace.

Prerequisites:

Before you configure any UI actions, you must perform certain steps to enable them so that they are available for configuration in the Security Analyst Workspace. See Enable UI Actions for details.

To add a new Related List UI action, follow these steps:

2. Click on the Group Name. The Related List Group configuration page is displayed.
3. Click on the Related List for which you want to add a UI action.
4. Click Add in the Related List UI Actions section.
5. Enter the following details:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Select a UI action from the choice list.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of action. This can be:</td>
</tr>
<tr>
<td></td>
<td>• Dialog based action: This type of action is used when user interaction or inputs are required to execute specific business logic.</td>
</tr>
<tr>
<td></td>
<td>• Server side action: This action executes the required business logic without any additional user input.</td>
</tr>
<tr>
<td>Application</td>
<td>The name of the application scope (Security Incident Response UI) in which the UI action is being added is displayed here.</td>
</tr>
</tbody>
</table>

**Note:** Before you configure any UI actions, you must perform certain steps to enable them so that they are available for configuration in the Security Analyst Workspace. See Enable UI Actions for details.

**Dialog Based Action**

If you select Dialog based action in the Type field, enter the following details:
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UI Page</td>
<td>Select the UI page associated with the action.</td>
</tr>
<tr>
<td>Dialog Title</td>
<td>Enter a title for the dialog action.</td>
</tr>
<tr>
<td>Dialog Width and Height</td>
<td>Enter the height and width of the dialog in pixels.</td>
</tr>
<tr>
<td>Script</td>
<td>For the selected UI Page, you can specify additional query parameters here. The template provided with the base system constructs and returns sysparm_incident_id, sysparm_record_table, and sysparm_related_sys_ids parameters only. You can override them by specifying different parameters here.</td>
</tr>
</tbody>
</table>

**Server side Action**

If you select Server side action in the Type field, specify the following:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scripted Rest Resource</td>
<td>Select the Scripted Rest Resource that defines the action.</td>
</tr>
</tbody>
</table>

⚠️ Note: The SIR UI ANALYST ACL must be added to the Rest resource.

6. Click **Submit**.

7. Navigate to **Security Incidents > Incidents (New UI)** page.

8. Click on a security incident number to view the security incident record. Launch the respective Related List to view the new UI action.

**Form configuration system properties**

These system properties define the form refresh intervals for the playbook tasks. To configure these properties, navigate to **Analyst Workspace Setup (New UI) > Analyst Workspace Properties**.

<table>
<thead>
<tr>
<th>Property</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sn_app_secops_ui.poller_interval.playbook_tasks</td>
<td>10000 ms</td>
<td>The interval time used by the playbook component to refresh its response tasks for every configured interval time.</td>
</tr>
<tr>
<td>sn_app_secops_ui.poller_interval_count.playbook_tasks</td>
<td>9 times</td>
<td>The number of times playbook component polls for response tasks.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Property</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sn_app_secops_ui.poller_interval.related_list</td>
<td>30000 ms</td>
<td>This interval time is used by the Explore component to refresh its Related List counts for every configured interval time.</td>
</tr>
</tbody>
</table>

**Enable playbooks for analyst selection**

Add new playbooks to the playbook selection list.

You can select an appropriate playbook to investigate security incidents in the Security Analyst Workspace (*Manage security threats using the Security Analyst Workspace*). The playbook selection option supports only the playbooks which are designed using Flow Designer.

![Playbook](image)

After you have created a playbook using Flow Designer, follow these steps to include it in the Selected Playbook choice list:
1. Navigate to the `sys_hub_flow.list` table.

2. Search for the new playbook you have created using Flow Designer.

3. Add the `sir_playbook` tag to the playbooks that you want to include in the Selected Playbook choice list.

**Note:** If you have old playbooks that have not been migrated from workflows to Flow Designer, they will not appear in the list. But, if a playbook created using workflows is assigned to a security incident either by a trigger condition or by manual selection (using Run Orchestration option in the classic UI), this playbook is launched when you open the security incident in the Security Analyst Workspace.

### Security Incident Response Analytics and Reporting Solutions

Analytics and Reporting Solutions contain preconfigured dashboards. The dashboards present important metrics for analyzing your Security Incident Response process, such as new security incidents or the average age of open security incidents.

Use the Performance Analytics widgets on the dashboard to visualize data over time, analyze your business processes, and identify areas of improvement. With Analytics and Reporting Solutions, you can get value from Performance Analytics for your application with minimal setup. You can always create your own objects as well.

**Important:** Set up and test Analytics and Reporting Solutions on a non-production instance before enabling them in production.

**Note:** Analytics and Reporting Solutions provide all the configuration records required to analyze default applications. Customize these records for use in your production environment. For more information, see Configure Analytics and Reporting Solutions.

The Security Incident Response Performance Analytics Solution is available from the ServiceNow Store. For information about downloading and installing this application, see Security Operations and the ServiceNow Store.
**Note:** To evaluate the functionality, you can activate Performance Analytics solutions and in-form analytics on instances that have not licensed Performance Analytics. However, you have the following limitations:

- You cannot create new indicators.
- You cannot collect data older than 180 days.

For full functionality, license Performance Analytics. For more information, see [Activate your Performance Analytics subscription](#).

**Related information**

Analytics and Reporting Solutions

[Activate your Performance Analytics subscription](#)

**CISO dashboard**

This dashboard reveals the overall security posture of your organization, including security vulnerability and incidents.
Vulnerability Profile tab

Security Controls Profile tab

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Business Risk Profile tab

End users and roles

<table>
<thead>
<tr>
<th>End user and goal</th>
<th>Required role</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISO: Needs clear visibility regarding the current security posture of the overall organization</td>
<td>sn_si.ciso</td>
</tr>
</tbody>
</table>

CISO dashboard indicators

The CISO dashboard presents the following key performance indicators:

**SI - Average Time to Identify**

A 7-day average of the time in minutes it takes to identify a security incident, calculated daily.

**Average Time to Contain**

A 7-day average of the time in minutes it takes to contain a security incident, calculated daily.

**Average Time to Eradicate**
A 7-day average of the time in minutes it takes to eradicate a security incident, calculated daily. Both Average Time to Contain and Average Time to Eradicate are based on the indicator SI - Average Duration Time broken down by Security Incident State.

**New Security Incidents This Week**

The weekly sum of the score of the daily Number of new security incidents indicator.

**Security Incidents Closed (weekly)**

The 7-day running sum of the daily Number of closed security incidents indicator.

**New Security Incidents by Priority**

Daily breakdown of the Number of new security incidents indicator by Priority.

**New vs Closed Security Incidents (weekly) volume**

The 7-day running sum time series of the Number of new incidents indicator charted against the 7-day running sum time series of the Number of closed incidents indicator.

**Security Incident Heatmap**

A global map showing the number of open security incidents in each country.

**Security Incident Treemap**

An interactive treemap where you can select to see:

- Security incidents per business service, broken down by business criticality
- Security incidents broken down by category or subcategory of incident
- Security incidents per assignment group or per assignee
- 'Victim stats' of security incident per affected resource or affected user

**Breakdowns**

The following breakdowns apply to the indicators on the dashboard:

- Business criticality
- Security Group
- Security Incident Age
- Security Incident Category
• Security Incident Close Code
• Security Incident Priority
• Security Incident State
• SI - Business Service
• Vulnerability

**Reports**
The dashboard includes the following reports:

<table>
<thead>
<tr>
<th>Title</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Incidents Open for More Than 30 Days by Assignment Group and State</td>
<td>Heatmap</td>
<td>Displays models with the most vulnerable items.</td>
</tr>
<tr>
<td>Risks by Category</td>
<td>Donut</td>
<td>Lists the age of reopened vulnerable items.</td>
</tr>
<tr>
<td>Citations by Authority Document</td>
<td>Donut</td>
<td>Number of active vulnerabilities</td>
</tr>
<tr>
<td>Security Incidents With Assignee That is not Active</td>
<td>Heatmap</td>
<td>Displays the number of open vulnerable items associated with vulnerabilities, (Common Vulnerability Enumeration (CVE) records), from most to least.</td>
</tr>
<tr>
<td>Security Incidents Not Updated for More Than 30 Days by Assignment Group and State</td>
<td>Heatmap</td>
<td>Displays publishers with the most vulnerable items.</td>
</tr>
<tr>
<td>Vulnerability Map</td>
<td>Map</td>
<td>A world map showing vulnerabilities by location</td>
</tr>
<tr>
<td>Title</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Most Vulnerable Models</td>
<td>Donut</td>
<td>The applications that contain the most vulnerabilities</td>
</tr>
<tr>
<td>Most Vulnerable CIs by Class</td>
<td>Donut</td>
<td>CIs by server type</td>
</tr>
<tr>
<td>Services with Critically Significant</td>
<td>List</td>
<td>Non-compliant controls by profile</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-compliant profiles</td>
<td>Bar</td>
<td>Non-compliant controls by profile</td>
</tr>
<tr>
<td>Control Overview</td>
<td>Bar</td>
<td>Number of compliant and non-compliant controls</td>
</tr>
<tr>
<td>Policy Exceptions</td>
<td>List</td>
<td>Policy exceptions with priority, owner, and short description</td>
</tr>
<tr>
<td>Risks by Category</td>
<td>Donut</td>
<td>The number of risks in each category of risk</td>
</tr>
<tr>
<td>Inherent Risk</td>
<td>Bubble</td>
<td>Inherent SLE vs Inherent ARO</td>
</tr>
<tr>
<td>Title</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Residual Risk</td>
<td>Bubble</td>
<td>Residual SLE vs Residual ARO</td>
</tr>
<tr>
<td>Moderate, High, and Very High Risks</td>
<td>Scores</td>
<td>The numbers of moderate, high, and very high risks, respectively</td>
</tr>
<tr>
<td>Risk by Profile</td>
<td>Stacked Bar</td>
<td>Risk count where you can select what to group by and what to stack by</td>
</tr>
</tbody>
</table>

**Security Incident Management Premium dashboard**

This dashboard uses advanced Performance Analytics visualizations to aid security managers to track the volume, performance and progress of security incidents from initial analysis/detection to containment, eradication, and recovery. The licensed version of Performance Analytics is therefore required.
## Security incident response by age

### Security Incident Response by Age

<table>
<thead>
<tr>
<th>Process by State</th>
<th>Process by Age</th>
<th>Data Quality</th>
<th>KPIs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process by State</td>
<td>Process by Age</td>
<td>Data Quality</td>
<td>KPIs</td>
</tr>
<tr>
<td>Security Incident Management Premium</td>
<td>Security Incident Response by Age</td>
<td>Security Incident Response by Age</td>
<td>Security Incident Response by Age</td>
</tr>
<tr>
<td>0 - 1 days: 2</td>
<td>1 - 5 days: 3</td>
<td>6 - 30 days: 33</td>
<td>30 - 90 days: 17</td>
</tr>
</tbody>
</table>

### August 20

#### 6 - 30 days

| 33 | ▼ (5.7%) |

#### Average age

| 18.50 | ▲ |

#### Average re-assignment times

| 1 | ▼ |

#### Average age of last update

| 0 | ▲ |

### Breakdowns

<table>
<thead>
<tr>
<th>Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 - 30 days, Aug 20: 33 ▼ (5.7%)</td>
</tr>
</tbody>
</table>

#### Security Group

<table>
<thead>
<tr>
<th>Name</th>
<th>Aug 20</th>
<th>Change</th>
<th>Trend</th>
<th>Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Security</td>
<td>5</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forensics</td>
<td>4</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endpoint Security</td>
<td>3</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIEM</td>
<td>3</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unicode Security</td>
<td>3</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directory Infrastructure Security</td>
<td>2</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

## End users and roles

### End user and goal

<table>
<thead>
<tr>
<th>Security Response Manager: Needs clear visibility into the overall state and volume of security incidents associated with applications and services.</th>
<th>Required role</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>End user and goal</td>
<td>Required role</td>
<td>Benefits</td>
</tr>
<tr>
<td>Security Response Administrator: Needs to pinpoint areas of concern quickly and have full control over</td>
<td>sn_si.admin</td>
<td>Can adjust risk calculation parameters to ensure vulnerable items that are most pertinent to the</td>
</tr>
<tr>
<td></td>
<td>sn_si.manager</td>
<td>Can review the overall security posture with the ability to adjust the members of assignment groups.</td>
</tr>
<tr>
<td>End user and goal</td>
<td>Required role</td>
<td>Benefits</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td>all Security Incident Response data while administering territories and skills, as needed.</td>
<td></td>
<td>organization are being addressed first.</td>
</tr>
<tr>
<td>Security Response Analysts: Need to quickly prioritize which vulnerabilities to focus on based upon criticality to the organization.</td>
<td>sn_si.analyst</td>
<td>Tier 1 and 2 security analysts work on security incidents. They can create and update security incidents, requests, and tasks, as well as problems, changes, and outages related to their incidents.</td>
</tr>
</tbody>
</table>

**Security Incident Management Premium indicators**
The Process by State and Process by Age tabs contain workbench widgets with the following indicators:

**Average age**
The Average age of open security incidents indicator uses the formula \[
\frac{\text{Summed age of open security incidents}}{\text{Number of open security incidents}} / 24
\] to give a result in days.

**Average reassignment times**
The Average re-assignment of open security incidents indicator uses the formula \[
\frac{\text{Summed re-assignment of open security incidents}}{\text{Number of open security incidents}}
\] to give a result in days.

**Average age of last update**
The Average age of last update of open security incidents indicator uses the formula \[
\frac{\text{Summed age of last update of open security incidents}}{\text{Number of open security incidents}} / 24
\] to give a result in days.

**% not updated in 5 days**
The % of open security incidents not updated in last 5 days indicator uses the formula \[
\left(\frac{\text{Number of open security incidents not updated in the last 5 days}}{\text{Number of open security incidents}}\right) \times 100
\]
The Data Quality tab has interactive filters for the Category of the security incident and the levels of Risk, Priority, and Severity. These filters are applied simultaneously to the following indicators:

**Security Incidents Open for More Than 30 Days by Assignment Group and State**

The Number of open security incidents filtered for an age of 30 days and broken down by Assignment group and State.

<table>
<thead>
<tr>
<th>Category</th>
<th>Analysis</th>
<th>Contain</th>
<th>Eradicate</th>
<th>Recover</th>
<th>Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - Critical</td>
<td>6</td>
<td>2</td>
<td>6</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>2 - High</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 - Moderate</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 - Low</td>
<td>2</td>
<td>3</td>
<td></td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

**Security Incidents With Assignee That is not Active**

The Number of open security incidents with no assignee or an assignee who is not active.

**Security Incidents Open for More Than 30 Days by Assignment Group and State**

The Number of open security incidents not updated in the last 30 days indicator broken down by Assignment group and State.

The KPI tab has the following additional indicators:

- % of new critical security incidents
- Average Age of Open Security Incidents
- Average Close Time of Security Incidents
- % Of Security Incidents that have been reassigned
- % of Security Incidents closed on first assignment
- % of security incidents closed by self-service
• % of security incidents not solved
• Average Close time of security incident tasks

**Breakdowns**
The following breakdowns apply to the indicators on the dashboard:

• Security Group
• Security Incident Age
• Security Incident Category
• Security Incident Priority
• Security Incident State

**Security Incident Management dashboard**
With this dashboard, security managers can easily track the volume, performance and progress of security incidents from initial analysis/detection to containment, eradication, and recovery.

**Overview tab**

![Graph and table showing security incident management dashboard](image)

**Basic Security Indicators**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of new security incidents</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of closed security incidents</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security incident backlog growth</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>-1</td>
<td>-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of open security incidents</td>
<td>54</td>
<td>55</td>
<td>56</td>
<td>56</td>
<td>56</td>
<td>55</td>
<td>-1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
New security incident tab

Closed security incidents tab
Security Incidents Daily tab

The **7d Running** and **28d Running** tabs follow the format of the **Daily** tab.

### End users and roles

<table>
<thead>
<tr>
<th>End user and goal</th>
<th>Required role</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Response Manager: Needs clear visibility into the overall state and volume of security incidents associated with applications and services.</td>
<td>sn_si.manager</td>
<td>Can review the overall security posture with the ability to adjust the members of assignment groups.</td>
</tr>
<tr>
<td>Security Response Administrator: Needs to pinpoint areas of concern quickly and</td>
<td>sn_si.admin</td>
<td>Can adjust risk calculation parameters to ensure vulnerable items that are most</td>
</tr>
</tbody>
</table>
## Security Incident Management indicators

The Security Incident Management dashboard presents the following key performance indicators:

### New Security Incidents

A chart of the number of new security incidents.

### Open Security Incidents

A chart where you can compare the number of open security incidents, the number of open security incidents not updated in the last 30 days, and the number of open security incidents not updated in the last 5 days.

### Basic Security Indicators

The last 6 days of scores of the number of new security incidents, the number of closed security incidents, the security incident backlog growth, and Number of open security incidents indicators.

### New Security Incidents by Priority

The number of new security incidents broken down by priority.

### Breakdowns

The following breakdowns apply to the indicators on the dashboard:

<table>
<thead>
<tr>
<th>End user and goal</th>
<th>Required role</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>have full control over all Security Incident Response data while administering territories and skills, as needed.</td>
<td></td>
<td>pertinent to the organization are being addressed first.</td>
</tr>
<tr>
<td>Security Response Analysts: Need to quickly prioritize which vulnerabilities to focus on based upon criticality to the organization.</td>
<td>sn_si.analyst</td>
<td>Tier 1 and 2 security analysts work on security incidents. They can create and update security incidents, requests, and tasks, as well as problems, changes, and outages related to their incidents.</td>
</tr>
</tbody>
</table>
• Security Group  
• Security Incident Age  
• Security Incident Category  
• Security Incident Priority  
• Security Incident State

**Security Incident Explorer dashboard**

With this dashboard, security managers are able to view security incidents summarized and grouped by category, subcategory, location, priority and business impact. These views let managers quickly gain insight into the frequency in which attacks are occurring and which business services are affected.

![Partial view of the Security Incident Explorer dashboard](image)

### End users and roles

<table>
<thead>
<tr>
<th>End user and goal</th>
<th>Required role</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Response Manager: Needs clear visibility into the overall state and volume of security incidents associated with applications and services.</td>
<td>sn_si.manager</td>
<td>Can review the overall security posture with the ability to adjust the members of assignment groups.</td>
</tr>
<tr>
<td>End user and goal</td>
<td>Required role</td>
<td>Benefits</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td>Security Response Administrator: Needs to pinpoint areas of concern quickly and have full control over all Security Incident Response data while administering territories and skills, as needed.</td>
<td>sn_si.admin</td>
<td>Can adjust risk calculation parameters to ensure vulnerable items that are most pertinent to the organization are being addressed first.</td>
</tr>
<tr>
<td>Security Response Analysts: Need to quickly prioritize which vulnerabilities to focus on based upon criticality to the organization.</td>
<td>sn_si.analyst</td>
<td>Tier 1 and 2 security analysts work on security incidents. They can create and update security incidents, requests, and tasks, as well as problems, changes, and outages related to their incidents.</td>
</tr>
</tbody>
</table>

**Security Incident Explorer indicators**
The Security Incident Explorer dashboard presents the following key performance indicators:

**Security Incidents**
The total volume of open and pending security incidents.

**Security Incident Closures by Priority**
The number of closed security incidents broken down by Priority.

**Security Incidents by Attack Category**
The number of open security incidents broken down by Category.

**Security Incident Assignment Heatmap**
A two-level breakdown of the number of open security incidents by assignment group and priority.

**Security Incident Heatmap**
A global map showing the number of open security incidents in each country.
Security Operations Efficiency dashboard

Security operations center (SOC) managers can view overall efficiency metrics and measure the individual performance of the SOC team members in the organization.

The SOC manager can use the Performance Analytics dashboard to improve efficiency and develop a picture of how SOC is performing in both general and specific areas over time.

**Analyst Efficiency tab**

![Analyst Efficiency dashboard](image-url)

- **Average Security Incidents worked per Analyst**: May 2019: 41
- **Closed Security Incidents per Analyst**: May 2019: 5
- **Average Security Incident Resolution**: 7.4 days
- **Average Security Incident Age**: 177.2 days

**Security Incident Backlog Analysis**

- **Name**: SecDps.EMEA
  - Security Incident Assignment: 6
  - Security Managers: 0
  - Security Incident Vendors: 1

**Closed Security Incident Analysis**

- **Name**: SecOps APAC
  - IT Security: 5
  - Network Security: 1
  - Security Incident Dispatchers: 3
  - Security Incident Qualifiers: 2

**Security Incident Age**

- **Name**: Windows Security
  - 1.3 days

**Security Incident Resolution Time**

- **Name**: Application Security
  - 2.1 days

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Click any of the indicators to drill down for further details. For example, click the indicator in the Average security incidents worked per analyst section.

The graph shows that the number of open security incidents have increased from 0 in March to over 40 in May. Notice the data displayed in the header:

- **Trend indicator:** Shows the change in number of open incidents in the latest time period for which the data has been collected. This chart shows data for the period March 2019 to May 2019 and the number of open incidents has increased by 19 in the month of May. Analyst efficiency is better if the number of open incidents has decreased over a period of time.

- **No. of scores:** The period for which the data has been collected (March to May 2019).

- **Sum:** The number of new open incidents for the period between March and May.

- **Change:** The number of new open incidents between March and April.

- **Average:** The average number of open incidents per analyst for the selected period.
## Analyst Efficiency Tab

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average security incidents worked per analyst</td>
<td>Average number of open security incidents per analyst for the specified period. The formula used is [\text{Average security incidents worked per analyst} = \frac{\text{Number of open security incidents}}{\text{Number of Security Agents}}].</td>
</tr>
<tr>
<td>Closed security incidents per analyst</td>
<td>The total number of incidents closed by each analyst in the selected category in the specified period. The formula used is [\text{Closed security incidents per analyst} = \frac{\text{Number of closed security incidents &gt; Security Incident Category = &lt;category_name&gt;}}{\text{Number of Security Agents / By month AVG +}}].</td>
</tr>
<tr>
<td>Average security incident resolution</td>
<td>The average time taken by each analyst to close security incidents in the specified period. The formula used to show the result in days is [\text{Average security incident resolution} = \frac{\text{Summed duration of closed security incidents &gt; Security Incident Category = &lt;category_name&gt; / By month AVG +}}{\text{Number of closed security incidents &gt; Security Incident Category = &lt;category_name&gt; / By month AVG +}} / 24].</td>
</tr>
<tr>
<td>Average security incident age</td>
<td>The average number of days for which security incidents remain open for each analyst. The formula used to show the result in days is [\text{Average security incident age} = \frac{\text{Summed age of open security incidents &gt; Security Incident Category = &lt;category_name&gt; / By month AVG +}}{\text{Number of open security incidents &gt; Security Incident Category = &lt;category_name&gt; / By month AVG +}} / 24].</td>
</tr>
<tr>
<td>Security incident backlog analysis</td>
<td>The total number of open security incidents in the specified period. Select an option from the Breakdown list to view the backlog for each analyst, security group, priority, and so on. You can also compare the number of open security incidents between two selected months.</td>
</tr>
<tr>
<td>Closed security incident analysis</td>
<td>The total number of security incidents that are closed in the specified period. Select an option from the Breakdown list to view the count for each analyst, security group, priority, and so on. You can also compare the number of security incidents that were closed between two selected months.</td>
</tr>
<tr>
<td>Security incident age</td>
<td>The average number of days for security incidents remain open in the specified period. Select an option from the Breakdown list to view the security incident age.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
### Analyst Efficiency tab (continued)

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
</tr>
</thead>
</table>
| for each analyst, security group, priority, and so on. The formula used to show the result in days is: \[
\frac{\left(\text{Summed age of open security incidents > Security Incident Category} = \text{category_name} > \text{Security Assignment Group} = \text{group_name} / \text{By month AVG} +\right)}{\left(\text{Number of open security incidents > Security Incident Category} = \text{category_name} > \text{Security Assignment Group} = \text{group_name} / \text{By month AVG} +\right)} / 24
\]

### Security incident resolution time

The average number of days taken to resolve security incidents during the specified period. Select an option from the Breakdown list to view the security incident resolution time for each analyst, security group, priority, and so on. The formula used to show the result in days is:

\[
\frac{\left(\text{Summed duration of closed security incidents > Security Incident Category} = \text{Malicious code activity} > \text{Security Assigned To} = \text{John Ashby} / \text{By month AVG} +\right)}{\left(\text{Number of closed security incidents > Security Incident Category} = \text{Malicious code activity} > \text{Security Assigned To} = \text{John Ashby} / \text{By month AVG} +\right)} / 24
\]

### Detection and Response Effectiveness tab

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyst Efficiency</td>
<td>Detection and Response Effectiveness</td>
</tr>
<tr>
<td>Incident Risk Score Analysis</td>
<td>Security Incident Stage Analysis</td>
</tr>
<tr>
<td>Mean False Positive Risk Score</td>
<td>False Positive Security Incident Duration</td>
</tr>
</tbody>
</table>

#### Security Incident Source Effectiveness

<table>
<thead>
<tr>
<th>Name</th>
<th>May 2019</th>
<th>Change</th>
<th>Trend</th>
<th>Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDS/IPS</td>
<td>66.7%</td>
<td>+0.3%</td>
<td>90.1%</td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td>74.4%</td>
<td>-0.1%</td>
<td>95.2%</td>
<td></td>
</tr>
<tr>
<td>Custom Inc Contact Type</td>
<td>73.4%</td>
<td>-0.3%</td>
<td>94.6%</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>96.3%</td>
<td>+0.2%</td>
<td>72.9%</td>
<td></td>
</tr>
<tr>
<td>Walk-In</td>
<td>87.2%</td>
<td>+0.1%</td>
<td>72.7%</td>
<td></td>
</tr>
</tbody>
</table>

#### Security Incident Source Volume Analysis

- Custom Inc Contact Type
- IDS/IPS
- Email
- Network Monitoring
- Endpoint Security

#### Closed Security Incident Analysis

- ...
## Detection and Response Effectiveness tab

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>True positive incidents</td>
<td>Percentage of true positive security incidents in the selected category for the specified period. The formula used is (1 - \frac{[\text{Number of false positive security incidents &gt; Security Incident Category = Malicious code activity / By month SUM +]}]}{\text{[Number of closed security incidents &gt; Security Incident Category = Malicious code activity / By month SUM +]}} \times 100).</td>
</tr>
<tr>
<td>False positive critical incidents</td>
<td>Percentage of false positive critical security incidents in the selected category for the specified period. The formula used is (\frac{[\text{Number of false positive security incidents &gt; Security Incident Risk Score = Critical Risk &gt; Security Incident Category = Malicious code activity / By month SUM +]}}{\text{[Number of closed security incidents &gt; Security Incident Category = Malicious code activity / By month SUM +]}} \times 100).</td>
</tr>
<tr>
<td>Note: Any security incident where the Closed code = Invalid vulnerability or False positive is treated as a false positive incident.</td>
<td></td>
</tr>
<tr>
<td>Mean false positive risk score</td>
<td>Average monthly risk score of closed security incidents that were identified as false positive incidents. A lower risk score indicates that the security analysts spent lesser time analyzing false positive incidents. The formula used is (\text{[Number of false positive security incidents &gt; Security Incident Risk Score = Critical Risk &gt; Security Incident Category = Malicious code activity / By month SUM +]}}).</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
### Detection and Response Effectiveness tab (continued)

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Indicator</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td></td>
<td>Category = Malicious code activity / By month SUM +] / [[Number of closed security incidents &gt; Security Incident Category = Malicious code activity / By month SUM +]]) * 100</td>
</tr>
<tr>
<td>False positive security incident duration</td>
<td>Average number of days that the security analysts spent in investigating false positive incidents. The formula used is (Summed duration of false positive security incidents] / [Number of false positive security incidents]) / 24</td>
</tr>
<tr>
<td>Security incident source effectiveness</td>
<td>Percentage of true positive security incidents identified by a specific source for the specified period. The source can be email, network activity, customer support, and so on. This data helps measure the effectiveness of the security incident source. The formula used is 1 - (Number of false positive security incidents &gt; Security Incident Category = Malicious code activity &gt; Security Incident Source = IDS/IPS / By month SUM +]) / [[Number of closed security incidents &gt; Security Incident Category = Malicious code activity &gt; Security Incident Source = IDS/IPS / By month SUM +]]) * 100</td>
</tr>
<tr>
<td>Security incident source volume analysis</td>
<td>Number of closed security incidents for current month for each Security incident source. You can also compare the number of security incidents for each source type between two selected months.</td>
</tr>
<tr>
<td>Security incident backlog analysis</td>
<td>The total number of open security incidents in the specified period and the average number of days for</td>
</tr>
</tbody>
</table>
Detection and Response Effectiveness tab (continued)

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>which the incidents remain open. You can also compare the number of open security incidents between two selected months. The formula used to calculate the average backlog period is ( \left( \frac{\text{Summed age of open security incidents &gt; Security Incident Category = Malicious code activity}}{\text{Number of open security incidents &gt; Security Incident Category = Malicious code activity}} \right) / 24 )</td>
</tr>
</tbody>
</table>

Closed security incident analysis

The total number of closed security incidents in the specified period and the average resolution time for these incidents. The formula used to calculate the average resolution time is \( \left( \frac{\text{Summed duration of closed security incidents > Security Incident Category = Malicious code activity}}{\text{Number of closed security incidents > Security Incident Category = Malicious code activity}} \right) / 24 \)

Incident Risk Score Analysis tab

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
## Incident Risk Score Analysis tab

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total risk exposure analysis</td>
<td>Total number of open incidents in each risk category (low, moderate, and critical) in the specified period. You can also compare the number of incidents in the different risk categories between two months.</td>
</tr>
</tbody>
</table>
| Normalized security analyst work by risk score | The total risk score for each security analyst for the specified period. This is calculated based on the number of true positive security incidents that the security analyst closed. The formula used is \[
\text{[[Summed Risk Score of Closed Security Incidents > Security Incident Category = Malicious code activity > Security Assigned To = SI Admin / By month SUM +]]} - \text{[[Summed Risk Score of False Positive Security Incidents > Security Incident Category = Malicious code activity > Security Assigned To = SI Admin / By month SUM +]]}
\]                                                                                                                                                                                                                                                                                                                                 |
| Security analyst work by mean risk score     | The average risk score for each security analyst for the specified period. The formula used is \[
\text{[[Summed Risk Score of Closed Security Incidents > Security Incident Category = Malicious code activity > Security Assigned To = SI Admin / By month AVG +]]} - \text{[[Summed Risk Score of False Positive Security Incidents > Security Incident Category = Malicious code activity > Security Assigned To = SI Admin / By month AVG +]]}
\]                                                                                                                                                                                                                                                                                                                                 |

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Security Incident Stage Analysis tab

You can see the number of open incidents on a specific day and the status (analysis, draft, contain, eradicate, recover, or review) of these incidents. On each stage, you can view average age, affected CIs, response tasks, and so on. Click on a link to view additional details or the breakdown of these incidents.

Security incident creation

Security incidents can be created manually from the form, or automatically via security events received from integrated third-party alert monitoring tools, such as Splunk.

If you have a security role, you can use any of the following methods to manually create security incidents.

Methods for manually creating security incidents

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manually created from the Security Incident list</td>
<td>On the Security Incident list, click New to create a new security incident.</td>
</tr>
<tr>
<td>Manually created from the Security Incident Catalog</td>
<td>You can create security incidents by selecting from categories of security threats defined in the security incident catalog.</td>
</tr>
<tr>
<td>Manually created from incidents</td>
<td>On the Incident form in incident management, click Create Security Incident to create a new security incident.</td>
</tr>
<tr>
<td>Manually converted from a security request</td>
<td>On the Security Request form, click Convert to Security Incident to create a new security incident.</td>
</tr>
</tbody>
</table>
Methods for manually creating security incidents (continued)

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manually created from an Event Management alert</td>
<td>On the Event Management Alerts form, click <strong>Create Security incident</strong> to create a new security incident from an alert.</td>
</tr>
<tr>
<td>Manually created from an alert</td>
<td>On the Event Management Alert form, click <strong>Create Security Incident</strong> to create a new security incident.</td>
</tr>
<tr>
<td>Manually converted from a vulnerability record (if the Vulnerability Response plugin is activated)</td>
<td>On the Vulnerability Items form, click <strong>Create Security Incident</strong> to create a new security incident.</td>
</tr>
</tbody>
</table>

Automatic creation of security incidents

Generally, security administrators are responsible for setting up alert rules used to automatically generate security incidents.

Security admin method for creating security incidents

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically created using alert rules</td>
<td>Security incidents can be created based on alert rules defined in the Event management in your data center application.</td>
</tr>
</tbody>
</table>

Security incident manual creation

You can create a security incident from the Security Incident form, as well as from several other forms.

You can create security incidents based on an existing record from the following forms:

- From any security incident list
- Incident form
- Event Management Alert form
- Vulnerable Items form
- Security Request form
Create a security incident from the Security Incident list

In addition to automatic methods for creating security incidents, you can create them manually, as needed.

Before you begin
Role required: sn_si.basic

Procedure

1. Navigate to any security incident list (for example, Security Incident > Incidents > Show All Incidents).

2. Click New.

3. Fill in the fields on the form, as appropriate.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select security tag</td>
<td>If needed, select a Security tag to add metadata to the record or identify who should have access to this security incident record. This field appears only after the security incident has been saved.</td>
</tr>
<tr>
<td>Number</td>
<td>[Read only] The security incident number.</td>
</tr>
<tr>
<td>Requested by</td>
<td>The person requesting the work to be performed.</td>
</tr>
<tr>
<td>Configuration Item</td>
<td>The server, computer, router, or other configuration item affected by the security issue.</td>
</tr>
<tr>
<td>Affected user</td>
<td>The person affected by the security issue.</td>
</tr>
<tr>
<td>Location</td>
<td>The location of the requester or resource. If a Configuration Item is not selected, this field is pre-filled with the location of the requester.</td>
</tr>
<tr>
<td>Category</td>
<td>The category that identifies the type of security issue.</td>
</tr>
<tr>
<td></td>
<td>If a category is selected, a workflow for analyzing this issue is executed when the record is saved. For example, if you select Denial of Service, the Security Incident - Denial of Service - Template workflow is executed.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Security Incident Response workflow templates.</td>
</tr>
<tr>
<td>Subcategory</td>
<td>The subcategory that further defines the issue.</td>
</tr>
<tr>
<td>Opened</td>
<td>[Read only] Displays the date and time the incident was opened.</td>
</tr>
<tr>
<td>State</td>
<td>The current state of the security incident. Upon security incident creation, this field defaults to Draft.</td>
</tr>
<tr>
<td>Substate</td>
<td>Identifies whether the security incident includes a pending problem or change.</td>
</tr>
<tr>
<td>Source</td>
<td>Identifies the source of the security incident, such as email, a phone call, or network monitoring.</td>
</tr>
<tr>
<td>Risk score</td>
<td>Displays the risk score calculated for this security incident. The value is based on the priority of the security incident, the type of security incident (Denial of Service, Spear Phishing, or Malicious code activity), and the number of sources that</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
 | triggered a failed reputation score on an indicator. The risk score aids in prioritizing security incident work for analysts. Three security incident properties allow you to further designate a color-coded dot to appear next to the risk score in list view to make them more easily identifiable. If you make changes to certain fields in the security incident, such as the Business impact or Priority, and save the record, the Risk score is automatically recalculated and displayed. The change is also reflected in the work notes and on the Risk Score Audits related list.

| **Note:** The risk score is also recalculated when affected users are associated with a security incident, affected services, or vulnerable items.

You can also manually enter a new Risk score. This can be useful if you want to keep a particular security incident at the top of the list of security incidents you are analyzing. If you enter a new Risk score, the Risk score override check box is automatically selected. Regardless of the changes made in the security incident, a manually-entered risk score is not automatically recalculated.

| **Note:** If you have upgraded your instance from a prior release, risk scores were calculated for all of your open security incidents. For more information, see Understanding security incident calculators.

| Risk score override | Select this check box to override the automatic update of the risk score. The override will be reflected in the work notes.
| Business impact | Select the importance of this security incident to your business. The default value is Non-critical. If, after the security incident record has been saved, you change the value in the Priority field or Risk fields, the Business impact is recalculated.
| Priority | Select the order in which to address this security incident, based on the urgency. If this value is changed after the record is saved, it can affect the Business impact calculation.
| Assignment group | The group to which this security incident is assigned.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigned to</td>
<td>The individual assigned to analyze this security incident. Assignments can be performed manually or automatically. For more information, see Assigning security analysts.</td>
</tr>
<tr>
<td>Short description</td>
<td>A brief description of the security incident.</td>
</tr>
<tr>
<td>Knowledge results</td>
<td>As you type the short description, links to related articles from the knowledge base appear. Scanning the information could solve your issue.</td>
</tr>
</tbody>
</table>

4. Right-click in the record header and select **Save**.
   If you added a new CI to the security incident, the following integration workflows are automatically executed:
   - **Security Operations - Get Running Processes workflow**. This workflow retrieves a list of running processes on a configuration item (CI) from a host or endpoint.
   - **Security Incident Response - Get Running Services workflow**. This workflow retrieves a list of running services from Windows-based CIs.
   - **Security Operations Integrations - Get Network Statistics workflow**. This workflow retrieves a list of active network connections from a host or endpoint.

5. To view the information retrieved by these workflows, click the **Show Enrichment Data** related link, and then click any of the indicated tabs.
Note: Additional workflows are executed based on the third-party integrations you have activated, as follows:

- **Tanium Endpoint Platform integration**: Tanium - Get Running Processes workflow

Related information

**Security Incident Response setup**

**Create a security incident from the Security Incident Catalog**

Users in your company can use the Security Incident Catalog to request various types of security-related analysis.

**Before you begin**

Role required: none
**Procedure**

1. Navigate to **Self-Service > Security Incident Catalog**.

2. Click the catalog item for which you want to make a request.
   If the item you selected from the main catalog contains subcategories, the list is shown. In the following example, **Malicious code activity** was selected.
3. Click the subcategory that best matches the type of request you want to make.
   The catalog entry form opens. In this example, the **Worm, virus, Trojan** subcategory was selected.
4. Enter the information for the request, and click Submit. The request is sent to your Security Incident department.

5. After you have submitted the request, you can track its progress by navigating to Self-Service > My Requests, and entering the request number.

Create a security incident from an Event Management alert

When Event Management is activated, you can manually create security incidents from the Alert form.

Before you begin

The Event Management plugin requires a separate subscription and must be activated by ServiceNow personnel. This plugin includes demo data and activates related plugins if they are not already active. The Service Analytics is activated automatically when Event Management is activated.

Role required: evt_mgmt_admin, evt_mgmt_operator, or evt_mgmt_user
Procedure
1. Navigate to Event Management > All Alerts.
2. Click the alert Number.
3. Click Create Security incident.
4. Click Update.

Security incident automatic creation
Third-party monitoring tools, such as Splunk, can be integrated with Security Incident Response so that security events imported from those tools automatically generate security incidents. You can also import data from third-party tools into security alerts.

To integrate alert monitoring tools to Security Incident Response, you must use the REST API to write to the Security Incident Import [sn_si_incident.import] table. Then, using the Security Incident Transform transform maps, the import set source table is mapped to fields in the target Security Incident [sn_si.incident] table.

If you attempt to import CI records that are not recognized by the transform map, the transform map script checks the record for the following (in this order) in an attempt to make a match:
- sys_id
- CI name
- fully qualified domain name
- IP address

⚠️ Note: If you find that the Security Incident Transform transform map is not adequate for the third-party alert monitoring tool you are using, duplicate the transform map, create a new one, and edit the fields, as needed.

Security incidents created from events and alerts
As events are imported from alert monitoring tools, they are first processed by Event Management and grouped into alerts. These alerts can be used to create security incidents based on customizable alert rules, or manually reviewed to select those alerts to be investigated as a security incident.

You can find a sample alert rule called Create security incidents from critical alerts in the Alert Rules module of the Event Management application. This alert rule automatically creates security incidents when critical security-related events are received from within ServiceNow or from third-party monitoring applications.
After the security incident has been created, it will be updated as new events are received. You can modify the task template in the alert rule to change the initial values for the security incident created by this alert rule. To handle each distinct variety of security incident that you would like to create, you can define other alert rules with different conditions.

Alternatively, if you are a user with the Security Admin role, you can manually create a security incident by clicking the Create Security Incident button from any suspicious alert.

It is important that the events received from external tools include the following information:

- The node set to the name, IP address, or sys_id of the CI that becomes the affected resource.
- The event classification is set to Security to distinguish them from other IT events.
- The event description, which populates the description of the security incident.
- The additional information can include any extra information that does not fit into the previously listed fields or other event fields, such as the category, attack vectors, return URL, or correlation ID. The format is a string that lists field names along with their values, using the following JSON format:

  ◦ \{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" \}

**Note:** For each field and value pair, if the field in the security incident where the column name matches the fieldName is empty, it is set to the fieldValue. If the field in the security incident is not empty, it is not changed. In either case, the event and all the fields and values encoded in the additional information are recorded in a work notes entry describing the event. If nothing changes in the security incident, a work note entry is not created. Any fields in a security incident, including custom fields you add to the table, can be set.

**Data imported into security alerts**

When an event is created with more JSON-encoded data, that data is imported into any field with a name that matches the fieldName of that value in the JSON data. If you have data in your third-party monitoring software (for example, Splunk) that is not common to the base system, you can add new fields to the Alert table to accommodate the data import.

The JSON format for importing data into alerts is the same format used for creating security incidents from events and alerts:

- \{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" \}
The only difference is that the data in the field is always overwritten with the fieldValue.

When the security event data is imported, it populates the fields in the Alert table with matching field names. If the alert is later turned into a security incident, the same additional information data populates matching fields in the security incident.

Create security incidents from User Reported Phishing emails

Use this feature to create security incidents from user reported phishing emails. The enhanced User Reported Phishing functionality includes aggregation capabilities, email header extraction, and configuration.

- Users can report phishing emails in multiple ways:
  - Emails can be forwarded as attachments.
  - If the Wombat plugin has been configured with the Microsoft Outlook client, users can:
    - Click the Report Phish button.
    - Forward phishing emails from a mobile device using the Report Phish option.

  - Users can upload a phishing email (in .eml format).
• User reported phishing includes **aggregation business logic** that identifies duplicate phishing emails reported by users in an organization. Users can use this capability to:
  ◦ Aggregate duplicate or similar user reported phishing incidents (company initiated phishing campaigns).
  ◦ Avoid triaging duplicate user reported phishing incidents and reduce the manual effort involved in consolidating incidents.
  ◦ Enable security analysts to work on a single user reported phishing incident.

• Provides phishing email headers within the user reported phishing incident.
  ◦ Security analysts can scan for key email header information within the incident.
  ◦ Manual effort in gathering header information from other sources is no longer required.

• The original phishing email submitted is stored as a **Phishing Email Record** in a new table.
  ◦ Security analysts can view details of the original phishing email like phishing email content, headers, origin.

• Security administrators can configure and make certain enhancements that include:
  ◦ Configurations to extract email headers from the email body (**Report Phish** submissions).
  ◦ Filters to capture selected headers.
Configurations to handle parent-child incident association when duplicate phishing email records are identified.
Flow Designer configurations to modify aggregation business logic based on the requirements.

Set up ingestion rules for User Reported Phishing.

As a user with the `sn_si.admin` role, you can define email matching rules to filter user reported phishing emails based on specific criteria. For example, you can define a rule where all emails sent either directly or through the Report Phish button to `security@acme.com` are categorized as user reported phishing emails.

Define User Reported Phishing properties.

Define the header information that needs to be captured from user reported phishing emails.

Phishing email records created from user reported phishing emails.

User-reported phishing emails are converted to security incidents based on the email matching rules that have been defined.

Transform user-reported phishing emails to security incidents.

The `Transform Phishing Email to Security Incident` flow converts or transforms phishing email records to security incidents.

Security incident records created from phishing email records.

View the security incident record details including the Related Lists, worknotes, and other important information.

Required components and plugins

The User Reported Phishing feature available in this release is an enhanced version of the existing user reported phishing functionality available in the London release. See the Create rules to validate user-reported phishing attacks topic in the London documentation for details.

Important Installation Instructions

This enhancement replaces the existing User Reported Phishing design. The new design includes the following updates:

- The existing User Reported Phishing email inbound actions (Type = Forward and Type = New) have been disabled.
- A new Create Phishing Email inbound action is now available.
- The **Transform user-reported phishing emails to security incidents** is a new flow that contains the security incident creation and aggregation business logic for the new design. You must activate this flow for the new design to take effect.

- The existing User Reported Phishing rules have been preserved during the upgrade.

**Note:** If you use custom email inbound actions and custom workflows for user reported phishing submissions, you must review both the old and new designs for conflicting or overlapping functionalities.

**User Reported Phishing Enhancement details:** The following are the details of the enhancement:

- Reporting the phishing email in multiple ways: See **Create security incidents from User Reported Phishing emails** for details. The phishing email is then moved to the `sn_si_phishing_email` table.

- Creating phishing email records: If the email-matching rules are met (See **Set up ingestion rules for User Reported Phishing**), the **Create Phishing Email** inbound action creates a phishing email record. The parsed email headers are stored in the `cm\_sn\_si\_phishing_email\_header` table and associated with the phishing email as a related list.

- Aggregating similar phishing records into a single security incident: The **Transform user-reported phishing emails to security incidents** flow creates security incidents from the phishing email records and aggregates similar records into a single incident. The aggregation conditions can be modified as required in this flow.

**Note:**

- The **User Reported Phishing** inbound actions available prior to the Security Incident Response 9.0 release are now disabled. Security incidents are no longer created through the disabled inbound actions.

- The Security Operations spoke application must be installed for the new design to take effect. This includes the **Transform user-reported phishing emails to security incidents** flow which is available in an inactive state by default. Activate this flow to create security incidents from the phishing email records.

The following image shows the differences between the old and the new designs:
To use the enhanced User Reported Phishing feature, the following plugins and components are required:

- **Security Support Common (sn_sec_cmn):** Includes:
  - Inbound action
  - New EmailUserReportedPhishing script
  - Ingestion Rules table

- **Security Incident Response (sn_si):** Includes:
  - Security incident table (sn_si_incident)
  - Security phishing emails table (sn_si_phishing_email)
  - Security phishing email headers table (sn_si_phishing_email_header)
  - EML upload record producer

- **Security Operations Spoke**
  - Flows and subflows for aggregating emails and transforming phishing emails to security incidents.

The following figure shows the new phishing emails table with references to the matched URP rule and target security incident record (sn_si_incident).
Set up ingestion rules for User Reported Phishing

As a user with the `sn_si.admin` role, you can define email matching rules to filter user reported phishing emails based on specific criteria. For example, you can define a rule where all emails sent either directly or through the Report Phish button to `security@acme.com` are categorized as user reported phishing emails.

**Before you begin**
Role required: `sn_si.admin`

**Procedure**

2. Click **New** to create a new Email Matching Rule.
3. Enter a name and define one or more conditions for the rule. Click **Submit** to save the rule. The following are some sample rules:
• **ToRule**: Filter emails that have been sent directly or forwarded to security@example.com email id.

  ![Image of ToRule configuration](image)

  **About this task**
  Use these options to configure the following user reported phishing settings.

  • Configuration to extract email headers from the email body. ([Report Phish submissions.](#))
  
  • Filter to select headers.

• **UserID Rule**: Filter emails that have been sent from a specific email id.

  ![Image of UserID Rule configuration](image)

  **Define User Reported Phishing properties**
  Define the header information that must be captured from user reported phishing emails.

  **Before you begin**
  Role required: sn_si.admin

  **About this task**
  Use these options to configure the following user reported phishing settings.
Procedure


2. Specify the configuration for extracting email headers from the email body:
   • Enter a string that identifies the beginning of the email header.
   • Enter a string that identifies the end of the email header.

   **Note:** Apply these settings only to headers captured as part of the email body of the phishing email. For instance, if the Wombat plugin has configured with the Microsoft Outlook client, when the user clicks the Report Phish button, the email headers are captured as per the configuration defined here. The header information is not captured if the phishing email is forwarded as an attachment.

3. Specify filters to eliminate headers that are not required for investigating the security incident.
   • Enter a comma-separated list of email headers that must be captured from the user reported phishing email. If you don't specify any value here, all the header information is captured.

4. Finally, enable or disable parent-child association.
• Select **Yes** to indicate that child security incidents must be created when user reported phishing emails are aggregated. If you select **No**, child security incidents are not created, but the user reported phishing emails are associated with the security incident and the security incident record is updated. See Transform user-reported phishing emails to security incidents for more information on how the child security incidents are created.

**Phishing email records created from user reported phishing emails**

User reported phishing emails are converted to security incidents based on the email matching rules that have been defined.

When a new phishing email is reported, the following actions take place:

• An email record is created in the `sys_email` table.

• The **Create Phishing Email** inbound action runs on the email record and uses the Email Matching Rules (see Set up ingestion rules for User Reported Phishing) to determine if it is a phishing email.

• When it has been identified as a phishing email, a phishing email record is created in the `sn_si_phishing_email` table.

• Finally, the Transform user-reported phishing emails to security incidents flow is applied to convert the phishing email record to a security incident.

To view the email details, navigate to **Security Incident > Show All Phishing Emails**. A list of phishing email records are displayed. Click the date link in the Created column to view the email record.
## Security Incident Phishing Email Details

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number</strong></td>
<td>The number assigned to the user-reported phishing email.</td>
</tr>
<tr>
<td><strong>Subject</strong></td>
<td>The subject of the email. The subject rule is useful in simulated phishing campaigns or tests. In this case, organizations send deceptive emails to their own staff to test their response to phishing and similar email attacks. In simulated phishing email tests, if the Microsoft Outlook email client with the Wombat plugin is being used, the user can click the Report Phish button to report the phishing email. The email is sent to the Security Operations team with Simulated Phishing appended to the Subject of the email. This is used to identify the email as a simulated phishing email.</td>
</tr>
<tr>
<td><strong>From</strong></td>
<td>The email address from where this phishing email originated. This information is available if the phishing email is forwarded as .EML file attachment or if the original headers are embedded in the email. If the user forwarded the phishing email directly, the From address may not be available.</td>
</tr>
</tbody>
</table>
### Security Incident Phishing Email Details (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reported by</td>
<td>The email id of the user who reported this phishing email. Click the Information icon to view additional details.</td>
</tr>
<tr>
<td>Message id</td>
<td>The id assigned to the message.</td>
</tr>
<tr>
<td>Matched URP rule</td>
<td>The User Reported Phishing rule that is to be applied on this email. Click the Information icon to view additional details.</td>
</tr>
</tbody>
</table>

#### Ingestion Rule

- **Name**: ToRule
- **Order**: 100
- **Active**: Checked
- **Condition**: To contains urp202+Phishing@service-now.com

As you can see, in this example, the **Condition** field shows that the ToRule is applied on this email and a security incident is created. See [Set up ingestion rules for User Reported Phishing](#) for more information on defining email matching rules.

<table>
<thead>
<tr>
<th>State</th>
<th>When a new phishing email record is created in the sn_si_phishing_email table, the State field is set to <strong>New</strong>. When this email record is converted to a security incident (see <a href="#">Transform user-reported phishing emails to security incidents</a>), the State field is updated to <strong>Processed</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header origin</td>
<td>This field indicates how the email headers originated or how the user reported the phishing email:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Email Header</strong>: The user forwarded the phishing email to the security operations team.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Email Text Body</strong>:</td>
</tr>
<tr>
<td>Field Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>◦ The user clicked on the <strong>Report Phish</strong> option (if the Wombat plugin has been configured with the email client).</td>
</tr>
<tr>
<td></td>
<td>◦ Based on the User Reported Phishing rule defined, the phishing email is forwarded to the security operations team.</td>
</tr>
<tr>
<td><strong>EML Attachment Header:</strong></td>
<td>◦ Attachment: The user forwarded the email as an attachment (.EML file).</td>
</tr>
<tr>
<td></td>
<td>◦ Service catalog submission: The user downloaded the email as a .EML file to the desktop and then uploaded it to a specified location. The security incident is then created from the email.</td>
</tr>
<tr>
<td><strong>EML Attachment Body:</strong></td>
<td>◦ The user clicked on the <strong>Report Phish</strong> option (if the Wombat plugin has been configured with the email client).</td>
</tr>
<tr>
<td></td>
<td>◦ Based on the User Reported Phishing rule defined, the phishing email is forwarded as an attachment to the security operations team.</td>
</tr>
<tr>
<td>Security Incident</td>
<td>This field is blank when the user-reported-phishing email is first reported. When the <strong>Transform user-reported phishing emails to security incidents</strong> flow has been executed, this email is converted to a security incident record and the number of this record is displayed here.</td>
</tr>
<tr>
<td>Raw headers</td>
<td>This field shows the complete header information extracted from the email as defined in the <strong>Define User Reported Phishing properties</strong> page. The headers are parsed into key value pairs and displayed in the Phishing Email Headers list.</td>
</tr>
</tbody>
</table>
Security Incident Phishing Email Details (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Body</td>
<td>This is the body of the user-reported phishing email.</td>
</tr>
</tbody>
</table>

**Transform user-reported phishing emails to security incidents**

The **Transform Phishing Email to Security Incident** flow is a new flow that converts or transforms phishing email records to security incidents.

**Before you begin**

1. **Note**: To enable the User Reported Phishing functionality, you must make a copy of the flow and activate it. If you have created custom inbound actions and custom flows to handle user reported phishing submissions, flow modifications suggested here are not required.

   - Role required: sn_si.admin
   - Flow Designer spoke must be installed.

**About this task**

This flow is automatically launched when a user reported phishing email record with the State set to **New** is created. This flow contains the logic to:

- Aggregate security incidents.
- Update security incidents with relevant notes.
• Add header data.
• Create child incidents as required.

Procedure
• Navigate to Flow Designer > Designer to view the flows available with the Security Operations spoke.

![Flow Designer screen](image)

• Click the Transform Phishing Email to Security Incidents link to view the flow.
• This flow is provided with the base system and is in Read Only mode and cannot be used. Click the more icon, make a copy of the flow and open it for your use. You can now make changes to your flow, such as modifying trigger conditions or actions, or adding and removing actions. After making the necessary changes, you must activate (See Activate a Security Incident Response flow) the flow so that it can be executed.
This figure shows the trigger and the steps executed with the flow. The right-hand panel shows the data flow. Click on an icon to expand the step and view the details.

- Click the **Trigger** icon. In the first step, you define or set the trigger for the flow. Specify the conditions for the trigger and task to be performed when the conditions are met. This flow is initiated when a **New** record is uploaded to the `sn_si_phishing_email` table.
In step 1, the flow verifies if the **Create child incidents for aggregated email submissions?** flag is enabled or disabled in the Transform user-reported phishing emails to security incidents page.

In step 2, the oldest parent security incident is identified. Notice the icon in step 2. This indicates that the Phishing Email Aggregation Subflow will be executed as part of this step.
Click the action designer icon to see a detailed view of the action. This subflow checks the phishing email and matches it with an existing security incident based on the specified criteria.

These two actions are performed when this subflow is executed. Click on the link of the first action to view additional details.
This action checks the emails that match the criteria for the new incoming email based on conditions such as:

- Security Incident State is not **Closed**.
- Subject or From value match the email matching rule conditions defined (See Set up ingestion rules for User Reported Phishing).

If these conditions are met, you can see the number of records that match the criteria in the Max Results field. The oldest or the first record in the list is designated as the parent record against which the security incidents will be aggregated.

- **Step 3** is applicable only if the Create child incidents for aggregated email submissions? flag was set to No in the Transform user-reported phishing emails to security incidents page. In this case, the phishing email is associated with the security incident record and the flow ends.
If the Create child incidents for aggregated email submissions? was set to Yes, the flow continues to run and a new security incident is created based on the user-reported phishing email.
• In step 5, users who received the phishing email (employees in the To and CC list of the phishing email) are added to the Affected Users related list in the security incident record.

• In step 6, allow listed observables are filtered from the list of observables in the security incident. These allow listed observables will not be added to the security incident.

• In step 7, unknown observables from the user-reported phishing email are identified and added to the Observables related list.

• In step 8, an email search query is generated which is a combination of the Subject and the From address of the email. This information is useful in identifying the employees in the organization who have been phished.
• In step 9, the user reported phishing email is associated with the security incident and the security incident record (created in step 4) is updated.

• In step 10, the parent security incident is identified and a check is made to see if it is an open security incident record.

• If the parent security is active, notes are added to the child and the parent security incident records indicating how they are associated with each other.

• In step 12, if no Affected Users were found (in step 5 of the flow), a worknote is added and the security incident record is updated.
In step 13, a worknote is added with the list of allow listed observables.

What to do next
You can click Test to simulate the actions in the flow before it is published. After testing the flow, click Activate to activate the flow so that it can be executed.

Click Executions to view the execution details of the flow.
When the flow has been executed, the phishing email record is converted to a security incident. See Security incident records created from phishing email records.

**Security incident records created from phishing email records**

Phishing email records stored in the `sn_si_phishing_email` table are converted to security incidents records.

To view the security incident associated with the phishing email record, click Security incident > Phishing Email > Show All Phishing emails.
Click the link in the Security Incident column associated with the phishing email record. The security incident details are displayed.
Related lists

Scroll down to the Related Links section of the security incident and click Show All related list. View details like child security incidents, affected users, associated phishing emails.

Child security incidents

Click the Child Security Incidents tab. You can see a list of child security incidents associated with the parent security incident based on the aggregation logic that has been applied. For every child record added, an automated system activity is added (in the Worknote section) to the parent record. This notifies the security analyst about the aggregated child record.

Note: You can see the child security incidents here only if the Create child incidents for aggregated emails submissions flag is set to Yes in the User Reported Phishing Properties page. See Define User Reported Phishing properties for details.

Associated phishing emails

Click the Associated Phish Emails tab. You see a list of phishing email records (duplicate records) associated with the parent phishing email record.
Associated phishing email headers

Click the Associated Phish Emails tab. You see the phishing email header details that have been captured as part of the security incident. You can view the rolled-up headers of all child records and phishing email records aggregated to the parent security incident.

Whitelisted observables

As the Transform user-reported phishing emails to security incidents flow is being executed, you can monitor the status of the security incident. When certain observables are marked as whitelisted, they are not added to the Observables Related list. By whitelisting the observables, you can ensure that only the important details are displayed. For example, if www.google.com is one of the URLs that has been whitelisted, the following system message is displayed.

Whitelisting observables ensures that only the important observables are monitored.

Capturing unmatched users

Some email ids in the To and CC list of the phishing email may not belong to users in the organization. These email ids are categorized as unmatched users.
and are not included in the Affected Users Related list. A worknote indicating that these are unmatched users is displayed.

User Reported Phishing in the Security Analyst Workspace

You can view security incidents associated with the phishing email records in the Security Analyst Workspace.

Navigate to Security Incident > New UI. The workspace opens in a separate browser tab. Click on the security incident associated with the phishing email record to view the security incident.

Click the binoculars icon. The original phishing email is displayed.
In the **Explore** tab, click **Incidents > Child Security Incidents**.

Click **Incidents > Associated Phish Headers**. You can view the rolled up headers of all child records and phishing email records aggregated to the parent security incident.
Click on the phishing email link to view the phishing email record associated with the security incident.

Click the Incident Timeline tab.
You can view the system updates that highlight:

- Identified duplicate child records.
- Whitelisted observables.
- Unmatched users who received the phishing email but do not belong to the Affected Users list.

**Frequently Asked Questions**

This section covers some of the frequently asked questions about the enhanced User Reported Phishing feature.

1. I have installed the new Security Incident Response spoke but I cannot view any user reported phishing incidents.

   By default, the User Reported Phishing functionality has been disabled.

   To enable this feature, you must make a copy of the read-only Transform user-reported phishing emails to security incidents flow and activate it before use.

2. While ingesting phishing emails and converting them into security incidents, what precautionary measures are used to handle malicious links and attachments in the phishing emails?

   The ServiceNow anti-virus scanner scans such malicious attachments and links. However, to ensure that security analysts can investigate the incidents accurately, the Security Incident Response application captures all the artefacts that are part of a phishing email. But the User Reported Phishing functionality mutes the malicious links in the phishing email so that security...
analysts don’t accidentally click these links. Regarding malicious attachments, security analysts must be cautious about downloading them.

3. Do we capture all malicious files that are part of the phishing emails for security incident enrichment?

Yes, we capture all files from the phishing emails. You can view these details are available as part of security incident observables in the form of a file hash.

4. Do we send malicious files and links from phishing emails to a sandbox instance for investigation?

Currently, we do not support out-of-the-box sandbox integrations for investigating malicious files and links.

5. Is there a time window or a trigger that defines the duration in which incoming duplicate phishing email records are associated with a parent security incident?

Duplicate phishing email records are aggregated only to an active parent security incident. If the parent incident is closed or canceled, then the incoming new duplicate phishing email will be created as a new security incident. However, in this scenario, within the new security incident, you can view the closed or canceled parent security incident in the Similar Security Incident related list.

Note: This behavior can be configured using the flow designer.

6. Does the User Report Phishing feature support the use of only the Microsoft Outlook Wombat plugin to capture email header details?

The User Reported functionality has been built to parse email headers and complies with RFC822 standards. So, similar to the Wombat plugin, all other Microsoft Outlook plugins that capture email headers based on RFC822 standards are supported.

Record creation from security incidents

After you have created and saved a security incident, you can create a change request (CHG), incident (INC), or problem (PRB) record from it. You can also create a customer service case from any security incident.

Create a change, incident, or problem from a security incident

After you have created and saved a security incident, you can create a change request (CHG), incident (INC), or problem (PRB) record from it.

Before you begin

Role required: sn.si_basic or higher
Procedure

1. Open a security incident using one of these methods.
   - Open an existing security incident by navigating to Security Incident > Unassigned > Incidents, and clicking a security incident.
   - Create a security incident by navigating to Security Incident > Unassigned > Incidents, click New, fill out the form, and save the record.

2. Right-click in the security incident header bar and click one of the following:
   - Create Change
   - Create Incident
   - Create Problem

   Note: This choice applies only if the popup property (sn_vul.popup) is enabled. When you click one of these buttons, a preview window opens to show you the information from the security incident that is used to create the change, incident, or problem. That is, the configuration item, its location, its priority, and the short and long descriptions. If you are creating a Change Request you can edit the Priority, Short description, and Description fields. If you are creating an Incident, you can edit the Impact, Urgency, Short description and Description fields. The fields in the associated security incident screen are not affected.

3. Click Submit to create the change, incident, or problem.

Create a Customer Service case from a security incident

Security Incident Response ships with a default field mapping that maps a security incident to a Customer Service (CS) case. You can create a CS case from any security incident, edit the Priority, and also add Optional notes.

Before you begin
Role required: sn_si.basic and sn_customerservice_agent

   Note: The Customer Service plugin must be activated to perform this task.

Procedure

1. Navigate to Security Incident.
2. Open the security incident that you want to add a CS case to.
3. Click Create Customer Service Case in the top header.
The pop-up window is prepopulated with information from the security incident based on your field mapping.

4. You can select a new **Priority** and add any **Optional notes**.

   - **Note:** The **Priority** field overwrites the default setting. The **Optional notes** are appended to the incident.

5. Click **Submit**. A CS case is created and displayed in the Customer Service Cases related list in the security incident.

6. You can click the CS case link to follow up on the case.

**Related information**

- Customer service case management

**Add a security incident to a security case**

If you determine that a security incident requires a higher level of analysis, add it to a new or existing case.

**Before you begin**

The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_si.admin, sn_ti.case_user_write
Procedure

1. If it not already open, navigate to the security incident that requires escalation. For example, you can navigate to Security Incident > Incidents > Assigned to Me, and open the security incident.

2. Click the Add to Security Case related link. The Add Security Incident(s) to Security Case dialog box opens.

3. If you have a case assigned to you that you want to add this security incident to, fill in the fields as appropriate, then click Submit.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Case</td>
<td>Select the security case.</td>
</tr>
<tr>
<td>Optional notes</td>
<td>As needed, enter additional notes that would be of value to the case analyst.</td>
</tr>
</tbody>
</table>

4. If you have one or more cases assigned to you, but want to create a new case and assign the security incident to it, click Create new case to show additional fields.
Note: If you do not have any cases assigned to you, the screen above opens first.

5. Fill in the fields as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Case Name</td>
<td>Enter the name of the new security case.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the case.</td>
</tr>
<tr>
<td>Case Type</td>
<td>Select the type of case being investigated.</td>
</tr>
<tr>
<td>Optional notes</td>
<td>As needed, enter additional notes that would be of value to the case analyst.</td>
</tr>
</tbody>
</table>

6. Click Submit.
   A message appears at the top of the security incident, along with a link to the new case.

Related information

Security Case Management

Create response tasks

After a security incident has been created, you can create response tasks to track separate actions to be performed to respond to the security issue.
Before you begin
Role required: sn_si.basic

Procedure
1. Navigate to the appropriate location to open the security incident for which you want to create tasks. For example:
   • To create a response task based on a security incident assigned to you, select **Security Incident > Incidents > Assigned to Me**.
   • To create a response task based on a security incident assigned to your team, select **Security Incident > Incidents > Assigned to Team > Incidents**.
   • To create a response task based on an unassigned security incident, select **Security Incident > Incidents > Unassigned Incidents**.
2. Open the security incident for which you want to add response tasks.
3. Click the **Add Response Task** button in the form header.
   
   **Note:** To create any other task, click the **Tasks** tab in the incident Related List. For more information on creating other types of tasks, see **Create a task**.
4. Fill in the fields on the form, as appropriate.

### Security incident

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select security tag</td>
<td>If you set up and activated <strong>security tags</strong>, you can select one or more tags to add metadata to the record or specify the degree of sensitivity of the response task. If you did not set up or activate security tags, this drop-down list is not displayed.</td>
</tr>
<tr>
<td>Number</td>
<td>[Read only] The automatically generated Security Incident Response number.</td>
</tr>
<tr>
<td>Parent</td>
<td>[Read only] The number of the related security incident.</td>
</tr>
<tr>
<td>Configuration Item</td>
<td>The configuration item (resource) affected by the security issue.</td>
</tr>
<tr>
<td>Affected User</td>
<td>The person affected by the security issue.</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority used to determine when this task is performed.</td>
</tr>
<tr>
<td>State</td>
<td>The current state of the security response task. Upon task creation, this field defaults to <strong>Draft</strong>.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Skills</td>
<td>The skill required to perform this task. Click the lock icon and select the skill required. After you have completed your selections, click the lock icon again.</td>
</tr>
<tr>
<td>Assignment group</td>
<td>The assignment group from which the assigned worker is selected.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>The individual assigned to perform the task.</td>
</tr>
<tr>
<td>Short description</td>
<td>A description of the Security Incident Response task.</td>
</tr>
<tr>
<td>Description</td>
<td>A description for the selected task.</td>
</tr>
<tr>
<td>Secure notes</td>
<td>The work notes that are encrypted and not visible to the customer.</td>
</tr>
<tr>
<td>Work notes</td>
<td>The work notes that are not visible to the customer.</td>
</tr>
<tr>
<td>Additional comments</td>
<td>Comments that you want to be visible to the customer.</td>
</tr>
</tbody>
</table>

5. When you have completed your entries, click **Submit**.

Note: After you have created Security Incident Response tasks, you can view them using any of the following applications under the **Response Tasks** module:

- Assigned to Me.
- Assigned to Team.
- Show Open Tasks
- Show All Tasks
- Unassigned Tasks.

**Manage Predictive Intelligence for User Reported Phishing**

The Predictive Intelligence for User Reported Phishing feature provides a significant solution in triaging and prioritizing user reported phishing emails.

This section describes the following:

- Predictive Intelligence for User Reported Phishing
- Required components and plugins
• Final verdict generation for User Reported Phishing
• Troubleshooting Predictive Intelligence for User Reported Phishing

Predictive Intelligence for User Reported Phishing

This feature assists security analysts in triaging and prioritizing user reported phishing emails.

The Predictive Intelligence framework provides solutions to train the system to predict, recommend, and organize data outcomes. For more details on predictive intelligence, see Predictive Intelligence. Using this framework, you can build models to automatically predict whether a user reported phishing email is suspicious or legitimate.

Using historical User Reported Phishing security incident data (email headers, email body and triage results captured through the security incident close codes), security analysts can train the system to classify the incoming user reported phishing submissions as ones that need to be further triaged (likely suspicious) and ones that are legitimate submissions.

By triaging incoming emails automatically, security analysts can easily prioritize the incident queue and focus on incidents that are likely to represent a risk to the organization first and foremost and spend less effort on emails that are very likely to be false positives. The prediction result also provides a confidence score on the classification to enable granular prioritization.

Required components and plugins

To use Predictive Intelligence for User Reported Phishing, you must install the following applications

<table>
<thead>
<tr>
<th>Plugin name</th>
<th>Minimum version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Incident Response</td>
<td>9.0.1 or 10.0.2</td>
</tr>
<tr>
<td>Predictive Intelligence</td>
<td>Orlando version</td>
</tr>
<tr>
<td>Predictive Intelligence for User Reported Phishing</td>
<td>10.0.2</td>
</tr>
</tbody>
</table>
Note: The following new enhancements are available with Security Incident Response 10.4:

- The ability to choose close codes from custom fields for model training.
- The ability to explicitly activate predictions after model building.
- The ability to generate a final verdict on the User Reported Phishing submission using a decision table. (requires Security Operations Spoke 10.3.0)

To use the new enhancements, you must upgrade the following applications:

<table>
<thead>
<tr>
<th>Plugin name</th>
<th>Upgrade to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Incident Response</td>
<td>10.0.4</td>
</tr>
<tr>
<td>Predictive Intelligence for User Reported Phishing</td>
<td>10.3.1</td>
</tr>
</tbody>
</table>

New and updated tables

- **sn_sir_ml_urp_config** (New): Contains the configuration for the URP ML application.
- **sn_sir_ml_urp_feature** (New): Records extracted from the sn_si_phishing email table.
- **sn_sir_ml_urp_feature_import** (New): Used to upload historical phishing email data.
- **sn_si_incident** (updated): The following new fields were added:
  - Prediction accepted
  - Prediction result
  - Confidence score

Script includes

- **URPMLUtil**: Retrieves configuration, run prediction job, and track prediction process.
- **URPMLProcessor**: Extracts and processes data from the sn_si_phishing_email table.
- **URPMLAction**: Executes flow to accept prediction result.
Final verdict generation for User Reported Phishing

Security Incident Response teams can now drive the finalized verdict for a user reported phishing record based on results from predictive intelligence and threat enrichment integrations.

This final verdict generation is enabled through a decision table construct and leveraged within a flow.

Prerequisites

- Ensure that all the plugins listed in Required components and plugins have been installed.

Navigate to Predictive Intelligence for Phishing > Final Verdict > Final Verdict for Phishing Security Incident.

The Decision Inputs tab shows the different conditions that were evaluated to arrive at the final verdict.

The following conditions are available with the base system:

- Predicted as suspicious: When predictive intelligence has classified the user reported phishing email as suspicious.

- At least one observable is malicious: When an observable involved in the security incident (For example, URL, Domain, IP, Hash) has been classified as malicious by threat intelligence sources.

- Observable enrichment are suspect: When enrichment on observables (For example, recency of phishing domain registration, country of phishing domain registration) are deemed to be suspect.
• Sender domain is spoofed: When the phisher’s email domain is suspected of spoofing a trusted domain.

• Sender name is spoofed: When the phisher’s email address is suspect of spoofing an trusted employee of an organization.

The **Decisions** tab shows the final verdict options that can be arrived at for a given security incident.

The following decisions are available with the base system:

• **Confirmed Phish**: When the conditions have led to the final verdict as being a confirmed phishing email.

• **Likely Phish**: When the conditions have led to the final verdict as a potential phishing attempt.

• **Likely Benign**: When the conditions have led to the final verdict as a benign submission.

You can see the conditions that were evaluated for each of the final verdict options. Click on the Label link to see the conditions.
You can customize the decision table provided with the base system or create your own decision table. This decision table can be leveraged in security incident response playbooks. The **Generate Final Verdict for Phishing Security Incidents** subflow is available with the base system. This subflow automatically generates the final verdict for a phishing security incident and applies a security tag based on that decision. You can include this subflow as part of the **Automated Phishing** playbook.

The inputs for this subflow are:

- **incident_id**: The sys ID of the phishing security incident.
- **c_level_names**: Comma separated list of names (For example, names of executives in the organization) likely being spoofed in the phishing attack.
- **trusted_domains**: Comma separated list of trusted email domains.
- **enrichment_keywords**: Comma separated list of keywords that indicate the maliciousness of the observable from enrichment results.
- **sender_email** (optional): The email address of the sender of the phishing email.

The output of this flow can be **Confirmed Phish**, **Likely Phish**, or **Likely Benign**.
Troubleshooting Predictive Intelligence for User Reported Phishing

This section covers a few common problem scenarios.

- **Problem:** I cannot modify the Predictive Intelligence configuration.
  
  **Solution:** Check if you have permissions to do so. You must log in as a user with the ml_admin role to modify thresholds. Some scenarios may require even higher privileges, like, for example, you need to modify the training data limit. For such scenarios, you must contact Customer Support for assistance.

- **Problem:** The model training failed.
  
  **Solution:** Check if the URLs of the ML scheduler have been setup. Navigate to **System Properties > All Properties** and check if the glide.shared_service_scheduler.url property has been configured.

- **Problem:** Prediction results are not available on a security incident.
  
  **Solution:**
  
  - Check if the predictor URL has been set up in the glide.prediction_service.url system property and make sure the data center matches with the URL.
  - Check if the Predict User Reported Phishing Email scheduled job is active.
Configure Predictive Intelligence for User Reported Phishing

Configure and prepare the model to identify user reported phishing emails.

Before you begin
Role required: ml_admin

Procedure
1. Navigate to Predictive Intelligence for Phishing > Configuration.
2. In Step 1 of the configuration, select one of the following options from the Close code source list:
   • Default close code: Select this option to specify the default security incident close codes that must be used by the training model to identify malicious emails and legitimate ones. Click the lock icon and select one or more False positive codes or Confirmed phishing codes.
   • Custom close code: Select the Custom close code option if you want to define close codes from custom fields that may be used as part of your existing incident response procedures. To define a close code, select a field from the security incident table and specify one or more filter conditions.

3. In Step 2, import historical data that can be used to train the model. Select the Data Source for importing the historical data. This can be:
• User reported phishing email table: You can see the number of records that can be imported as historical data. Select this option and click **Import**.

• Custom data source: You can attach a single formatted CSV file that contains historical data records. Select the file and click **Import**.

**Note:** The CSV file that you import must contain the following headers:
- Label
- Header
- Body text

Each record must contain a Malicious or Legitimate tag in the Label column in the CSV file.

Click **Cancel Import** to stop importing the data. The import process is canceled and all records that have been imported so far are deleted.

4. After you have imported the historical data, click the link to refresh the page. You can then either import more training data or continue with the next step.

5. In Step 3, verify if the number of records available for training meet the minimum threshold requirements.

**Note:** The default values for maximum and minimum number of training records are displayed. These thresholds can be modified in the **Platform Machine Learning Properties** page. Contact Customer Support for assistance.

6. If the training data is sufficient, click **Train model**. You can update the inputs for training in the screen below.
7. Prediction inputs that you can modify include:
   • What are you interested in predicting?
   • What input data is helpful to predict the output field?
   • What historical data do you want to use to train the solution and how frequently do you want to retrain it?
   The default values for these inputs are displayed. You can modify them and click either of the following:
   • **Update**: Updates the training model definition.
   • **Update & Retrain**: Updates the training model definition and retrains the model (Triggers the **Train Model** function).

8. Finally, when you have completed training the model, click the **Activate Prediction** check box. Predictions are now provided on every user reported phishing record using that model.
   If you would like to stop providing predictions on the user reported phishing records, clear the **Activate Prediction** check box and click **Deactivate**.

**Assigning security analysts**

Depending on your settings in the SIR Administration Configuration screen, you can assign security analysts to security incidents manually; automatically by using a workflow; or automatically by using auto-assignment.

**Manual analyst assignment**

You can configure the Security Incident Response Administration Configuration screen to require that security analysts be assigned manually whenever someone or the SIR application creates a security incident or generates a security response task.

If a security incident or response task cannot be auto-assigned, you can set the SIR Administration Configuration screen to require the manual assignment of security analysts. This is a good choice if you have a limited number of security analysts for completing requests or if you simply do not want to auto-assign them.

**Workflow-based security analyst assignment**

You can configure the Security Incident Response Administration Configuration screen to use a selected workflow to assign the security analyst whenever
someone or the SIR application creates a security incident or security response task.

In the Security Incident Administration configuration screen, you can choose to use a workflow to assign an analyst to each security incident or security response task. This option is a good choice for organizations that use a custom process for resolving security issues or otherwise have a process that can be automated.

**Automatic security analyst assignment**
You can configure the Security Incident Response Administration Configuration screen to auto-assign the security analyst whenever someone or the SIR application creates a security incident or security response task. Auto-assignment allows you to define, based on the needs of your organization, the criteria by which analysts are assigned automatically to security incidents.

**Agent auto-assignment based on agent ratings**
If auto-assignment is enabled and a security incident or a response task is created, the following actions occur:

- The available security analysts are evaluated based on the criteria defined in the configuration.
- An appropriate security analyst is automatically assigned to the task.
- The task is moved to the **Assigned** state.

If the configuration is set up to consider more than one set of conditions, such as skills, location, time zone, or group coverage area, the security analysts are evaluated based on the weighting property settings and other criteria. These configuration settings help you auto-assign agents based on optional properties. The calculated ratings are used to determine the best agent for the security incident or response task. Any combination of rating-based methods can be enabled in the application configuration screen.

When a task is created, a rating for each type of enabled selection criteria is calculated for each available agent. The agent whose total rating is highest is considered for auto-assignment.

The settings for the auto-assignment weighting properties, found in **Security Incident > Administration > Properties**, are included in the rating calculations.

These values help you prioritize which auto-assignment selection criteria is more important to your organization. Set the priority values between 1 (less important) and 10 (important).

For an example of how the weighting properties affect agent ratings, see **Agent auto-assignment using multiple selection criteria**.
Agent auto assignment using location

Agents can be auto-assigned based on the home location in their user record and the location of the tasks.

Auto-assignment by location is performed when the **Auto-selection of agents will consider location of agents configuration** option is enabled.

When a task (security incident or response task) is created, the agent closest to the task location is considered for the task. If the application is configured so that only location is considered, the closest agent is auto-assigned the task.

When a task is created, agent locations are compared to the following ranges to determine each agent location rating.

<table>
<thead>
<tr>
<th>Distance (mi.) from agent to task</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 to 0.1</td>
<td>1</td>
</tr>
<tr>
<td>0.11 to 0.5</td>
<td>0.9</td>
</tr>
<tr>
<td>0.51 to 5</td>
<td>0.7</td>
</tr>
<tr>
<td>5.1 to 10</td>
<td>0.5</td>
</tr>
<tr>
<td>10.1 to 20</td>
<td>0.4</td>
</tr>
<tr>
<td>20.1 to 30</td>
<td>0.3</td>
</tr>
<tr>
<td>30.1 to 40</td>
<td>0.2</td>
</tr>
<tr>
<td>40.1 to 100</td>
<td>0.1</td>
</tr>
<tr>
<td>&gt;100</td>
<td>0</td>
</tr>
</tbody>
</table>

If the application is configured to use other selection criteria, such as skills, time zone, or schedule, the ratings of all selection criteria are weighted and summed up. The agent with the highest overall rating is auto-assigned for the task. See Agent auto-assignment using multiple selection criteria for details.

Agent auto-assignment using skills

Agents can be auto-assigned based on their skills and the skills required to perform the task. Assign skills to their user records using **Skills > Users**.

Auto-assignment by skills can be performed when the **Auto-selection of agents for tasks requires them to have skills** configuration option is set to **all** or **some**.

When a task that includes skills is auto-assigned, an agent's skills are compared with the skills required to perform the task. A rating is calculated based on the
skills configuration option. If the option is set to **some**, the agent with the closest skills match is auto-assigned the task. If the option is set to **all**, only agents who possess all the required skills are considered. If no agents possess all the skills required to perform the task, no one is auto-assigned.

A skills rating is calculated as:

\[ \frac{\text{Skills}_{agent}}{\text{Skills}_{task}} \]

Where:

- \( \text{Skills}_{agent} \) is the number of skills possessed by the agent that match the skills required for the task.
- \( \text{Skills}_{task} \) is the total number of skills required for the task.

For example, if a task requires four skills, and Agent A possesses three of them and Agent B possesses two of them:

- Agent A skill rating = \( \frac{3}{4} \) or 0.75
- Agent B skill rating = \( \frac{2}{4} \) or 0.5

If the application is configured to use other selection criteria, such as location or time zone, the ratings of all selection criteria are weighted and summed up. The agent with the highest overall rating is selected for the task. See **Agent auto-assignment using multiple selection criteria** for details.

### Agent auto-assignment using time zones

Agents can be auto-assigned based on the time zone defined in their user records and the time zone of the tasks.

If the **Auto-selection of agents will consider time zone for the task** configuration option is enabled, auto-assignment by time zone can be performed.

When a task is created, agents in the time zone closest to the task time zone are considered for the task. If the application is configured so that only time zone is considered, only an agent in the same time zone can be auto-assigned the task.

**Note:** It is important that the time zones for the agent and the task set correctly.

When a task is created, agents are rated based on the time zone of the task and the time zone of the agent using the following formula:

\[ 1 - \frac{\text{abs}(\text{Task}_\text{tz} - \text{Agent}_\text{tz})}{12} \]

where:
• abs is the mathematical function to compute the absolute value.
• Task_tz is the offset between the time zone of the task and GMT.
• Agent_tz is the offset between the time zone of the agent and GMT.

For example, a task is created in New York City (GMT-4), and two agents are available to perform the task, one in Los Angeles (GMT-7) and one in Paris, France (GMT+1).

The rating of the agent in Los Angeles is calculated as:
\[ 1 - \frac{\text{abs}((-4) - (-7))}{12} \] or 0.75

The rating of the agent in Paris is calculated as:
\[ 1 - \frac{\text{abs}((-4) - (+1))}{12} \] or 0.58

So if the auto-assignment of the task is based on the time zone alone, it is assigned to the agent from Los Angeles.

If the application is configured to use other selection criteria, such as skills or location, the ratings of all selection criteria are weighted and summed. The agent with the highest overall rating is selected for the task. See Agent auto-assignment using multiple selection criteria for details.

Agent auto-assignment using group coverage areas

Agents can be auto-assigned based on the group coverage area defined in their user records.

Agent auto-assignment using multiple selection criteria

When a task is created, the agents ratings are calculated. For more information, see:
• Agent auto assignment using location
• Agent auto-assignment using skills
• Agent auto-assignment using time zones

Auto-assignment is based on the following calculation:
\[
\frac{\text{Criteria}_1 \text{ rating} \times \text{Criteria}_1 \text{ weight} + \text{Criteria}_2 \text{ rating} \times \text{Criteria}_2 \text{ weight} + \text{Criteria}_3 \text{ rating} \times \text{Criteria}_3 \text{ weight}}{\text{Number of criteria types used}}
\]

where:
• Number of criteria types used = 1, 2, or 3 depending on the location, skill, and time zone settings used.

This example calculates agent auto-assignment based on location and skills. The example is based on the following assumptions.
• The **Auto-selection of agents will consider location of agents** configuration option is enabled for the application.

• The **Auto-selection of agents requires them to have some of the required skills for the task** configuration option is enabled for the application.

• The **Skills Weight** property is set to 10 for the application.

• The **Location Weight** property is set to 5 for the application.

• Agents A and B are available to perform a task, and the task requires four specific skills.

• Agent A location is 5 miles from the site of the task and possesses three of the four required skills.

• Agent B' location is one-quarter mile from the site, and possesses two of the required skills.

Auto-assignment for the agents uses this calculation: 
\[ \frac{(\text{Location rating} \times \text{Location weight}) + (\text{Skills rating} \times \text{Skills weight})}{2} \]

• The auto-assignment calculation for Agent A is: 
\[ \frac{(0.7 \times 0.5) + (0.75 \times 1)}{2} = 0.55 \]

• The auto-assignment calculation for Agent B is: 
\[ \frac{(0.9 \times 0.5) + (0.5 \times 1)}{2} = 0.475 \]

In this example, Agent A is auto-assigned the task.

**Managing security incidents and inbound requests**

After a security incident has been created, there are numerous types of information that can be added and viewed as your analysis of the issue progresses toward resolution.

**Create an inbound request**

Unlike security incidents, inbound requests are generally of a lower priority. Requests for a lookup, scan, or a new badge are examples of inbound requests.

**Before you begin**

Roles required: sn_si.basic role or higher
Procedure

1. Navigate to one of the Requests forms. For example, Security Incident > Inbound Requests > Assigned to Me, and click New.
2. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>[Read only] The automatically generated security request number.</td>
</tr>
<tr>
<td>Company</td>
<td>The requester company.</td>
</tr>
<tr>
<td>Location</td>
<td>The CI location, if applicable. This field is pre-filled when the CI is selected.</td>
</tr>
<tr>
<td>Configuration Item</td>
<td>The configuration item affected by the request.</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority of the request.</td>
</tr>
<tr>
<td>Opened</td>
<td>[Read only] The date and time that the request was opened.</td>
</tr>
<tr>
<td>State</td>
<td>The current state of the security request. Upon security request creation, this field defaults to Draft.</td>
</tr>
<tr>
<td>Assignment group</td>
<td>The assignment group from which the assigned worker is selected.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>The individual assigned to perform the work.</td>
</tr>
<tr>
<td>Short description</td>
<td>A brief description of the security request, which is visible to the requester.</td>
</tr>
<tr>
<td>Description</td>
<td>The full description of the request, which is visible to the requester.</td>
</tr>
<tr>
<td>Work notes</td>
<td>Work notes, which are visible to the requester.</td>
</tr>
</tbody>
</table>

3. When you have completed your entries, click Submit.
4. If you must escalate the request to a security incident, click Convert to Security Incident.

Manage observables

Observables are artifacts found on a network or operating system that are likely to indicate an intrusion. Typical observables are IP addresses, MD5 hashes of
malware files or URLs, or domain names. Threat Intelligence observable table data is available from within a security incident.

Observables information includes value, type, context, and timestamp.

You can create or delete observables manually or automatically through lookup requests.

A new **Finding** column has been added to the **Threat Lookup Results** tab. Possible values are: Malicious and Unknown.

- If an IoC lookup request does not find a security incident observable, it is labeled Unknown.
- If an IoC lookup request does find a security incident observable, it is labeled Malicious.

During an upgrade, existing items have the **Finding** column set to Malicious.

![Note:](image)

While Threat Intelligence observables table data is part of a security incident, no other interaction with the Threat Intelligence module is included. For full threat functionality, the Threat Intelligence plugin is available by subscription.

**Related information**

Create a security incident observable

**Show IoC information for a security incident**

You can view IoC information, such as observables and sightings search results associated with a security incident.

**Before you begin**

Role required: sn_si.basic

**Procedure**

1. If it is not already open, open the security incident for which you want to view IoC-related information.
2. Click the **Show IoC** related link.
3. Click any of the related lists to view or add information for the security incident.
<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observables</td>
<td>View or manually add or edit observables associated with the security incident. For more information, see Manage observables.</td>
</tr>
<tr>
<td>Associated Indicators</td>
<td>If Threat Intelligence is activated, you can view any other indicators associated with any of the same threat records.</td>
</tr>
<tr>
<td>Sightings Search Results</td>
<td>Contains Sightings Search results.</td>
</tr>
<tr>
<td>Sightings Search Details</td>
<td>Contains Sightings Search record details.</td>
</tr>
<tr>
<td>Threat Lookups</td>
<td>Stores enrichment data from malware detection systems. This tab only appears when the Threat Intelligence plugin is installed.</td>
</tr>
<tr>
<td>Associated Attack Modes/Methods</td>
<td>If Threat Intelligence is activated, you can view any other attack types associated with any of the same threat records.</td>
</tr>
<tr>
<td>Security Scan Requests</td>
<td>If Threat Intelligence is activated, you can view scan and lookup requests attached to the security incident.</td>
</tr>
<tr>
<td>Resources with Similar IoC</td>
<td>If Threat Intelligence is activated, you can view any other resources with similar indicators.</td>
</tr>
<tr>
<td>Users with Similar IoC</td>
<td>If Threat Intelligence is activated, you can view any other users with similar indicators.</td>
</tr>
</tbody>
</table>

4. Click any of the following related links to further update the security incident:
   - Show Affected Items
   - Show Related Items
   - Show Enrichment Data
   - Show Response Tasks

5. When you have completed your entries, click Submit.

Create a security incident observable

You can create and view an observable within a security incident and take appropriate action. Having observables available in the security incident is scalable and reduces response time.
Before you begin
Role required:
sn_ti_observable.write (write)
sn_ti_observable.read (read)
sn_ti_observable.admin (delete)

Procedure
1. Navigate to Security Incident.
2. Choose an incident.
3. Click Security Incident Observables related list tab.
4. Click New.
5. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select classification tag</td>
<td>If you set up and activated security tags to add metadata to the record, you can select one or more tags to specify the degree of sensitivity of the observable. If you did not set up or activate security tags, this drop-down list is not displayed.</td>
</tr>
<tr>
<td>Value</td>
<td>The value (for example, IP address or hash) associated with the observable.</td>
</tr>
<tr>
<td><strong>Note:</strong> If a call on an IP address or hash, returned malware or some other failure, the IP address or hash value is automatically added to the Observable [sn_ti_observable] table. As such, it can be searched for from the Observables form.</td>
<td></td>
</tr>
<tr>
<td>Observable type</td>
<td>Select the observable classification, such as an IP address or file hash. These observable types are defined in the Observable Types module.</td>
</tr>
<tr>
<td><strong>Note:</strong> For a File type observable, select the Observable Type: File to upload the file attachment.</td>
<td></td>
</tr>
<tr>
<td>Incident count</td>
<td>The number of times the observable value has been encountered.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Is composition</td>
<td>This field displays only after the observable record has been saved.</td>
</tr>
<tr>
<td></td>
<td>If the <strong>Observable Type</strong> is set to anything other that <strong>Observable Composition</strong>, and this new observable is a composition, select this check box.</td>
</tr>
<tr>
<td></td>
<td>If the <strong>Observable Type</strong> is already set to <strong>Observable Composition</strong>, the check box is selected and read-only.</td>
</tr>
<tr>
<td></td>
<td>An observable composition is an observable that contains child observables.</td>
</tr>
<tr>
<td>Finding</td>
<td>Select one of the following: None, Unknown or Malicious. Unknown is the default.</td>
</tr>
<tr>
<td></td>
<td>✨ Note: After an upgrade, existing observables are marked Malicious.</td>
</tr>
<tr>
<td>Operator</td>
<td>This field appears only when the <strong>Is composition</strong> check box is selected. Depending on your setting in this field, the observables and their children are considered when deciding whether an associated indicator is present.</td>
</tr>
<tr>
<td></td>
<td>Set this field to <strong>AND</strong> if <strong>all</strong> the child observables must be present for an associated indicator to be considered present.</td>
</tr>
<tr>
<td></td>
<td>Set it to <strong>OR</strong> if <strong>any</strong> of the child observables are present for an associated indicator to be considered present.</td>
</tr>
<tr>
<td>Must not be present</td>
<td>This field displays only after the observable record has been saved.</td>
</tr>
<tr>
<td></td>
<td>If selected, this field signifies that the absence of the observable is the potential issue (for example, a missing registry key).</td>
</tr>
<tr>
<td>Location</td>
<td>Using the settings in two properties and a script include definition, you can load <strong>Load more IoC data</strong> in this field.</td>
</tr>
<tr>
<td>Notes</td>
<td>Enter any additional notes about the observable.</td>
</tr>
</tbody>
</table>

6. Right-click in the form header and click **Save**. You can now click any of the following related lists to view additional information.
## Related List

<table>
<thead>
<tr>
<th>Related List</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related Indicators</td>
<td>Lists indicators that have been identified by the threat source.</td>
</tr>
<tr>
<td>Associated Tasks</td>
<td>Lists changes associated with the observable.</td>
</tr>
<tr>
<td>Child Observables</td>
<td>Lists related observables that have been identified by the threat source.</td>
</tr>
<tr>
<td>Matching Resources for IP</td>
<td>If the observable is an IP address, this list shows any resources (configuration items) that have a matching IP address.</td>
</tr>
<tr>
<td>Observable Sources</td>
<td>Lists the sources of this observable, along with the confidence level of the source.</td>
</tr>
<tr>
<td>Security Annotations</td>
<td>Lists security annotations added to this observable.</td>
</tr>
</tbody>
</table>

### 7. Returning to the security incident the following information is available.

**Note:** When you add an observable to the security incident, the system checks for any other configuration items or users associated with it. The **Related Configuration Items** and **Related Users** related list tabs are updated accordingly.

<table>
<thead>
<tr>
<th>Column</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observable</td>
<td>The value (for example, IP address or hash) associated with the observable.</td>
</tr>
<tr>
<td>Observable Type</td>
<td>The specific type of observable.</td>
</tr>
<tr>
<td>Context</td>
<td>Selected by the user. Choices are:</td>
</tr>
<tr>
<td>Column</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IP - Source or Destination</td>
<td>• <strong>Note:</strong> If Threat Intelligence and Palo Alto Networks - Firewall are activated, changing or adding a value to this field causes the Get Log Data workflow to execute. The workflow retrieves enriched threat log data from the firewall and attaches it to the security incident. The information is also parsed and displayed in the Firewall Logs section under the Enrichment Data tab.</td>
</tr>
<tr>
<td>URL - Referrer</td>
<td>• <strong>Note:</strong> When the user clicks a link in a phishing email, a referrer is the URL of the final jump before the malware URL is accessed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Incident Count</th>
<th>The number of incidents that this observable appears in. This value is automatically updated when the observable is added to another incident manually or through a workflow.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated</td>
<td>Data and time the list was last updated.</td>
</tr>
</tbody>
</table>

**Note:** If the Threat Intelligence plugin is installed, you can also view the observable in the Observables list in the IoC Repository.

### Related information

- Edit a security incident observable list
- Add multiple security incident observables

### Manage file observables

Manage file observables provides stringent security measures to store the suspicious files and enables the files type observables for sandbox integration.

**About this task**

You can create and view file type observables for a security incident. The suspicious files which are part of the observables are stored in a specific location, which can be accessed by the security analyst to download the file only with a specific role.

**Role required:** sn_ti_malicious_attachment_access (upload)

Upload the file type observables:
• Automatically: When the security incidents are created for the phishing emails, the attachments in the phishing email are created as file type observables.

• Manually: A security analyst can also upload the suspicious files to create file type observables.

Procedure
1. Navigate to a security incident.
2. Select Observables from the Show All Related Lists tab.

   If there are any attachments in the phishing email, then by default those attachments are created as file type observables in the corresponding security incident. Each attachment is created as two observables such as file type and file hash observable.

3. To upload the secure attachments manually:
   • Click Upload Secure Attachment.
   • On the Upload Secure Attachments, Click Choose file to upload one or more files. Each file is considered as a single observable record.
   • Click Create File Observables to create the file type observables such as one is the file type and other one is the file hash which is a unique identifier.

File type observables

Select the file type observable to process for further integrations such as sandbox, threat lookup. In addition, you can also download the attachments from the file type observable.
Note:
The threat lookup (VirusTotal) retrieves the file from the secured attachments for the new file type observables and the below system properties are not applicable for the new file type observables.

- sn_ti.scan.delete_attachment_after_hash
- sn_ti.scan.use_file_hash

For a quick reference, the file type observable is mapped as a child to the hash observable and hash observable is mapped as a child to file observable.

If the phishing email attachments are exceeding more than the defined size then the observables are not created. You must modify the system properties to support the larger size files.

<table>
<thead>
<tr>
<th>System property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.email.inbound.max_total_attachment_size_bytes</td>
<td>If you are forwarding the phishing email directly, use this system properties value to increase the file size from 18MB to a desired file size.</td>
</tr>
<tr>
<td>com.glide.attachment.max_get_size</td>
<td>If you are forwarding the phishing email as an attachment, use this system property value to create the below system properties under global scope to increase the file size from 5MB to the desired size.</td>
</tr>
</tbody>
</table>

- You can also create a new file type observable as follows:
  - Click **New**.
  - Select the **Observable type Category: File**
  - Click **Upload** button to attach a file.

Edit a security incident observable list

You can edit which observables in the list associated with a security incident to display.

Before you begin
Role required: sn_si.basic
Procedure
1. Navigate to **Security Incident**.
2. Choose an incident.
3. Click **Security Incident Observables** related list tab.
4. Click **Edit**.
5. Add or remove observables from the list. Create a filter for long lists.

6. Click **Save**.

**Note:** When you add an observable to the security incident, the system checks for any other configuration items or users associated with it. The **Related Configuration Items** and **Related Users** related list tabs are updated accordingly. Also, if the Threat Intelligence plugin is activated, and you have at least one **Security Incident Response integrations** integration implementation activated, the **Security Operations Integration - Threat Lookup** capability executes one or more workflows, and threat security lookups are performed on the observables you added. The results appear in the **Threat Lookup Results** tab.
Related information
Add multiple security incident observables
Create a security incident observable

Add multiple security incident observables
To save time, you can add multiple security incident observables to the security incident observables list.

Before you begin
Role required: sn_ti_write
⚠ Note: When adding multiple security incident observables, duplicates are ignored during processing.

Procedure
1. Navigate to Security Incident.
2. Choose an incident.
3. Click the Add Multiple Observables related link.
4. Enter or paste multiple observables. Entries can be of any Observable Type. Accepted formats are: comma, new line, tab, or pipe separators.

⚠ Note: When you add an observable to the security incident, the system checks for any other configuration items or users associated with it. The Related Configuration Items and Related Users related list tabs are updated accordingly.

⚠ Note: Observable values not auto-detected are assigned to type Unknown.
5. Click Submit.
Automatic security incident observable log data enrichment

When certain applications and integrations are set up, including Threat Intelligence and the Palo Alto Networks - Firewall integration, observables information in a security incident can be automatically enriched with threat log data whenever the Source IP for its observables is modified.

When a modification occurs, a business rule initiates a workflow that retrieves data from threat logs on your firewall and enriches the observables information in the security incident.

Before observables can be enriched, the following steps must be performed.

- Threat Intelligence must be activated.
- The Palo Alto Networks Firewall integration must be activated and configured. This can also include Set up SSH credentials to the MID Server.

After that setup has been completed, the act of changing the Source IP of observables associated with a security incident causes a business rule to execute the Security Operations Palo Alto Networks - Get Log Data workflow. Workflow activities queue up a search query on the firewall and return a Job ID that is used to retrieve threat logs data from the firewall and attach them as an XML file to the security incident.

Related information

- Get AutoFocus Session Info Enrichment workflow
- Security Operations Integration Palo Alto Networks Firewall Launcher workflow
- Security Operations Palo Alto Networks - Check and Block Value workflow
- Get Log Data workflow
- Get WildFire Data Enrichment workflow

Publish observables to a third-party watchlist

You can publish one or more observables or associated indicators to a third-party watchlist. Currently, the only implementation that supports this functionality is CrowdStrike Falcon Host.

Before you begin
Role required: sn_si.analyst

About this task
• Note: If no implementations are available, capability actions are not displayed in product menus.
Procedure

1. Navigate to a security incident.
2. Select Observables from the Related List tab.
3. Click Publish to Watchlist in the Actions on selected rows... drop-down menu.

The dialog box appears.

4. Enter or choose the implementation.

Note: A workflow is triggered by the Security Operations Integration - Publish to Watchlist capability when you select the CrowdStrike Falcon Host implementation.

5. Click Submit.
Manage lookups and scans
You can perform lookups and vulnerability scans from security incidents and from the security incident catalog to identify potential threats and vulnerabilities.

Submit an IoC Lookup request from a security incident
An IoC lookup automatically runs whenever observables are added to a security incident. Also, if your security incident has attachments, they can be easily found with the press of a button.

Before you begin
For automatic IoC lookups, the Threat Intelligence plugin must be activated.
Role required: sn_si.basic

**Note:** By default, the **Lookup Type** for **File** is inactive.

Procedure
1. Create a new security incident or open an existing one if you intend to attach new files to it.
2. Click the paperclip icon in the form header and attach one or more files.
3. When you have completed your entries on the form, right-click the form header and click **Save**. After the record has been saved, a **Lookup attachments** button appears.
4. Click **Lookup attachments**.

**Note:** The work notes under **Incident Details** report the progress of the lookup process.
5. You can click the lookup number at the end of the message to view the lookup record. You can click the Lookup reference link to view detailed results.

Submit an IoC Lookup request from the Security Incident Catalog
If the Security Incident Response plugin is activated, you can submit threat lookups for files, hash values, URLs, and IP addresses from the Security Incident Catalog. The requests are submitted and you can view the results in the **My Requests** module.
Before you begin
Role required: none

About this task
Lookups are automatically performed for the default lookup type for each lookup source listed in the lookup record. The results of the lookup request are available in the My Requests module.

Procedure
1. Navigate to Self-Service > Security Incident Catalog.
2. Click IoC Lookup.
3. Click Lookup files, hash values, URLs or IP addresses.
4. Enter one or more of the following:

<table>
<thead>
<tr>
<th>IoC Lookup request</th>
<th>Description</th>
</tr>
</thead>
</table>
| Files              | Click the paperclip icon, then locate and attach the files you want to lookup.  
  Note: By default, the Lookup Type for File is inactive. Files are converted and submitted as a hash value. |
| URLs               | In the URLs field, enter the URLs you want to lookup, separated by commas. For example: www.abc.com, www.xyz.net. |
| IP addresses       | In the IP addresses field, enter the IP addresses you want to lookup, separated by commas. |
| Hash values        | In the Hash values field, enter the hash values you want to lookup, separated by commas.  
  Note: When the Lookup Type for File is inactive, this value is the default action for both File and Hash values. |
5. When you have made your selections, click Submit.
6. To view the status and/or results of the lookups, navigate to Self-Service > My Requests.
7. Click the SR number for the request.
   The work notes under Activity list the tasks performed during the lookup, including the creation of individual lookups for each file, hash value, URL, or IP address, and the lookup results.
Submit a vulnerability scan request from a security incident

If your security incident has one or more configuration items (servers, computers, and so on), they can be scanned for vulnerabilities from the Security Incident Response form.

Before you begin
The Vulnerability Response plugin must be activated.
Role required: sn_si.write

Procedure
1. Create a security incident and include at least one resource. You can also open an existing incident that has configuration items.

2. When you have completed your entries on the form, right-click the form header and click Save. After the record has been saved, a Scan for Vulnerabilities related link appears.

   Note: If the Scan for Vulnerabilities related list is not shown, you must navigate to Vulnerability > Scanners, set up at least one scanner, and set its default to true.

3. Click Scan for Vulnerabilities.

   Note:
   A message appears at the top of the security incident form, along with a link to the scan record.

   Scan request SR0001002 has been created to check for vulnerabilities.

4. You can click the scan request number to view the scan record. The incident details show the results of the scan in the Security Scan Request record.

Submit a vulnerability scan request from the Security Incident Response catalog

You can submit vulnerability scans for CIs and IP addresses from the Security Incident Response catalog. The requests are submitted and you can view the results in the My Requests module.

Before you begin
Role required: none
Procedure

1. Navigate to Self-Service > Security Incident Catalog.
2. Click Vulnerability scan.
3. Click Scan Configuration Item and IP addresses.
4. Enter one or more of the following to be scanned.

<table>
<thead>
<tr>
<th>Vulnerability Scanners</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item to be scanned</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Configuration item</td>
<td>In the Configuration Item to scan field, select the CI to be scanned.</td>
</tr>
<tr>
<td>IP addresses</td>
<td>In the IP addresses to scan field, enter the IP addresses, separated by commas.</td>
</tr>
</tbody>
</table>

5. When you have made your selections, click Submit. If an observable is found, an indicator is created, according to STIXX standards.

6. To view the status and/or results of the scans, navigate to Self-Service > My Requests.

7. Click the SR number for the request. The work notes under Activities list the tasks performed during the scan, including the creation of individual scans for each CI or IP address, and the results of the scans.

Manage on-demand orchestration

During Security Incident Response analysis, a security analyst may want to perform a task that is driven by a security incident workflow. For example, run a process dump on a particular CI. This can be accomplished with on-demand orchestration.

Each registered Security Operations application includes several on-demand orchestrations in the base system. You can define custom on-demand orchestrations, as needed.

On-demand orchestration can be invoked from a choice list at the bottom of the following lists and forms in Security Incident Response:

- Security Incident form
- Security Incident list
- Security Incident Observables related list
- Configuration Items related list

Note:
A property in Security Support Common called `sn_sec_cmn.use_on_demand_tbl_as_whitelist` defines which workflows are available for on-demand execution.

If the property is set to `true`, only workflows specified in the On Demand Orchestration [sn_sec_cmn_on_demand_orchestration] table are available.

If the property is set to `false` (default), all workflows for applications configured in the SecOps Application Registry are available.

Depending on the setting of the property, the list of workflows available is tailored to the type of information being analyzed.

Perform on-demand orchestration from the Security Incident form

On-demand orchestration can be invoked from a choice list at the bottom of the Security Incident form.

Before you begin
Role required: sn_si.write

Procedure
1. Navigate to Security Incident > Incidents > Show Open Incidents.
2. Select the record (security incident, observable, or CI) for which you want to run a workflow.
3. Click the Run Orchestration related link.
   The Run Orchestration dialog box opens. The appearance of the dialog box depends on the setting of the `sn_sec_cmn.use_on_demand_tbl_as_whitelist` property in Security Support Common.
4. Click the lookup icon and select the workflow you want to run. The selected workflow runs. For details, see Security Incident Response Orchestration workflows and activities.

Perform on-demand orchestration from the Security Incident list

On-demand orchestration can be invoked from the Security Incident list, as well as from related lists in Security Incident Response.

Before you begin
Role required: sn_si.write

Procedure

1. Navigate to Security Incident > Incidents > Show Open Incidents.
2. Select the check box next to the security incident for which you want to run a workflow.
3. Click the Actions on selected rows choice list at the bottom of the screen, and click Run Orchestration. The Run Orchestration dialog box opens. The appearance of the dialog box depends on the setting of the sn_sec_cmn.use_on_demand_tbl_as_whitelist property in Security Support Common.
4. Click the lookup icon and select the workflow you want to run. The selected workflow runs. For details, see Security Incident Response Orchestration workflows and activities.

Define new on-demand orchestrations

In the base system, you can select on-demand orchestrations that execute predefined workflows. You can define new on-demand orchestrations to customize how workflows are invoked from the Run Orchestration choice lists.

Before you begin
Role required: sn_si.write

Procedure

1. Navigate to Security Operations > Utilities > On-Demand Orchestration
2. Click New.
3. Fill in the fields, as appropriate.
## On Demand Orchestration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workflow</td>
<td>Select the workflow to be included in the <strong>Run Orchestration</strong> choice list.</td>
</tr>
<tr>
<td>Table</td>
<td>Select the table on which the selected workflow is executed. If the table does not match the table configured for the selected workflow, you must select the Advanced check box and modify the <strong>Execution script</strong> to pass the correct record to the workflow on execution.</td>
</tr>
<tr>
<td>Roles</td>
<td>As needed, select additional roles to restrict who can see this workflow in the <strong>Run Orchestration</strong> choice list.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to activate this on-demand orchestration record.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Select this check box to modify the execution script so that it passes the correct record to the selected table for this workflow.</td>
</tr>
<tr>
<td>Execution script</td>
<td>Modify the execution script so that it passes the correct record to the selected table for this workflow.</td>
</tr>
<tr>
<td></td>
<td>This field appears only if the Advanced check box is selected.</td>
</tr>
</tbody>
</table>

4. Right-click in the record header, and select **Save**. The **Workflow Versions** related list appears.
5. If you need to make additional modifications to the workflow, you need to check it out.

Related information

Work with workflow versions

Register new Security Operations applications for on-demand orchestration

In the base system, Security Operations applications are automatically registered when they are activated. Registration allows the workflows associated with the applications to be available for on-demand orchestration requests. If needed, you can define new applications and associate workflows with them for on-demand orchestration.

Before you begin
Role required: sn_si.write

Procedure

1. Navigate to Security Operations > Utilities > SecOps Application Registry, and click Register Application.
   The Security Operations Application screen appears.

2. In the Application field, click the lookups (magnifying glass) icon.
   The Applications screen appears.
3. Click **New**.
The Application Creator screen appears.
4. After the application has been generated, you can create scripts for setting up on-demand orchestration.

Note: Setting up on-demand orchestration for new applications requires advanced technical knowledge of scripting and creating triggers for the scripts (business rules, UI action, workflows, and so on). For more information, contact ServiceNow Professional Services.

Add information to a security incident

After a security incident is created, you can add more details to aid in analysis, such as access roles and different kinds of notes.

Before you begin
Role required: sn_si.basic

Procedure
1. If it is not already open, open the security incident you want to update.
2. Click the Incident Details tab.
3. Fill in the fields, as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read access</td>
<td>Gives a user with the <strong>special access</strong> role read access to the security incident. The user is able to read and write work notes.</td>
</tr>
<tr>
<td></td>
<td>Note: If a user is added to both Read access and Privileged access lists, then only the Privileged access permissions persist.</td>
</tr>
<tr>
<td>Watch list</td>
<td>Click the lock icon to add users who are notified when changes to the security incident occur. After the field is unlocked, options are available for adding or removing multiple users or entering user email addresses. When you have completed your entries, click the lock icon to lock the field.</td>
</tr>
<tr>
<td>Privileged access</td>
<td>Gives a user with the <strong>special access</strong> role read and write access to all fields of the security incident except <strong>Assigned to</strong>. Users with special access roles have their own module containing all security incidents assigned to them. No other modules are</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Field</td>
<td>available to them. No one else can see the Visible to Me module.</td>
</tr>
<tr>
<td>Note:</td>
<td>Only an assigned user or someone with a security role (for example, sn_si_analyst or sn_si.admin) can change the Assigned to field.</td>
</tr>
<tr>
<td></td>
<td>If a user is added to both Read access and Privileged access lists, then only the Privileged access permissions persist.</td>
</tr>
<tr>
<td>Work notes list</td>
<td>Click the lock icon (🔒) to add users who are notified when new work notes are added. After the field is unlocked, options are available for adding or removing multiple users or entering user email addresses. When you have completed your entries, click the lock icon to lock the field.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a full description of the security incident, along with any information that can help to find the cause or resolve the issue.</td>
</tr>
<tr>
<td>Secure notes</td>
<td>Click the lock icon to unlock the field, enter work notes that are visible to the security users, and click the icon again to lock it.</td>
</tr>
<tr>
<td>Work notes</td>
<td>Type work notes that are not visible to the customer. Work notes appear in the Activity area.</td>
</tr>
<tr>
<td>Activity</td>
<td>Displays information manually entered in Work notes, and all dynamically updated task activity (actions, comments, work notes, and so on) on related records for this security incident. Work notes appear with a yellow color band.</td>
</tr>
</tbody>
</table>

Automatically generated notes appear with a gray color band.
4. You can limit the types of information displayed in the **Activity** field by clicking the filter icon.

![Filter Icon]

- All
- Additional comments
- Assigned to
- Attachments
- Automation activity
- Configuration item
- Impact
- Opened by
- Priority
- State
- Work notes

**Note:** The **Automation activity** check box allows you to include any enrichment performed by this security incident, including workflow activities, risk score updates, and so forth.

5. Click any of the following tabs to further update the security incident:

- **Related Records**
- **Post Incident Review**
- **Closure Information**

6. When you have completed your entries, click **Submit**.

**Add related problems, changes, and incidents to a security incident**

You can add related records, such as problems, changes, and incidents to existing security incidents.

**Before you begin**

**Role required:** sn_si.basic
Procedure

1. If it is not already open, open the security incident you want to update.
2. Click the Related Records tab.
3. Fill in the fields, as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem</td>
<td>Select a Problem (PRB) record that resolves the underlying issue that caused this security incident to be created. The PRBs for this incident are typically created by right-clicking in the security incident form header and selecting Create Problem.</td>
</tr>
<tr>
<td>Parent</td>
<td>Select a task record related to the underlying issue that caused this security incident to be created.</td>
</tr>
<tr>
<td>Parent security</td>
<td>Select a security incident record related to the underlying issue that caused this security incident to be created. See Parent and child security incident relationships.</td>
</tr>
<tr>
<td>Incident</td>
<td>Select an Incident (INC) record that resolves the underlying issue that caused this security incident to be created. The incident is typically created by right-clicking in the security incident form header and selecting Create Incident.</td>
</tr>
<tr>
<td>Change request</td>
<td>Select a Change Request (CHG) record that resolves the underlying issue that caused this security incident to be created. The change request is typically created by right-clicking in the security incident form header and selecting Create Change.</td>
</tr>
</tbody>
</table>

4. Click any of the following tabs to further update the security incident:
   - Incident Details
   - Post Incident Review
   - Closure Information

5. When you have completed your entries, click Submit.

Invoke a process dump for an enriched process in Windows

A security analyst can run a process dump on a specific process, dump it into a file, and post it to a shared site on an internal network. An analyst can then view a deny listed process, highlighted in red in a security incident, and perform additional analysis.
Before you begin
The following are required:

• A client running Windows Vista or higher, or a server running Windows Server 2008 or higher.

• The ProcDump command-line utility installed, with a system environment variable that points to the procdump executable file path. The name of the variable must be PROCDUMP. This name is used in a powershell script.

Role required: sn_si.analyst

Procedure
1. Navigate to the security incident with the enriched process on which you want to invoke a procdump. For example, you can navigate to Security Incident > Show Open Incidents, and open a security incident.

2. Click the Enrichment Data tab.

3. Click the Retrieve Running Processes enrichment record.

4. Select the check boxes for the running processes you want to perform a procdump for, click the Actions on selected rows drop-down list at the bottom of the list, and click Run Procdump.
   An initiated prodump workflow for selected process message appears at the top of the list, and the Security Incident Response - Run procdump workflow executes.

View information in a security incident
You can perform several other actions on an existing security incident using the related links.

Before you begin
Role required: sn_si.basic

Procedure
1. If it is not already open, open the security incident you want to update.

2. Within Related Links, you can perform the following tasks:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Manual Runbook</td>
<td>View a list of runbooks available for this security incident.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Response Workflow</td>
<td>View any workflow associated with this incident.</td>
</tr>
<tr>
<td>Add Multiple Observables</td>
<td>Adds a list of observables in comma, new line, tab, or pipe delimited formats.</td>
</tr>
<tr>
<td>Add to Security Case</td>
<td>Adds the security incident to one or more security cases. You can also create a new security case and add this security incident to it.</td>
</tr>
<tr>
<td>Get QRadar IP Summaries</td>
<td>If a QRadar integration is available, and contains valid CIs, source, and destination IP addresses, it triggers the QRadar workflows and displays the results in work notes.</td>
</tr>
<tr>
<td>Run Orchestration</td>
<td>Choose and run a Security Operations workflow.</td>
</tr>
<tr>
<td>Show SLA Time Line</td>
<td>You can view an SLA timeline from a Task SLA record or from an SLA definition.</td>
</tr>
<tr>
<td>Show All Related Lists</td>
<td>Displays all standard related lists and any lists added manually.</td>
</tr>
<tr>
<td>Note: Manually added items are available only in this view.</td>
<td></td>
</tr>
<tr>
<td>Show Affected Items</td>
<td>Displays the lists of CIs, users, and services directly affected by this incident</td>
</tr>
<tr>
<td>Show Related Items</td>
<td>Displays the lists of related incidents, CIs, users, and groups affected by this incident</td>
</tr>
<tr>
<td>Show IoC</td>
<td>Displays the lists of observables, indicators, malware, modes and methods, and security scan requests associated with this incident.</td>
</tr>
<tr>
<td>Show Enrichment Data</td>
<td>Displays the lists of enrichment data, processes, services, statistics, lookups, firewall logs, and compromised user</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Show Response Tasks</strong></td>
<td>Displays the lists of tasks, SLAs, risk score audits, outages, and Exchange searches associated with this incident.</td>
</tr>
<tr>
<td><strong>View Details in External System</strong></td>
<td>If this security incident was generated from an external application, directly or by events, and a link to the originating data was provided, the View Details in External System action opens the URL. You can view and search through the logs that generated this incident.</td>
</tr>
<tr>
<td><strong>Scan for Vulnerabilities</strong></td>
<td>If Vulnerability Response is activated, and you have selected at least one affected CI for the security incident, you can submit a scan request to determine what vulnerabilities exist on the CI.</td>
</tr>
</tbody>
</table>

**Parent and child security incident relationships**

You can associate and track the impact of any given issue using parent and child security incident relationships in Security Incident Response.

Using the Related Records tab, you can add a Parent security incident issue to any Security Incident Response form. This feature automatically makes the incident a child that appears in the Related Lists - Child Security Incidents tab of the parent issue.

ℹ️ **Note:** You cannot make an existing parent security incident its own child by using the same number for both incidents.
You can add one or more **Child Security Incidents** to any security incident record, as well, using the **Edit** button in the **Child Security Incidents** tab. In the following example, all three records are connected.
**Note:** All work notes recorded in the parent are propagated to any active children in Activities under the Incident Details tab.

When a parent is closed or canceled, any active children are also closed or canceled. Any active Response Tasks on the child incident(s) are canceled. If there are no other open Tasks, the child incident is closed. When closed, the Post Incident Interview records the closure and the information found on the Closure Information tab is propagated from the parent to the children.
View affected items for a security incident

You can view affected items, such as CIs, affected users, and affected services associated with a security incident.

Before you begin
Role required: sn_si.basic

Procedure
1. If it is not already open, open the security incident for which you want to view affected items.
2. Click the Show Affected Items related link.
3. Click any of the related lists to view or add information for the security incident.
## Tab Description

### Configuration Items
Affected configuration items (CI). After affected CIs are identified, you can manually add affected resources from this related list.

### Affected Users
After affected users are identified, you can manually add affected users from this related list.

### Affected Services
View or add business services associated with the security incident.

**Note:** If an affected CI is added after the security incident is opened, it is a good idea to right-click in the form header and select **Refresh Impacted Services**.

---

**Note:** If the Security Operations Integration - Get Running Processes integration capability is active, and you add a CI to a security incident, the Get Running Processes workflow runs and retrieves a list of running processes on the CI.

If the Security Operations Integration - Isolate Host integration capability is active, you can select one or more CIs and restrict their system connections to other devices. To do this, select the check boxes for the CIs and click **Isolate Host** from the **Actions on selected rows** choice list.

### 4. Click any of the following related links to further update the security incident:

- Show Related Items
- Show IoC
- Show Enrichment Data
- Show Response Tasks

### 5. When you have completed your entries, click **Submit**.

#### View related items for a security incident

You can view related items, such as similar and child security incidents, related users, vulnerability groups, and vulnerable items associated with a security incident.

**Before you begin**

Role required: sn_si.basic

---

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Procedure

1. If it is not already open, open the security incident for which you want to view related items.
2. Click the **Show Related Items** related link.
3. Click any of the related lists to view or add information for the security incident.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Child Security Incidents</td>
<td>Select a task record related to the issue that caused this security incident to be created.</td>
</tr>
<tr>
<td>Similar Security Incidents</td>
<td>View any other security incidents associated with any of the same observable records.</td>
</tr>
<tr>
<td>Related Configuration Items</td>
<td>Displays a list of security incidents containing configuration items with the same observable as this security incident. This list can be filtered using the CI exclusions filter group. When an observable is added to a security incident this list is automatically updated. By default, observables with a context type of Destination are excluded.</td>
</tr>
<tr>
<td>Related Users</td>
<td>Displays a list of security incidents containing users with the same observables as this security incident. This list can be filtered using the User exclusion filter group. When an observable is added to a security incident this list is automatically updated. By default, observables with a context type of Destination are excluded.</td>
</tr>
<tr>
<td>Related Filter Group</td>
<td>After configuration items are identified, any matching CI or Filter group are automatically added.</td>
</tr>
<tr>
<td>Vulnerability Groups</td>
<td>If Vulnerability Response is activated, you can view vulnerability groups associated with this security incident.</td>
</tr>
<tr>
<td>Vulnerable Items</td>
<td>If Vulnerability Response is activated, you can view vulnerability items associated with this security incident.</td>
</tr>
<tr>
<td>Risks</td>
<td>If any of the core Risk Manager plugins (Policy and Compliance Management, Audit, Management, or Risk Management) are activated, you can view or add risks associated with the security incident.</td>
</tr>
</tbody>
</table>
### Tab Description

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can add this related list from the form header context menu under <strong>Configure &gt; Related Lists</strong>.</td>
<td></td>
</tr>
<tr>
<td>Configuration item events</td>
<td>If Event Management is activated, you can view events.</td>
</tr>
<tr>
<td>Configuration item alerts</td>
<td>If Event Management is activated, you can view alerts.</td>
</tr>
<tr>
<td>Customer Service Cases</td>
<td>If Customer Service is activated, you can view Customer Service case information.</td>
</tr>
</tbody>
</table>

4. Click any of the following related links to further update the security incident:
   - Show Affected Items
   - Show IoC
   - Show Enrichment Data
   - Show Response Tasks

5. When you have completed your entries, click **Submit**.

### View enrichment data for a security incident

You can view enrichment data, such as running processes, running services, and network statistics associated with a security incident.

**Before you begin**

Role required: sn_si.basic

**Procedure**

1. If it is not already open, open the security incident for which you want to view enrichment data.

2. Click the **Show Enrichment Data** related link.

3. Click any of the related lists to view or add information for the security incident.

   **Note:** Raw data details are stored in an attachment to the enrichment data record. If they exceed the field limit, displayed details are truncated.
<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running Processes</td>
<td>Stores the records created by the Security Incident Response Get Running Processes workflow.</td>
</tr>
<tr>
<td>Running Services</td>
<td>Stores the records created by the Security Incident Response Get Running Services workflow.</td>
</tr>
<tr>
<td>Network Statistics</td>
<td>Stores the records created by the Security Incident Response Get Network Statistics workflow.</td>
</tr>
<tr>
<td>Domain Lookups</td>
<td>If the WhoisXML API Integration plugin is activated, stores the records created by a Whois lookup.</td>
</tr>
<tr>
<td>Firewall Logs</td>
<td>Stores enrichment data from firewall logs, such as the Palo Alto Network firewall logs.</td>
</tr>
<tr>
<td>Compromised User Info</td>
<td>Stores accounts identified as being compromised through a Have I Been Pwned? lookup.</td>
</tr>
</tbody>
</table>

**Note:** The Security Enrichment Data tab shows raw enrichment data from Security Incident Response workflows, such as retrieving network statistics or running processes. This tab can be viewed by clicking the Show All Related Lists related link.

4. Click any of the following related links to further update the security incident:
   - Show Affected Items
   - Show Related Items
   - Show IoC
   - Show Response Tasks

5. When you have completed your entries, click **Submit**.

**View response task information for a security incident**

You can view response task information, such as task SLAs, risk score audits, and outages associated with a security incident.

**Before you begin**

Role required: sn_si.basic
Procedure

1. If it is not already open, open the security incident for which you want to view response tasks.

2. Click the **Show Response Tasks** related link.

3. Click any of the related lists to view or add information for the security incident.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tasks</td>
<td>Displays tasks already defined for the security incident. You can manually create a response task or create another type of task from this related list.</td>
</tr>
<tr>
<td>Response Tasks</td>
<td>Displays actions to be performed in response to the security incident.</td>
</tr>
<tr>
<td>Task SLAs</td>
<td>View or add active task SLAs that were defined for the security incident.</td>
</tr>
<tr>
<td>Risk Score Audits</td>
<td>An audit record for each instance of a risk score being changed.</td>
</tr>
<tr>
<td>Outages</td>
<td>View or manually add new outage records associated with the security incident.</td>
</tr>
<tr>
<td>Email Search</td>
<td>A list of records that holds search criteria to run queries on an email server, such as a Microsoft® Exchange Server (based on the implementation installed), and stores the results received.</td>
</tr>
</tbody>
</table>

**Note:** If the Security Operations Integration - Email Search and Delete capability is not active, the **Email Search** related link is not displayed.

4. Click any of the following related links to further update the security incident:
   - Show Affected Items
   - Show Related Items
   - Show IoC
   - Show Enrichment Data

5. When you have completed your entries, click **Submit**.
**View related events and alerts in security incidents**

As a security incident is being worked on, you can view the details of the events. For alerts, you can view and acknowledge these alerts, and create incidents or security incidents from them as needed.

**Before you begin**

You must have the Security Incident Response Event Management support plugin activated.

Role required: si.sn_agent

**Procedure**

1. Navigate to any security incident list (for example, **Security Incident > Incidents > Unassigned Incidents**).

2. If the resources affected by the security incident you are viewing have received alerts or events within the previous 24 hours, one or both of the following related lists appear.
   - Security Incident CI Alerts
   - Security Incident CI Events

3. Click the related list you want to view.

<table>
<thead>
<tr>
<th>Related list</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Incident CI Alerts</td>
<td>You can view details for alerts received within the previous 24 hours. You have the option of clicking <strong>Acknowledge</strong> to indicate that you are aware of the alert and it is being handled. Use <strong>Close</strong> to indicate that the alert is not important.</td>
</tr>
<tr>
<td>Security Incident CI Events</td>
<td>You can view details for event received within the previous 24 hours.</td>
</tr>
</tbody>
</table>

**View security incident to customer service case mapping**

Security Incident Response ships with a default field mapping that maps a security incident to a Customer Service case. You can view the security incident to CS case default map.

**Before you begin**

Role required: sec_cmn.read
Procedure

2. Click Security Incident to CSM Case Field Mapping to view the default map.

3. You can edit the mapping, as needed.
4. When you have completed your changes, click Update.

View a Security Incident Response runbook

Runbooks give you access to procedures related to tasks you are working on.

Before you begin

Role required: sn.si.knowledge_admin

Procedure

2. Select a runbook from the list.
3. To create a runbook, click **New**. See **Create a runbook** for instructions.

**Identify all configuration items affected by a security incident**

If you know which resource (server, desktop or other configuration item) is behind a security incident and want to identify related resources and business services that can be affected, you can use the Business Service Management (BSM) map.

**Before you begin**

Role required: admin or sn_si.admin

**About this task**

The BSM map displays the upstream and downstream dependencies for a selected root CI.

There are two methods you can use to view the BSM map for a CI:

- If you want to view CIs from the context of a task, view from the security incident form.
- If you do not want to view CIs from a task viewpoint, view from the navigation bar.

**Procedure**

1. From the Security Incident form, populate the **Configuration item** field, and click the BSM map icon ( ).

   The BSM map screen displays the map for the last incident you accessed in Incident Management or the last security incident you accessed in Security Incident Management.
2. Click the icons next to a configuration item to view different kinds of details about the resource (server, desktop, or other CI). For example, click the alert icon (⚠️) to view alerts associated with the CI.

⚠️ Note: To view a list of all the available icons, click Filters above the BSM map and expand Filter Task Types.

3. To arrange the map in different configurations, select any of the formats listed above the map (Vertical, Horizontal, Radial), or click Filters to filter the map for easier viewing.

4. If you opened the BSM map from the security incident form, you can add a dependent CI to the security incident by right-clicking the CI and selecting Add Affected CIs.
   You can also add multiple CIs at a time. Drag a box around the CIs you want to add, right-click the box, and select Add Affected CIs.
   The CIs are added to the Affected CIs related list of the security incident.

Calculate the severity of a security incident

You can calculate the severity of a security incident using predefined calculators.
Before you begin
Role required: sn_si.basic

Procedure

1. If it is not already open, open the security incident you want to calculate the severity for.
2. Click the form header context menu and select Calculate Severity:

The severity is calculated based on the predefined rules for base calculators. For more information, see Understanding security incident calculators.

Search for and delete phishing emails

Deleting phishing emails can help reduce exposure to a specific attack across an organization. You can manage phishing emails on your email server by searching, granting approvals, and deleting them.

Before you begin
Roles required: sn_sec_cmn.cap_email_read
You can determine how many users were targeted by a phishing attack by querying an email record associated with a security incident.

Supported software:

- Microsoft® Exchange Server 2010

Limitation: When searching the body of emails, you can search a maximum of 1,500 mailboxes.

**About this task**

This feature is used by the Security Operations Integration - Email Search and Delete workflow to run a query against your email server. Depending on the search criteria you select, the search identifies all emails within a phishing attack, and returns the total number of emails affected or details from the emails affected.

**Procedure**

1. Navigate to **Security Incident > Show Open Incidents**.
2. Choose a security incident.
3. If the **Email Search** related list is not visible, click the **Show All Related Links** related link.
4. Click the **Email Search** related list.
5. Click **New**.
6. Fill in the fields, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the search query</td>
</tr>
<tr>
<td>Query from criteria</td>
<td>A preview of the query run on the email server. Generated from all the associated active search criteria records.</td>
</tr>
</tbody>
</table>
7. Right-click in the form header and select **Save**.

8. Click the **Email Search Criteria** tab and click **New**.

9. Fill in or edit the fields, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email search</td>
<td>Displays the name of the email search. You can change it if needed.</td>
</tr>
<tr>
<td>Search field</td>
<td>Field to search in the email server. The search field has the following choices:</td>
</tr>
<tr>
<td></td>
<td><strong>Subject</strong>&lt;br&gt;This criteria searches for emails that contain the Subject line text specified in the Search text field. For emails that meet this search criteria, the total number of phishing emails and the details of each email, including the email date received, email read status, recipient,</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>and message ID, are returned.</td>
</tr>
</tbody>
</table>

**From**

This criteria searches for emails that contain the sender's full email address (for example, jane.doe@abc.com) specified in the **Search text** field. For emails that meet this search criteria, the total number of phishing emails and the details of each email, including the email date received, email read status, recipient, and message ID, are returned.

ℹ️ **Note:** You cannot use the **From** and **Recipient** fields in the same query.

**Recipient**

This criteria searches for emails that contain the recipient's full email address (for example, john.doe@abc.com) specified in the **Search text** field. It also searches for emails in the To, Cc, and Bcc fields. For emails that meet this search criteria, the total number of phishing emails and the details of each email, including the email date received, etc.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>email read status, recipient, and message ID, are returned.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You cannot use the From and Recipient fields in the same query.</td>
</tr>
<tr>
<td>Body</td>
<td>This criteria searches for emails that contain the body text specified in the Search text field. For emails that meet this search criteria, the total number of phishing emails is returned.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When searching the body of emails, you can search a maximum of 1,500 mailboxes.</td>
</tr>
<tr>
<td>Cc:</td>
<td>This criteria searches for emails that contain the Cc full email address (Ex: <a href="mailto:jane.doe@abc.com">jane.doe@abc.com</a>) specified in the Search text field. For emails that meet this search criteria, the total number of phishing emails is returned.</td>
</tr>
<tr>
<td>Bcc:</td>
<td>This criteria searches for emails that contain the Bcc full email address (Ex: <a href="mailto:jane.doe@abc.com">jane.doe@abc.com</a>)</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>specified in the <strong>Search text</strong> field. For emails that meet this search criteria, the total number of phishing emails is returned.</td>
</tr>
<tr>
<td><strong>Attachment</strong></td>
<td>This criteria searches for emails that contain either the attachment file name or attachment contents specified in the <strong>Search text</strong> field. For emails that meet this search criteria, the total number of phishing emails is returned.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Only plain text attachments are supported for searching the attachment contents.</td>
</tr>
<tr>
<td><strong>Retention Policy</strong></td>
<td>This criteria searches for emails that contain retention policy numbers specified in the <strong>Search text</strong> field. For emails that meet this search criteria, the total number of phishing emails is returned.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to activate this email search query.</td>
</tr>
<tr>
<td>Operator</td>
<td>Possible values are AND and OR. You can define how search criteria are combined to run in the email server.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Order</td>
<td>The order in which the search query is built from the search criteria.</td>
</tr>
<tr>
<td>Search Text</td>
<td>The text to search for. Single quotation marks, double quotation marks, and colons are not supported.</td>
</tr>
</tbody>
</table>

10. Click **Submit**.

11. Repeat as needed to define additional search criteria.

12. You can view the results of the search by clicking the **Email Search Results** tab.

Each line of the Email Search Result Entries form represents a separate email.

13. After you have created a search criteria record, two buttons appear in the Email Search form: **Delete from Email Server(s)** and **Search on Email Server(s)**.

14. To search for emails in the selected server that meet the search criteria you defined, click **Search on Email Server(s)**.
Create a security incident knowledge article

As you work with security incidents and response tasks, knowledge articles automatically display to provide pertinent information about the task you are performing. Your organization can create and maintain articles in the security incident knowledge base.

Before you begin
Role required: sn_sir.knowledge_admin

About this task
Knowledge articles share security information, document the types of cyber threats that your organization faces, and provide answers and responses to these threats.
If needed, you can organize knowledge articles into runbooks, which create associations between the articles and specific tasks. For example, you can configure a runbook with conditions that cause a knowledge base article about phishing to be displayed when you are creating a security incident for a phishing attack. For more information, see Create a Security Incident Response runbook.

Knowledge articles in runbooks can also be associated with specific tasks in a playbook. For more information, see Associate a knowledge article with a playbook task.

The benefits of knowledge articles include the following.
• Employees have one source of information that is easy to search.
• Information can be kept up-to-date, as knowledge articles have a defined life cycle: create, review and update, publish, and retire.
• When you manually create a security request, incident, or response task, a list of relevant articles is presented as you type the short description.

Note: It is important to assign a knowledge manager to each security incident knowledge base.

Procedure
1. Navigate to Security Incident > Catalog & Knowledge > Knowledge.
2. Click the Create an Article icon ( CREATE ).
3. Fill in the fields on the form, as appropriate.
## Knowledge form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>The automatically generated KB number.</td>
</tr>
<tr>
<td>Knowledge base</td>
<td>The knowledge base selected for this article.</td>
</tr>
<tr>
<td>Category</td>
<td>The category for this article.</td>
</tr>
<tr>
<td>Published</td>
<td>When this knowledge article was published. This value is set when the article is created, and updated when the article is published.</td>
</tr>
<tr>
<td>Valid to</td>
<td>When this knowledge article expires. This article will not appear in search results after this date or if a date is not selected.</td>
</tr>
<tr>
<td>Image</td>
<td>An image that appears beside the article when searching from the legacy knowledge portal.</td>
</tr>
<tr>
<td>Workflow</td>
<td>[Read-Only] The publication state of the article, such as Draft or Published. When inserting a new article from an existing article, the state of the new article is reset to Draft.</td>
</tr>
<tr>
<td>Source</td>
<td>The task this knowledge article was created in response to, if any. This field is set automatically when you create the knowledge article from a task record.</td>
</tr>
<tr>
<td>Attachment link</td>
<td>Check box for downloading an attached file automatically when a user accesses the article, instead of opening the article view. Add an attachment to the article to use this option.</td>
</tr>
<tr>
<td>Display attachments</td>
<td>Check box for displaying attachments to users viewing this knowledge article. Attachments appear below the article text. Add one or more attachments to the article to use this option.</td>
</tr>
<tr>
<td>Short description</td>
<td>The title of the article. This title appears when browsing and searching knowledge, and at the top of the article.</td>
</tr>
<tr>
<td>Text</td>
<td>Content for the article. Use the WYSIWYG HTML editor to create content. A preview of the content appears when browsing and searching knowledge.</td>
</tr>
</tbody>
</table>
Note: If you are creating a knowledge article to be associated with a playbook task, set the Knowledge base field to Security Incident Response Runbook.

4. Click Submit to create the article.

What to do next
Any additional steps required to publish the article, such as approvals, depend on the publishing workflow for the knowledge base.

Related information
Create a Security Incident Response runbook

Escalate a security incident
If an escalation path exists for a security incident, the Escalate button is available in the security incident header.

Before you begin
Role required: sn_si.admin
You must have an escalation group created to see this button. See Create a Security Operations user-defined escalation group for more information.

Procedure
1. Navigate to Security Incident > Show Open Incidents.
2. Open the incident you want to escalate.
3. Click on the Escalate button.

4. Choose an escalation group.
5. Enter a reason for the escalation.
Manage post incident activities

Based on the requirements of your business, a review of the origins and handling of security incidents is often needed.

The Post Incident Review functionality in ServiceNow provides many tools for automating, tracking, auditing, and simplifying this process.

This section describes the following:

- Assign post incident review roles
- Configure an assessment trigger condition
- Perform a questionnaire-based post incident review
- Create post incident review assignment rules
- Post incident review report

Assign post incident review roles

You can target questions to specific pre-defined groups by assigning roles to Post Incident Review (PIR) categories.

Before you begin

Role required: admin

Procedure

1. Navigate to Assessments > Metric Definition > Types.
2. Under the Types column, search for a Post Incident Review record.
3. Open the record.
4. Assign one or more roles for this category of questions.

6. Click Submit. Updates Assignment Group and Assigned to on the security incident.
5. Click Update.
7. Choose a user
8. Add one or more metric type roles to the user record.

ℹ️ **Note:** The roles must correspond to roles assigned in the Post Incident Review category.

**Configure an assessment trigger condition**

Define rule conditions and generate mandatory and optional assessments for specific security incidents.

**Before you begin**

Role required: sn_si.admin

ℹ️ **Note:** To use the Post Incident Review Assessment Trigger Conditions feature, you must upgrade to Security Incident Response 11.0. Before upgrading, you must revert any customizations done to the Post Incident Review Metric type and trigger conditions. In addition, you may also have to revert the customizations done to the business rules specific to the post incident review.

- Require assessments to be complete
- Store assignee

**Procedure**

1. Navigate to Security Incident > Administration > Post Incident Review Setup.
2. In the Assessment Trigger Conditions Configure section, click Configure.
Note: On the Assessment Trigger Configuration form, in the Assessments Configurations section, the Generate Assessments check box is selected by default.

- When you select the check box, an optional assessment is created for every security incident.
- When you deselect the check box, the assessments are not generated. The assessment rules are not displayed and you cannot configure conditions for the security incidents.

3. On the Assessment Trigger Configuration form, in the Conditions section, specify the required information.

a. Click Insert a new row.

b. In the Name field, specify the rule name.

c. In the Fulfilment field, specify the fulfilment type.

d. To configure a condition, click the rule record and define conditions in the Condition field.
Note:

- If you create a rule without defining a condition in the **Condition** field, then the condition is evaluated as true and the rule is applicable for all security incidents.

- You can define a specific rule to make the assessments either mandatory or optional, and the assessments are not generated for the remaining security incidents which don’t match the defined rules.

### Trigger conditions

**Assessment trigger conditions examples**

The following examples provide different scenarios on how mandatory and optional assessment trigger conditions are generated.

- On the Assessment Trigger Condition form, generate mandatory assessments when the **Priority** and **Business Impact** for a security incident is set to **Critical** on the **Assessment Trigger Rule** page. In such scenario, the security analysts cannot close the incident until the mandatory assessments are completed.
Mandatory assessment example

- As you can see, in this example, if a security incident is in a Review state, security analysts cannot close the security incident without completing the Post Incident Review Assessment. An assessment link is available to take the assessment to the security analysts who are assigned (or who had requested for the assessment) to the incident.

- On the Assessment Trigger Condition form, generate optional assessments when the Priority and Business Impact for a security incident is set to High. In this example, if the security analysts do not complete the assessments and close the security incident, the assessments are automatically canceled.

- In case, if the mandatory or optional assessments does not match the security incident, assessments are not generated for such security incidents. A security analyst can close the security incident without completing the Post Incident Review assessment.

Perform a questionnaire-based post incident review

You may decide that a post incident review of the security incident is warranted. A post incident review describes what happened, helps to determine why the incident occurred, and identifies how it can be avoided or handled in the future.
Before you begin
Role required: sn_si.admin, sn_si.manager, sn_si.analyst

Note: Any user can participate in a post incident review questionnaire, regardless of role. Roles can be assigned to a review.

About this task
The ServiceNow Security Incident Response application can automate the collection of post incident review information from everyone involved with a security incident by using questionnaires. If you decide to use a questionnaire as part of a post incident review, a list of questions, relevant to the security incident, is sent to the user-defined list of participants. As each user completes the questionnaire, the post incident report is automatically generated. The report compiles all the information related to the security incident, as well as all responses to the post incident review.

While an initial list of questions is provided with the base system, they are customizable. You can create categories and add new questions to them, or you can change individual questions within existing categories. You can ask questions based on roles. You can define when certain questions are asked. There can be questions you ask only for your UNIX servers, for example, or only when there is criminal activity. You can define questions that are asked depending on the answer to another question or on the value in a field on the form. There can even be questions that are filled in entirely by querying the database.

After the security incident is resolved and moved to Review state, assessments are generated for all assigned users and users who are directly added from the Request assessments list.

The questionnaire can be a helpful tool for gathering information about the handling of the security incident from various sources.

During the review, you can add more users to the list or remove existing users from the list, unless they have already started filling out the questionnaire. If you add new users to the list, they receive the questions when the record is saved. The security incident cannot be closed until all questionnaires have been completed. As questionnaires are completed by each user, the post incident report is automatically generated (and regenerated) and displayed on the Post Incident Review tab.

To start a post incident review:
Procedure

1. Create a security incident, or open an existing one by navigating to Security Incident > Incidents > Assigned to Me (or Assigned to Team or Unassigned Incidents).

2. Click the Post Incident Review tab.

3. The Request assessments field defaults to the individual in the Assigned to field. Click the lock icon to add other users to the review list. After the field is unlocked, options are available for adding or removing multiple users, roles, or entering user email addresses.

4. When you have completed your entries, click the lock icon to lock the field.

   **Note:** You can also define conditions which, when met in a security incident, can cause specific users to be automatically added to the Request assessments field for that security incident. For example, when a security incident Category is changed to Phishing, specific individuals who have expertise in phishing threats can be added to the post incident review list. For more information, see Create post incident review assignment rules.

5. Click Update.

   When the incident goes into the Review state (or immediately, if it is already in the Review state), each of the users in the review list receives an initial email notification. Reminders are sent as the due date nears. When each user accesses the questionnaire from the email link or by going to Post Incident Review > My Pending Reviews, the questions shown are drawn from all categories that fit this security incident. If new users are added to the review list before the due date is reached, they are sent notifications when the security incident is saved.

6. As users complete their questionnaires, the post incident report compiles the data and displays the report in the Post Incident Review tab. The questionnaire data is displayed in the Findings tab.

Create post incident review questionnaire categories

You can use the questionnaire categories that come with the base system or create your own categories.

**Before you begin**

Role required: sn.si_admin

**About this task**

To create a new category of questions:
Procedure

1. Navigate to Security Incident > Post Incident Review.

2. Click Review Questions.
   
   A list of categories is displayed, along with their order and filters that define under what conditions the questions are asked (for example, only when the security incident category is Criminal activity). Each category is a section in the post incident review questionnaire and the questions in each category are included only when the security incident matches the Condition filter. For example, for a category of questions applying only to Linux servers, you would set up a filter that selected security incidents where the affected resource type was Linux Server. In that category, you would then create all questions needed when a security incident was on a Linux Server. You use one of the categories supplied in the base system or create a new category. This procedure assumes that you want to create a new category before defining questions.

3. Click New in the list of categories.

4. Fill in the fields on the form, as appropriate.

### Security incident

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the category that appears on the security incident questionnaire.</td>
</tr>
<tr>
<td>Type</td>
<td>Post Incident Review is the default.</td>
</tr>
<tr>
<td>Create Stakeholders</td>
<td>Unused by Security Incident Response.</td>
</tr>
<tr>
<td>Table</td>
<td>This field is autoassigned once the form is submitted.</td>
</tr>
<tr>
<td>Filter</td>
<td>Enter the condition that determines when questions in this category are used.</td>
</tr>
<tr>
<td></td>
<td>If a security incident record matches this filter, the questions is included in a post incident review for that security incident. Filters can use any data on the record, or on other records linked to this record. For example, the department of the requesting user’s manager.</td>
</tr>
<tr>
<td>Application</td>
<td>Scope application for the incident.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weight</td>
<td>Numeric value that represents the importance of this metric relative to other metrics in the same category. By default, the weight is 10.</td>
</tr>
<tr>
<td>Total Metrics</td>
<td>Number of metrics used by the category.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the questionnaire.</td>
</tr>
</tbody>
</table>

5. Click **Submit** to save the category.

---

**Compose post incident review questions**

You can use the questions that come with the base system or create your own questions.

**Before you begin**

Role required: sn.si_admin

**About this task**

The methods for gathering post incident review information can be in the form of questions or as data automatically collected using scripts.

Questions can depend on the answers to other questions. For example, you might ask if all necessary logs were available. If the answer is No, you ask a follow-up question to ascertain which of the needed logs were not enabled.

Scripted data collection, also called script metrics, gather data related to the security incident via scripts you write. This action can go well beyond the data in the security incident record itself. For example, a script metric could gather the recent outage time for a server affected by this security incident.

Finally, you can mix the two types. Questions can have default values taken from a script, or simply from a field in the security incident record. When you use a **Default Answer from ...** type of question, you can choose if you want the user to always answer the question – with the default value providing them an initial value – or if you want the user to only be asked the question if the script or field comes up empty.

To create a new question:

**Procedure**

1. Navigate to **Security Incident > Post Incident Review**.
2. Click the category for which you want to create a new question.
3. Click the **Assessment Metrics** tab.
4. Click **New**. You can also click an existing question to modify it.

5. Fill in the fields on the form, as appropriate.

### Metric form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the metric (question or script). If the metric is a scripted data collection, this name appears on the post incident report.</td>
</tr>
<tr>
<td>Category</td>
<td>The category that the metric belongs to. The system automatically populates this category if you create a new metric from the Metric Category form.</td>
</tr>
<tr>
<td>Method</td>
<td>Indicates the type of metric, as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Assessment</strong>: A question that has no default value. There are several data types that can be defined in the <strong>Data Type</strong> field on the <strong>Field Type</strong> tab, such as check boxes, choice lists, text input.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Script</strong>: Scripted metric. Obtain values by writing a custom script. The <strong>Script</strong> method is compatible with the <strong>Duration</strong>, <strong>Number</strong>, and <strong>Percentage</strong> data types.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default answer from field</strong>: A question where the default response comes from a selected field in the security incident. Selecting this option adds two fields to the <strong>General</strong> tab:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default answer</strong>: Select the field in the security incident that contains the default answer for the question. For example, for the question: &quot;Who initially reported this incident?,&quot; the <strong>Requested by</strong> field would be a likely choice.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Ask question</strong>: Specifies when to ask the question: always or only if the <strong>Default answer</strong> field is empty. Using the example above, the question would be asked if the <strong>Requested by</strong> field is empty.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default answer from script</strong>: A question where the default answer comes from a script. The answer may be a</td>
</tr>
</tbody>
</table>
number, string, or percentage. The **General** tab adds a field:

- **Ask question**: as the Specifies when to ask the question: always or only if the script does not provide a default answer. The script is defined on the **Field Type** tab.

**Note:** If you select a **Data type** that is incompatible with the selected **Method**, the system automatically changes the **Method** to a compatible value.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weight</td>
<td>[Required] Numeric value that represents the importance of this metric relative to other metrics in the same category. By default, the weight is 10. This field is visible and required unless the <strong>Data type</strong> is <strong>Date</strong>, <strong>Date/Time</strong>, or <strong>String</strong>. These data types are not included in results calculations.</td>
</tr>
<tr>
<td>Order</td>
<td>[Required] Numeric value that determines the order of the metric question on assessment questionnaires, relative to other metric questions in the same category. The metric with the smallest order value appears as the first question in the category section. By default, the order is 100. <strong>Note:</strong> It does not matter which order value you use for metrics with the Script method, as they do not appear on questionnaires.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box that determines whether this metric is used. If the check box is not selected, it is as if the metric record does not exist.</td>
</tr>
<tr>
<td>Mandatory</td>
<td>Check box that makes the metric question mandatory (selected) or optional (cleared) on assessment questionnaires. Users cannot submit questionnaires until they provide valid responses to all mandatory questions, which are denoted by a red field status indicator. This field is visible only if the <strong>Depends on</strong> field is empty, and the data type is not <strong>Checkbox</strong>.</td>
</tr>
</tbody>
</table>

6. Click the **General** tab and fill in the fields, as appropriate.
General tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Question</td>
<td>Text to use as the question on security incident review questionnaires. Enter a clear, straightforward question that is easy to answer, such as <strong>How did we contain the incident</strong>.</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the metric and what it evaluates. If the <strong>Method</strong> is <strong>Assessment</strong>, include details that help users understand how to answer the question. This text appears as a hint when a user points to the question text on the questionnaire.</td>
</tr>
</tbody>
</table>
| Depends on and Displayed when      | Select a question in the **Depends on** field that the current question depends on. For example, the question, "What additional logs were needed?" depends on the question "Were all needed logs available?"

Next, use the **Displayed when** field to identify when you want the dependent question to appear in questionnaires. For example, if you want the dependent question to be asked only when the user answers **No** to the "Were all needed logs available?" question, select **No** in the **Displayed when** field.

**Note:** The system prevents the creation of recursive dependencies between metrics. For example, if Metric A depends on Metric B, Metric B cannot depend on Metric A.

7. Click the **Field Type** tab and fill in the fields, as appropriate.

Field Type tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Data type | The data type of the expected response the list of types available depends on for the selected method. If the method is **Assessment**, the data type determines how users answer the corresponding question on questionnaires. If the method is **Script**, the data type determines how the system calculates assessment results.

**Note:** If another metric depends on this metric, you cannot change the data type.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Randomize answers</td>
<td>Check box that determines whether to present the answer options for this metric question in a random order each time a user opens an assessment questionnaire that contains the question. Answer preference can be influenced by the order in which answer options appear. This can result in biased results. Randomizing answer options can help prevent this bias. This field is visible only if you select <strong>Likert scale</strong> or <strong>Choice</strong> in the <strong>Data type</strong> field.</td>
</tr>
<tr>
<td>Dependent plugin</td>
<td>[Required if the <strong>Method</strong> is <strong>Script</strong>.] Plugin that contains the tables queried in the script. The system executes the metric script only if the plugin is active. The default available values are <strong>Asset Management</strong>, <strong>CMDB</strong>, <strong>Core</strong>, <strong>Cost Management</strong>, <strong>Procurement</strong>, and <strong>Software Asset Management</strong>. This field is visible only if the <strong>Method</strong> is <strong>Script</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the Core default value is used, the script is always run.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you are an administrator, you can add more choices of plugins to the field.</td>
</tr>
<tr>
<td>Scale definition</td>
<td>Setting that determines whether lesser or greater numerical values equate to a good score in assessment result calculations. Select <strong>Low</strong> if lesser numerical values are better, such as for a metric that measures the number of defects for a vendor. Select <strong>High</strong> if greater numerical values are better, such as for a metric that measures user satisfaction on a scale of one to five. The default value is <strong>High</strong>. This field is visible and required unless the <strong>Data type</strong> is <strong>Date</strong>, <strong>Date/Time</strong>, or <strong>String</strong>. The results for these data types are not included in results calculations.</td>
</tr>
<tr>
<td>Min</td>
<td>Lowest numerical value to be used as an answer option on assessments or as a scaled value in a scripted metric. This field is visible and required only if certain data types are selected. If the data type is <strong>Choice</strong> or <strong>Likert Scale</strong>, this...</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Field</td>
<td>field is read-only and is set automatically based on the smallest metric definition <strong>Value</strong>.</td>
</tr>
<tr>
<td>Max</td>
<td>Highest numerical value to be used as an answer option or scaled value. This field is visible and required only if certain data types are selected. If the data type is <strong>Choice</strong> or <strong>Likert Scale</strong>, this field is read-only and is set automatically based on the largest metric definition <strong>Value</strong>.</td>
</tr>
<tr>
<td>Script</td>
<td>Script that obtains the desired system information. The script has one input variable, set with the ID of the security incident (primary), and three possible output variables set by the script, string_result, scaled_result, and actual_result. When the data type is String, only the string_result is required. This field is visible and required when the <strong>Method</strong> is <strong>Script</strong>, or the default value comes from a script.</td>
</tr>
<tr>
<td>Template</td>
<td>A predefined set of common answers to use for the question. For example, a frequency template would likely start with a value of &quot;Never,&quot; and go up to the top value of &quot;Always.&quot; This field is visible and required only if the <strong>Data type</strong> is <strong>Template</strong>.</td>
</tr>
</tbody>
</table>

**Note:** If another metric depends on this metric, you cannot change the template.

8. **Optional:** When you have completed your entries, click **Update**.

**Create post incident review assignment rules**

In addition to manually adding users post incident review assessment list for a security incident, you can define assignment rules for automatically adding users to the list.

**Before you begin**
Role required: n_si.admin, sn_si.manager, sn_si.analyst
Procedure

1. Navigate to Security Incident > Administration > Post Incident Review Assignment.
2. Click New.

3. Fill in the fields, as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of this assignment rule.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to make the rule active.</td>
</tr>
<tr>
<td>Order</td>
<td>Enter a numerical value to specify where in the list of assignment rules this rule should appear. Lower numbers appear at the top of the list.</td>
</tr>
</tbody>
</table>

**Note:** Only the first matching assignment rule is executed, and only the users defined in that rule are added to the assessment list.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Use the condition builder to define the conditions that must be met in the security incident for this rule to be executed. For more information, see the example below.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign to users</td>
<td>Click the lock icon to add users to the review list. After the field is unlocked, options are available for adding or removing multiple users, roles, or entering user email addresses.</td>
</tr>
</tbody>
</table>

4. Click Submit.

**Example: Malicious code activity**

In the post incident review assignment rule shown here, when a security incident with the Category field set to Malicious code activity transitions to the Review state, the three users identified (who happen to be experts in dealing with
malicious code activity) are added to the list of users who will receive the post incident review questionnaire for this security incident.

Post incident review report

The post incident review reports feature allows you to set up and download the post incident review reports using the Post Incident Review tab.

The security admin can create and configure the report templates and map those templates to the security incident using the report configuration. A security analyst can then view or download the report after the security incident is resolved and the status is updated to Review state.

A PDF report is generated and attached to the security incident when the incident is moved to the Closed state after successful configuration.

Note:

1. The reports feature is applicable and supported from Orlando Patch9.
2. To opt to the previous implementation, click here to refer to the implementation procedure.

To customize your post incident review reports, you must do the following configuration.

1. **Report Templates**: Customize and configure the following report template features to add additional information on the report:
   a. Timeline
   b. Branding
   c. Template Scripts

2. **Report Configuration**

This section describes the configuration procedure:
Report Templates

Use the Report Templates section to create primary and additional report templates that are applied to the security incidents to generate the Post Incident Review report. You can format and configure the report based on your requirements. The templates also help you to include the assessment details in the template.

Following are a few optional steps that can be performed while building the template:

1. Configuring the branding information.
2. Setting up the page size and page margin.
3. Adding any security incident related fields (both custom and standard).
4. Using the following predefined custom tokens:
   a. $sessionUser: returns the logged in username
   b. $date: returns the current date
   c. $if_not_null_start and $if_not_null_end: these tags are used against any fields then the tags are displayed only if the value exists. For example:

      ```
      ${if_not_null_start:problem}
      Problem Category: ${problem.category}
      ${if_not_null_end:problem}
      ```

5. Including the related list data using the Template Scripts.

6. Including the timeline information using the Timeline Filters.

7. Managing and formatting the template content such as attachments, tables, and images.

**Note:** The enhanced report template tool bar features are available only from the Paris release version.

Report templates key points:

1. The images attached to the report template are displayed on the Post Incident Review report only when they are included in the sys_attachment table.

   **Note:** Images selected from the db_image table will not be displayed on the post incident review report.

2. Videos are not supported in the post incident review report.

3. The URL's in the PDF are non-clickable. To enable the URLs non-clickable (.) is denoted as (dot).
4. The report is not generated if the size of the report template exceeds 50MB.

5. The font family selected for the report template content will not be applied to the PDF if it is not supported by the PDF generator.

   Note: If the corresponding font is not there, PDF generator will identify the alternative closest font and then generate the PDF.

6. If you provide higher page margin values, generate post incident review report is failed. For example, Top and Bottom margin > 450\# and Left and Right margin > 450.

7. If a large text is included in the report template without spaces then the text may be truncated. Preview the text and modify it accordingly.

The security admin can preview the report using the Preview Report button available on the Report Template page.
Note:

Select a Security incident to preview a report with this template option and click Preview Report.

Branding

You can add the branding template name, header# and footer image, header and footer text, generate page numbers, and include the branding record in the report template after it is created.

Following is a sample# branding report format:

Report template branding key points:

1. The maximum size allowed for the header and footer image is 5MB. If the size exceeds more than the specified limit then an error message, ‘Image format cannot be recognized' is displayed in the security incident.

2. The footer text length is limited to 100 characters.
a. If the footer image text and report content is overlapped while previewing, you must make changes to the branding record.

b. If the footer text contains URL link, then it may overlap on to the footer image. Preview and correct it as required.

Timeline

Timeline configuration allows you to create and modify the timeline filters as required. You can filter the activity types that should be included in the report, configure if the child tasks should be included or excluded in the report, and configure if the images should be included or excluded in the report.

If you want to utilize and populate any timeline configuration then you must add the tag as mentioned below:

- ${timeline:timeline name}

Two sample timeline configurations as an example are provided in the set up that are used in the Phishing Report template and Default Report template. You can modify and reuse the configurations.

Template Scripts

Use the template scripts to include the related lists data, date and time stamp, and any other data that are not directly dot-walkable. Following is an example:

Construct a template script to display the related list on report template:
1. To prepare the related list data, call `PostIncidentReportUtils.fetchRelatedListDataForReport` method.

2. To represent the step 1 data in the table format and style, call `ReportTemplateUtil.constructTable` function method.

If you want to utilize and populate any template script, then you must add the tag `template_script:script name` as mentioned below:

- `{{template_script:script name}}`

Following are a few sample template scripts provided to configure and modify your post incident reports:

<table>
<thead>
<tr>
<th>Script name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>formatted_current_date</code></td>
<td>Returns the current local date and time in the DDMMYYYY 00.00 AM or PM format. For example, 21 Jan 2021 3:51 PM PST.</td>
</tr>
<tr>
<td><code>si_affected_users</code></td>
<td>Returns the affected users from the related list in a tabular form.</td>
</tr>
<tr>
<td><code>si_assessments</code></td>
<td>Returns the post incident assessment results in a tabular form.</td>
</tr>
<tr>
<td><code>si_associated_phish_emails</code></td>
<td>Returns the associated phishing emails from the related list in a tabular form.</td>
</tr>
<tr>
<td><code>si_associated_phish_headers</code></td>
<td>Returns the associated phishing headers from the related list in a tabular form.</td>
</tr>
<tr>
<td><code>si_business_criticality</code></td>
<td>Returns color coded business criticality value.</td>
</tr>
<tr>
<td><code>si_malicious_observables</code></td>
<td>Returns the malicious observables from the related list in a tabular form.</td>
</tr>
<tr>
<td><code>si_observables</code></td>
<td>Returns the observables from the related list in a tabular form.</td>
</tr>
<tr>
<td>Script name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------</td>
</tr>
<tr>
<td>si_priority</td>
<td>Returns color coded priority value.</td>
</tr>
<tr>
<td>si_response_tasks</td>
<td>Returns the response tasks from the related list in a tabular form.</td>
</tr>
<tr>
<td>si_time_to_identify</td>
<td>Returns the duration spent in Draft and Analysis state.</td>
</tr>
<tr>
<td>si_time_toResolve</td>
<td>Returns the time to resolve the incident.</td>
</tr>
</tbody>
</table>

Report template scripts key points:

1. If a related list is added with more than 5 columns, the table data is truncated during the PDF generation. Each column minimum width is set to 124px.

2. If a template script is unable to load the content in the report template due to technical issues, an error message is displayed on the report, ‘Error while evaluating the template script’ and the security admin must evaluate the correctness of the script to resolve the issue.

3. si_assessments: By default, all the assessment categories are added to report. The security admin can filter the data by modifying the template script as required. Add the below parameter to filter the data:

   • categories: sys_id1, sys_id2;

4. Time to resolve and time to identify scripts: Use the definition records that are part of the metric related list. If the definition records are unavailable for the security incident, then create or add those definition records to populate the values for the two fields.
**Note:**

OOTB, security admin doesn’t have access to view the version records of any table. You must add admin role to access the version records and revert to the previous version.

---

**Report Configuration**

Use the Report Configuration section to set up the conditions and apply the report templates to the Security Incidents. You can add one primary report and one or more additional report templates to the same condition.

Following is an example condition that is provided to apply the Phishing Report template to the Phishing category incidents and the other one to apply the Default Report template to all the security incidents. The Default Report template would be applied to the security incidents if the conditions are not met.
Procedure to turn off the new implementation

1. Deactivate the following business rules:
   a. Generate PIR PDF
   b. Create Knowledge On Closure New

2. Activate the following business rules:
   a. Generate PIR when in Review and Close
   b. Create Knowledge On Closure
   c. [Regen PIR on closure/cancel/delete]

3. Activate the following UI rule:
   a. Hide PIR field when empty

4. Go to form layout in the security incident form. Under Post Incident Review section:
   a. Remove PIR report picker from PIR section
   b. Add Post Incident Report field to PIR section

Manage Post Incident Review Report

Manage post incident review report includes the information that was configured and applied by the Security Admin, and the security analysts can modify the timeline filters at run-time and download it.

About this task
The Security Analyst can select either of the available primary or additional report templates, and configure the timeline filters, preview, and download the report. The Security Analyst can also directly download the report with the timeline configuration which was last applied.

The Security Analyst can access the reports using the Post Incident Review tab.

Procedure

1. Navigate to the security incident in the Review State.

2. Click Post Incident Review tab.
3. If the security incident is in the **Review** state:

   **Report Template:**

   - By default, the primary report template that was configured on the setup page will be applied to the security incident and will be available to download.

   - The analyst can choose other reports from the drop down list to configure and download the report.

4. **Configure/Preview:**

   A security analyst can preview and modify the report template configuration. In the current configuration, the security analyst can only modify the timeline filters.

   In case the configuration is modified for the primary report before the security incident is closed, the post incident review report which is attached to the security incident will be updated as per the modifications done by the security analyst. After closure, the analyst will be able to modify the configuration and download the report on the go. However, the attached report would follow the last configuration before closure.

   **To Configure/Preview the report:**

   a. Select the desired report template from the **Report Template** drop down list on the **Post Incident Review** tab.

   b. Click **Configure/Preview** tab.

   c. **Update** or configure the timeline filters as required.
d. Use the **Show Images** checkbox to either include or exclude the images from the timeline. If unchecked, then only the names of the images are included in the timeline section.

e. Use the **Show Child Tasks** check box to list all the child tasks associated with the security incident.

5. **Save** the configuration and click **Preview** tab to preview and download the report.

6. Click **Download** to directly download the report.

![Timeline Configuration](image)

**Close security incidents**

When a security incident has transitioned to the Review state, it is possible to close it and enter an appropriate closure code. Closure codes can be searched on later for ease of location.

**Before you begin**

Role required: sn_si.write

**About this task**

ℹ️ **Note:** In previous versions of Security Incident Response, users could close security incidents or requests as spam. In the Istanbul release, the spam option is no longer available. Spam security incidents or requests can be canceled or deleted, as appropriate.
Procedure

1. If the security incident you want to close is not already open, navigate to Security Incident > Incidents > Show All Incidents, and locate the security incident you want to close.

   Note: If there are any post incident review assessments that have not been completed for this security incident, the security incident cannot be closed. Return to Security Incident > Post Incident Review > All Incomplete Reviews, locate the reviews that are incomplete, and either ask the reviewers to complete their reviews or cancel the remaining assessments.

2. Click the Closure Information tab and fill in the fields, as appropriate.

   Security incident

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create knowledge article</td>
<td>Select this field to automatically create a draft knowledge base article that contains the contents of the post incident review.</td>
</tr>
<tr>
<td>Close code</td>
<td>Select the close code that best describes the reason you are closing this security incident.</td>
</tr>
<tr>
<td></td>
<td>• Investigation completed</td>
</tr>
<tr>
<td></td>
<td>• Threat mitigated</td>
</tr>
<tr>
<td></td>
<td>• Patched vulnerability</td>
</tr>
<tr>
<td></td>
<td>• Invalid vulnerability</td>
</tr>
<tr>
<td></td>
<td>• Not resolved</td>
</tr>
<tr>
<td></td>
<td>• False positive</td>
</tr>
<tr>
<td>Closed by</td>
<td>Displays the user who closed the security incident after the record is updated.</td>
</tr>
<tr>
<td>Closed</td>
<td>Displays the date and time of closure after the record is updated.</td>
</tr>
<tr>
<td>Close notes</td>
<td>Enter any additional notes that describe the outcome of closing this security incident.</td>
</tr>
</tbody>
</table>

3. Click Update.
4. The assigned user can manually change the State to Closed. When a parent incident is closed, all response tasks belonging to the child incident are canceled. If there are no other types of tasks, the child incident is also closed.

Add closure information to a security incident
When a security incident is in the Review or Closed state, you can enter closure information.

Before you begin
Role required: sn_si.basic

Procedure
1. If it is not already open, open the security incident you want to update.
2. Click the Related Records tab.
3. Fill in the fields, as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create knowledge article</td>
<td>Select this check box to generate a knowledge article using the contents of the post incident report.</td>
</tr>
<tr>
<td>Close code</td>
<td>Select the close code that best describes the reason for closing the security incident.</td>
</tr>
<tr>
<td>Closed by</td>
<td>[Read only] Displays the user who closed the security incident.</td>
</tr>
<tr>
<td>Closed</td>
<td>[Read only] Displays the date and time the security incident was closed.</td>
</tr>
<tr>
<td>Close notes</td>
<td>How the security incident has been closed, including lessons learned, resolution, and so on.</td>
</tr>
</tbody>
</table>

4. Click any of the following tabs to further update the security incident:
   - Incident Details
   - Post Incident Review

5. When you have completed your entries, click Submit.
Manage security threats using the Security Analyst Workspace

Security Incident Response includes a new user interface called the Security Analyst Workspace that features powerful tools for assisting in analysis, including the playbook, peek view, and tabs for working on multiple security incidents.

Purpose-built for security analysts, the powerful tools in the Security Analyst Workspace allow you to analyze the ever-growing volume of data associated with security incidents. And automated actions significantly reduce the security incident investigation time, which can be the difference between stopping an attack and suffering a breach.

Before using the Security Analyst Workspace

Before you can begin using the Security Analyst Workspace, you must ensure that your instance has at least London Patch 3 installed, you have the correct roles defined, and have downloaded the Security Incident Response UI application from the ServiceNow Store.

Note: If your instance is running a version earlier than London Patch 3, you must request the Security Incident Response UI plugin through the HI Customer Service system.

Access the Security Analyst Workspace

To access this new workspace, navigate to Security Incident > Incidents (New UI).

The workspace opens in a separate browser tab.
Locate the security incidents you want to analyze with Quick Filters

The Security Analyst Workspace provides several tools for filtering the list of security incidents so you can quickly find the security incidents you want to analyze. The Quick Filters let you select a subset of the security incidents based on criteria in the filter.

Simply click the quick filter you want to use.

Note: You can click an Edit button to identify which quick filters you want displayed on the list screen. A minimum of one filter must be selected, up to a maximum of six.

You can define additional quick filters, as well as primary filters for the Security Analyst Workspace, using the Classic UI. For more information, see Set up primary and secondary filters for Security Analyst Workspace.

Personalize the security incident list

As with all lists in your instance, the Security Analyst Workspace provides tools for personalizing the list and sorting the information displayed to meet your analysis needs.
Save time with Peek view

Before opening a security incident record, you can save time using the Peek view. This feature allows you to quickly locate vital security artifacts without having to reload the entire page. Simply click the > icon to the left of a security incident number to take a peek.

The peek view provides a snapshot of vital information in a single view. This view can save valuable time when you are working with multiple incidents. You can click the down arrows on certain fields to make on-the-fly updates, such as assigning an assignment group or a specific analyst.
Perform quick actions on a security incident
After you have selected and opened a specific security incident, you can perform time-saving actions on the record.

- If your security incident is open, click the **Edit Record** icon to make quick changes to any of its fields. If the record is closed, you can change only its tag.

- Click **Manage Attachments** to attach files to the security incident. You can also download or remove attached files and edit the encryption applied to the attachments.

- Click **Compose Email** to send a quick email to a colleague. Emails can be free-form, or you can send canned emails selected from a list of templates. Emails sent and replies received are captured in the Incident Timeline.

**Note:** You can create custom templates that contain reusable content for emails and email notifications. Variables can be used for inserting information specific to the security incident or alert, such as the subject line, priority, or threat category. Use the Security Incident [sn_si_incident] table for emails and email notifications related to Security Incident Response. For more information, see **Email templates**

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Click **More** to view a quick snapshot of the security incident, such as the description, business impact, and priority. You can also click the down-arrow in the **Assignment group** and **Assigned to** fields to make on-the-fly changes to those fields.

Work with multiple security incidents
The tabbed interface allows you to keep several security incidents open simultaneously so you can switch between them with a single click. This can save time and allow you to see the big picture when threats from multiple sources are identified.

View analysis information in the security incident tabs
When you open a security incident record, three tabs are shown:

- **Overview**
- **Explore**
- **Incident Timeline**

**Overview tab**
Use the **Overview** tab to view information in a security incident in a single location. No need to open another application or console.
The tiles that are displayed on the **Overview** tab are customizable. You can collapse and expand them as needed, and you can move them around by dragging the **Grip** icon. Click the **More options** icon to delete a tile or change its heading text.
**Explore tab**

Configure the tiles displayed on the **Overview** tab using the **Explore** tab. Simply select the tiles you want to view from the left-hand pane, and click the **Pin** icon. Pinned tiles automatically appear in the **Overview** tab.

The left-hand pane of the **Explore** tab includes a wide variety of information that you can display on the **Overview** tab. For example, expand **Observables** to display these related lists.

- Observables
- Threat Lookup Results
- Security Scan Results
- Domain Lookups
- Observable Enrichment

Additional related lists are available under **Users**, **Configuration Items**, and **Incidents**.

**Incident Timeline tab**

Use the **Incident Timeline** tab during your investigation for tracking purposes. Every time an action is performed on a security incident, the system records it in the Incident Timeline.

- You can also manually add worknotes to the timeline by typing them in the **Add work notes** box and clicking **Post**.
- You can search for a specific timeline activity using the Search box.
• The **Filter Activity** icon allows you to display only the types of timeline activity you want to see (for example, only incidents created by a specific analyst).

• You can add or remove the Incident Timeline from the **Overview** tab using the **Pin/Unpin** icon.

![Incident Timeline](image)

**Handle security incidents using the Playbook**

Resolve certain types of security threats in a step-by-step manner using the built-in Security Analyst Playbooks. For example, an analyst can use the playbook to resolve phishing attacks and threats caused by malicious code activities. For more information, see Resolve security threats with the playbook.

**Resolve security threats with the playbook**

Use the Playbook to resolve certain types of security threats in a step-by-step manner. For example, you can resolve phishing attacks and threats caused by malicious code activity using playbooks.

**Before you begin**

Role required: sn_si.admin or admin

**About this task**

Each group of tasks (Analysis, Contain, and so forth) leads you through a series of questions and other activities for resolving the threat.
As you work through each task, enter work notes to help analyze similar attacks in the future. After a threat is identified, you can also use information in the playbook to quarantine the threat, isolate similarly affected assets, and remove malware.

Knowledge articles, included in each task, provide tips and other information to help you perform the needed steps.
The base system includes knowledge articles for each of the playbook tasks. You can, however, write your own knowledge articles and associate them to playbook tasks.

**Note:** For an example of how to use the playbook to analyze and resolve a specific threat, see Resolving user-reported phishing attacks with the playbook.

**Procedure**

1. Navigate to **Security Incident > Incidents (New UI).**

   The Security Incidents screen shows security incidents that have been assigned to you.

2. You can click the **Assigned to me** choice list to select a different filter, such as all open incidents or all unassigned incidents. Or you can click one of the Quick Filters to view security incidents of a particular type, such as only Critical incidents.

3. Click the security incident you want to analyze.

   Consider prioritizing security incidents with high risk scores.

4. If the playbook pane on the right-hand edge of the screen is closed, click the playbook icon (📖) to open it.

   If no playbook is assigned to the security incident, you can select a playbook from the Selected Playbook choice list as shown below:
You can also assign a different playbook to the security incident. To include a playbook in the Selected Playbook choice list or to change the playbook for a security incident, see Enable playbooks for analyst selection for details.

The playbook specific to the type of security threat opens. It is divided into categories of similar tasks. For example, you use the tasks in the Analysis group to determine the validity and scope of the threat. The Contain group includes tasks for isolating the threat to a specific user or asset. The tasks in the Eradicate group guide you through the process of removing the malware or reimaging the host.

5. Click the first group (Analysis), and then click the first task in the playbook.

6. Follow the prompts in the task.
   • Some tasks ask a question, such as "Is Email Part of Campaign?" Perform the necessary analysis to answer the question, and select Yes or No.
   • If you have defined knowledge articles and associated them with playbook tasks, the articles appear when you start work on a task.
   • Some tasks are transitional. They simply instruct you to perform an action, such as adding observables to a security incident. After you complete the action, click Mark as Completed.

As you complete tasks, subsequent tasks are presented to you based on the choices you make. Grayed out groups (such as Recover, Review, and so forth) may be activated by your choices.

7. Continue working on each task presented to you until you have completed all tasks to resolve the threat and close the security incident.

Related information

Add a custom task to the playbook
Resolving user-reported phishing attacks with the playbook

The Phishing playbook guides you through the tasks necessary for analyzing and resolving a phishing attack reported by one of your company’s employees.

How security incidents are created from user-reported phishing attacks

During Security Incident Response setup, your system administrator creates a series of email matching rules that can identify emails that contain signs of a phishing attack. When employees receive a suspicious email that contains the common signs of a phishing attack (as defined by your security policies), they can send it as an .EML attachment to the phishing email address defined by your organization.

When the email is received at the phishing email address, the .EML attachment is parsed and its information is compared to the email matching rules. If a match is found, a security incident containing the following information is created:

• The short description includes User Reported Phishing, followed by the actual subject from the originating email.
• The .EML file is attached to the security incident.
• If the .EML contained any observables, they are parsed, and enrichment and threat lookups are automatically performed.
When a Phishing category security incident is opened, the Phishing Playbook is automatically available. Simply click the playbook icon (📖) to open the playbook.
The Phishing playbook contains tasks to help you analyze, contain, and eradicate a phishing threat. The tasks are organized into states (for example, Analysis, Contain, and so forth). When all tasks for a state have been completed, the playbook guides you to the next state.

Analyzing security incident details
When the security incident is in the Analysis state, you are given tasks to perform basic investigation of the incident, including:

- Determining the validity of the incident.
- Studying the impact of the potential threat.
- Coordinating an effective response to the incident.

As you work through the tasks:
• Familiarize yourself with the knowledge articles.
• Open the email attachment and examine it for signs of common phishing elements.
• Review threat lookup results.

**Controlling the security incident**

When the security incident is in the **Contain** state, you are given tasks to review the details of the email. To ensure that threats cannot enter your organization, update your network defenses, in the form of Intrusion Defense System (IDS) and Intrusion Prevention System (IPS) signatures and rules.

As you work through the tasks:
• Take actions to limit threat impacts, such as isolating the impacted devices.
• Examine the observables attached to the email.
• Determine whether any email contents are associated with a known threat, including:
  ◦ URL
  ◦ Email sender
  ◦ Phishing URL
  ◦ IP address of the sender's SMTP server

**Eradicating the malware**

After you deploy updated signatures and rules to your antivirus solution, use the tasks in the **Eradicate** state to determine if malware is present and handle it accordingly.

As you are work through the tasks:
• Scan the endpoints of affected devices for the presence of malware.
• Remove any malware found.
• As a last resort, wipe and reimage the host devices.

**Reviewing the security incident**

If you have determined that a phishing attack was a false alarm when performing the Analysis tasks, the security incident moves to the **Review** state and you need to notify your users so they know it is safe to open the email attachment.
Closing the security incident
When all tasks in the playbook have been completed, the security incident is moved to the **Closed** state. You must enter closing comments before the incident can be closed.

Cancelling a security incident
When a security incident is in the **Review** state, and you have successfully informed your users that the email is not a threat, the **Cancelled** state becomes active and you can cancel the security incident.

⚠ **Note:** The Recover task is not used in the Phishing playbook.

Associate a knowledge article with a playbook task
As you analyze security threats using the Security Incident Response playbook, you can view knowledge articles for each task if defined by your organization. If knowledge articles are not present, you can create them and associate them with playbook tasks.

Before you begin
As you use the playbook in Security Incident Response, take note of the text associated with each task. For example, the first task in the Phishing category is **Was Alert Employee-Submitted?** This is the short description of the task and you need this text (exactly as it appears in the playbook) to associate a knowledge article with the task.

Role required: sn_sir.knowledge_admin, and either sn_si.admin or admin

Procedure
1. Navigate to Security Incident > Catalog & Knowledge > Knowledge.
2. Create and publish a knowledge article for a specific playbook task.
4. Create a runbook, filling in the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge article</td>
<td>Select the published knowledge article you want to associate with the playbook task.</td>
</tr>
<tr>
<td>Table</td>
<td>Select Security Incident Response Task [sn_si_task].</td>
</tr>
<tr>
<td>Condition</td>
<td>Set the condition builder to:</td>
</tr>
</tbody>
</table>
5. Click **Submit**.
   The next time you run the playbook and select this task, the associated knowledge article is displayed.

**Related information**

- Create a security incident knowledge article
- Create a Security Incident Response runbook

**Add a custom task to the playbook**

The Security Analyst Workspace base system includes a series of tasks for each threat category. You can create custom tasks that meet the unique needs of your system or customers.

**Before you begin**

Role required: sn_si.basic or security_admin
Procedure

1. With the playbook open, click **Add Task**.

The Add Custom Task screen opens.
2. Fill in the fields, as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>[Read only] The automatically-generated security incident task number.</td>
</tr>
<tr>
<td>Parent</td>
<td>The number of the related security incident.</td>
</tr>
<tr>
<td>Configuration item</td>
<td>The configuration item affected by the security issue, if any.</td>
</tr>
<tr>
<td>Affected user</td>
<td>The user affected by the security issue, if any.</td>
</tr>
<tr>
<td>Priority</td>
<td>Select the priority used to determine when this task should be performed.</td>
</tr>
<tr>
<td>Security Incident State</td>
<td>The current state of the security response task. You can select a future state, if needed.</td>
</tr>
<tr>
<td>Outcome type</td>
<td>If you have the sn_si.basic role, select <strong>Yes/No</strong> as the outcome type.</td>
</tr>
<tr>
<td></td>
<td>If you have the security_admin role, you can create a custom outcome type with multiple custom output values. For example, you can define a task with dependant values based on the threat category. For more information, see Choice lists</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assignment group</td>
<td>The assignment group from which the assigned worker will be selected.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>The individual assigned to perform the task.</td>
</tr>
<tr>
<td>Short description</td>
<td>A description of the Security Incident playbook task.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the selected task.</td>
</tr>
</tbody>
</table>

3. When you have completed your entries, click **Add Task**. The task is inserted in the playbook following the current task.

**Sightings searches on user-reported phishing and malware attacks**

Perform sightings searches on emails or observables to determine how often certain types of attacks, such as phishing attacks or communications with a malicious IP or URL occur in your network. Each occurrence is considered a sighting. Sightings searches for observables must be configured for your log stores or security information and event management (SIEM).

The following terms are used to describe user-reported phishing attacks:

- **Phished user**: A user who has received a phishing email.
- **Victim user**: A user who has interacted with the phishing URL, typically by clicking a link in the phishing email. This action potentially exposes credentials to the attacker.

As you start analyzing a phishing incident, you can perform **email sightings search** or **observable sightings search** to identify other users in your organization who are impacted by the same phishing attack. Search your log stores to identify phished and victim users. After you have identified the list of affected users, create child security incidents to perform comprehensive incident response procedures using the tools available in Security Incident Response.
Note: You can also use the following approach to perform a sightings search:

- Navigate to Security Incidents > Show All Incidents and click on a security incident.
- Click Show IoC under Related Links. A list of observables is displayed.
- Select an observable from the list and from the Actions list, select either of the following options:
  - Run Web Traffic Sightings Search
  - Run Email Traffic Sightings Search
- Specify the time frame and click Search to perform a sightings search.

Watch this three-minute video to learn how to use the sighting search feature to locate phished users, and track phishing and malware observables within the log store on your network. How to use the sighting search feature to locate phished users, and track phishing and malware observables within the log store on your network.

Saved sighting search configurations
Configure sighting searches and create saved configurations for SIEMs or other log stores for instances of observables to determine the presence of malicious observables in your environment.

Note: Saved Searches and Inplace queries are supported for Splunk Integration only.

Related information
Create sightings search configuration records

Perform an email sightings search for user-reported phishing attacks
Search for users who have received phishing emails based on observables such as email subject, sender name, or message ID. You can then contain and eradicate these phishing emails from your organization.

Before you begin
Role required: sn_si.analyst

About this task
Search the Splunk email traffic logs to gather the list of recipients of a suspicious email. The search can be performed using the email sender, email message ID, or the email subject associated in a security incident as the criteria.
Note:

- This implementation of sightings search for email-based observables has been tested only with the Splunk Enterprise log store.
- The Splunk log events must be Common Information Model (CIM) compliant for the sightings search query to return accurate results.

Procedure

1. To see the security incidents assigned to your team, navigate to Security Incident > Incidents (New UI).

2. From the Security Incidents list, select one of the filters, such as all open incidents, all incidents assigned to you, or all incidents.

   To view security incidents of a particular type, such as critical incidents or phishing emails, click one of the Quick Filters.

3. Click the security incident that you want to analyze.

   The Overview tab provides an overview of the security incident including a list of observables, affected users, and similar security incidents.
4. Click the **Explore** tab.

5. Under **Incident Data**, navigate to **Investigation > Search Email & Observables**.

6. Expand the Search Criteria section.

7. Select **Email Search** as the type of search that you want to run, and specify the rest of the search criteria.
Search criteria form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrations</td>
<td>Integrations type. Select <strong>Log Store</strong> from the list.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This feature is supported only with the Splunk log store.</td>
</tr>
<tr>
<td>From</td>
<td>Full email address of the sender (for example, <a href="mailto:jane.doe@example.com">jane.doe@example.com</a>).</td>
</tr>
<tr>
<td>Message ID</td>
<td>Email message ID from the log store.</td>
</tr>
<tr>
<td>Subject</td>
<td>Subject for the phishing email.</td>
</tr>
<tr>
<td>Search Window</td>
<td>Time window for the search (for example, the last 24 hours).</td>
</tr>
</tbody>
</table>

8. From the **Select Action** list, select **Search** and then click **Run**.

The Splunk log store is searched using the criteria that you enter, and the users targeted by the phishing attack are shown on the **Email Search Results** tab. The total number of phishing emails and the details of each email, including the email date received, recipient, and message ID, are displayed.

9. To view the list of users who received the phishing email, click the > symbol in the Search Date column.
10. To view a list of users who received the email, navigate to Users > Affected Users.

The Phished User column identifies the email recipients.

Note: The Affected Users page shows only the user records that are present on the ServiceNow instance.

11. To further investigate the users who are targets of the phishing attack, follow these steps:

a. Select the check boxes next to the user names.

b. From the list, select Create Child Security Incident, and click Run.

A message is displayed to show that a child security incident has been created. To view the child security incidents associated with a parent incident, click the Explore tab and navigate to Incidents > Child Security Incidents.

Results

The list of phished users is displayed.
Perform an observable sightings search for user-reported phishing and malware attacks

Perform sightings searches on observables to find out how many users have visited a malicious or suspicious website within a specific period.

Before you begin
Role required: sn_si.analyst

About this task
You can perform a network traffic search on observables such as the URL, destination host, or the destination IP address associated with a security incident.

Note:
- This implementation of sightings search for observables has been tested only with the Splunk Enterprise log store.
- The Splunk log events must be Common Information Model (CIM) compliant for the sightings search query to return accurate results.

Procedure
1. To see the security incidents that are assigned to your team, navigate to Security Incident > Incidents (New UI).
2. From the Security Incidents list, select a different filter, such as all Incidents Assigned to Me, All Open Incidents, or All Incidents.
   To view security incidents of a particular type, such as critical incidents or phishing emails, click one of the Quick Filters.

3. Click the security incident that you want to analyze.
You can see an overview of the security incident including a list of observables, affected users, and similar security incidents.

In the Observables section, notice that the Observable column shows the email address, subject, and URL. Notice also that the Finding column shows that the URL was automatically scanned when the phishing email was submitted and determined to be a known malicious URL. The Incident Count column shows the other incidents that share the same observable. These artifacts indicate that you are likely ready to move on to containment procedures for this phishing attack, including determining how many users in the organization have been affected.

4. Navigate to **Explore > Investigation > Search Email & Observables**.
5. Expand the Search Criteria section and click **Observable Search**.
6. Enter the observable that you are searching for, and a time window for the search (for example, Last 24 Hours).

7. From the Select Action list, select Search.
   The Splunk log store is searched using the criteria that you entered and the key users targeted by the malicious attack are shown on the Observable Search Results tab.

8. To view the users who received the email, navigate to Users > Affected Users.
   The Phished User column identifies the recipients of the phishing email and the User Interaction column identifies users who clicked a phishing URL or interacted with a suspicious email address. The User Interaction column is set to true or false, depending on whether the user clicked the malicious link or IP.

   **Note:** The Affected Users page shows only the user records that are present on the ServiceNow instance.
9. To further investigate the users who clicked the phishing email and potentially compromised their credentials:

a. In both the Phished User and User Interaction columns, select the check boxes next to the user names that show true.

b. Click Create Child Security Incident and then click Run. A message is displayed to show that a child security incident has been created. To view the child security incidents associated with a parent incident, click the Explore tab and navigate to Incidents > Child Security Incidents.

Results
The list of phished users is displayed.

Create sightings search configuration records
Create multiple sightings search configuration records and use them while querying multiple log stores or varying the search parameters.

Before you begin
• The CIM add-on must be installed on the Splunk instance
• Saved Searches and Inplace queries are supported for Splunk Integration only.
• Role required: sn_si.admin

About this task
You can also create sightings search configuration records to invoke saved searches on the Splunk enterprise log store.

Note: The search configuration queries rely on Splunk log data to be Splunk Common Information Model (CIM) compliant.

With saved search configurations, you can:
• Create custom searches that combine multiple event records.
• Design-efficient and effective searches.
• Use parameterized inputs in the Splunk saved search.

The base system includes the sample configurations as shown in this image:
The saved search and inplace configuration queries are example queries and can be substituted with appropriate parameters for your environment. Create additional saved search configurations as required. When you define a saved search configuration, the name and the parameters in the search query must match the saved configuration defined on your Splunk instance. If the name and parameters are not the same, you may not see accurate results when you perform a sightings search.

**Note:** On your Splunk instance, navigate to the Searches, Reports, and Alerts page and locate your saved search query. Click the Permissions link to navigate to the Permissions page. Select the All Apps radio button and enable the Read Permission option for Everyone. This will change the Sharing column value from Private to App for your saved search query. If this is not set, saved search query may not return any results.

To verify if the saved search configuration matches the configuration defined on your Splunk instance:

1. Navigate to **Settings > Searches, Reports, and Alerts**.
2. Change **App Context** to **All**.
   - A list of search reports is displayed.
3. Confirm that the saved search query is present in the list.

For example, the Sightings Search Configuration form contains the email address and email sender as search parameters:
In your Splunk instance, define the saved search with the same name, Default Saved Search - Emails, and the same search parameters for the email address and email subject. If the name and search parameters are not the same, sightings search does not generate accurate result.

**Procedure**

1. Navigate to **Security Operations > Integrations > Sightings Search Configuration** and create a new record (see table for field descriptions).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the configuration.</td>
</tr>
<tr>
<td>Is saved search</td>
<td>Saved search configuration is created if you select this option.</td>
</tr>
<tr>
<td>Sightings search source</td>
<td>The source for the sightings search. Select the Splunk log store as the source.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Option for the saved search status. Only active search configurations can be used to perform a sightings search.</td>
</tr>
<tr>
<td>Observable type</td>
<td>Observable type can be any observable type such as IP, hash value, URL, domain name, and so on.</td>
</tr>
<tr>
<td>Maximum observables per search</td>
<td>Maximum number of observables to be returned from the search.</td>
</tr>
<tr>
<td>Search</td>
<td>The default search string is $(observable), but you can define your own search query by specifying parameters that are supported by the Splunk log store.</td>
</tr>
</tbody>
</table>

2. Click **Submit**.

**Results**
You have created a sightings search configuration record.

**What to do next**
After defining the search query, click **Generate Sightings Search Test Query**, and specify a list of observable values to generate a test query based on this saved search configuration.

### Playbook Resources

Security Incident Response provides a rich set of playbook resources that include a comprehensive library of playbooks, subflows, and actions. You can create or configure playbooks quickly and easily without writing complicated code. You can use these playbooks to resolve security threats (see **Resolve security threats with the playbook** for details) in a step-by-step manner.

Playbook resources include the following:

<table>
<thead>
<tr>
<th>Security Incident Response Playbooks</th>
<th>Action Library</th>
</tr>
</thead>
<tbody>
<tr>
<td>The playbooks provided with the base system are designed to accelerate the security incident investigation process by automating complex and mundane tasks.</td>
<td>Complex actions that are critical for building playbooks are available as <strong>Action Libraries</strong>. These Action Libraries enable security administrators to create playbooks without writing any complicated code. See <strong>Action Library</strong>.</td>
</tr>
<tr>
<td>Playbooks are highly configurable and are built using ServiceNow’s Flow</td>
<td></td>
</tr>
</tbody>
</table>
Activate a Security Incident Response flow

Security administrators and flow designers can use the Security Incident Response flows to automate the process of resolving security incidents in the organization.

Before you begin
Role required: sn_si.admin, action_designer, and flow_designer

About this task
The flows provided with the base system are in an inactive state. Activate these flows before you use them.

Procedure

1. Download and install the Security Operations Spoke application. This Spoke application provides security operations actions that you can use while defining Security Incident Response flows.


Notice that the flows have a published status and are inactive.
3. For example, click the **Security Incident - Automated Phishing Playbook - Template V1** link to view the flow.

Note: You cannot edit the flows provided with the base system as they are read-only flows. You can use these flows as they are or make a copy and modify them as required.

4. Click **Activate** to activate the flow.

**Results**
The Automated Phishing Playbook flow is active and ready to use.

**Security Incident Response Playbooks**
Using the Flow Designer, security administrators and flow design authors can more easily transition from manual or undocumented playbooks to automated and repeatable playbooks. The drag-and-drop feature provides flexibility in moving objects, condition checks, parallel branching, decision tables, and more.

Security Incident Response flows included with the base system are:
- Automated Phishing playbook
- Malware playbook
• Failed Login Manual playbook
• Child Security Incident Automation playbook

Activate these flows before you use them. See Activate a Security Incident Response flow for details.

Automated Phishing playbook

The Automated Phishing playbook helps you resolve certain types of security threats in a step-by-step manner. With the flow designer templates, you can automate the steps in the phishing response playbook and resolve incidents quickly and efficiently.

You can use templates authored with flow designer to automate the tasks in the Phishing Response Playbook to analyze and resolve phishing attacks in your organization.

The phishing response playbook includes the following flows and subflows:

• Security Incident - Automated Phishing Response Template: This template is designed to automate the phishing response tasks and contains a sequence of actions including a trigger.

• Security Incident - Phishing Manual Template: This template is the existing manual phishing response workflow. Set the category to Phishing to activate the flow.

These templates contain a sequence of reusable actions designed to respond to phishing attacks. Each flow has a trigger (condition), a sequence of actions and subflows that you can annotate for readability. To access these flows, you must install the Security Operations Spoke.

⚠️ Note: Activate these templates before you can use them. See Activate a Security Incident Response flow for details.

• Run Threat Lookups for Observables: Performs threat lookups of selected observables.

• Enrich Observables: Allows you to enrich observables with additional information from various sources.

• Assess Phishing Email Impact: Allows you to assess the impact of the phishing email. When you receive an email at the phishing email address, this subflow parses the .EML attachment and compares the information to the email matching rules.
• Eradicate Phishing Emails: Allows you to delete or eradicate phishing emails to help reduce exposure to a specific attack.
• Run Sighting Search on Observables: Determines the prevalence of a threat over time or test remediation or eradication efforts.
• Create Block Requests: Blocks communication with observables associated with the incident.

These subflows represent a set of reusable operations that you can use in multiple playbooks. You can use these subflows to define custom templates (flows) according to your requirements.

To create custom templates (flows), follow the instructions in Flows.

Run the automated phishing response playbook flow

Using the flow designer, you can define and automate tasks in the playbook to analyze and resolve phishing attacks against your organization.

Before you begin
• Role required: sn_si.admin, flow_designer, and action_designer
• Install and configure the following integrations with the right credentials:
  ◦ Block Request (Security Operations Palo Alto Networks NGFW Integration)
  ◦ Observable Enrichment
  ◦ Sighting search
  ◦ Threat Lookup
  ◦ Microsoft Office Exchange

About this task
When employees receive a suspicious email that contains the common signs of a phishing attack (as defined by your security policies), they can send it as an .EML attachment to the phishing email address defined by your organization. Using the tasks defined in the automated phishing playbook flow, you can triage, analyze, contain, and eradicate a phishing threat. These tasks can be invoked as part of different incident states (for example, Analysis, Contain, and so forth). When a phishing security incident is created, the automated phishing flow can be automatically triggered. Using flow designer, you can view the details of the various incident response actions as they are invoked.

Note: The Security Incident - Automated Phishing Response Template V1 playbook flow is Read Only. You can make a copy of the flow and make changes as required.
The following steps describe how to make a copy of the phishing playbook template and walks you through some of the tasks in the flow.

**Procedure**

1. Navigate to Flow Designer > Designer to view the flows available with the Security Operations Spoke.

2. Click the Security Incident - Automated Phishing Response Template VI link.

3. In the Flow page, click the more icon , make a copy of the flow and open it for your use. You can modify the trigger conditions, add or remove actions, and make other changes to the flow.

   ![Flow Diagram](image-url)

   This image shows the trigger conditions, and the steps that the flow executes. The right-hand panel shows the data flow. Click an icon to expand the step and view the details.

4. Click the Trigger icon. In the first step, you define or set the trigger for the flow. Specify the conditions for the trigger and how often you want the flow to execute the trigger.
When the conditions defined in the flow (Category is Phishing and Source is Email) are met in the incident record, the tasks in the automated phishing flow start executing sequentially. You can modify the trigger, add annotations, add or delete conditions, and so on.

5. Click the **Update Security Incident Record** link.

The **Update Security Incident Record** is the first step in the flow. Click the annotation icon to add a note to the security analyst indicating that a phishing incident has occurred, and the automated phishing playbook flow has begun executing.

6. Proceed with the step 2 in the flow. Click the **Create Response Task** link.

In this step, the flow creates an automated response task to acknowledge receipt to the submitter of the incident or the affected user.
Notice the Parent Task [Security Incident] field references the parent record associated with this step. You can pick any reference record by using the data pill picker icon or drag the relevant reference item from the right-hand panel. Notice the lock icon. The lock icon indicates that step does not require any user intervention.

7. In step 3, the flow collects additional details of the affected user (typically the user who submitted the incident) to ensure that it can send a notification successfully. You can specify conditions to check if the affected user's status is active and the user is able to receive notifications.

Notice the conditional step icon in step 3. The flow executes the next step (3.1) only if the specified conditions are met.
When the conditions defined in step 3 have been met successfully, the email is sent.

8. In step 4, after the email has been sent, the response task is marked as closed.

9. In step 5, all the observables involved in the incident (such as email subject, email address from which the phishing email was sent, phishing URL) or observables belonging a selected category (hash, file, or domain) are collected to perform additional automated actions in the subsequent playbook steps.
Click the action designer icon 📚 to see a detailed view of the action.
To view the Action Designer page, expand a step in the flow and click the action designer icon.

10. In step 6, an automated response task is created. This task captures the beginning of process of getting the reputation of all observables and performing enrichment with configured integrations.

11. In step 7, two subflows are called:
   - Run Threat Lookups for Observables: This subflow is used to get the reputation of all observables using threat look up implementations.
   - Enrich Observables: This subflow is used perform enrichment of observables with configured implementations.
Notice the icons for this task. The parallel operations icon 🔄 indicates that both the tasks will be performed in parallel and the subflow icon 🎯 indicates that the task being performed is a subflow as shown below:

Notice the number 5 in the observables field. This indicates that the threat lookup will be run on observables retrieved in step 5. This subflow in turn calls existing workflows and actions as shown in the Subflow Designer.

12. In step 8, after the subflows have been completed, the response task is marked as Closed.
13. In step 9, the Confirm Threat from Observable Triage subflow is called. This subflow is used to confirm the presence of a threat indicator in the incident. If the threat is confirmed, an 'IOC Detected' flag is added to the incident.

14. When the threat is confirmed, in step 10, you update the security incident and add a note indicating that threat containment tasks will be launched.

15. Step 11 is an automated response task that captures the start and completion of the task used to assess the impact of the phishing emails.

16. In step 12, the Assess Phishing Email Impact subflow is called. This subflow is used to search for users who have received the phishing email using supported implementations.
17. In step 13, the task is marked as closed to indicate that the Assess Phishing Email Impact subflow has been executed.

18. Step 14 is used to retrieve all observables that have been marked as malicious.

19. Step 15 is an automated response task that captures the start and completion of the sighting search of observables task.
20. In step 16, the Run Sightings Search on Observables subflow is called. This subflow performs a sightings search using the configured implementation.

![Run Sightings Search on Observables V1](image)

- **Subflow**: Run Sightings Search on Observables V1
- **end_date**: 
- **observables**: 14 observables
- **max_rows**: 
- **share_sighting_results**: 
- **Incident SysId**: Trigger Security Incident Record Sys ID
- **domainId**: Trigger Security Incident Record Domain
- **start_date**: 

21. In step 17, the task is marked as closed to indicate that the Run Sightings Search on Observables subflow has been completed.

![Update Security Incident Response Task Record](image)

- **Action**: Update Record
- **Record**: Security Incident Response Task
- **Table**: Security Incident Response Task [sn_si_task]
- **Fields**: State (Closed Complete)

22. After you have identified the malicious observables, in step 18, you update the security incident record to indicate that the containment actions will now commence.
23. Step 19 is an automated response task that captures the start and completion of the block requests task.

24. In step 20, the Create Block Requests subflow is called. This subflow is used to block malicious observables.

25. In step 21, the task is marked as closed to indicate that the Create Block Requests subflow has been completed.
26. In step 22, the Eradicate Phishing Emails subflow is called. This subflow is used to delete phishing emails from user mailboxes.

27. After the phishing emails have been deleted, in step 23, you update the security incident record to indicate that the incident status needs to be reviewed.
28. In the last step, the flow creates an automated response task. This task is used to send a reminder to the security analyst to save all the incident response actions for future reviews.

What to do next
You can click Test to simulate the actions in the flow before you publish it. After testing the flow, click Activate to activate the flow and execute it.

Click Executions to view the execution details of the flow.
View automated phishing response playbook flow action designer

You can drill down to the Action Designer to view detailed information about the actions being performed for a specific step in the automated phishing response playbook flow.

This page describes the Action Designer page for the Get Observables from Task step. Click a task in the Action Outline panel to view the details.

Action Input

This section shows details on how the action was created including the incident id, the type of observable (hash or IP) and observable finding (malicious emails only).

Get M2M Records

This section shows the conditions that have been defined to search for observables in a specified table.

Get Observables

This section shows the script used to retrieve observables based on the specified filter conditions. Finally, the observables meeting this criteria and the count is displayed.
Note: All actions defined in this flow are reusable and can be modified according to your requirements.

View the automated phishing response playbook subflow designer

You can drill down to the Subflow Designer to view detailed information about the subflow being executed as part of the automated phishing response playbook flow.

You can launch the Subflow Designer to view additional details of a subflow. The Subflow Designer page for the Run Threat Lookups for Observables subflow is shown here. Click the icon in the image below to view the Subflow Designer.
In the Subflow Designer page, you can see the inputs and outputs for this subflow, and the underlying workflow actions that are being executed.

**Note:** This subflow is read only and cannot be edited. You can add or delete subflows to the step but you cannot modify the subflow.

**Automated Malware playbook**

The Automated Malware playbook provides a sequence of automated steps that helps you resolve malware alerts quickly and efficiently.

Use the malware playbook flow to automate the steps involved in handling malware alerts from the endpoint or the network. The flow template includes trigger conditions, a sequence of actions and subflows that are annotated for readability.

These templates contain a sequence of reusable actions designed to respond to phishing attacks. Each flow has a trigger (condition), a sequence of actions and subflows that are annotated for readability. To access these flows, you must install the Security Operations Spoke and Security Operations Palo Alto Networks - WildFire app from the ServiceNow Store.

**Note:** You must activate these templates before you can use them.

The following flows and subflows are included:
• Security Incident - Automated Malware Playbook Template: This template is designed to automate the responses to malware alerts and contains a sequence of actions including a trigger.

• Security Incident - Malware Manual Template: This template is the existing manual malware response workflow that is activated when the category is set to Malicious Code Activity.

Subflows
• Confirm Threat from Observable: Verifies if the observables is malicious and needs to be addressed.
• Set Incident Severity: Sets a severity status for the incident.
• Ransomware Playbook: Determines whether it is a ransomware attack.

These subflows represent a set of reusable operations that can be used in multiple playbooks. You can use these subflows to define custom templates (flows) according to your requirements.

To create custom templates (flows), follow the instructions in Flows.

Run the automated malware playbook flow
Use this flow to automate tasks in the playbook to analyze and resolve malware attacks against your organization.

Before you begin
• Role required: sn_si.admin, flow_designer, and action_designer
• Install and configure the following integrations with the correct credentials:
  ◦ Palo Alto Networks WildFire for Security Operations
  ◦ Sighting Search (Splunk)
  ◦ Block Requests
  ◦ Threat Lookup
  ◦ Enrich Observables

Verify that these integrations are working properly before you activate the Security Incident - Automated Malware Playbook Template.

you will see an error "workflow on action number 15.4.1 not found" as shown below:

If you do not want to install this App, delete steps 15.2, 15.3, and 15.4 from the automated malware playbook flow.

- Ensure that the following conditions have been met:
  - The security incident has been assigned to a security analyst who belongs to the appropriate approval group.
  - The security analyst handling the incident must have a valid email address.
  - The necessary configuration items and observables have been added to the security incident.

- For step 21 (Ask for Approval), change the Group from Security Incident Assignment to your preferred group.

- Step 21 of the flow is a mandatory task approval step where an approval request is sent to the administrator. To approve the request, the administrator must navigate to the Task Approvals page and set the State field to Approved. If the task is not approved, the flow designer cannot proceed further and the process ends.

About this task
When a malicious code activity is detected in the network, a security incident is created and the automated malware playbook flow is launched. You can use the tasks defined in the automated malware playbook flow to triage, analyze, contain, and eradicate the threat.

Procedure
1. Navigate to Flow Designer > Designer to view the flows available with the Security Operations spoke.
2. Click the Security Incident - Automated Malware Playbook Template VI link.
3. In the Flow page, click the more icon, make a copy of the flow and open it for your use. You can now make changes to your flow, such as modifying trigger conditions or actions, or adding and removing actions.
This shows the trigger and the steps that will be executed with the flow. The right hand panel shows the data flow. Click on an icon to expand the step and view the details.

4. Click the **Trigger** icon. In the first step, you define or set the trigger for the flow. Specify the conditions for the trigger and task to be performed when the conditions are met.

When the condition defined in the flow (Category is Malicious Code activity) is met in the incident record, the tasks in the automated phishing flow start executing sequentially. You can modify the trigger, add annotations, add or delete conditions, and so on.

5. The first step in the flow is **Update Security Incident Record**.
Click the link and click the annotation icon to add a note to the security analyst indicating that there has been some malicious code activity, and the automated malware response playbook flow has begun executing.

6. Proceed with the step 2 in the flow. Click the **Create Task** link.

In this step, an automated response task is created to check if all the necessary observables have been captured and if the investigation can begin.

7. If the Outcome type is **No**, this indicates that no observables and CIs are available to initiate the investigation. Update the security incident record to indicate that the playbook cannot proceed further.

8. If the Outcome type is **Yes**, the Set Incident Severity subflow automatically assigns the correct severity to the security incident.

9. In the next step, the security incident record is updated.

10. In the next step, all observables involved in the incident or a selected category are collected to perform additional automated actions in the subsequent playbook steps.
11. In the next step, an automated response task is created. This task captures the beginning of process of getting the reputation of all observables and performing enrichment with configured integrations.

12. In step 8, two subflows are called:
   - Run Threat Lookups for Observables: This subflow is used to get the reputation of all observables using threat look up implementations.
   - Enrich Observables: This subflow is used perform enrichment of observables with configured implementations.

Notice the icons for this task. The parallel operations icon \( \parallel \) indicates that both the tasks will be performed in parallel and the subflow icon \( \circ \) indicates that the task being performed is a subflow as shown below:

Notice the number 5 in the observables field. This indicates that the threat lookup will be run on observables retrieved in step 5. This subflow in turn calls existing workflows and actions.

13. In the next step, the Run the Look Up Records action is executed. This action is used to look up workflow context records where the parent workflows can be one of the following.
• Threat Lookup Abstract Workflow Context
• Observable Enrichment Abstract Workflow Context

14. In the next step, the reputation and enrichment results are reviewed for every 8 records.

15. Continue reviewing the next steps:

a. Update Security Incident Record: Updates the security incident record to indicate that the reputation lookup and enrichment activities have been completed.

b. Get Observables from Task: Retrieves all the malicious observables associated with the security incident.

c. Create Task: Checks and confirms if the automated triage runs have been successful.

16. If there are observables that have been flagged as malicious:

a. Update Security Incident Record: Post a worknote indicating that a threat has been detected.

b. Create Input Query from Observables: If more than ten observables have been flagged as malicious, the Sighting Search on Observables subflow (on Splunk or Carbon Black) is executed.

17. If the observables are not flagged as malicious, the flow continues with the following steps:

a. Update Security Incident Record: Post a worknote indicating that no threat has been detected

b. Get Observables from Task: Identifies all SHA256 Hash Ids from the incident.

c. Look Up Observable Records: Looks up records that meet this criteria.

18. Continue reviewing the next steps:

a. For each malicious observable, the Security Operations Palo Alto Networks - Get Wildfire Data Enrichment workflow is executed.

b. Reviews the investigation results to see if they are satisfactory. A response task is created to check if the suspected malware is a ransomware attack. If yes, the Ransomware Playbook subflow is executed.

c. In the next step, an email is sent with a summary of the analysis and request for approval to initiate containment procedures.

d. A task is created to capture details of the approval requested.
e. The next step is to update the security incident record. Post a worknote informing the security analyst that the approval request has been made.

f. Requests approval to contain the malware attacks from your SOC manager.

i. **Note:** When an approval request will be generated by the flow, the Work note will be updated with the following message:

An Approval request has been made for <task id> proceeding with containment. To approve this task, as a SOC manager, follow these steps manually:

- Navigate to the Task Approvals page.
- You will see the list of approvals. Click the <task id> that is to be approved.
- Change State to Approve and Save the updated <task id>.

h. Next, a task is created to initiate containment procedures.

i. The Run the Create Block Requests for Malicious Observables subflow is executed and an incident record is created with a request to rebuild the infected device and its assets.

j. Next, a task is created to run sightings search to confirm if the environment is secure. The sightings search is repeated till no sightings found.
k. Next, a task is created to indicate that the security incident record is ready for review.

l. Finally, the record is updated and moved to the Review stage.

What to do next

You can click **Test** to simulate the actions in the flow before it is published. After testing the flow, click **Activate** to activate the flow so that it can be executed.

Click **Executions** to view the execution details of the flow.

---

Failed Login Manual playbook

With sophisticated security measures in place, attackers still use brute-force methods to obtain access to email accounts. However, it is hard to anticipate such attacks because there are high chances of such incidents being false positives.

Unsuccessful login attempts may either be false positives or attempts made by attackers to obtain access to user email accounts. In such scenarios, the Failed Login Manual playbook can provide guidance and help optimize the investigation of failed login security incidents.
### Prerequisites

<table>
<thead>
<tr>
<th>Role:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. sn_si.admin</td>
</tr>
<tr>
<td>2. flow_designer</td>
</tr>
</tbody>
</table>

| Spoke: Install Security Operations Spoke (sn_sec_spoke) |

This playbook covers the following capabilities to investigate security incidents:

1. Checks if the affected user is an active/inactive user
2. Filters whitelisted observables
3. Enriches the observables
4. Performs automated threat lookup.
5. Sends automated email to user to confirm the failed login attempt.
6. Assigns tasks to analyst to investigate user access
7. Identifies malicious observables and block IPs and URLs.
8. Resets user password.
9. Updates security incident status
10. Assigns tasks to security analyst to handle post incident review.

<table>
<thead>
<tr>
<th>Capabilities required</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Threat Lookup (Example: Virus Total)</td>
</tr>
<tr>
<td>• Observable Enrichment (Example: Whois, ReverseWhois)</td>
</tr>
<tr>
<td>• Sighting Search (Example: Splunk, QRadar)</td>
</tr>
<tr>
<td>• Observable Blocking (Example: CheckPoint, Palo Alto)</td>
</tr>
</tbody>
</table>

Visit the [https://store.servicenow.com/sn_appstore_store.do#!/store/home](https://store.servicenow.com/sn_appstore_store.do#!/store/home) ServiceNow Store website to view all available apps.

### Security analyst experience

To understand how to resolve security threats in a step by step manner, see Resolve security threats with the playbook.

### Deeper understanding of the Failed Login playbook with Flow Designer capabilities

**Getting Started**

1. Login as a user with sn_si.user and flow_designer roles.
2. Navigate to Flow Designer > Designer and click on the Failed Login playbook.
3. Make a copy of the following flows to copy the Failed Login Manual Playbook and make necessary modifications. (This is an optional step. Follow this step only if you plan to customize or make specific changes to the flow).
   - Failed Login Manual Playbook V1
   - Failed Login - Parse User's reply and Update Response Task V1

4. Make the necessary modifications according to your requirement. (This is an optional step. Follow this step only if you plan to customize or make specific changes to the flow).

5. Activate the playbooks.
   - Activate the main flow to use the playbook available with the base system.
   - Activate the copied flows after making any modifications according to your requirements.

The following image shows a copy of the Failed Login Manual playbook. Review the steps below to get an understanding of the various actions in the playbook.

This playbook is triggered and associated with the security incident when the following conditions are met:
• Category is Failed Login
• Has one or more affected users
• Security incident is not closed or cancelled

The following steps walks you through the actions, tasks, and subflows that are available in the Failed Login Manual playbook.

1. When the playbook starts executing, in Step 1, the playbook is automatically updated with a worknote showing the security incident with the failed login category has been assigned.

2. In Step 2, the playbook is updated and moved to the Analysis state.

3. In Step 3, the playbook checks if the Affected User is an active or inactive user. If the user is inactive, a worknote is added to the security incident that the user account is inactive.
**Note:** In step 3 of the flow, the flow checks inactive users in the `sn_si_incident` table available in ServiceNow. This step is provided as a guideline and must be modified for your specific environment. If you want to use this functionality, we recommend that you have an Active Directory integration set up in your environment. You can check with your Active Directory integration to find the user status and depending on the response, you can design the next steps for your playbook.

If you do not have an Active Directory integration, replace this step with a manual task for the security analyst to work with the IT team to block the user and move forward with the rest of the steps in the playbook.

4. In Step 4, the observables for the security incident are retrieved.

5. In Step 5, the observables are identified.

6. If no observables are found, a manual response task is created in Step 6 and the flow ends.

7. If observables are found, in Step 7, observables that are not whitelisted are identified.
8. If at least one of the observables is not whitelisted, the following steps are performed:
   
a. Steps 8.1 and 8.2 are executed. Observables are retrieved and an automated response task is initiated.

b. After the automated task has been created, Step 8.3 (8.3.1.1 and 8.3.2.1) is run and the Enrich Observables and Threat Lookup integrations are executed. Note that these are subflows that have been included in the playbook.

c. In Step 8.4, after the integrations have been completed, the security incident record is updated.

d. In Step 8.5, a new response task is created to indicate the next automated task that will take place.

e. In Step 8.6, the Sighting Search integration will be run on the observables.
f. After the Sighting Search subflow has been completed, in Step 8.7, the security incident is updated.

g. In Step 8.8, the observables are checked to see if they are malicious.

h. If the observables are not malicious, and if the user account is active, an automated email is sent to the user to reconfirm the unsuccessful login attempts. A manual response task is created to identify the observables and add them to the security incident. The playbook then ends at this stage.

i. If the observables are malicious, three response tasks are created:

   i. An automated email is sent to the user to confirm (Yes or No) the unsuccessful login attempts. If the user responds Yes:

      1. The security incident status is updated to Contain.

      2. An automated email is sent to the user to reset the password.

      3. The Reset Password subflow is initiated and an email is sent to the user when the task has been completed.

   ii. If the user responds No, an automated email is sent to the user to reconfirm the response. The security analyst has to manually take appropriate actions.

   Note: The Reset Password step is provided as a guideline. The steps in the flow resets the password for the users account in the Servicenow System. But the process to reset the password may be different depending on your environment. You can check with your Active Directory integration to reset the password of users automatically. If you do not have an Active Directory integration, replace this step with a manual task for the security analyst to work with respective IT team to reset users password and move forward with the rest of the steps in the playbook, upon completing the respective task.
iii. If the user does not respond to the automated email, the security analyst must update the security incident manually and provide a response. A manual task is created to validate if the user account has been compromised.

9. In Step 8.10.3, the security incident is state is updated.

10. In Step 8.10.4, an automated task is created to verify if the Create Block Requests for Malicious IPs and URLs capability implementation is available. If the capability implementation is available, the Create Block Requests subflow is executed. If this is not available, the security incident is updated and a worknote is posted to indicate that the capability implementation is not available.

11. In Step 9, the security incident is updated and the state is set to Review.

12. In Step 10, a response task is created for the user to complete the post incident review before closing the task.

Child Security Incident Automation playbook

Duplicate security incidents are categorized as child security incidents for a parent security incident.

The Child Security Incident Automation playbook helps reduce the time required to investigate and close duplicate security incidents. This playbook automatically rolls up unique artifacts of the child security incident (observables, affected users, CIs) to the parent security incident. Thus, this playbook enables analysts to investigate only the security incident without worrying about the duplicate incidents.

<table>
<thead>
<tr>
<th>Prerequisites</th>
<th>Child Automation playbook (Key capabilities)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role:</td>
<td>The Child Automation playbook covers the following capabilities:</td>
</tr>
</tbody>
</table>
Prerequisites

1. sn_si.admin
2. flow_designer

Spoke: Install Security Operations
Spoke (sn_sec_spoke)

<table>
<thead>
<tr>
<th>Prerequisites</th>
<th>Child Automation playbook (Key capabilities)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. sn_si.admin</td>
<td>1. Updates the security incident to the</td>
</tr>
<tr>
<td>2. flow_designer</td>
<td>Analysis stage.</td>
</tr>
<tr>
<td></td>
<td>2. Captures unique affected users and CIs</td>
</tr>
<tr>
<td></td>
<td>from the child security incident and adds</td>
</tr>
<tr>
<td></td>
<td>them to the parent security incident.</td>
</tr>
<tr>
<td></td>
<td>3. Captures unique observables from the</td>
</tr>
<tr>
<td></td>
<td>child incident and adds them to the</td>
</tr>
<tr>
<td></td>
<td>parent security incident.</td>
</tr>
<tr>
<td></td>
<td>4. Closes or cancels the child security</td>
</tr>
<tr>
<td></td>
<td>incident when the parent security</td>
</tr>
<tr>
<td></td>
<td>incident is closed or cancelled.</td>
</tr>
</tbody>
</table>

Security analyst experience

To understand how to resolve security threats in a step by step manner, see
Resolve security threats with the playbook.

Deeper understanding of the Child Security Incident Automation playbook with Flow Designer capabilities

Getting Started

1. Login as a user with sn_si.user and flow_designer roles.


3. Make a copy of the Child Security Incident Automated Flow V1 and make necessary modifications. (This is an optional step. Follow this step only if you plan to customize or make specific changes to the flow).

4. Activate the playbook.
   • Activate the main flow to use the playbook available with the base system.
   • Activate the copied flow after making any modifications according to your requirements.

The following image shows a copy of the Child Security Incident Automated Flow VI playbook. Review the steps below to get an understanding of the various actions in the playbook.
This playbook is triggered when:

- The parent security incident field is not empty.
- The parent security incident is in Draft, Analysis, Contain, or Eradicate state.
The following steps walks you through the actions and tasks that are available in the playbook.

1. When the playbook starts executing, in Step 1, if the security incident is in a Draft state, it is updated and set to the Analysis state.

2. In steps 2 and 3, affected users of the child security incident are retrieved and rolled up to the parent security incident. While updating the parent security incident, only unique affected users are added.

3. In steps 4 and 5, configuration items associated with the child security incident are retrieved and rolled up to the parent security incident. While updating the parent security incident, only unique configuration items are added.

4. In steps 6 and 7, observables associated with the child security incident are retrieved and rolled up to the parent security incident. While updating the parent security incident, only unique observables are added.
5. In steps 8 and 9, worknotes are posted to the parent and child security incidents indicating that the affected users, configuration items, and observables have been rolled up from the child to the parent security incident.

6. Once the parent security incident is closed or cancelled, the child security incident is also closed or cancelled by default.

**Action Library**

Complex actions that are critical for building Security Incident Response playbooks are available as Action Libraries. The actions listed below enable security administrators to create playbooks without writing any complicated code.

<table>
<thead>
<tr>
<th><strong>Action Name</strong></th>
<th><strong>Description</strong></th>
<th><strong>Example scenario</strong></th>
<th><strong>Input</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a security tag to the security incident</td>
<td>Use this action to add a security tag automatically using flow designer logic.</td>
<td>If the flow detects an IOC, the IOC Detected tag can be automatically added using this action.</td>
<td>• Input: security incident, security tag</td>
</tr>
<tr>
<td>Add observables to the security incident</td>
<td>Use this action to add observables to a selected security incident.</td>
<td></td>
<td>• Output: not applicable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Input: security incident</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• observables</td>
</tr>
<tr>
<td>Action Name</td>
<td>Description</td>
<td>Example scenario</td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>------------------</td>
<td></td>
</tr>
<tr>
<td>• By default, the list of observables are separated by the comma (,) delimiter but this can be modified. You can specify another single special character as a delimiter. While adding observables, the type (URL, IP address, hash) is automatically set.</td>
<td>• Output: not applicable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• When the observables are added to the security incident, the type (URL, IP address, hash) is automatically set.</td>
<td>• delimiter</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• When the observables are being added, the Filter Whitelisted Observables option identifies whitelisted observables and does not add them to</td>
<td>• filter whitelisted observables and post activity note</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action Name</td>
<td>Description</td>
<td>Example scenario</td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>------------------</td>
<td></td>
</tr>
<tr>
<td>the security incident’s observables related list. An automated system activity (response) is added to indicate that these observables have been removed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get affected users (Related Lists) from multiple security incidents V1</td>
<td>Retrieves all the affected users listed in the Affected Users related list for the specified security incidents.</td>
<td>You may have parent security incidents with multiple child security incidents. Use this action to roll-up affected users from all the child security incidents to the corresponding parent security incidents. Only unique affected users are rolled-up and all duplicates are eliminated.</td>
<td></td>
</tr>
<tr>
<td>Get affected users from multiple security incidents</td>
<td>Retrieves the primary affected user for the specified security incident. It does not include the affected users from the Affected User related list.</td>
<td>• While investigating a phishing security incident, send an email to the primary affected users (who reported the phishing</td>
<td></td>
</tr>
</tbody>
</table>

- Input: security incidents
- Output:
  - affected user
  - count
<table>
<thead>
<tr>
<th>Action Name</th>
<th>Description</th>
<th>Example scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get affected users (Related List) from a security incident</td>
<td>Retrieves all the affected users listed in the Affected Users related list for a specified security incident.</td>
<td>incident) to confirm if any of the users clicked on the malicious links in the phishing email.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Update the parent security incident severity or risk score based on the count of primary affected users.</td>
</tr>
<tr>
<td>Add affected users to security incident</td>
<td>Adds all affected users to a security incident.</td>
<td>Suppose you have a parent security incident with multiple child security incidents. You can use this action to roll-up affected users from all the child security incidents to the corresponding parent security incident. Only unique affected users are rolled-up</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Input: security incidents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Output:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ affected users</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ count</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Input:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ security incident</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Output: not applicable</td>
</tr>
<tr>
<td>Action Name</td>
<td>Description</td>
<td>Example scenario</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Get configuration items of the affected users</td>
<td>Retrieves the configuration items (CIs) of all affected users.</td>
<td>In phishing or malware scenarios, you can use this action to update the Affected Configuration Items (CI) related list and investigate the CIs. You can then update the severity or risk score of the security incident based on the number of identified CIs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Get all child security incidents for a security incident | Retrieves all child security incidents related to a specific parent security incident. | • Example scenario: Use this action to:  
  ◦ Update the status of the child security incidents when their corresponding parent security incidents status get updated.  
  ◦ Update the severity or risk score of the security incident | Input:                                                                                   | Output:                                     |
<p>|                                                 |                                                                             |                                                                                                                                                                                                                | ◦ security incident                      | ◦ child security incident                   |
|                                                 |                                                                             |                                                                                                                                                                                                                | ◦ incident state                         | ◦ count                                      |</p>
<table>
<thead>
<tr>
<th>Action Name</th>
<th>Description</th>
<th>Example scenario</th>
<th>Input:</th>
<th>Output:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get configuration items for the observables (type IP address)</td>
<td>Retrieves all configuration items (CIs) for observables of type IP address.</td>
<td>An IP address observable can be associated with a configuration item. For example, the IP address of a server. If you use this action, you can retrieve information for the server.</td>
<td>• observable ip address</td>
<td>• configuration items • count</td>
</tr>
<tr>
<td>Is observable malicious</td>
<td>Confirms the presence of one or more malicious observables in a set of observables.</td>
<td>After the threat lookup has been completed and you have identified the presence of malicious observables, you can increase the severity or risk score of a security incident.</td>
<td>• security incident</td>
<td>• malicious (true/false)</td>
</tr>
<tr>
<td>Filter out whitelisted observables</td>
<td>Use this action to whitelist observables from a given set of observables.</td>
<td>You can identify certain observables that can be ignored from a set of observables. These observables will not be taken into account while</td>
<td>• security incident</td>
<td>• whitelisted observables • count</td>
</tr>
</tbody>
</table>
### Action Name | Description | Example scenario
--- | --- | ---
Get user group for affected user | Retrieves the user group details of affected users. | In an organization, if two or more users report phishing emails, you can find out the group they belong to and identify if more users have been affected. • Input: user • Output: ◦ user groups ◦ count

### Security Incident Response reporting
Security managers can pinpoint areas of concern using high-level graphical interfaces.

### Access Security Incident Response Explorer
You can access the Security Incident Response Explorer dashboard to view security incident activity in order to instantly pinpoint areas of concern and quickly resolve issues.

**Before you begin**
Role required for homepage and dashboard:
sn_si.admin (to write)
sn_si_basic (to read)

**Procedure**
1. Navigate to **Self-Service > Homepage** or navigate to **Self-Service > Dashboards**.
2. Choose Security Incident Explorer from the reports list.
Security Incident Response Overview

The Security Incident Response Overview provides an executive view into security incident activity, providing trends and reports, and drill-downs into specific data.

The Overview module displays security incident information that is tailored to the role of the user. You can point to any part of a chart (bar, pie, data point, heatmap, and so on) to view general data specific to that part. See the following image. If you click any part of a report, a list opens to provide detailed information.

Security Incident Manager Overview

Users with the Security Incident Administrator and Security Incident Manager roles view the Security Incident Manager Overview. It contains the following reports in the base system.

**Security Incident Manager Overview reports**

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Team Critical Security Incidents</td>
<td>Single</td>
<td>The number of critical security incidents assigned to the team.</td>
</tr>
<tr>
<td></td>
<td>score</td>
<td></td>
</tr>
<tr>
<td>Team High Security Incidents</td>
<td>Single</td>
<td>The number of high security incidents assigned to the team.</td>
</tr>
<tr>
<td></td>
<td>score</td>
<td></td>
</tr>
<tr>
<td>SLAs expiring within 24 hours</td>
<td>Single</td>
<td>The number of SLAs that expire within the next 24 hours.</td>
</tr>
<tr>
<td></td>
<td>score</td>
<td></td>
</tr>
<tr>
<td>Risk vs Severity</td>
<td>Heatmap</td>
<td>The distribution of security incidents assigned to the team by risk and severity.</td>
</tr>
</tbody>
</table>
### Security Incident Manager Overview reports (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Incidents by CI Class, last 3 months</td>
<td>Bar chart</td>
<td>The count of security incidents assigned to the team by configuration item class.</td>
</tr>
<tr>
<td>Trend of All Security Incidents</td>
<td>Trend</td>
<td>Plots the count of the number of security incidents received by category or priority.</td>
</tr>
<tr>
<td>Unauthorized Access Security Incidents</td>
<td>Bar chart</td>
<td>Displays the types of security incident categories received over time.</td>
</tr>
<tr>
<td>Average Time to Contain</td>
<td>Single score</td>
<td>The average time it takes to contain all security incidents.</td>
</tr>
<tr>
<td>Average Time to Contain Critical</td>
<td>Single score</td>
<td>The average time it takes to contain all critical security incidents.</td>
</tr>
<tr>
<td>Average Time to Identity</td>
<td>Single score</td>
<td>The average time it takes to identify all security incidents.</td>
</tr>
</tbody>
</table>

### Security Analyst Overview

Users with the Security Incident Analyst role view the Security Analyst Overview. It contains the following reports in the base system.

### Security Analyst Overview reports

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>My Critical Priority Work</td>
<td>Single score</td>
<td>The number of critical security incidents assigned to me.</td>
</tr>
<tr>
<td>My High Priority Work</td>
<td>Single score</td>
<td>The number of high security incidents assigned to me.</td>
</tr>
<tr>
<td>My SLAs expiring within 24 hours</td>
<td>Single score</td>
<td>The number of SLAs assigned to me that expire within the next 24 hours.</td>
</tr>
<tr>
<td>Security Incidents assigned to me</td>
<td>Bar chart</td>
<td>Security Incidents assigned to me by incident state or category.</td>
</tr>
<tr>
<td>Work assigned to me by Type</td>
<td>Bar chart</td>
<td>Security tasks (incidents, tasks, or requests) assigned to me by type or priority.</td>
</tr>
<tr>
<td>Security Incidents, Requests, Tasks assigned to me</td>
<td>List</td>
<td>A list of all security incidents, security requests, and tasks assigned to me.</td>
</tr>
</tbody>
</table>
Security Analyst Overview reports (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Incident Location</td>
<td>Map</td>
<td>Regional location of the security incidents.</td>
</tr>
<tr>
<td>Count</td>
<td>Map</td>
<td>Number of security incidents per region.</td>
</tr>
<tr>
<td>Min/Max Count</td>
<td>Color Spectrum Bar</td>
<td>The minimum and maximum numbers of security incidents per region represented by a color spectrum bar.</td>
</tr>
<tr>
<td>Percentage of Count</td>
<td>Map</td>
<td>Percentage of the total incident count per region.</td>
</tr>
</tbody>
</table>

Security Incident CISO Overview with Security Incident Analytics activated

When the Security Incident Analytics plugin is activated, users with the Security Incident CISO and System Administrator roles view the Security Incident CISO Overview. The following CISO reports are provided in the base system.

Security Incident CISO Overview reports (with Security Incident Analytics activated)

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Security Incidents This Week</td>
<td>Single score</td>
<td>The number of new security incidents received in the current week.</td>
</tr>
<tr>
<td>Security Incidents Closed This Week</td>
<td>Single score</td>
<td>The number of security incidents closed in the current week.</td>
</tr>
<tr>
<td>New Security Incidents (Running 7 Days)</td>
<td>Single score</td>
<td>The number of security incidents opened within the last 7 days.</td>
</tr>
<tr>
<td>Security Incidents Closed (Running 7 Days)</td>
<td>Single score</td>
<td>The number of security incidents closed within the last 7 days.</td>
</tr>
<tr>
<td>Daily New Security Incidents vs Closed Security Incidents</td>
<td>Trend</td>
<td>New and Closed security incident counts over time by day.</td>
</tr>
<tr>
<td>Weekly New Security Incidents vs Closed Security Incidents</td>
<td>Trend</td>
<td>New and Closed security incidents over time by week.</td>
</tr>
</tbody>
</table>
Security Incident CISO Overview reports (with Security Incident Analytics activated) (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Incident Close Code</td>
<td>Trend</td>
<td>Full count of closure codes over time.</td>
</tr>
<tr>
<td>Security Incident Business Impact</td>
<td>Treemap</td>
<td>Business services with security incidents with available groupings by business criticality.</td>
</tr>
<tr>
<td>Average Time to Contain (Weekly)</td>
<td>Trend</td>
<td>The 7-day average time it takes to contain a security incident over time.</td>
</tr>
<tr>
<td>Average Time to Eradicate (Weekly)</td>
<td>Trend</td>
<td>The 7-day average time it takes to eradicate a security incident over time.</td>
</tr>
<tr>
<td>Average Time to Identity (Weekly)</td>
<td>Trend</td>
<td>The 7-day average time it takes to identify a security incident over time.</td>
</tr>
<tr>
<td>Security Incident Location</td>
<td>Map</td>
<td>Regional location of the security incidents.</td>
</tr>
<tr>
<td>Count</td>
<td>Map</td>
<td>Number of security incidents per region.</td>
</tr>
<tr>
<td>Min/Max Count</td>
<td>Color Spectrum Bar</td>
<td>The minimum and maximum numbers of security incidents per region represented by a color spectrum bar.</td>
</tr>
<tr>
<td>Percentage of Count</td>
<td>Map</td>
<td>Percentage of the total incident count per region.</td>
</tr>
</tbody>
</table>

Security Incident CISO Overview without Security Incident Analytics activated
When the Security Incident Analytics plugin is not activated, users with the Security Incident CISO and System Administrator roles view the Security Incident CISO Reporting Overview. The following CISO reports are provided in the base system.

Security Incident CISO Overview reports (without Security Incident Analytics activated)

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Security Incidents This Week</td>
<td>Single score</td>
<td>The number of new security incidents opened in the current week.</td>
</tr>
<tr>
<td>Security Incidents Closed This Week</td>
<td>Single score</td>
<td>The number of security incidents closed in the current week.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
### Security Incident CISO Overview reports (without Security Incident Analytics activated) (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Security Incidents (Running 7 Days)</td>
<td>Single score</td>
<td>The number of security incidents opened within the last 7 days.</td>
</tr>
<tr>
<td>Security Incidents Closed (Running 7 Days)</td>
<td>Single score</td>
<td>The number of security incidents closed within the last 7 days.</td>
</tr>
<tr>
<td>Weekly New Security Incidents</td>
<td>Trend</td>
<td>The new security incidents opened on a weekly basis.</td>
</tr>
<tr>
<td>Weekly Closed Security Incidents</td>
<td>Trend</td>
<td>The security incidents closed on a weekly basis.</td>
</tr>
<tr>
<td>Security Incident Close Codes</td>
<td>Trend</td>
<td>Security incident close codes over time.</td>
</tr>
<tr>
<td>Business Services with Security Incidents - Business Impact</td>
<td>Treemap</td>
<td>Business services with security incidents with available groupings by business criticality.</td>
</tr>
<tr>
<td>Average Time to Contain</td>
<td>Single score</td>
<td>The average time it takes to contain all security incidents.</td>
</tr>
<tr>
<td>Average Time to Contain Critical</td>
<td>Single score</td>
<td>The average time it takes to contain all critical security incidents.</td>
</tr>
<tr>
<td>Average Time to Identity</td>
<td>Single score</td>
<td>The average time it takes to identify all security incidents.</td>
</tr>
</tbody>
</table>

**Note:** The Security Incident Response base system includes Performance Analytics Solutions for displaying preconfigured best practice dashboards. The dashboards present important metrics for analyzing your Security Incident Response process, such as new security incidents or the average age of open security incidents. For more information and installation instructions, see Security Incident Response Analytics and Reporting Solutions.

**Security incident map**

The security incident map provides data by geographical location. The world map is highlighted in every area in which an incident occurs. When the Security Incident Analytics plugin is activated, you can add the security incident map.
to the Security Incident Response overview. After it has been added, you can configure the map by modifying the map filters.

**Add map to Security Incident Response overview**

You can add the map to the Security Incident Response overview to view security incident data by geographical location. A map allows you to drill down to security incident information by location.

**Before you begin**
Role required: sn_si.admin

**Procedure**

1. Navigate to **Security Incident > Overview**.
2. Click **Add content** in the top left corner of the page to open the widget selection control.
3. In the first selection box, click **Reports**.
4. In the second selection box, click **Security Incident**.
5. In the third selection box, click **Security Incident map**.
6. At the bottom of the screen, click the location on the screen you want to add to the report.
7. Close the **Add content** box.
Modify security incident map

Administrators in the global domain, can modify how the security incident map handles security incidents using filters.

Before you begin
Role required: sn_si.admin

Procedure
1. Navigate to Reports > Administration > All.
2. Search for Security Incident map.
3. Click Edit Report.

4. Click Add Filter Condition to add or edit filters.
5. Click Run to see the changes applied.
6. Click Save.

Security incident treemaps

When the Security Incident Analytics plugin is activated, you can add the security incident - service impact and security incident - real-time treemaps to the Security Incident Response overview. After they have been added, you can configure the treemaps by modifying treemap categories and indicators.

Add treemaps to the Security Incident Response overview

Treemaps display hierarchical (tree-structured) data as a set of nested rectangles. Each branch of the tree is given a rectangle, which is then tiled with smaller rectangles representing subbranches. Treemaps allow you to display security incident information in a dynamic, engaging way.

Before you begin
Role required: sn_si.admin
Procedure

1. Navigate to Security Incident > Overview.

2. Click Add content in the top left corner of the page to open the widget selection control.

3. In the first selection box, click Treemap.

4. In the second selection box, select the treemap you want to insert from the following list:
   - Security Incident - Service Impact
   - Security Incident - Real time
   - Security Incident - Business Impact
   - Vulnerability Significance

   **Note:** The Business Impact treemap appears on the Security Incident Response homepage by default. The Service Impact and Real time treemaps require that the Security Incident Analytics plugin are activated.

5. In the third selection box, select the level of granularity of information you want retrieved for the selected treemap.

   **Note:** For the Security Incident - Service Impact treemap, select Security Incident in the third selection box. This selection provides a drop-down list with multiple data categories.
6. At the bottom of the screen, click the location on the screen you want to add the gauge.

7. Close the Add content box.

Create or update a treemap category
You can modify the predefined categories for the security incident treemaps or create categories as needed.

Before you begin
Role required: sn_si.admin
The treemaps use performance analytics as the data source. The Performance Analytics module requires a separate plugin.

About this task
In the base system, treemap categories such as Incident Risk, Denial of Service, and Incident Severity are included. You can modify these categories or define more categories as needed.

Procedure
1. Navigate to Security Incident > Administration, and open the treemap definition you want to configure categories for:
   - Service Criticality Reporting Definition
   - Real-time Definition
2. Optional: Change the treemap definition name.
   In the base system, the default name for the service impact treemap definition is Security Incident. The default name for the real-time treemap definition is Security Incident - Real time.
3. Unless you are using a custom-built treemap, do not change the PA Indicator Group value.
4. To deactivate the treemap definition, clear the Active check box. If, for example, you deactivate the Denial of Service category from the system impact dashboard, that treemap category is not available.
5. In the Treemap Categories related list, select a category to modify or click New to create a new category.
6. Fill in the fields.
## Treemap Category form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name that is displayed for the category in the <strong>Categories</strong> list above the treemap.</td>
</tr>
<tr>
<td>Order</td>
<td>The order that the category appears in the <strong>Categories</strong> list above the treemap.</td>
</tr>
<tr>
<td>Treemap</td>
<td>The name of the treemap that uses this category.</td>
</tr>
<tr>
<td>Color</td>
<td>The color displayed for this category in the treemap.</td>
</tr>
<tr>
<td>Active</td>
<td>Select to activate this category.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the category.</td>
</tr>
<tr>
<td>Visible by all roles</td>
<td>Select to make this category visible to all users regardless of their role.</td>
</tr>
<tr>
<td>Roles</td>
<td>If you did not select the <strong>Visible by all roles</strong> check box, select the roles able to view this category.</td>
</tr>
</tbody>
</table>

7. Click **Submit** or **Update**.

### Create or update a treemap indicator

You can modify the predefined indicators for a treemap category or create new indicators. For each indicator, you can configure its data source and specify how lists of security incidents are opened from treemaps that are viewed with the indicator.

**Before you begin**

Role required: **sn_si.admin**

The treemaps use performance analytics as the data source. The Performance Analytics module requires a separate plugin.

**Procedure**

1. Open the treemap definition that you want to configure indicators for.

<table>
<thead>
<tr>
<th>Treemap definition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service impact treemap</td>
<td>Navigate to <strong>Security Incident &gt; Administration &gt; Service Impact Definition</strong>.</td>
</tr>
</tbody>
</table>
2. In the **Treemap Categories** related list, select the category that you want to configure indicators for.

3. In the **Treemap Indicators** related list, select an indicator to modify or click **New** to create a new indicator.

4. Fill in the fields.

### Treemap Indicator form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name that is displayed for the indicator in the <strong>Indicators</strong> list on the service impact dashboard.</td>
</tr>
<tr>
<td>Short description</td>
<td>A description that is displayed for the indicator in the <strong>Indicators</strong> list above the treemap.</td>
</tr>
<tr>
<td>Result limit</td>
<td>The maximum number of results allowed. The upper limit is 100.</td>
</tr>
<tr>
<td>Result Precision</td>
<td>The number of digits to display after the decimal point. This field is displayed for the real-time treemap definition only.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box to activate this indicator.</td>
</tr>
<tr>
<td>Category</td>
<td>The category name entered on the previous screen.</td>
</tr>
<tr>
<td>Direction</td>
<td>Indicates whether the tile on the treemap is minimized or maximized. This field is displayed for the real-time treemap definition only.</td>
</tr>
<tr>
<td>Unit</td>
<td>The unit of measure to be used for the metric. This field is displayed for the real-time definition only.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Automatic Refresh Interval</td>
<td>How frequently to refresh the treemap.</td>
</tr>
<tr>
<td>Order</td>
<td>The order the indicator appears in the <strong>Indicators</strong> list above the treemap.</td>
</tr>
</tbody>
</table>

5. Click the **Data Source Configuration** tab and configure one of the following data source options for the indicator.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
</table>
| Performance analytics         | Select **Performance Analytics** from the **Data source** field, then make the following entries:  
  - **Indicator**: The indicator used to group the PA data.  
  - **Default breakdown**: The default breakdown used to break the selected PA indicator into multiple parts. |
| Custom script                 | Select **Custom Script** from the **Data Source** field. Then use the HTML editor to customize the script as needed. The result of running the script must be an array in order for the information to display in the treemap. |
| Query conditions              | Select **Query Condition** from the **Data Source** field, and then make the following entries:  
  - **Query table**: The base table to be queried.  
  - **Aggregate type**: The type of aggregate (SUM, COUNT, AVG, MIN, MAX) to be used.  
  - **Aggregate field**: The field to be used by the query.  
  - **Group by**: The field to sort the queried data. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> To enhance the query, click <strong>Add Filter Condition</strong> and <strong>Add &quot;OR&quot; Clause</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

6. Click the **Click Through** tab, and specify how lists of security incidents are opened from the treemap.

   a. In the **Click through URL navigation type** field, select whether you want the list of security incidents to open in a new window, in the same window, or in a dialog box.

   b. **Optional:** In the **Click through URL script** field, modify the sample script if needed.

7. Click **Submit** or **Update**.

**Add vulnerability significance charts to an overview**

If the Vulnerability Response plugin is activated, you can add vulnerability significance definition charts and other visualizations to the Overview.

**Before you begin**

Role required: sn_si.admin

**Procedure**

1. Navigate to the Overview page to which you want to add the vulnerability significance gauge.

2. Click **Add content** in the top left corner of the page to open the widget selection control.

3. In the three selection boxes, make the selections depending on the gauge (tree map or score report) you want to add:
   - To add the Vulnerability Significance tree map, make these selections:
     - Treemap
     - Vulnerability Significance
     - Vulnerability Significance
   - To add the Vulnerability Significance score report, make these selections:
     - Performance Analytics
     - Score
     - Services with Vulnerability Significance
4. Click the location on the screen you want to add the gauge.
5. Close the Add content box.

Security Incident Response integrations

Starting with the Madrid release, all Security Operations core applications and non-core third-party integrations are available from the ServiceNow Store. This allows you to obtain new and updated features more rapidly. This section provides instructions for activating the integrations and configuring both ServiceNow and third-party integrations. Also included are some basic guidelines for developing your own integrations, as well as details on specific integrations included in the base system.

Integration Configurations
The base system includes a series of "cards" for each of the integration implementations you can activate and use. Also, cards are displayed for any integrations posted on the ServiceNow Store that have dependencies on Security Operations plugins. The integration cards can be viewed by selecting Security Operations > Integration Configurations.
You can filter the visible integrations using the **Category** drop-down menu. The **Show Configurations** drop-down menu lets you see multiple instances of implementations that allow their creation.

**Buttons on integration cards**
Integration cards display different buttons depending on the current state of the integration and the source of the card.
<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Plugin</td>
<td>Click this button to install the applicable plugin to activate the integration. After the plugin is installed, the button changes to <strong>Configure</strong>.</td>
</tr>
<tr>
<td>Configure</td>
<td>Click this button to enter information for configuring the integration. For some integrations, you may need to enter API keys or URLs acquired from the website of the third-party integration.</td>
</tr>
<tr>
<td>New</td>
<td>Certain integrations, such as Carbon Black and IBM QRadar, allow you to define multiple implementations of the same integration. For those integrations, click <strong>New</strong> after the plugin is activated. The cards allow you to install plugins (where applicable) and configure the implementations for use.</td>
</tr>
<tr>
<td>Open Page</td>
<td>In the base system, your instance performs a query to the ServiceNow Store for any applications that have dependencies on Security Operations plugins. When those applications are found, and the associated application plugins are activated, integration cards for them are displayed with the other security integration cards. Click <strong>Open Page</strong> to access the website of the third-party application to configure the integration. After you have completed the configuration, the <strong>Open Page</strong> button changes to <strong>Configure</strong>.</td>
</tr>
</tbody>
</table>

**ArcSight ESM Event Ingestion for Security Operations integration**

The ArcSight ESM event ingestion integration with the Security Incident Response product allows security incident analysts to collect correlated events and automate creation of security incidents with the ServiceNow platform. Data is ingested continually based on a configured polling schedule, and it is used by analysts to identify and respond to potential cyber security threats.

With this integration, correlated events that are candidates for security incidents can be ingested on a periodic basis. You can map fields in correlated events to security incident fields, preview the setup of an event as a security incident, and setup scheduled ingestion of events to automatically create security incidents on an ongoing basis.

**Overview**

This integration provides a security operations center (SOC) analyst with visibility to correlation events in ArcSight ESM. This data can be integrated into Now Platform Security Incident Response (SIR) security incidents for further investigation and remediation. Profiles are created in your Now Platform instance to handle different correlation event types that are created and made
available via correlation query viewers in ArcSight ESM. These profiles customize how different ArcSight ESM correlated event fields are displayed on SIR security incidents.

**Key features**
This integration includes the following key features:

- Create multiple event ingestion profiles to create SIR security incidents for specific types of threats such as malware and unauthorized access attempts.
- Drag-and-drop mapping of ArcSight ESM correlation event field values to associated SIR security incident fields.
- A preview of the SIR security incident layout based on sample correlation events to validate event mapping details.
- Ingest historical correlation events as well as new notable events on configurable intervals.
- Filter out correlation events that do not meet SIR incident generation criteria, e.g. low priority events
- Aggregate events to existing SIR security incidents based on matching field values to avoid duplicate security incidents.
- Update correlation events based on SIR incident creation and/or closure conditionals via a bi-directional interface.

**Supported Now Platform versions**
This integration supports the New York Patch 6 and Orlando Now Platform releases.

The following Security Operations applications must be installed and activated from the ServiceNow Store. Install and then activate one application at a time in the order listed below to ensure a smooth installation:

1. Security Integration Framework
2. Security Support Common
3. Security Incident Response
4. Event and Alert Ingestion for Security Operations
5. Integration Hub Plugins
   - a. ServiceNow Integration Hub Runtime
   - b. ServiceNow Integration Hub Action Step - REST
For more information about installing the Security Operations core applications, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.

**ArcSight ESM supported versions**

This integration has been tested with Version 7.0.0.2436 of the ArcSight ESM Manager. The integration supports both ArcSight ESM on-premises and Cloud/Hosted service environments.

**MID Server**

This integration requires an installed and configured MID Server in your Now Platform® instance to connect to the ArcSight ESM service when the ArcSight ESM server is deployed within your corporate network. If you are using the ArcSight ESM cloud service, a MID Server is not required. See the ServiceNow Product Documentation website for more information about MID Servers.

**References**

<table>
<thead>
<tr>
<th>Reference</th>
<th>Document Identifier</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ArcSight ESM product documentation</td>
<td>ArcSight product documentation.</td>
</tr>
<tr>
<td>2</td>
<td>ServiceNow Product documentation website</td>
<td>ServiceNow Product Documentation website</td>
</tr>
</tbody>
</table>

**Set up your Now Platform® instance for the ArcSight ESM event ingestion integration**

The following section lists the setup tasks that you are required to complete in your Now Platform® instance prior to installing the application from the ServiceNow Store.

**About this task**

Refer to the following table and verify that you have completed all the listed tasks before you download and install the application to ensure a smooth installation and configuration.

Role required: admin

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have assigned the required Now Platform®</td>
<td>The following roles are required for the installation, setup, and use of the integration in your Now Platform® instance.</td>
</tr>
<tr>
<td>Setup task</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| A user with the Now Platform® administrator role (admin) installs the application from the ServiceNow Store and assigns the security incident administrator (sn_si.admin) role. A user with the sn_si.admin role oversees the following tasks in the Now Platform®:  
  ◦ Names, creates, and edits event profiles.  
  ◦ Selects and maps values from ArcSight ESM correlation events to security incidents.  
  ◦ Previews security incident details for accuracy prior to finalizing the configuration.  
  ◦ Schedules on-going correlated event ingestion.  
  ◦ Enables correlated event updates when a SIR incident is created and closed.  
  ◦ Assigns the security incident analyst (sn_si.analyst) role.  
  ◦ Users with the sn_si.analyst work with security incidents. |  
<p>| Verify that you are using version 7.0.0.2436 or later of the ArcSight ESM Manager. Earlier versions are not supported. | If you have access to the ArcSight ESM Query Viewer, you have access to the API that is required for this integration. There is no other special setup required for the API. |
| Set up the Query Viewer in ArcSight ESM. | Before you can ingest correlation events, you must configure the Query Viewer in the ArcSight ESM console. See Set up the ArcSight ESM Query Viewer for details. |
| Optional | A correlation event goes through many stages in its life cycle before it is closed. ArcSight ESM provides default stages like Initial, Monitoring, |</p>
<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create custom stages in ArcSight ESM for correlation event updates.</td>
<td>Queued, and Closed. Some of these stages require user inputs but other stages are automatically applied to the event without any user intervention (the User Required field is unchecked in the ArcSight ESM console. You can create custom stages that do not require any user intervention and use them in your Now Platform® instance. See Additional options: Automate correlated event updates and closure based on SIR incident status for details.</td>
</tr>
<tr>
<td>Verify that you have installed and configured a MID Server Application.</td>
<td>Configured MID Server Application</td>
</tr>
<tr>
<td>Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration.</td>
<td>Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation.</td>
</tr>
<tr>
<td></td>
<td>1. Security Incident Response</td>
</tr>
<tr>
<td></td>
<td>2. Security Integration Framework</td>
</tr>
<tr>
<td></td>
<td>3. Security Support Common</td>
</tr>
<tr>
<td></td>
<td>4. Event and Alert Ingestion for Security Operations: This application requires:</td>
</tr>
<tr>
<td>Setup task</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>• com.glide.hub.integration.runtime =&gt;</td>
<td>ServiceNow IntegrationHub Runtime</td>
</tr>
<tr>
<td>• com.glide.hub.action_step.rest =&gt;</td>
<td>ServiceNow IntegrationHub Action Step - REST</td>
</tr>
<tr>
<td>5. Threat Core</td>
<td>For more information about installing the Security Operations core applications, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.</td>
</tr>
</tbody>
</table>

**What to do next**

You have successfully set up your Now Platform® instance for the integration. The next step is to install the ArcSight ESM Security Event Ingestion for Security Operations application from the ServiceNow Store for the integration.

**Set up the ArcSight ESM Query Viewer**

Create a query viewer and define filters that will include recently created correlation events that will be ingested ServiceNow.

**Procedure**

1. Log into the ArcSight ESM console to create a query viewer.
2. To create a new query, navigate to **File > New > Query**.
3. Define conditions for the Query Viewer in the Inspect/Edit panel.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the query.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Query On</td>
<td>Select Event from the drop down list.</td>
</tr>
<tr>
<td></td>
<td>To ingest the most recent data, select the date from the events are to be ingested. Specify a date that is a day or a few days earlier than the current date.</td>
</tr>
<tr>
<td>Note:</td>
<td>You cannot specify a date that is more than 7 days older than the current date. If you are ingesting a large number of events, you must specify a date that is 1 or 2 days older than the current date.</td>
</tr>
<tr>
<td>Start Time</td>
<td>This is the current date.</td>
</tr>
<tr>
<td>End Time</td>
<td>The maximum number of events that can be ingested at a time. Specify a value that is less than 5000 here.</td>
</tr>
<tr>
<td>Row Limit</td>
<td></td>
</tr>
</tbody>
</table>

5. Click on the Fields tab.
6. Select the fields that must be included during ingestion. You must select the Event ID, Name, and End Time fields for ingestion to be successful.

7. Click the Add 'ORDER BY' columns link and select Event ID field and specify the sort order as Descending to ensure that the latest events are ingested.

8. Click the Conditions tab. Right click Event under Event Conditions under the Summary section.

9. Click New Condition > Root > Type and select the Event Type as Correlation.

10. Click OK to save the query.

11. The next step is to create a Query Viewer for this query. Navigate to File > New > Query Viewer.
12. Click the **Fields** tab and ensure that the mandatory fields (Event ID, Name, End Time) you have specified in your query are selected.

13. Click **Apply** to save the Query Viewer. The new Query Viewer that you have created is listed in the Query Viewers section. Click on the Query Viewer to see the data being ingested.
Install and configure the ServiceNow application for the ArcSight ESM Event Ingestion integration

Before you run the integration on your Now Platform® instance, complete these installation and configuration steps so the application properly integrates with the Security Incident Response and Security Operations products on your Now Platform instance.

Before you begin
Role required: sn_si.admin

Procedure
1. If you have not installed the ArcSight ESM application from the ServiceNow Store for the integration, see Install a Security Operations integration and follow the steps to install it.
2. After you have successfully installed the application, navigate to Integrations > Integrations Configurations and locate the ArcSight ESM tile.
3. To configure the application, click New.
4. Alternatively, if a Configure button is displayed on a tile, click it to edit an existing configuration.
5. In the Event Ingestions Configuration dialog that is displayed, fill in the fields.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the ArcSight ESM Manager that will be used in the integration profile configuration to distinguish amongst multiple ArcSight ESM Manager sources if required. Spaces are supported for names, but parentheses are not supported.</td>
</tr>
<tr>
<td>ArcSight API Endpoint URL</td>
<td>URL for your ArcSight ESM Manager server. Note that the URL should include the API port, for example: <a href="https://arcsight-esm.com:8443">https://arcsight-esm.com:8443</a></td>
</tr>
<tr>
<td>API Account User Name</td>
<td>User name that you created for your API user account in the ArcSight ESM Manager console.</td>
</tr>
<tr>
<td>API Password</td>
<td>Password that you created for your API user account in the ArcSight ESM Manager console.</td>
</tr>
<tr>
<td>On Premises Deployment</td>
<td>Default is unchecked. If you are using the cloud-based version of ArcSight ESM that has direct Internet access, verify that the check box is cleared. For an on-premises deployment, select this check box and specify the MID Server Application.</td>
</tr>
<tr>
<td>MID Server Application</td>
<td>Specify a MID Server Application name here. This MID Server Application can point to any of the MID Servers that have been configured and any MID Server that is available will be used. If you do not have a Mid Server Application configured, you must create a new MID Server Application for this integration.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---

|  | Note: The MID Server Application can be configured only by users with system administrator role. |

To create a new MID Server Application, follow these steps:

**a.** Navigate to **Mid Server > Applications** and click **New**.

**b.** Enter a name for the MID Server Application and select a MID Server to be used as the default.

**c.** Deselect the Included in application ALL check box and click **Save**.

**d.** Click **Edit**. In the **Edit Members** page, select all available MID Servers, move them to the MID Servers List, and click **Save**.

**e.** The selected MID Servers will be listed as shown below.

![MID Servers List](image)

Depending on the availability, one of the MID Servers configured with the MID Server Application will be used.

**6.** Enter the configuration details and specify the MID Server Application you have created.
Each correlation event that you ingest from your ArcSight ESM Manager console requires a unique event profile in your instance. However, the ArcSight ESM source that you configure on the Event Ingestion Configuration form can be reused for multiple profiles as long as each profile ingests unique correlation event types.

7. Click Submit. After it is successfully validated and submitted, each ArcSight ESM server configuration is saved on the Security Integrations page as a tile. If your saved configuration tiles are not displayed on the Security Integrations page, on the top right corner of the page, from the Show Configurations choice list, click Yes.

What to do next
You have successfully installed and configured the application. The next step is to create an event profile.

Create a profile for ArcSight ESM correlation event ingestion integration
As a user with the sn_si.admin role, you create a profile in your Now Platform instance and determine which correlation events create security incidents. Before Now Platform Security Incident Response (SIR) security incidents are
created from correlation events, the field values from events are displayed on a layout of a Now Platform security incident so that you can preview how the actual security incident will be created.

**About this task**

Correlation events are automatically ingested into the Security Operations environment of your Now Platform instance depending on the profile type defined. A profile is an encapsulation of one type of correlation event like unauthorized access attempts or malware.

After a correlation event has been ingested, you can map individual correlation event fields to corresponding fields in the security incident. You can filter correlation events to specify which events create security incidents. For example, you may prefer filters that create security incidents only for correlation events identified as high-risk. You can also define additional event aggregation criteria so that incoming duplicate correlation events are aggregated to an open security incident. Finally, you can define an ingestion schedule and activate the profile.

Names for the event profiles in your Now Platform instance must be unique and can only be mapped to one active event profile at any given time.

**Create and name the profile for ArcSight ESM event ingestion integration**

You can set up a profile to ingest correlation events.

**Before you begin**

Role required: sn_si.admin

**Procedure**

1. To create an event profile for a correlation event in your Now Platform instance, navigate to ArcSight ESM Integration > ArcSight ESM Event Profile.

2. Click **New**.

3. Fill in the fields.

   An example of a completed form follows the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the profile. If names are not unique, an error will be displayed and duplicate profile names are not saved.</td>
</tr>
<tr>
<td></td>
<td>Profile names in your Now Platform instance must be unique.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Active</td>
<td>Check box is cleared by default. If this option is disabled, the profile is not active and ingestion will not take place.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You should complete all sections in the profile before making it active.</td>
</tr>
<tr>
<td>ArcSight Source</td>
<td>The ArcSight ESM server configured during the initial authentication step. If you have multiple ArcSight ESM servers configured, select the appropriate server for the correlation event types that will be ingested for the profile. You are required to select a value.</td>
</tr>
<tr>
<td>Query Viewer ID</td>
<td>Enter the Resource ID of the configured Query Viewer in the ArcSight ESM Console. The Resource ID is a unique identifier for any Query Viewer configured in the ArcSight ESM server. Once the Resource ID is submitted, the name of the Query View will be returned to ensure that the right Query Viewer has been selected. See the section below for screenshot view of how to determine the Resource ID for the selected Query Viewer in ArcSight ESM.</td>
</tr>
<tr>
<td>Order</td>
<td>Default is 100. If you have created multiple profiles, this value provides a run time execution priority when two or more profiles share the same triggering conditions. The workflow in the profile with the lowest number has the highest priority.</td>
</tr>
<tr>
<td>(Optional) Description</td>
<td>Additional text to help you distinguish this profile from other profiles.</td>
</tr>
</tbody>
</table>
The following figure is an example of a completed form.

After you have entered the profile details, click **Continue**. The Query Viewer ID is validated and if a corresponding Resource ID is present in the ArcSight ESM Query Viewer, the name of the Query Viewer will be returned as shown below. If the validation fails, check if the Resource ID exists in the ArcSight ESM console. If the Resource ID is not found, find the correct Resource ID and enter it in the profile.

What to do next

The next step is to select the correlation event types for ingestion from the Query Viewer that was selected in the prior step.
Select correlation events for ArcSight ESM event ingestion integration

Based on the ArcSight ESM source and the Query Viewer configured, select a correlation event rule for the profile.

About this task

View the available correlation events listed in the Correlation Event Selection in your Now Platform instance so you can determine which correlation events you want to ingest and create security incidents. You can only select one correlation rule type from the list for each profile.

Role required: sn_si.admin

The Query Viewer ID and the Query Viewer Name as specified in the Query Viewer form is displayed. Select a correlation event from the list that you can use to create a configuration mapping for the ingested correlated event.

Click on the drop down list in the Correlation Events List field. A list of correlation events that are present in the ArcSight ESM Query Viewer Console is displayed.

Click Continue to proceed to the next step in the wizard.

Mapping correlation event fields for the ArcSight ESM event ingestion integration

After you identify the specific correlation event rule from the list, the next step is to map correlation event fields to the fields in the security incident form.

Overview

For the mapping step, you can ingest sample correlation events for the selected correlation rule. During this mapping phase, you can ensure all relevant correlation event field data is mapped to the appropriate place on the SIR incident form and then visualize the SIR incident in the preview section.

The following figure shows the default mapping configuration that is provided for creating the correlation event profile. You can customize the fields that populate the security incident.
When you click **Retrieve Events**, the correlation event field names and the corresponding values are populated on the left side of the form. These are the ArcSight ESM correlation event fields that are available to map to the security incident fields.

You may prefer to review a few sample correlation events on your console to ingest for the field mapping configuration step. This step is labeled **Mapping** on the progress bar. If this page is not displayed, click **Mapping** on the progress bar. You can ingest up to five sample correlation events from the ArcSight ESM Manager for the selected correlation rule to assist with the field mapping process. There are options to either ingest the five most recent correlation events for the selected Correlation Event or ingest up to five specific correlation events based on the event IDs.

Below is a summary of the steps required to map correlation events:

- **Field Mapping**: Edit the mapping configuration by dragging correlation event fields from the left side and dropping them on the SIR incident mapping section on the right. The mapping on the right associates the incoming correlation event field with an outgoing security incident field.

- **Mapping Experience**: Customize the mapping grid by adding or removing fields using the + icon at the bottom of the SIR incident field mapping section. Track overlooked or previously mapped fields with the color coding that is provided (mapped fields are greyed out, blue fields are unmapped).

- **Incident Generation Conditions**: Once the mapping section is complete, you can define filter conditions so that you can filter which correlation events
should create security incidents versus correlation events that should be filtered out, for example, low priority correlation events. This is done in the Incident Generation Conditions section located below the Correlation Event Sample Ingestion section.

- Event Aggregation Criteria: Define additional event aggregation criteria that aggregates an incoming correlation event to an existing SIR security incident instead of creating similar, potentially duplicate incidents. Using field matching value criteria for each profile, this additional aggregation capability can reduce the number of active, overlapping security incidents by placing all related security notable event data on a single security incident.

- Format Field Translation: In certain cases, event field values in the ArcSight ESM correlation event may not translate directly to the fields on the SIR security incident. For these values, you can use a script editor to format field values on the security incident during the mapping step. Use the script editor if you want to format values that are similar, but not identical.

For example, with the script editor, a category value of Malware Alert and Virus Infection may have different field values for the source category but both values can be translated to a common Malicious Code Activity in the Category field on the SIR security incident using the Format Field Translation functionality.

The next step is to ingest sample correlation events and map values to the SIR security incident fields.

Create mappings for ArcSight ESM event ingestion integration

In this step, you ingest sample correlation events and map values to the SIR security incident fields.

About this task
As a user with the sn_si.admin role, you can review up to five sample correlation events from the Correlation Event Sample Ingestion column on the left of the form to assist with mapping and translating event field values to the security incident fields in the SIR Incident Field Mapping column on the right.

Create custom mappings by adding or removing the fields on the mapping grid on the right side of the form. Fields displayed by default are typically important fields to populate on the security incident response form. However, these fields can be removed and any additional fields can be displayed using the + and - buttons. Create custom maps by adding or removing the fields on the mapping grid on the right side of the form. Customizing the fields permits you to map ArcSight ESM fields that are not displayed on the default mapping grid on the security incident.
Procedure

1. If the mapping form is not displayed, click **Mapping** on the progress bar.

2. You can either pull the most recent sample correlation events for the selected correlation rule or provide the unique correlation event IDs for the specific correlation events that you want to use for your correlation event mapping experience. From the drop down list, select one of the following:
   - Retrieve most recent correlation events
   - Select correlation events based on event ID

   Click **Retrieve Events** to pull the latest sample correlation events from the ArcSight ESM console for the selected correlation search rule.

   The correlation event fields and values results are displayed as individual tabs.

   The pull for sample correlation events may take a few moments. A message indicating that the transaction is working is displayed at the top of the screen.

   In the following figure, the field-name value pairs for the ingested correlation event, or the imported sample events, are displayed on the left side of this form after the ingestion pull is completed. These values are the values that you map to the security incident fields on the **SIR Incident Field Mapping** side of the form.

   ![Image of correlation event form]

3. To map a field value from the left side of the form to a field on the security incident on the right side of the form, click-hold a blue field name on the left side of the form.
4. Drag the field name, for example, `agent.hostname`, and drop it on a field in the Input Expression column next to a field name in the Security Incident column.

To help you ensure that no event fields are overlooked or duplicated in the mapping process, fields are color-coded. Light blue fields on the left indicate that a correlation event field is not yet selected and mapped on the security incident. You may prefer to associate an incoming correlation field with more than one field on a security incident.

A gray field indicates that a field has been selected and mapped to a field on the security incident. This color-coding helps you track which event fields have already been utilized for future security incident field mappings.

5. To add fields to the default fields displayed on the security incident on the right side of the form, follow these steps.

a. On the right of the form in the SIR Incident Field Mapping section, at the bottom of the grid, click the plus icon. A new field is displayed.

b. In the Security Incident column, expand the choice list that is displayed, and select a field.

In the expanded choice list for the new field, some fields are shaded. In the following figure, **Affected User** has a gray background, because it has been mapped in the security incident. Similar to the color-coding for the correlation events fields on the left side of the form, this color-coding for the
security incident fields on the right helps you track the already mapped SIR incident fields.

Note: So that multiple observables can be displayed on the same security incident, the Observable field can be mapped multiple times with different values. Similarly, the Configuration Item and Work notes fields support multiple values. If you try to map two values to a field that cannot support multiple values, when you preview the incident, an error message is displayed that there is no value for the field. Similarly, if a field on a security incident has a choice list from which you can choose multiple options, and you try to map an option to that field that is not displayed on the choice list, the field is not populated on the security incident.

c. Alternatively, type a value in the Search field for the new row.

d. From the left side of the form, left-click to select the Event ID that you want in the Input Expression field. With the drag-and-drop feature, map it next to your new field.

6. Optional: Open the script editor and continue editing. For more information about the script editor, see Use the script editor to format correlation event values for ArcSight ESM integration.

(Optional) Incident generation filtering conditions

7. Optional: After you have completed the preceding field mapping steps, you can use the same field values in the Incident Generation Conditions builder to define additional criteria that an incoming correlation event must satisfy to create a SIR security incident. To set incident generation conditions, follow these steps.
a. Scroll to the *Incident Generation Conditions* section on the form and select the **Filter based on conditions** check box to enable the option.

(Optional) The Filter conditions builder is displayed. Use these filters to create security incidents that match the specific conditions described by the fields.

The options in the choice lists for the first field in the Filter conditions builder match the fields that are displayed on the *Correlation Event Sample Ingestion* section for the events you ingested. These fields are dynamic and change depending on the correlation events that you ingest. Criteria that you enter are case-sensitive, and they must match exactly the values of the ArcSight ESM correlation event.

Using the choice lists and fields of the condition builder, set filters for the first row.

b. To add more conditions, to the right of the fields, click **AND** or **OR**.

If **AND** is selected, all conditions must be matched. If **OR** is selected, either condition can be matched.

c. **Optional:** In the second row, set a second filter condition.

(Optional) The following image is an example with two conditions that must be matched before security incidents are created.

![Incident Generation Conditions](image)

(Optional) You have set the incident generation conditions so that security incidents are created only when both of the filtering conditions that you entered are matched.

This type of incident generation condition filtering helps you narrow down the security events, and limit the number of unnecessary security incidents that you create without modifying the underlying correlation search or
filter out events in ArcSight ESM. If additional filtering criteria are set, only correlation events that match all criteria are mapped to incidents.

**Note:** If any of the event field names have special characters such as quotes ("), hyphens (‘), underscores (-), or ampersands (@), these characters may need to be replaced for mapping translation purposes and possibly create a duplicate event name. The mapping can be done appropriately but a numerical suffix is appended to differentiate fields with duplicate event names. For example, if the first event field is `events.event` and the second event field is `events.event`, these fields cannot be uniquely identified as the remaining standard text characters are the same. In this case, a suffix is added to the second event field and the field is renamed to `events@event(1)`.

**Event Aggregation Criteria to Handle Similar Correlation Events and Prevent Duplicate Incidents**

**8. Optional:** To avoid creating duplicate security incidents, define additional event aggregation criteria so that incoming correlation events are aggregated to an open security incident. To set the criteria, follow these steps below:

**a.** Scroll to the **Event Aggregation Criteria** section on the form and select the Aggregation conditions check box to enable this option.

(Optional) The Incident Field Matching Values columns are displayed. These field names are the fields on the security incident that include any custom fields that are configured on the SIR security incident.

**b.** From the Available list, select the field values that you want to match on existing security incidents in your Now Platform and move them to the Selected list.

(Optional) All the field values that you select must be matched to append this incoming correlation event to an existing security incident. This includes fields, such as Observables and Configuration Items, that may have multiple correlation event field values mapped to them. All values must match. If only a subset of the values are matched, the event aggregation conditions will not be met and a new security incident will be created. See screen shot below for multi-value field mapping.
If a new correlation event matches all the values that are selected in the aggregation field conditions in the mapping step, the new correlation event is automatically added to the most recently opened security incident with the same field values. As a SOC analyst working with security incidents, you can view all the added aggregated correlation events on a related list on a security incident. All of the aggregated correlation events on a security incident are displayed on the Aggregated ArcSight Events related list. This list details associated time stamps and aggregated field values. This information helps you understand why these correlation events are being aggregated to existing security incidents. If this tab is not displayed, scroll to the left side of the record under Related Links and click the Show All Related Lists link.

Note: If you do not see this related list, follow these steps:

• Right click the Security Incident form header and click Configure > Related Lists.

• Select Aggregated ArcSight Events in the Available list, move it to the Selected list and click Save.

• Click Show Related Lists. You will now see the Aggregated ArcSight Events tab in the Related List section.
**c. Optional:** To log a work note for each time an event is aggregated on the security incident, select the check box to enable this option. The work note logs that a new correlated event has been added along with a link to the correlated event details.

You have successfully mapped values from a correlation event to fields on a SIR security incident. Also, you have configured additional conditions to limit the creation of security incidents with incident generation filtering criteria. You also aggregated correlation events to existing SIR security incidents when event field values match the configured aggregation criteria.

**9. Choose one to continue with the profile configuration.**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continue</td>
<td>The Mapping form is displayed. <strong>Preview</strong> is selected on the progress bar. The next step is to preview the fields you mapped on a SIR security incident.</td>
</tr>
<tr>
<td>Update</td>
<td>Your data is saved and the ArcSight ESM Event Profiles list is displayed.</td>
</tr>
<tr>
<td>Previous</td>
<td>The Correlation Event Selection form is displayed.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete this event profile and the Event Profiles list is displayed.</td>
</tr>
</tbody>
</table>

**Preview the security incident for the ArcSight ESM event ingestion Integration**

After you complete the mapping step, preview the values that you mapped in a Now Platform Security Incident Response (SIR) security incident. This preview step permits you to verify that you have mapped all the correlation fields that you want displayed on the security incident.

**About this task**

As a user with the sn_si.admin role, preview a security incident and edit the mapping again as required to fix fields with errors or to populate any missing data. If the preview is not successfully completed, you cannot proceed to the scheduling step. Previews of security incidents are not saved as actual incidents in the Security Incident Response product.
Role required: sn_si.admin

Procedure
1. If the security incident preview is not displayed, click **Preview** in the progress bar.
2. From the Sample Event IDs choice list, select an item. The security incident is displayed. Do not change any information in the fields. This view is a read-only view, and a record of this security incident is not saved.
3. Review the field mapping of the correlation event values on the security incident.

The preceding image is an example of a preview with a mapping error. In this example, a field value from the correlation event does not have an acceptable value for the reference field on the SIR incident form. An error message is displayed that indicates an input value was not found for the Category field which is a reference field with a specific set of values. As a result, this mapped field value will not appear on the SIR security incident form without further modification.

4. To resolve this error, click **Mapping** in the progress bar.
5. Edit the mapping to fix incorrect values or populate any missing data.
6. Preview the mapping again and continue to fix any errors that are described in error messages.
The following figure is an example of the Incident Details tab on the bottom half of a security incident after all error messages are resolved. For this example, the Description and Work notes fields were mapped, and these fields are populated with the values from the value pairs pulled from the ArcSight ESM correlation event samples.

What to do next
If no error messages are displayed, and you are satisfied with the field mapping on the security incident, the next step is to define the schedule.

Create a schedule for ArcSight ESM event ingestion
You can define the polling or pull schedule for new correlated events. During this step, you can verify the existing settings for correlation event retrieval or modify the scheduling as needed. This step also permits you to retrieve historical correlation events using a date range.

About this task
You can choose whether you want to ingest any historical correlation events during the Scheduling step. You also choose how often you will poll for future new correlation events that match the profile configuration.

As a user with the sn_si.admin role, you configure these polling intervals on a per-profile basis. The performance of the ArcSight ESM correlation event ingestion integration may be impacted by the different polling intervals. When scheduling, you may prefer to balance reducing polling overhead on the ArcSight ESM
server against a desire to be notified as soon as possible when an event is created or updated. A five-minute default value is set for any profile, but you may prefer to modify this setting to as low as one minute if required.

**Pulling new and updated correlation events**

**Procedure**

1. If the Scheduling page on the progress bar is not displayed, select *Scheduling*.
2. Choose one to schedule how and when correlation events are pulled from the `<ArcSight>` console.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Ongoing Event Ingestion field selected</td>
<td>On-going Event</td>
</tr>
<tr>
<td>• One-Time Retrieval field cleared</td>
<td>Based on the default setting, the Now Platform instance pulls from the ArcSight ESM server for new correlation events every five minutes. Security incidents are created if correlation events are found and incident generation filtering criteria are matched. To balance ingestion polling overhead desire to get the most current data, five minutes is the default setting. However, this value can be modified to as low as one minute if needed.</td>
</tr>
<tr>
<td>• Ongoing Event Ingestion field cleared</td>
<td>One-Time Retrieval</td>
</tr>
<tr>
<td>• One-Time Retrieval field selected</td>
<td>Use this configuration if you want a one-time pull to ingest historical correlation events. When this setting is configured, a profile is used once to retrieve correlation events from historical events that are based on a date range. To the right of the <em>Since date</em> field, click the calendar icon. In the calendar that is displayed, select the date that you want to start pulling alerts. Starting with the <em>Since date</em> value, correlation events are retrieved up through the current date.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Note that you can retrieve events as far back as seven days from the current date. This functionality is not intended to retrieve significant amounts of historical events for archival reasons but rather a minimal amount of in-flight events that are being actively worked at the time of profile activation.

After the correlation events are pulled, this setting will not retrieve more correlation events for this profile going forward from the current date. This setting populates the security incident with all the correlation events that are found for the range you enter.

As an example for scheduling an initial correlation event ingestion time, if you have a daily ArcSight ESM security check that runs once a day at 4 AM local time, you can set up the corresponding correlation event profile in your Now Platform instance to run at 4:05 AM local time to capture the security failure event right away and create a security incident. Enter 04 05 00 in the Initial event ingestion field. In the Increment (Minutes) field, enter 1440 (24
hours) to schedule the next event ingestion for 24 hours from the initial event ingestion. Both the initial event ingestion time and next event ingestion time are displayed in the fields.

3. To configure the settings for this example, follow these steps.

a. With the Scheduling page displayed, select the **Ongoing event ingestion** check box to enable this option.

b. In the **Increment (minutes)** field, enter **1440** (24 hours).

c. Click the **Set initial correlated event ingestion time** check box to enable editing for the Initial event ingestion and Next event ingestion fields.

d. In the Initial event ingestion time field, enter **04 05 00**. In the **The Next event ingestion time (estimated)** field, the time of the next event ingestion is displayed.

4. Click **Continue** to navigate to the Additional Options page.

ℹ️ **Note:** The default number of security incidents that can be created and aggregated in a day, and the flow time period are defined in the ArcSight ESM Integration Settings. You can modify these settings if required. See **ArcSight ESM Integration Settings for event ingestion integration** for details.

**Additional options: Automate correlated event updates and closure based on SIR incident status**

The ArcSight ESM integration has a bi-directional interface that allows for both correlation events to create security incidents, as well as an ability to update the correlation events once the security incident is created and/or closed with relevant incident details such as security incident number, assignment group, SIR incident URL, and so on.

**Before you begin**

Role required: sn_si.admin

**Procedure**

1. If the Additional Options page on the progress bar is not displayed, select **Additional Options**.

2. Follow the instructions below to complete the configuration for updating correlated events when the security incident is created:
<table>
<thead>
<tr>
<th>Option or Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Correlated Events upon SIR Incident Creation</td>
<td>Select this option if you want to update the correlation event stage in ArcSight ESM and update the event with additional comments when a security incident is created from the correlation event. This can occur for correlation events that could either create a new security incident, as well as aggregate existing security incidents.</td>
</tr>
<tr>
<td>Note:</td>
<td>If this option is not selected, the event stage will not be updated when the security incident is created.</td>
</tr>
<tr>
<td>Correlated Event Stage Update</td>
<td>Select a stage option from the Correlated Event Stage Update choice list that displays all available stages retrieved from the ArcSight ESM server.</td>
</tr>
</tbody>
</table>

**Correlated event stage not configured**: If you have not configured any correlated event stages in your Now Platform instance, you will only see the **Assign Stage - Initial Setup** in the Correlated Event Stage Update choice list. To configure the stage, follow these steps:

- Enter a resource ID in the Enter Stage Resource ID field and click **Submit**. The resource ID is validated in the ArcSight ESM console and the following screen is displayed.

  ![Correlation Event Updates](image)

- Click **Save** to save the new stage (**Monitoring**).
- Click the Select Correlated Event Stage drop down list.
• You can select the newly created stage from the list.

Correlated event stage already configured: If you have already configured the correlated event stage, follow these steps:

• Select Use Previously Assigned Stage in the Correlated Event Stage Update choice list.

• Select an existing stage from the Select Correlated Event Stage choice list as shown below.

Initial Comments posted back to Correlated Event: In addition to updating the correlation event stage value, you can also post comments to the correlation stage annotations. As indicated in the instructions, you may edit the default text displayed in the comments section including adding or modifying the substitution variables using format ${field name}$ for any field on the Security Incident Response incident form.

Note: You can either use the default stages defined in the ArcSight ESM console or create your own custom stages. To create a new stage, follow these steps:

• In the ArcSight ESM console, select File > New > Stage. The Inspect/Edit tab is displayed.

• Define the new stage and do not select the User Required check box. Ensure that the stage is defined correctly and is in the correct position in the event life cycle.

3. In the Automating Correlated Event Closure section, you can define how to update the security incident when it is closed. Enter the following details:
<table>
<thead>
<tr>
<th>Option or Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Correlated Events upon SIR Incident Closure</td>
<td>Select this option if you want to update the correlation event status and add additional comments when a security incident is closed from the correlated event. This will occur for both the initial triggering notable events that create the security incident, as well as aggregated events.</td>
</tr>
<tr>
<td></td>
<td>✉️ <strong>Note:</strong> If this option is not selected, the event stage will not be updated when the security incident is closed.</td>
</tr>
<tr>
<td>Correlated Event Stage Update</td>
<td>Select a stage option from the menu that displays all available stages retrieved from the ArcSight ESM server. Select the stage value to be set for all correlation events when a security incident is to be closed.</td>
</tr>
<tr>
<td></td>
<td>✉️ <strong>Note:</strong> The stages displayed here are based on the stages configured in the Correlation Event Initial Updates section.</td>
</tr>
<tr>
<td>Select Correlated Event Stage</td>
<td>Select an appropriate status here.</td>
</tr>
<tr>
<td>Closure CommentsPosted back to Correlated Event</td>
<td>In addition to updating the correlation event status value, you can also post closure comments to the correlation event annotations. As indicated in the instructions, you may edit the default text displayed in the comments section including adding or modifying the substitution variables using format ${field name}$ for any field on the Security Incident Response incident form.</td>
</tr>
</tbody>
</table>
4. **Click Finish** to complete the configuration.

A confirmation dialog is displayed. You have successfully completed the setup and configuration for the integration. Activate this profile to pull correlation events from the ArcSight ESM console based on your scheduling.

**ArcSight ESM Integration Settings for event ingestion integration**

Use this option to modify the ArcSight ESM default ingestion settings.

To modify the system properties, log in as a user with the `sn_si.admin` role and navigate to **ArcSight ESM Integration > ArcSight ESM Integration Settings**.

The default configuration settings are displayed. You can modify these settings if required.

<table>
<thead>
<tr>
<th>ArcSight ESM Integration Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>All properties used in ArcSight ESM Event Ingestion Integration.</td>
</tr>
<tr>
<td>ArcSight limiter for aggregation of Security Incidents.</td>
</tr>
<tr>
<td>100</td>
</tr>
<tr>
<td>ArcSight limiter for daily Security Incidents creation.</td>
</tr>
<tr>
<td>1000</td>
</tr>
<tr>
<td>This is timeout for Arcsight Flows which runs at time of ArcSight ESM Profile setup.</td>
</tr>
<tr>
<td>300000</td>
</tr>
<tr>
<td>This is timeout for Arcsight Flows which runs at time of ArcSight ESM Scheduled Ingestion.</td>
</tr>
<tr>
<td>600000</td>
</tr>
</tbody>
</table>

**Save**
Troubleshooting ArcSight ESM event ingestion integration

This section provides information on how to troubleshoot any errors that may occur during event ingestion.

Integration runs

Navigate to Event Ingestion Common > Integration Runs. An integration run takes place every minute and captures details regarding the events ingested during the scheduled job.

You can see the list of integration runs and status of each run (Success, Timed-out, Waiting) and the number of security incidents that were created. Click on the Number link to drill down to the detailed Integration Run page.
You can view details like the number of events that were ingested, the status, which event that was transformed into a security incident, and the different tasks there were performed during the ingestion. Additionally, you can click the link to view the flow execution details.

**Flow execution details**
Click the execution details link to see the flow associated with the event ingestion.
You can view a step by step execution of the flow detailing the various actions and subflows that were executed as part of the flow.

**Copy ArcSight ESM profile for event ingestion integration**

Copy an existing profile and its associated settings instead of creating new profiles. If you are creating multiple profiles, and you want to reuse the settings of an existing profile, you may prefer to copy profiles to save time.

**Before you begin**
Role required: sn_si.admin

**About this task**
As a user with the sn_si.admin role, if you copy a profile, the profile name is initially modified to avoid duplicate profiles. In addition, the copied profile is disabled (false) so it is not activated accidentally prior to completing the configuration. Copy profiles and use existing maps for security incidents that you have already previewed and verified.

**Procedure**
1. Navigate to ArcSight ESM Integration > ArcSight ESM Event Profile.
2. In the ArcSight Profiles list that is displayed, select a profile that you want to copy, and, from the Actions on selected rows choice list, click **Copy.**
The profile is copied and displayed on the list. The copy has all the settings of the original profile including the mapping and scheduling configuration. The name of the profile contains copy. Although the original profile is enabled (true), the copy is disabled at this point (false). You may prefer to edit values of the copied profile and rename it so the configuration settings apply to the new profile as required.

You have successfully copied the settings from an existing profile to a new profile. Note that the Active column status is set to false as the profile needs to be activated.

Use the script editor to format correlation event values for ArcSight ESM integration

In addition to the directly mapped fields from the ingested correlation event values, use the script editor to format field values on the security incident during the mapping step. The script editor changes the values of a ArcSight ESM correlation event field so that values that are supported by the Now Platform SIR security incident are mapped to the Category, Configuration item (CI), Observable, and other security incident fields.

About this task
In certain cases, ArcSight ESM correlation event values are mapped to reference fields such as, Category, Configuration item (CI), and Observable
fields on the security incident. As a user with the sn_si.admin role, you may prefer to edit the mapped event field values to translate format or data values to conform with incident field formats and values expected. If you want to translate the value of a ArcSight ESM correlation event to a value that is supported by these fields on the SIR security incident, use the script editor.

Role required: sn_si.admin

Procedure

1. With the mapping form displayed, click the link to open the script editor.

2. From the choice list, select a destination field for the value that you want to edit.

3. Alternatively, in the SIR Incident Field Mapping section, click the bracket icon [{}], next to a field to open the script editor for that field.

   In certain instances, a script include may be appropriate for the Configuration item field. For a correlation event, for example, a value for the Configuration item may not be matched.

   As shown in the following figure, if a match for a host name cannot be found in the Now Platform CMDB for the Configuration item field, you can edit the rule so that if an IP address is found, it populates the Configuration item field.

   The editor opens with the field displayed in Destination Field.

4. Enter any changes to then script, and click Update to save your changes. The ArcSight ESM Field Translations table is displayed.

5. Close the table to return to the Mapping form.

Flow Designer usage with ArcSight ESM event ingestion integration

Using the Integration Hub and Flow Designer, several flows, subflows, and actions are available with the ArcSight ESM integration.

To view these subflows, navigate to Flow Designer > Designer and click on the SubFlows tab. The figure below shows the important subflows used during profile creation and the scheduled ingestion job.
These subflows are listed in the sequence in which they are executed below:

- **Connection and credential validation**: This subflow validates ServiceNow connectivity with the ArcSight ESM server and the specified credentials. This subflow is used when you click the **Configure** button in the **ArcSight ESM - Event Ingestion** tile in the **Security Operations > Integrations > Integrations Configuration** page.

- **ArcSight Get Auth Token**: This subflow generates the ArcSight ESM Authentication token from the Username and Password using the ArcSight ESM Login Service. The Login Service provides the authentication token that can be used to call any other ArcSight ESM endpoint. This subflow is used in all other subflows.

- **Query Viewer ID Validation**: This subflow verifies if the Query Viewer ID specified during profile creation is present in the ArcSight ESM server.

- **Correlation Rule Retrieval**: This subflow retrieves the correlation rules based on the Query Viewer ID.

- **Get Sample Event**: This subflow fetches the sample correlation events from the ArcSight ESM server. These sample events are then mapped to the security incident fields in the Mapping section of the profile.

- **Stage Resource ID Validation**: This subflow validates the specified Stage Resource ID in the ArcSight ESM console and fetches the Resource Name.
• **Update Correlated Event Comments:** This subflow updates the Correlated Event comments in the Initial and Closure of Incident sections in the Additional Options page of the profile.

• **Retrieve Correlated Events Based on Polling Schedule:** This subflow runs the scheduled job that fetches the correlated events based on the polling interval.

During execution, the above subflows also trigger several other subflows and actions either directly or indirectly as shown below.

<table>
<thead>
<tr>
<th>Flows</th>
<th>Subflows</th>
<th>Actions</th>
<th>Executions</th>
<th>Help</th>
<th>+ New</th>
<th>+ New</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Can Invoke Rest from Arcsight Source</td>
<td>can_invoke_rest_from_arcsight_source</td>
<td>Security Operations ArcSight ESM Event</td>
<td>Published</td>
<td>true</td>
<td>2020-01-07 00:46:32</td>
</tr>
<tr>
<td></td>
<td>Check Closure Update Events REST Step Status</td>
<td>check_closure_update_events_rest_step_status</td>
<td>Security Operations ArcSight ESM Event</td>
<td>Published</td>
<td>true</td>
<td>2020-02-13 04:48:08</td>
</tr>
<tr>
<td></td>
<td>Check Initial Update Events REST Step Status</td>
<td>check_initial_update_events_rest_step_status</td>
<td>Security Operations ArcSight ESM Event</td>
<td>Published</td>
<td>true</td>
<td>2020-02-13 04:48:55</td>
</tr>
<tr>
<td></td>
<td>Connection and Credential Validation</td>
<td>connection_and_credential_validation</td>
<td>Security Operations ArcSight ESM Event</td>
<td>Published</td>
<td>true</td>
<td>2020-02-13 04:50:26</td>
</tr>
<tr>
<td></td>
<td>Correlation Rule Retrieval</td>
<td>correlation_rule_retrieval_5</td>
<td>Security Operations ArcSight ESM Event</td>
<td>Published</td>
<td>true</td>
<td>2020-02-13 04:51:40</td>
</tr>
<tr>
<td></td>
<td>Finish Profile Event Inspection</td>
<td>end_process_run</td>
<td>Security Operations ArcSight ESM Event</td>
<td>Published</td>
<td>true</td>
<td>2020-02-13 04:53:48</td>
</tr>
<tr>
<td></td>
<td>Get Profile Inspection Information</td>
<td>get_last_run_date</td>
<td>Security Operations ArcSight ESM Event</td>
<td>Published</td>
<td>true</td>
<td>2020-02-13 04:54:11</td>
</tr>
<tr>
<td></td>
<td>Get Sample Events</td>
<td>get_sample_events</td>
<td>Security Operations ArcSight ESM Event</td>
<td>Published</td>
<td>true</td>
<td>2020-02-13 04:55:59</td>
</tr>
<tr>
<td></td>
<td>Query Viewer ID Validation</td>
<td>query_viewer_id_validation</td>
<td>Security Operations ArcSight ESM Event</td>
<td>Published</td>
<td>true</td>
<td>2020-02-13 04:56:52</td>
</tr>
<tr>
<td></td>
<td>Retrieve correlated events based on poll</td>
<td>retrieve_correlated_events_based_on_poll</td>
<td>Security Operations ArcSight ESM Event</td>
<td>Published</td>
<td>true</td>
<td>2020-02-13 04:58:28</td>
</tr>
<tr>
<td></td>
<td>Stage Resource ID Validation</td>
<td>get_stage_resource_name</td>
<td>Security Operations ArcSight ESM Event</td>
<td>Published</td>
<td>true</td>
<td>2020-02-13 05:00:00</td>
</tr>
<tr>
<td></td>
<td>Update Correlated Event</td>
<td>update_correlated_event</td>
<td>Security Operations ArcSight ESM Event</td>
<td>Published</td>
<td>true</td>
<td>2020-02-13 23:12:18</td>
</tr>
<tr>
<td></td>
<td>Update Correlated Event Comments</td>
<td>update_correlated_event_comments</td>
<td>Security Operations ArcSight ESM Event</td>
<td>Published</td>
<td>true</td>
<td>2020-02-15 02:08:37</td>
</tr>
<tr>
<td></td>
<td>Validate MID Server Status</td>
<td>validate_mid_server_status</td>
<td>Security Operations ArcSight ESM Event</td>
<td>Published</td>
<td>true</td>
<td>2020-02-13 05:03:46</td>
</tr>
</tbody>
</table>

**Carbon Black - Incident Enrichment integration**

Use the Carbon Black integration to investigate and respond to security incidents using APIs to query and interact with endpoints associated with security incidents.

**Find Carbon Black - Incident Enrichment integration resources**

- Get started with the Carbon Black - Incident Enrichment integration
- Security Operations Carbon Black Integration - Get Running Processes workflow
- Security Operations Carbon Black Integration - Isolate Host workflow

© 2021 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
• Security Operations Carbon Black Integration - Remove Host Isolation workflow

Understand integration concepts
• Types of ServiceNow integrations provided
• Security Operations workflow triggers

Get help from ServiceNow resources
• Ask or answer questions in the Security Operations community
• Search the Known Error Portal for known error articles
• Contact Customer Service and Support
• Upgrade to Madrid

Get started with the Carbon Black - Incident Enrichment integration
The Carbon Black incident enrichment facilitates the investigation of a security incident by querying logs for potentially malicious indicators. Before you can use the Carbon Black - Incident Enrichment integration, you must download it from the ServiceNow Store and add the appropriate Endpoint Base URL and MID server.

Before you begin
Role required: sn_si_admin

Procedure
1. Download the integration from the ServiceNow Store.
2. When the download is complete, access the Carbon Black website and obtain the Endpoint Base URL and API Token under your profile.
4. In the Carbon Black - Incident Enrichment card, click Configure.
5. Fill in the fields, as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of this configuration.</td>
</tr>
<tr>
<td>Endpoint Base</td>
<td>The endpoint URL you acquired from the Carbon Black site.</td>
</tr>
<tr>
<td>Link URL</td>
<td>The Link URL that links to a Carbon Black instance, when available.</td>
</tr>
<tr>
<td>API Token</td>
<td>The API token you acquired from the Carbon Black site.</td>
</tr>
<tr>
<td>Max Rows</td>
<td>The maximum number of rows you want to search. The default is 1000 rows.</td>
</tr>
<tr>
<td>Earliest Result (days)</td>
<td>The earliest results you want to see in number of days.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Perform binary and process search</td>
<td>Select this to perform binary searches to find binary files such as file hashes, and process searches for .exe processes that may have run.</td>
</tr>
<tr>
<td>Include raw data samples in search results</td>
<td>Select this to include samples of raw data in your sightings search results. The amount of data returned depends on your setting in the number of rows of raw data property in Security Incident Response properties.</td>
</tr>
<tr>
<td>MID Server</td>
<td>Select Any to use any active MID Server, or select a specific MID Server name.</td>
</tr>
</tbody>
</table>

**Note:** Configuring this integration activates workflows. To manage the workflows, navigate to the Workflow Editor.

6. Click Submit.
   The integration configuration card displays.

7. To return to the original list of integration configuration cards, select No from the Show Configurations drop-down list.

**Carbon Black integration**

The Carbon Black integration enables you to investigate and respond to security incidents using APIs to query and interact with endpoints associated with security incidents.

<table>
<thead>
<tr>
<th>Explore</th>
<th>Set up</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Security Incident Response integrations</td>
<td>• Get started with the Carbon Black integration</td>
</tr>
<tr>
<td>• Carbon Black - Incident Enrichment integration</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use</th>
<th>Develop</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Security Operations workflow triggers</td>
<td>• ServiceNow Security Operations integration development guidelines</td>
</tr>
<tr>
<td>• View affected items for a security incident</td>
<td>• Tips for writing integrations</td>
</tr>
<tr>
<td>• Security Operations - Get Running Processes workflow</td>
<td>• Developer training</td>
</tr>
</tbody>
</table>
Get started with the Carbon Black integration

Carbon Black is an advanced security system easily integrating with Security Operations. Before you can use the Carbon Black integration, you must download the integration from the ServiceNow Store and add the appropriate Endpoint Base and API Token.

**Before you begin**
Role required: sn_si_admin

**Procedure**

1. Download the integration from the ServiceNow Store.

2. When the installation is complete, access the Carbon Black website and obtain the Endpoint Base URL and API Token under your profile.

3. In your instance, navigate to **Security Operations > Integrations > Integration Configurations**. The available security integrations appear as a series of cards.

4. In the Carbon Black card, click **New**.
5. Fill in the fields, as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of this configuration.</td>
</tr>
<tr>
<td>Endpoint Base</td>
<td>The endpoint base you acquired from the Carbon Black site.</td>
</tr>
<tr>
<td>API Token</td>
<td>The API token you acquired from the Carbon Black site.</td>
</tr>
<tr>
<td>Use MID Server</td>
<td>Select this check box if it is not already checked.</td>
</tr>
<tr>
<td>MID Server</td>
<td>Select Any to use any active MID Server, or select a specific MID Server name.</td>
</tr>
<tr>
<td>Enable Isolate Host</td>
<td>Select this check box to allow selected configuration items to be isolated from the Configuration Items related list tab in a security incident.</td>
</tr>
</tbody>
</table>

ℹ️ Note: Configuring this integration activates workflows. To manage the workflows, navigate to the Workflow Editor.
Check Point Anti-bot - Email Parser integration

Check Point Anti-bot - Email Parser integration is supported using an email parser that consumes email notifications from Check Point Anti-bot to create security incidents and drive enrichment and response workflows.

Configure the Check Point Anti-bot - Email Parser integration

The Check Point Anti-bot - Email Parser integration uses email notifications to drive enrichment, and response workflows.

Before you begin
Role required: sn_si_admin

About this task
A Check Point Anti-bot email parser template is provided to use for the integration. It must be configured and activated before the integration takes place. Updating the parser activates it.

Procedure

2. In the Check Point Anti-bot - Email Parser card, click Configure.

3. In the Check Point Anti-bot - Email Parser Configuration dialog box, click the Configure Email Parser link.
4. Click the **Check Point Anti-bot** link to edit the settings in the template email parser provided. At a minimum, fill in the *Email is from* field.
   To create an email parser, see Create email parsers in Security Operations.

5. Check the **Active** box.

6. Click **Update** in the **Email Parser** form.
   The email parser is active. You do not need to return to Integration Configurations.

**Check Point Next Generation Threat Prevention integration**

This document describes the steps required to integrate Check Point Next Generation Threat Prevention (NGTP) capabilities with ServiceNow Security Incident Response (SIR) so that applications function properly together.

Once installed and configured, the security incident analyst uses this integration to block malicious IP addresses, URLs, and Domains using Block Request List capabilities with the ServiceNow Security Incident Response (SIR) products. This Block Request List is configured on Check Point Gateways as a Custom Intelligence Feed. The Custom Intelligence Feeds feature provides an ability to add custom cyber intelligence feeds into the Next Generation Threat Prevention engine. It allows fetching feeds from a third-party server, in this case the ServiceNow Security Incident response application, directly to the Check Point Next Generation Gateway to be enforced by Anti-Virus and Anti-Bot blades. The security incident response analyst creates entries for Check Point Block List from observables determined to be malicious on ServiceNow SIR security incidents.

For most implementations, a Block Request List is a csv file that is hosted on an external web server. For this integration, this web server is your Now Platform instance, which permits the Check Point next-generation Threat Prevention Engine to fetch the list of IP Addresses, URLs and Domains to be blocked.

To enforce the blocking observables on Check Point Gateway, ensure that Threat Prevention Policy is configured with Anti-Bot and Anti-Virus Blades activated. As the Block List entries are modified, the Threat Prevention Engine dynamically imports the list at the configured interval and enforces policy without a configuration change or a commit on the firewall. For this integration, Now Platform has created a table containing Block List entries that are retrieved by authorized Check Point next-generation Gateway at the configured retrieval intervals.

The integration includes the following features:

- **Flexibility to create multiple Block Lists that apply to multiple Check Point Gateways.**

- **Detailed reporting on the types of sites being blocked (phishing, malware, and allow listed sites).**
• Tagging of Now Platform security incidents with Block List entries by the observable type (URL, domain, IP address).

• Configuring Block List expiration periods to maintain Block List size by automatically expiring or removing older entries.

• Searching Block List entries between different Block Lists.

• Linking Block List entries to observable records and security incidents that include threat intelligence results and details about why an entry is blocked.

Integration architecture diagram
Below is the high-level architecture diagram depicting the components involved and integration points between NOW Platform and Check Point Systems.

![Integration architecture diagram](image)

Note: The Check Point Systems logo, Anti-Virus Blade image, and Anti Bot Blade image are from Check Point Systems®. They are the Property of Check Point Systems.

Plugins
The integration requires that the Security Incident Response (com.snc.security_incident) plugin be activated.
To install Security Incident Response plugins:

1. Log in to your instance with your HI credentials.
2. Verify you have the system administrator (admin) role.
3. Navigate to System Definition>plugins in your instance.
4. Select and click Security Incident Response.

Once these plugins have been installed, you are able to upload the new Check Point integration plugin from the ServiceNow store and follow the configuration instructions in this document: Check Point NGTP Block Request Integration (com.snc.secops.checkpoint)

**Supported Check Point OS versions**

This integration requires the Custom Intelligence Feed of Check Point. Install the hot fix of Custom Intelligence Feature known as Check Point R80.10 Jumbo HF take 121 and above. Refer to the Check Point Custom Intelligence Feed Documentation’s Installation section for more information on product compatibility matrix.

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

After installing the hot fix, ensure that below commands are accessible on Check Point Gateway. SSH to the Gateway and login to expert mode.

```
!ge-93440b> expert
Enter expert password:
Warning! All configurations should be done through clish
You are in expert mode now.
[[Expert@ge-93440b:0]# ioc_feeds --help
External indicators configuration
positional arguments:
show, add, delete, modify
optional arguments:
  -h, --help  show this help message and exit
  --feed_name  Set feed name
  --transport  Set feed transport protocol: http, https, local_file, local_directory
  --resource  Set feed resource URL
  --state  Set feed enforcement Active / Inactive
  --feed_action  Set feed action: Prevent, Detect, Ask
  --proxy  Set feed proxy
  --proxy_user_name  Set feed proxy user name
  --user_name  Set user name for remote feed
  --test  Set test as true if feed is for testing purposes only
  --format [ \{ \} ]  Enter format in order to fetch custom csv file
  --delimiter  Enter delimiter in order to fetch custom csv file
  --comment [ \{ \} ]  Enter comment char in order to fetch custom csv file
Missing a few arguments.
[Expert@ge-93440b:0]#
```

**Supported ServiceNow versions**

Kingston and London Release versions are supported.
References
Below are some of the Check Point references which are useful in setting up the Pre-requisites.

3. To set up HTTPS Inspection on Check Point follow the link below. https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108202

Permissions and roles
The following ServiceNow roles are required.

• Administrator (admin) for installation of the integration application plugin

• Security incident administrator (sn_si.admin) for creating Block Lists in ServiceNow and approving requests for adding and deactivating Blocklist Entries.

• Security analyst (also referred to here as a SOC Analyst, sn_si.analyst) for creating and maintaining Block List Entry records.

For more information on assigning the security analyst role, on the ServiceNow documentation website, https://docs.servicenow.com/category/kingston, navigate to Security operations>Security Incident Response> Assigning security analysts.

Check Point NGTP setup
Before you can use the Check Point NGTP integration, you must create an API account, set up policies, and activate the integration.

Create an API account for the Check Point NGTP integration
An API account role is required in your Now Platform instance for this integration. The Username and Password associated with this account are created in the Now Platform and entered in Check Point, so the Check Point authenticates with the Now Platform when retrieving Block List entries.

Before you begin
Role required: admin
About this task
The Now Platform admin creates an API account role (sn_sec_checkpoint.api_account_access). This account is used exclusively for entering credentials required for authentication on Check Point, so the Gateway can retrieve Block Lists from the Now Platform. This account is a separate, unique API user account in the Now Platform instance, and assigned to the Check Point administrator.

Procedure
1. Navigate to Organization > Users.
2. Click the Users module.
3. On the Users list that is displayed, click New.

A new form is displayed.
4. Fill in the form, as needed.

**Note:** The values for User ID title, and email address shown in the following table and figure are example values.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>Unique User ID for the role in your Now Platform instance. This user ID is entered in the <strong>Username</strong> field in the <strong>Client Authentication</strong> section of the Block List Configuration Check Point gateway. An example is CKPT API account SN.</td>
</tr>
<tr>
<td>First Name</td>
<td>Person you are assigning</td>
</tr>
<tr>
<td>Last Name</td>
<td>Person you are assigning</td>
</tr>
<tr>
<td>Title</td>
<td>Job Title, for example FW admin.</td>
</tr>
<tr>
<td>Password</td>
<td>Unique password created for this role. This password is entered in the <strong>Password</strong> field in the <strong>Client Authentication</strong> section of the Block List Configuration on Check Point gateway.</td>
</tr>
<tr>
<td>Email</td>
<td>Unique email address</td>
</tr>
</tbody>
</table>

5. Click **Submit**.
   Once submitted, you can assign the role.

6. On the Users list in the User ID column, click the name of the user ID you entered, CKPTAPI account SN, for example.
7. On the open record in the Roles section, click **Edit**.

8. On the **Edit Members** form that is displayed, enter `sn_sec_checkpoint.api_account_access` in the **Collection** field.
9. In the **Collection** column, select then move `sn_sec_checkpoint.api_account_access` to the **Roles List**.

10. Click **Save**.

11. Navigate to **Users**, and in the **User** column on the list, click the ID name that you created for the role (CKPT API account SN).
12. The user record is displayed. This record verifies that the user account has been assigned.

**Set up the Check Point NGTP integration**

Complete the following steps to set up the Check Point Next Generation Threat Prevention integration. This would ensure that the pre-requisites for the integration to work are in place.

**Before you begin**
Role required: admin
Procedure

1. Verify that Threat Prevention Policy is configured with Anti-Bot and Anti-Virus Blades activated. Refer the Check Point User Guide mentioned in Reference section for detailed information on setting up Anti-Bot and Anti-Virus Blades.

   **Note:** The images in this topic are privileged and proprietary and are used with permission from Check Point Software Technologies, Ltd.

   a. Login to **Smart Console**.

   ![Smart Console Login](image1)

   b. Navigate to **Security Policies > Threat Prevention > Policy**.

   ![Smart Console Policy](image2)

   c. Open the Threat Prevention Policy in Edit Mode.

   ![Policy Edit Mode](image3)
d. Active Protections → Severity should be “Medium or above"

e. Activation Mode → High Confidence should be “Prevent"

f. Blades Activation à Anti-Virus and Anti-Bot should be selected.

g. Publish the changes (if any) and Install the Policy.

2. If not already configured, Custom Intelligence Feeds should be added after activating Anti-Bot and Anti-Virus Blades. Refer to the Installation section of Check Point Custom Intelligence Feed Feature
If not already configured, set up the Check Point Gateway to route all the internet traffic via HTTP Proxy (optional if configuring HTTPS Inspection).

**Note:** For URL blocking on Check Point NGTP, there are certain settings that need to be ensured. HTTPS internet traffic uses the SSL (Secure Sockets Layer) protocol and is encrypted to give data privacy. However, HTTPS can hide malicious traffic which should have been blocked. For Check Point Gateway to get the visibility into HTTPS traffic, either route the traffic via HTTP Proxy or setup HTTPS Inspection (recommended). This section details the steps to follow to setup HTTP Proxy on Check Point Gateway.

a. Login to *Smart Console*.

b. Navigate to *Servers and Gateways*, and double-click on the applicable server.
c. Navigate to **Network Management > Proxy**.

d. Provide the Proxy Details to be used for routing the HTTP traffic.

e. Ensure that HTTP requests from Client Endpoint are via the HTTP Proxy.

4. If not already configured, enable HTTPS inspection (optional if HTTP Proxy configured). When most of the traffic is over SSL, it is recommended to use HTTPS Inspection Blade. This makes the traffic transparent to GW. Enable HTTPS Inspection on Check Point Gateway, as follows.
a. Login to **Smart Console**.

![Smart Console Login](image)

b. Navigate to **Servers and Gateways**, and double-click on the applicable server.

c. Navigate to **HTTPS Inspection**.

![HTTPS Inspection](image)

d. Follow the steps to configure **HTTPS Inspection** in the Check Point User Guide.

**Activate the Check Point NGTP integration**

If you have not installed the application, follow the instructions to install it.

**Before you begin**

Role required: admin
Procedure

1. Log in to the instance you want to install the application on.
2. Navigate to System Applications > Applications.
3. Click the Downloads tab. A list of applications available for installation is displayed.
4. Locate the Check Point Next Generation Threat Prevention application, select it, and click Install.
   Your application is automatically installed onto your instance.

Working with block lists

The ServiceNow Check Point Next Generation Threat Prevention Integration supports Block Lists that accept IP, URL, and Domain observables.

ServiceNow configured block list is a csv file that is hosted on an external web server, which for this integration is the Now Platform instance. Custom Intelligence Feed is configured on the Check Point Gateway, which pulls the IP addresses, URLs, and domains from the Now Platform at pre-configured interval.

This integration supports three types of Block Lists:

- **IP Address** (This includes an individual IP Address (IPv4 only) for block list, and CIDR blocks (ranges) of addresses for allow list).
- **URL**
- **Domain**

Observables supported by the Check Point NGTP integration

The section lists descriptions of the observables supported by this integration and example formats for each type.

<table>
<thead>
<tr>
<th>Observable Type</th>
<th>Examples</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>• example.com</td>
<td>Wildcards are not supported.</td>
</tr>
<tr>
<td></td>
<td>• mail.example.com</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>95.153.103.54 (IPv4)</td>
<td>Represents a single, distinct interface address. The integration supports only IPv4 and CIDR formats (CIDR</td>
</tr>
<tr>
<td>Observable Type</td>
<td>Examples</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>format is only supported for allow listing purpose). For allow list purpose, integration has support for IP address observables includes CIDR (Classless Inter-Domain Routing) ranges, for example, 95.153.100.0/22.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** An error message is displayed when you try to attach a single IP address to a Block List that you have already allowed listed as a part of a CIDR range. For example, the single address 95.153.103.54 is part of the CIDR range represented by 95.153.100.0/22 (95.153.100.0-95.153.103.255).

<table>
<thead>
<tr>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
</table>
| - https://www.example.com  
- http://www.example.com | The HTTPS URL are formatted by the application to trim the path from the URL and retain the domain name only. Check Point NGTP relies on HTTP CONNECT request to evaluate the web traffic and enforce blocking. For HTTPS CONNECT request, the entire URL isn’t visible in the request and only |
<table>
<thead>
<tr>
<th>Observable Type</th>
<th>Examples</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>domain name is visible. When a user blocks any HTTPS URL with specific path (example; <a href="https://www.example.com/path">https://www.example.com/path</a>), the application trims the path automatically (<a href="http://www.example.com">www.example.com</a>). The application maintains the relationship between original observable and the formatted URL. Below is the screenshot of Block List Entry which shows the formatted URL and the original observable.</td>
</tr>
</tbody>
</table>

For HTTP URLs with a specific path (for example, http://www.example.com/path), Check Point would block the specified URL as the entire URL is visible in CONNECT request.
Create a block list for the Check Point NGTP integration

Create a Block List in your Now Platform instance. Once approved and activated, you can create entries for these Block Lists from observables determined to be malicious on Now Platform Security Incident Response (SIR) incidents and request approval to block them.

Before you begin
Role required: Security Incident Administrator (sn_si.admin)

About this task
Create the Block List on your Now Platform instance so that the Check Point can import objects — IP addresses, URLs, domains — included in the list. Custom Intelligence Feed is configured on Check Point Gateway which pulls the IP addresses, URLs, Domains from Now platform at pre-configured interval. To ensure blocking the observables, the Threat Prevention Policy should be configured with Anti-Bot and Anti-Virus Blades activated.
Note: The figures in this topic are shown with Tabbed forms cleared in System Settings.

Procedure

1. After the application installation is complete, navigate to Integrations > Integration Configurations.
2. Locate the Check Point Next Generation Threat Prevention card and click Configure.
3. Click **Create new Block List**.

4. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Check Point Block Request List name. Include the observable type (URL, IP, domain) in this field so the security analyst can easily recognize the intention of the Block List by its name. The name should also clearly indicate what firewall policy these Block List objects are mapped to. Some examples of Block List names are, Outbound Malware IP, or Outbound Phishing URL.</td>
</tr>
<tr>
<td>Active</td>
<td>This check box is cleared by default to indicate that the Block List is inactive. When inactive, the Block List is unable to receive additional entries. When the check box is selected (When Change Request is closed or change request is not generated), the Block List is activated and available for Block List entries.</td>
</tr>
<tr>
<td>Display Tag</td>
<td>Check box is selected by default to automatically tag the observable and the associated security incident record if the observable is blocked on Block List. When selected, the “Tag for observables” field is available on the form.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>A tag name is created by default from the value you enter in the Name field with a Check Point-prefix, for example, Check Point-Malware OutBound IP. You can change the tag name and color. The tag name is displayed in the field “Tag for observables”, once the Block List is saved. When the check box is cleared, no tag is created, and the “Tag for observables” field is not available on the form.</td>
</tr>
<tr>
<td><strong>Observable Type</strong></td>
<td>Select an observable type this Block List accepts from the list: IP Address (including CIDR for allow list), URL, or domain.</td>
</tr>
<tr>
<td><strong>Tag Type</strong></td>
<td>Tags that are available from the list. A Block list is a list of observables that you want the Check Point Next Generation Threat Prevention to block. A allow list is a list of observables you do not want to block in Check Point Next Generation Threat Prevention in any case. By default, the Block list tag color is black, and the allow list tag color is Gray. You can change the color.</td>
</tr>
<tr>
<td><strong>Create Change Request</strong></td>
<td>This check box is selected by default to automatically create a change request and change tasks in your Now Platform instance, which are attached to the Block List record. The change request is used to configure the Block List retrieval URL in the Check Point Next Generation firewall gateway. This option is recommended if your firewall administrator is also using the Now Platform for firewall policy or rule changes. If you create a request, once it is closed, the Block List is automatically activated. Clear the check box to manually activate the Block List after receiving notice via email from the firewall administrator that the Custom Intelligence Feed has been configured on all the Check Point Gateways. When the check box for Create change request is cleared, the Change request field is unavailable.</td>
</tr>
<tr>
<td><strong>Request Approval</strong></td>
<td>This check box is selected by default to request approvals for activating/removing Block List entries from Block Lists. Approval is requested from the users having role Security Incident</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Administrator (sn_si.admin). Approval request will be sent via email to the approvers. Once the approval is accepted, the entry will be activated on that Block List. When the check box is not selected, the entries for that Block List will not follow approval workflow and will be directly activated on block list.</td>
<td></td>
</tr>
<tr>
<td>Tag for Observable</td>
<td>This field is displayed only if the Display tag check box is selected. Field is automatically populated after the Block List is saved with a default value from the Name field. If Block List is created with name ‘Malware URL’, the tag name derived is ‘Block List – Malware URL’</td>
</tr>
<tr>
<td>Change Request</td>
<td>When the Create change request check box is selected, the change request number is displayed on the Now Platform instance once the Block List is saved. When the check box for Create change request is cleared, this field is not displayed.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the Check Point Block List. The name generally contains the types of sites and observables you would expect to be on this Block List, and you can use this field for more details.</td>
</tr>
<tr>
<td>Expiration Period (days)</td>
<td>Expiration period of the Block List. 0 (the default) indicates that the Block List entry never expires. If you change this value, this entry is active for the number of days you enter. You can enter a minimum value of 1 which is 24 hours, and there is no maximum value.</td>
</tr>
<tr>
<td>Retrieval URL</td>
<td>Retrieval URL will be generated automatically, once the Block List is saved. To configure this Block List on Check Point Gateways, you must use this URL. Once this URL is configured, Check Point fetches observables to be blocked in csv format.</td>
</tr>
</tbody>
</table>
5. Click Submit.

6. If the Check Point Block Request List is not displayed, navigate to **Check Point NGTP Integration > Block Request Lists**.

The new Block List is displayed. The Block List status is still inactive (false), which means the Block List is not available to accept entries. If Create change request was configured, a message is displayed indicating a change request and tasks have been created in your Now Platform instance.

7. In the **Name** column, click an item to open the record. The Block List record is displayed. This example shows a Malware Outbound IP Block List. The following fields, options, and links are displayed on the new record after submission and described in the following table.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Retrieval URL</td>
<td>Emails a notice that the Block Link is available for configuration to the Check Point firewall administrator.</td>
</tr>
<tr>
<td>Retrieval URL</td>
<td>This URL is used to configure Custom Intelligence Feed on Check Point Gateways.</td>
</tr>
<tr>
<td>Note:</td>
<td>If you have your System Settings set to Tabbed forms, this link is displayed on the Block List Retrieval Info tab at the bottom of the record.</td>
</tr>
<tr>
<td>Now Platform change request</td>
<td>A link to the change request record is displayed in the Change Requests section when configured, and the request number is displayed in the Change request field.</td>
</tr>
<tr>
<td>Update</td>
<td>Modify data and update the editable fields.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete the record.</td>
</tr>
</tbody>
</table>

8. Create and add more Block Lists as required. The Block Lists are displayed on the Check Point Block Request Lists Page.

**What to do next**
Activate the Block Request List manually, or with a Now Platform change request.
Activate a block list for the Check Point NGTP integration

After the Block List has been created in your Now Platform and the URL is available, the Check Point administrator configures the Block List as Custom Intelligence Feed on all the Check Point Next Generation Gateways. Before it can accept Block List entries, the Block List must be configured in Check Point and activated in the Now Platform.

Before you begin
Role required: Security Incident Administrator (sn_si.admin)

About this task
After the Block List is configured, as the security incident administrator, you can activate the Block List manually, or, the Block List is automatically activated upon completion of a Now Platform Change Request. The Change Request must be approved and moved from the inactive state to the active state before it can accept Block List entries.

Procedure
1. Navigate to Check Point NGTP Integration > Block Request Lists, and select the Block Request Lists module.

2. In the Check Point Block Request Lists list that is displayed, select your new Block List in the Name column.

3. On the record that is displayed, note the Email Retrieval URL button, the active Block List Retrieval URL link, and, if configured, the Now Platform change request in the Change Requests section. Also note that the Active check box is cleared.
4. The following figure shows the Block List Retrieval URL displayed as a tab with Tabbed forms selected in your system settings. Click the Block List Retrieval URL tab to display the retrieval URL. The link to the change request (CH0030270) is also displayed.

5. To complete the configuration and move the Block List from inactive to active, you must choose one of the following options to notify the firewall administrator that the retrieval URL is available.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click Email Retrieval URL.</td>
<td>Email Block List Retrieval URL directly to the firewall administrator. This option permits the firewall administrator to finish the configuration on the Check Point platform. Choose this option if the firewall administrator is not using the Now Platform.</td>
</tr>
<tr>
<td>Complete the Now Platform change request and assign the configuration tasks to the firewall administrator.</td>
<td>This option is available only if the firewall administrator for Check Point is also using the Now Platform, and the Now Platform change management and approval processes are configured.</td>
</tr>
</tbody>
</table>

**Note:** Users with the Security Incident Administrator (sn_si.admin) role can approve the Now Platform change request. Once the configuration tasks are completed and the change request has been closed, the Block List is activated automatically.

**What to do next**
After you notify the firewall administrator that the retrieval URL is available, and you confirm the Block List has been configured in Check Point, as the security incident administrator, your next step is to activate the Block List. You either activate the Block List manually or, if configured, use the Now Platform change request form to activate the Block List. The Block List is automatically activated when the change request is closed.

**Configure a block list as a Custom Intelligence Feed on the Check Point NGTP integration**
The firewall administrator must configure the Custom Intelligence Feed corresponding to the Block List created in NOW platform.

**Before you begin**
Role required: admin

**About this task**
This task needs to be performed on each of the Check Point NGTP Gateway. The firewall administrator would need the SSH access of the Gateway servers. If your organization has Now Platform change management and approval processes, verify that email send/receive capability is enabled.
The firewall administrator would need the retrieval URL of Block List and the ServiceNow user credentials with role Check Point API Account Access Role (sn_sec_checkpoint.api_account_access).

If Firewall administrator is not using NOW platform, the NOW Security Incident Administrator can provide the required information via an Email. Alternately, if firewall administrator is using NOW platform, the Change Request associated with Block List can be assigned to firewall administrator. This Change Request has the required information to configure Custom Intelligence Feed.

For more information on setting up Custom Intelligence Feed on Check Point Gateways, refer to: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

Procedure

1. Verify that email send/receive capability is enabled in your Now Platform instance by navigating to Email properties > Administration > Email Properties. Under Outbound Email Configuration, verify that Email sending and Email receiving are selected.

2. SSH to Check Point Gateway with expert mode.

3. Execute the command to add Custom Intelligence Feed. The command execution is interactive and prompts for feed format and password.
   - When prompted for Feed Format, enter ‘cp_csv’
   - When prompted for NOW platform user password with API Access. The command execution would warn about the server certificate (NOW platform) not being trusted by the machine and would prompt to add the server security certificate to machine’s trusted store. Enter Y. “Status:Succeed” message would appear, confirming that the Feed is successfully added.

```
[Exp:tag-93448603]# jac feeds add --feed-name phishing_url --transport https --resource https://<NOW-INSTANCE>.service-now.com/api/x_edge/check_point/retireme_block_list?feed_id=<feed_id> --user-name <now_chkpt_api_user> --feed-action Prevent
Enter Feed format. Should be cp_csv|txt|ia|ia_csv
Enter Feed Format: cp_csv
[None] cp_csv csv format files will be loaded
Enter Password
Password: <now_chkpt_api_password>
Default value for active is: true
Feed-Name: phishing_url
Feed is Active
File will be fetched via HTTPS
Location: https://<NOW-INSTANCE>.service-now.com/api/x_edge/check_point/retireme_block_list?feed_id=<feed_id>
Action: Prevent
User-Name: admin
 [==============================================================================================================] 88.8% ...Setting file from the server
This server security certificates not trusted by your machine.
SHA256 Fingerprint=SHA256 Fingerprint of the NOW instance.
Do you want to trust it for this specific feed? [ynl]: y
Fetching active feeds
Update summary
[None] feed: phishing_url, Status: Succeed
[None] activating Scheduler
[Exp:tag-93448603]
```

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Submit block list entries from a security incident for the Check Point NGTP integration

Observables attached to a security incident record are submitted for approval as Block List entries to different Block Lists. An optional approval process for Block List entries is part of the preconfigured workflow. The Gateway imports Block List entries — IP addresses, URLs, domains — that are included in Block Lists.

Before you begin
Role required:
• Security Incident Analyst (sn_si.analyst) to submit block list entries.
• Security Incident Administrator (sn_si.admin) to approve block list entries. This authority can be assigned as required by your organization.

About this task
Users with the sn_si.analyst role submit Block entries by requesting a block on observables attached to a security incident record. Once submitted, a Block List entry with a status of Pending is generated and sent for approval. The following example shows a block request for a URL observable.

Procedure
1. Navigate to Security Incident > Show All Incidents, and click a security incident record to open it.
2. Click the Show IoC related link.
3. In the Observables related list, select the observables you want to block and, from the Actions on selected rows list, select Block Request.
4. In the dialog box that is displayed, click the search icon (🔍)

5. From the list, select the Block List you want to attach this entry to.

   **Note:** For this example, the entry observable type (IP) should match the Block List observable type (IP).

6. In the Block Request dialog box with the Block List name displayed in the Implementation field, click **Block**.
7. From the list that is displayed, select the Block List you want to attach this entry to.

**Note:** For this example, the entry observable type (IP) should match the Block List observable type (IP).

8. In the Block Request dialog box with the Block List name displayed in the **Implementation** field, click **Block**.
9. Navigate to **Check Point NGTP Integration > Block Request List Entries**, and click **Block Request List Entries**.

![Check Point NGTP Integration Block Request List Entries](image)

10. In the Check Point Block Request List Entries list, click your observable in the **Entry value** column to open the record. For this example, the record for **74.125.34.95** is displayed.

![Check Point Block Request List Entry](image)

The status is Pending, the Active check box is cleared, and the work notes show that there is a request to add the observable. This Block List Entry request is ready for approval.

The icon next to the Observable field is a link to the Now Platform Observable table.

The value in the Observable field (74.125.34.95) links to the Observable table, and it matches the format that was brought over from the Security Incident Response incident-triggering event.
Submit block list entries directly from the Block List Entry Table

For observables determined to be malicious, and not associated with a specific Now Platform security incident, you submit Block List entries from the block list.

Before you begin
Role required: Security Incident Administrator (sn_si.analyst)

About this task
When you want to block an observable that you have determined is malicious or allow an observable you have determined is not malicious, and the observable is not associated with a specific Now Platform security incident record, you submit Block List entries directly from the block list. Examples of these types of Block List entries might be URLs or domains for specific sites.

Procedure
1. Navigate to Check Point NGTP Integration > Block Request Entries.

2. Click the Block Request Lists module.

3. In Check Point Block Request List Entries list, click New.

4. In the Entry value field, enter a value for your observable. The two possible outcomes of this entry:
   • The remaining fields on the form are completed automatically.
   • A matching observable is found, and a message is displayed that a matching observable exists. Select the Block List you want to attach this entry to and click Submit. Select the Block List you want to attach this entry to prior to setting the Expiration period.

A message is displayed that instructs you to complete the form. A matching observable has not been found, and you must complete the form. After you complete it, select the Block List you want to attach the observable to and click Submit. An observable record is created. The following figure shows an example of an existing domain observable and how the fields are completed automatically.
5. Click the search icon to select the Block List you want to attach the entry to.

6. Click Submit.

7. If you have email approval configured in your workflow, an approval email request is sent. If a message is displayed that requests you to fill in the rest of the information manually, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observable type</td>
<td>Observable type that is supported from the dialog.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Block List name</td>
<td>Block List you want to the entry to.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Select the Block List you want to attach the entry to prior to setting the Expiration period.</td>
</tr>
<tr>
<td>Enable override (default is selected)</td>
<td>Lookup result or source. When configured, permits you to enter a Lookup result and the source used to find the results. These fields are typically populated when a security incident record is created. In this case, there is no lookup result or source, and you fill in these fields in manually.</td>
</tr>
<tr>
<td>Lookup Result</td>
<td>Select <strong>Unknown</strong> or <strong>Malicious</strong>.</td>
</tr>
<tr>
<td>Source</td>
<td>Source that performs a threat lookup on the Block List entry, for example, ThreatCrowd, etc</td>
</tr>
<tr>
<td>Expiration period</td>
<td>The expiration period inherited from the Block List by default. You can override this value, but only during the creation of the entry. 0 indicates that the Block List entry never expires. If you change this value, this entry is active for the number of days you enter. You can enter a minimum value of 1, and there is no maximum value. For example, if you enter 30 days at 2:01 PM on May 1, the Block List entry will expire at 2:01 PM on May 31. However, scheduler checks for expired entries at 00:00 every day and changes the state of the entry to ‘expired’ at 00:00 June 1.</td>
</tr>
</tbody>
</table>

8. Click **Submit**. If you have changed the default expiration period of the Block List entry, a warning confirmation dialog box is displayed indicating that the period differs from the selected Block List.

Confirmation

Expiration period entry differs from default value configured for this Block List. Please confirm that you would like to submit this value?

<table>
<thead>
<tr>
<th>No</th>
<th>Yes</th>
</tr>
</thead>
</table>

© 2021 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Confirms your expiration override, saves the record, and returns you to the Check Point Block List Entries. If you have email approval configured in your workflow, an approval email request is sent.</td>
</tr>
</tbody>
</table>
| No     | Cancels the override. At this point, you can change the value for the **Expiration period**.
  After changing the value, click Submit to return to the Check Point Block Entries list. |

9. If not displayed, navigate to **Check Point Block Request List Entries**, and note that the status for the entry is **Pending**.

The entry is now ready for approval.

**Approve block list entries for the Check Point NGTP integration**

An approval process for Block List entries is part of the preconfigured workflow. You approve Block List entries before the entries are activated on Block Lists. After you approve the Block List entry, the Gateway retrieves the entry, and your observable is blocked from that point forward.

**Before you begin**

Role required: sn.si.admin

Approval for Block List entries is assigned to Security Incident Administrator (sn_si.admin) by default, but this authority can be assigned as required by your organization. In the following example, the Now Platform admin has approval authority.

**About this task**

When the approval process is enabled, a Block List entry is not activated or deactivated on the Block List until it is approved.
Procedure

1. Navigate to **Check Point NGTP Integration > Block Request List Entries**, and open the Block List Entry record.

2. On the Block List Entry record, scroll to the **Approval Requests** section.

3. In Approval requests, click an item in the **State** column to open it. The approval record is displayed.

4. Choose one option for approving the Block List entry.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approve</td>
<td>On the entry record, the Status field changes to Added, and the Active check box is selected.</td>
</tr>
<tr>
<td></td>
<td>The Deactivate button is displayed and active.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Work notes show that the request for the Block List entry has been approved.</td>
<td>Reject</td>
</tr>
<tr>
<td>On the entry record, the Status field changes to Rejected, and the Active check box is cleared indicating the entry is not blocked on the Gateway.</td>
<td>Work notes show that the request for the Block List entry has been rejected.</td>
</tr>
</tbody>
</table>

After you have approved the Block List entry and it is activated, the Check Point next-generation firewall retrieves the Block List entry after the next retrieval interval. After the entry is retrieved, the observable is blocked from that point forward. In the following figure, note that the Active check box is selected, the status is Added, and the work notes indicate that the request has been approved.

After the Block List entry is approved and activated, the security incident record is marked with a security tag. The tag is displayed at the top of the record.
The security tag is also displayed on the observable record.

Block list entry exceptions for the Check Point NGTP integration

There are restrictions for adding Block List entries to Block Lists. If duplicate, compatibility, or CIDR (Classless Inter-Domain Routing) conflicts exist when you try to add Block List entries to Block Lists, error messages are displayed that help you resolve these errors.

Compatibility exception

Each Block List only accepts entries that are compatible with its observable type. If you create a Domain Block List and you try to attach an IP address observable to it, an incompatible error message is displayed. For example, a domain Block List can only accept domain observables, as illustrated in the following figure.
Duplication exception
An observable cannot be activated on multiple Block Lists of the same observable type. If a URL observable is already activated on a URL Block List, and you try to activate the same observable on a Phishing URL Block List, a duplication error message is displayed.

CIDR (Classless Inter-Domain Routing) exception
If you attempt to attach a single IP address to an allow list, and this IP address is part of a CIDR observable already on a Block list/White list, a CIDR conflict error is displayed. This error indicates that the single IP address is already included on the Block list or allow list as part of the CIDR observable. For example, 192.168.24.25 is part of the CIDR block 192.168.0.0/22.
Edit the security tag name for the Check Point NGTP integration (optional)

If the Display tag check box is selected when you create the Block List record, you can edit the tag names and colors of the security tags. Security tags help you track observables that are already blocked.

Before you begin
Role required: sn.si.admin

About this task
Security tags help you quickly identify which security incidents have observables on a block list. Tags also help you identify whether an observable is already blocked, or, if it has been removed from a Block List. By default, the color of the security tag is black for block list entries and gray for allow list entries. You can change the names and colors of the tags to help you recognize certain tags more easily.

Procedure

1. Navigate to Check Point NGTP Integration > Block Request List Configuration.

2. Click an item in the Name column to open it. The Block List record is displayed.
   By default, the security tag name is the same value you entered in the Name
field of the Block List when you created it. By default, the name also includes a Block List prefix, for example, Block List – Malware Malicious URLs.

3. Click the information icon next to tag for observables then Open record.

The Security Tag Form is displayed.

4. In the Name field, modify the security tag name and click **Update**. The updated Block List record is displayed with the modified tag name. In the following example, Outbound has been added to the tag name. Keep the Check Point prefix in your new tag name to help you identify the tag is associated with the Check Point next-generation firewall integration.
The security tags are displayed for each observable type (IP, URL, Domain) on the Security Incident record and the Observable record each time that observable is added to Block List.

If an observable has already been added to a Block List, and a security tag is displayed on a security incident for this observable, the Block List security tag also is displayed automatically on any subsequent security incident records that are created. This duplication tells you that the observable is already on a block list. You do not need to add this observable and re-block it.

When an observable is no longer blocked, a security tag is not displayed on the security incident record or the observable record. In this instance, no security tag indicates that the expiration date of the observable may have passed, or the observable has been deactivated from a Block List.
Uninstall the Check Point NGTP integration

If you want to uninstall Check Point NGTP Integration from your Now Platform instance and remove all remnants from the integration, refer to the ServiceNow documentation site for instructions on uninstalling applications.

CrowdStrike Falcon Host integration

The CrowdStrike Falcon Host integration allows you to push observables in a security incident into a watchlist, making them able to generate additional alerts. This integration is an implementation of the CrowdStrike Falcon Host - Publish to Watchlist workflow.

<table>
<thead>
<tr>
<th>Explore</th>
<th>Set up</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Security Incident Response integrations</td>
<td>• Get started with the CrowdStrike Falcon Host integration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use</th>
<th>Develop</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Perform lookups on observables</td>
<td>• ServiceNow Security Operations integration development guidelines</td>
</tr>
<tr>
<td>• Publish to Watchlist activity</td>
<td>• Tips for writing integrations</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Troubleshoot and get help</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Integration troubleshooting</td>
</tr>
<tr>
<td>• Ask or answer questions in the Security Operations community</td>
</tr>
<tr>
<td>• Search the Known Error Portal for known error articles</td>
</tr>
<tr>
<td>• Contact Customer Service and Support</td>
</tr>
</tbody>
</table>

Get started with the CrowdStrike Falcon Host integration

The Integration Configuration feature allows you to quickly activate and set up third-party security integrations, including the CrowdStrike Falcon Host integration. Before you can use the CrowdStrike Falcon Host integration, you must download it from the ServiceNow Store and then add a user name and password.
Before you begin
Role required: sn_si_admin

- If you are upgrading CrowdStrike Falcon Host integration from a previous version, then you must delete the existing configuration and set up a new configuration. The new integration supports OAUTH2 authentication. This update requires you to enter the API Client ID and the API Client Secret to authenticate and complete the configuration.

- In the CrowdStrike Falcon Host portal API Scopes, enable the Read and Write setting for IOCs (Indicators of Compromise).

Procedure
1. Download the integration from the ServiceNow Store.
2. When the installation is complete, navigate to Security Operations > Integrations > Integration Configurations. The available security integrations appear as a series of cards.
3. In the CrowdStrike Falcon Host card, click Configure.
4. On the form, fill in the fields to complete the configuration:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the integration, for example, demo-1.</td>
</tr>
<tr>
<td>API Client ID</td>
<td>The client ID that you obtain from the settings section of your account profile in CrowdStrike Falcon Host portal.</td>
</tr>
<tr>
<td>API Client Secret</td>
<td>The client secret key that you obtain from the settings section of your account profile in CrowdStrike Falcon Host portal.</td>
</tr>
</tbody>
</table>

5. Click Submit.

Results
After it is configured, the CrowdStrike Falcon Host integration can be selected for publishing observables to watchlists in Security Incident Response.
Security Operations CrowdStrike Falcon Host - Publish to Watchlist workflow

The Security Operations CrowdStrike Falcon Host - Publish to Watchlist workflow is used to specify the watchlist for generating alert or events. The alerts and events are displayed in the CrowdStrike Falcon Host system based on how it is configured.

Before you begin
Role required: n_si.analyst

About this task
This workflow is triggered by the Security Operations Integration - Publish to Watchlist capability when you select one or more observables associated with a security incident, and use the Publish to Watchlist UI action to push the observables to a watchlist. The observables can then be used to generate additional alerts. For more information, see Publish observables to a third-party watchlist.

Activities specific to this integration are described here. For more information on other activities, see Common integration workflow activities.

Collect CrowdStrike Falcon Host Configurations activity

The Collect CrowdStrike Falcon Host Configurations workflow activity gathers configuration information to use in the workflow.

The Collect CrowdStrike Falcon Host Config activity can be used with any workflow to gather the CrowdStrike Falcon Host configuration settings.

Results
Possible results for this activity are:
Results

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Configuration succeeded.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to verify the configuration. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_name</td>
<td>CrowdStrike Falcon Host user name</td>
</tr>
<tr>
<td>password</td>
<td>CrowdStrike Falcon Host password</td>
</tr>
</tbody>
</table>

Publish to Watchlist activity

The Publish to Watchlist workflow activity pushes observables in a security incident into a watchlist for generating alert or events. The alerts and events are displayed in the CrowdStrike Falcon Host system based on how it is configured.

The Publish to Watchlist activity can be used with any workflow to publish observables to a watchlist.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Configuration succeeded.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to verify the configuration. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>observables</td>
<td>The list of observables from Security Incident Response.</td>
</tr>
<tr>
<td>user_name</td>
<td>The user name of the individual responsible for the CrowdStrike Falcon Host integration.</td>
</tr>
<tr>
<td>password</td>
<td>The password of the individual responsible for the CrowdStrike Falcon Host integration.</td>
</tr>
<tr>
<td>task_sys_id</td>
<td>The system identifier for this publish to watchlist job.</td>
</tr>
<tr>
<td>capabilityExecutionId</td>
<td>The name of the associated capability.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>The status of the publish activity.</td>
</tr>
</tbody>
</table>

**CrowdStrike Falcon Insight for Security Operations integration**

With the CrowdStrike Falcon Insight for Security Operations integration, you can use real-time response and network containment to perform remediation actions on the endpoints, implement profiles to gather specific details about the host, and perform specific queries or actions on the endpoint.

The integration enriches the Now Platform security incidents and provides additional insight into the scope of an incident. Since CrowdStrike captures all relevant endpoint event activity, you can use the Now Platform to focus on investigations and remediation.

**See also**

<table>
<thead>
<tr>
<th>Document identifier</th>
<th>Document title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CrowdStrike Falcon Sandbox</td>
<td>CrowdStrike Falcon Insight FAQ</td>
</tr>
<tr>
<td>ServiceNow product documentation website</td>
<td>ServiceNow Product Documentation website</td>
</tr>
</tbody>
</table>
Getting started with the CrowdStrike Falcon Insight integration

You can activate and set up the CrowdStrike Falcon Insight to interface with your Now Platform instance and Security Incident Response product.

Before you begin

Before you can use CrowdStrike Falcon Insight for the Security Operations integration, you must download it from the ServiceNow Store.

Review the following setup checklist and verify that you have completed all the tasks for a smooth integration.

Checklist

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Assign and verify the required Now Platform and Security Incident Response roles. | These roles are required for configuration and verification of the expected results:  
  - The admin role installs the integration from the ServiceNow Store and assigns the sen_si.admin role.  
  - The sn_si.admin role configures the integration, creates and activates profiles, and then assigns the sn_si.analyst role.  
  - The sn_si.analyst role responds to security incidents, launches profiles manually, and can submit requests for such actions as isolating the host and removing the host isolation for an approved group. |
| Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you configure this integration. | The ServiceNow IntegrationHub Enterprise Pack Installer [com.glide.hub.integrations.enterprise] plugin is required. This plugin enables the execution of IntegrationHub actions and flows:  
  The Security Incident Response plugin (com.snc.security_incident) is required. This plugin automatically installs all the dependencies that are required. |
### Checklist (continued)

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications that are required by the integration. Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If these applications are not already installed, you must install and activate each application one at a time in the following order to ensure a smooth installation:</td>
</tr>
</tbody>
</table>

#### Set up an approval group.

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>An optional approval capability is available for isolating host machines, restoring them to the network, and initiating sightings searches. To enable this option, you require prior approval from the sn_si.admin role before host machines are isolated and restored to your network, or when sightings searches are performed. If you require an extra level of control over these actions, enable the <strong>Require</strong></td>
</tr>
</tbody>
</table>
### Checklist (continued)

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
</table>
| approval option when configuring the profile. The approval authority is assigned to the user with the sn_si.admin role. You can also reassign this approval authority to an approval group. | **Assign and verify the CrowdStrike Falcon Platform roles.** The following roles are required on the CrowdStrike Falcon Platform for the integration configuration:  
  - The Falcon administrator role is required to view, create, or modify API clients or keys.  
  - The Real Time Responder – Administrator role is required for creating and executing custom scripts.  
  - The Real Time Responder – Active Responder role is required for creating and executing custom scripts. |
| Verify that the custom scripts roles and permissions are enabled in the CrowdStrike Falcon Platform. | This integration uses CrowdStrike’s custom scripts for few of the enrichment capabilities.  
  - Verify that the Real Time Responder – Administrator and the Real Time Responder – Active Responder roles are available.  
  - Verify that the **Default(Windows) policy** option is enabled in Configuration > Response Policies in the CrowdStrike Falcon UI.  
  - Verify that the **Real Time Response and Custom Scripts** under Real Time Functionality is enabled in the CrowdStrike Falcon UI. |
Checklist (continued)

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate API clients and keys in the CrowdStrike Falcon Platform.</td>
<td>Create the CrowdStrike API clients or keys in the CrowdStrike Falcon Platform to use in the Now Platform integration configuration.</td>
</tr>
</tbody>
</table>

Create an approval group

Create an optional approval group who can approve requests for isolating host machines, restoring them to the network, and initiating sightings search.

Before you begin

As an administrator, you can reassign the approval authority when configuring the profile. Before you can reassign the approval authority to a group, an approval group must be available on the Groups in your instance.

Note: The approvals option in the profile configuration appears only for Isolate Host and Remove Host Isolation capabilities.

Role required: admin

Procedure

1. Navigate to User Administration > Groups.
2. In the groups list, click New.
3. Enter the following details to complete creating the group:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the group that you see when you submit an approval request.</td>
</tr>
<tr>
<td>Group email</td>
<td>(Optional) Group email distribution list or the email address of the point of contact, such as the group manager.</td>
</tr>
<tr>
<td>Manager</td>
<td>(Optional) Name of the group manager. Click the search icon to view the list.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Parent</td>
<td>(Optional) Name of the parent group, if associated with a parent.</td>
</tr>
<tr>
<td>Type</td>
<td>(Optional) Define categories of groups.</td>
</tr>
<tr>
<td>Vendors</td>
<td>(Optional) Assign the vendor_manager role to users who are in your organization's vendor management process.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Additional information about the group.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.
   The new group is displayed in the Groups list.

   You have successfully created an approval group. This group is available to process requests, when you enable the **Require approval** option during the configuration of this profile.
   
   To monitor and process requests submitted by users with the sn_si.analyst role, each member of the approval group navigates to **My Approvals** in the Now Platform.

**What to do next**
The next step is to **install and configure** the CrowdStrike Falcon Insight application from the ServiceNow Store.

**Create CrowdStrike API client and generate keys**
Create the CrowdStrike API client and generate the client ID and key, which you use to configure the CrowdStrike Falcon Insight integration.

**Before you begin**
Role required: CrowdStrike Falcon administrator

**Procedure**
1. On the CrowdStrike Falcon Platform, navigate to **API Clients and Keys**.
2. In the OAuth2 API Clients table, click **Add new API client**.
3. Enter the following details to define your API client:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Name</td>
<td>Enter the client name. This is a required field.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description for the client name.</td>
</tr>
<tr>
<td>API Scopes</td>
<td>Defining the scopes is required. Enable the following API scopes:</td>
</tr>
<tr>
<td></td>
<td>• Enable Read and Write scopes for Hosts API</td>
</tr>
<tr>
<td></td>
<td>• Enable Read scope for Indicators API</td>
</tr>
</tbody>
</table>

4. Click **Add** to save the API client and generate the client ID and secret key.

**Install and configure CrowdStrike Falcon Insight**

Install and configure the CrowdStrike Falcon Insight for Security Operations application from the ServiceNow Store on your Now Platform instance.

**Before you begin**

Role required: admin

ℹ️ **Note:** You can associate a capability with only one profile. You cannot associate a capability with multiple profiles. When you configure CrowdStrike servers, you cannot reuse a CrowdStrike capability with multiple profiles that share the CrowdStrike server. Your profiles can have the same CrowdStrike capability, however each profile should use its own CrowdStrike server.

**Procedure**

1. Download the CrowdStrike Falcon Insight for Security Operations integration from the ServiceNow Store and install.

2. Navigate to **Security Operations > Integrations > Integration Configurations**.

3. Search for the CrowdStrike Falcon Insight for Security Operations integration tile, and click **Configure**.
4. On the configuration tile, select **Create new configuration** and click Submit.

5. Enter the following details to complete the configuration:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>Name for the CrowdStrike server. For example, CS server. This name identifies the server helps you distinguish the credentials, accounts, and identify each server to avoid conflicts with profiles.</td>
</tr>
<tr>
<td>CrowdStrike API URL</td>
<td>Base URL hosting the CrowdStrike API. Enter the URL with the HTTPS protocol. For example, <a href="https://api.crowdstrike.com">https://api.crowdstrike.com</a>.</td>
</tr>
<tr>
<td>Client ID</td>
<td>A unique ID for a CrowdStrike server.</td>
</tr>
<tr>
<td>Client Secret</td>
<td>A secret key for the client ID.</td>
</tr>
</tbody>
</table>

6. Click **Validate and Update**.
   After the integration is successfully validated and submitted, it is saved on the Security Integrations page as a tile. You can view the CrowdStrike Falcon Insight module in the application navigator.

**Create a capability profile for the CrowdStrike Falcon Insight integration**

Create a profile and select the CrowdStrike capabilities that you want the profile to run.
Before you begin
Consider the intention of the profile before you create profiles and add CrowdStrike capabilities to it. Refer to the following table when you create profiles.

The following table lists the capabilities that you must add to a profile when you want the profile perform certain queries or actions.

Create a single profile that runs queries for system details, lists logged in users, fetches running services, fetches running processes, fetches network stats, isolates host, and removes isolate host. Alternatively, create multiple profiles, each with its own, single capability.

**Profile types and required CrowdStrike capabilities**

<table>
<thead>
<tr>
<th>Primary purpose of the profile</th>
<th>CrowdStrike capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gather system details and logged in users</td>
<td>• Get System Details</td>
</tr>
<tr>
<td></td>
<td>• Get Logged On User</td>
</tr>
<tr>
<td>Fetch the network stats, processes, and services running for a host</td>
<td>• Get Network Stats</td>
</tr>
<tr>
<td></td>
<td>• Get Running Processes</td>
</tr>
<tr>
<td></td>
<td>• Get Running Services</td>
</tr>
<tr>
<td>Isolate a host</td>
<td>• Isolate Host</td>
</tr>
<tr>
<td>Remove isolation for a host</td>
<td>• Remove Isolation</td>
</tr>
</tbody>
</table>

Role required: sn_si.admin

**Procedure**

1. Navigate to CrowdStrike Falcon Insight Integration > CrowdStrike Capability Profiles.
2. Click New.
3. Complete the following fields to create a profile with CrowdStrike capabilities.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the CrowdStrike capability profile.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>This name helps you identify the profile type and is also the name for the security tag associated with this profile by default.</td>
<td></td>
</tr>
<tr>
<td>Source</td>
<td>Name of the CrowdStrike server. You can only view previously configured servers from the list.</td>
</tr>
<tr>
<td>CrowdStrike Capabilities</td>
<td>Capabilities of the CrowdStrike profile.</td>
</tr>
<tr>
<td>Order</td>
<td>Describes the flow priority. The value for this field indicates the order that Flows are executed when two or more profiles share triggering conditions.</td>
</tr>
<tr>
<td></td>
<td>The Flow with the lowest number has the highest priority.</td>
</tr>
<tr>
<td></td>
<td>To set the order of operation, enter a value. For example, 100, 200, 300, 400.</td>
</tr>
<tr>
<td></td>
<td>Default: 100</td>
</tr>
<tr>
<td>Active</td>
<td>Indicates that the profile is active.</td>
</tr>
<tr>
<td></td>
<td>When the profile is active, it automatically triggers when a security incident is created that matches the filtering conditions that you have specified in the configuration.</td>
</tr>
</tbody>
</table>

The following illustration shows a complete form for a profile with the Get System Details capability.
4. Click **Next** to continue to Profile Configuration.

**What to do next**
The next step is to **configure your profile**. Ensure that you have reviewed the concepts for configuring profiles and trigger conditions before you configure the profile.

**Understand how trigger conditions work with a configuration item for a profile**
Configure the profile settings so that it runs only when a set of specific conditions is met.

After you create a profile and select the CrowdStrike capabilities that you want the profile to run on, configure the profile settings so that it runs only when a set of specific conditions is met.

You can set trigger conditions so the profile runs automatically when the default field values match the Now Platform security incident. Alternatively, you can set up a profile so that it searches for specific field values on the security incident.

By default, the integration uses the Configuration Item (CI) field on the Security incident. The Configuration Item (CI) field on the Now Platform security incident is the principle value on a security incident. This value is used to match the IDs of your assets with the information stored in the Now Platform database. When a SIR security incident is created by a security event, and a profile is activated, your assets are scanned for a matching value for a host name, or an IP address based on the value of the CI field.

In an ideal case, a matching value is found in the database, and data is gathered from the CrowdStrike console for the matching asset. This is pulled
into your Now Platform instance, and displayed on the related lists of a security incident.

The following illustration shows an example of the Configuration Item field populated with a host name on a SIR security incident.

When the Configuration item (CI) field is not populated on the security incident with a host name, or an IP address that matches the database, you can select an alternate field on the security incident to display any matching CI enrichment data that you find while scanning your assets.

During the configuration step of the profile setup, you can select an alternate CI trigger field for endpoint identification to ensure that the CI enrichment data from the CrowdStrike lookup is populated on the associated security incident. You can select any field on the security incident as an alternate CI trigger field including custom fields that you create. By selecting this alternate CI field as a backup, you ensure that your profiles run even if the CI field is not populated on the associated security incident upon incident creation.
The following example shows an alternate field populated with a host name on a SIR security incident. In this illustration, the alternate field is the Description field.

Configure profiles and security incidents for the CrowdStrike Falcon Insight integration

After you create a profile and select the CrowdStrike capabilities that you want the profile to run, configure the settings so that the profile is invoked only under the defined conditions.

Before you begin

Configure the profile so that it runs only when the conditions you specify are fulfilled. Define the conditions on which security incidents automatically trigger the CrowdStrike capabilities that you selected for the profile. You can also select an alternate input field for the Configuration Item (CI) field and set filtering conditions so that only those security incidents that are related to your triggering event automatically trigger the profile.

Note: You can navigate to the Profile Configuration page only after you have entered the Profile Details. For more information, view Create a capability profile for the CrowdStrike Falcon Insight integration.

Role required: sn_si.admin

Procedure

1. Navigate to CrowdStrike Falcon Insight Integration > CrowdStrike Capability Profiles.

2. Create a new profile and click Next on the Profile Details page. The Profile Configuration page appears.
3. Review and configure the following sections:

**Define Incident Criteria (Automation)**

Define the security incident conditions that automatically trigger the CrowdStrike Falcon Insight capabilities for the profile. If you do not select the **Define Incident Criteria** option, then the capabilities are invoked manually from the Security incident.

a. Select **Define Incident Criteria** option to automatically trigger CrowdStrike capabilities.

b. In the **Filter Conditions**, select a field and its corresponding requirement to define conditions that must be met.

c. You can add **New Criteria** and also define the OR or the AND condition.

**Approvals**

Select the **Require Approval** option to provide an extra level of control when using the CrowdStrike capabilities for isolating host machines, restoring them to the network, and initiating sightings search.
The approvals option in the profile configuration appears only for **Isolate Host** and **Remove Host Isolation** capabilities.

ℹ️ **Note:** The approval authority is assigned to the user with the `sn_si.admin` role. You can also reassign this approval authority to an approval group. For more information, see [setup an approval group](#).

### Additional Configuration

When the Configuration item (CI) field is not populated on the security incident with a host name, or an IP address that matches the database, you can select an alternate field on the security incident to display any matching CI enrichment data that you find while scanning your assets. Use the additional configuration to set up the profile so that it searches for specific field values on the security incident. By default, the integration uses the Configuration Item (CI) field on the security incident.

1. Select **Define Alternative Field** option to define an alternative input field.
2. Select the input field from the **Alternate CI Trigger Field**.

ℹ️ **Note:** For more information, see [Understand how trigger conditions work with a configuration item for a profile](#).

### Tags

You can optionally tag security incidents with the CrowdStrike Falcon Insight capabilities initiated, and capabilities completed tags.

Select the **Display Tags** option to enable tagging security incidents. By default, this option is disabled for all profiles.
4. Click **Done**.

**Verify CrowdStrike Falcon Insight profile trigger conditions**

Test the profile and verify that the trigger condition filters that you have configured work as expected.

**Before you begin**

Once you activate the profile, based on the configured trigger conditions you can view the query results in the Now Platform security incidents.

Role required: sn_si.admin

**Procedure**

1. Navigate to **Security Incidents > Show All Incidents**.
2. Select **New** to create a security incident.
3. Fill in the required information and click **Save**.
4. Review the work notes and activities section. View the profile initiated and profile completed tags in the work notes section as the following snapshot illustrates.
5. Review additional details in the **CrowdStrike Falcon Insight System Details** related lists.

Manually trigger CrowdStrike Falcon Insight profile from security incident

You can manually trigger a profile after reviewing a security incident.

**Before you begin**

Once you activate the profile, based on the configured trigger conditions you can view the query results in the Now Platform security incidents.

Role required: admin

**Procedure**

1. Navigate to **Security Incidents > Show All Incidents**.
2. Select the security incident that you want to review with the CrowdStrike Falcon Insight information.
3. In the related lists section, click **CrowdStrike Falcon Insight System Details**. The **CrowdStrike Falcon Insight Profiles** dialog appears.
4. Browse and select a profile from the list of available profiles and click Submit. The selected profile is triggered manually. Review the work notes and activities section. View the profile initiated and profile completed tags in the work notes section as the following snapshot illustrates.
5. Review additional details in the CrowdStrike Falcon Insight System Details related lists.

6. Click **Update** to update the profile and return to the CrowdStrike Falcon Insight Profiles list.

**Create and configure a profile for sightings search**

Use sightings search to locate infected machines across your organization's network and address security incident response cases.

**Before you begin**
Role required: sn_si.analyst

**About this task**
As an analyst you launch sightings searches based on enrichment data from system queries. You use the queries to determine which internal systems and configuration items (CIs) in your organization may be infected with malicious files or processes.

For example, if a phishing incident is reported that contains an IP observable (Sightings search - IP), you may want to determine how many users have
opened the suspicious file. Similarly, if a Now Platform security incident is created for a malware incident that contains a malicious process (process hash), you may want to see how many hosts have this process. In both scenarios, after the file and process hash observables are determined to be malicious from the results of your enrichment queries, you launch a sightings search across the CIs and the internal systems of your network. The search helps you identify if there are additional sightings of these suspicious observables in your network.

The search capability is the only CrowdStrike capability type that a sightings search profile supports. Searches can be launched only from profiles that have the sightings search capability. During the configuration, select one server, or identify multiple servers for a search to run on. Through the sightings search profile, you connect to servers for a particular search type, specifically, a process hash or an IP. The option to connect to a single server or multiple servers in a sightings search profile permits you to determine the scope of a particular search on various components in your organization.

When multiple servers are enabled for sightings searches, a user with the sn_si.analyst role views multiple work notes and security tags, a distinct set for each CrowdStrike server that is configured in the sightings search profile. If the approval option is enabled, approvals are also required for each CrowdStrike server that is configured.

**Procedure**

1. Navigate to **CrowdStrike Falcon Insight Integration > Sightings Search Profiles**.
2. Click **New**.
3. Enter the following details to complete the configuration. Configure this profile to determine what servers to search for a specific CrowdStrike Falcon Insight search capability.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the capability profile.</td>
</tr>
</tbody>
</table>
| CrowdStrike Falcon Insight Capability | CrowdStrike sightings search capability. Select the search capability that you want for the search. Choose one of the following for a search:  
  • Sightings Search - Ip  
  • Sightings Search - Process Hash |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>The option is cleared by default to indicate that the profile is disabled. When the option is selected and the profile is enabled (activated), the sightings search is available to invoke from a Now Platform security incident. If results are returned and displayed on the Running Processes related list on the security incident from an enrichment query, you launch the search directly from the security incident. When the option is cleared and the profile is disabled, the profile is inactive and not available to invoke from a Now Platform security incident. If there are no results returned from the Running Processes enrichment query, the sightings search action is not an available option on the related security incident.</td>
</tr>
<tr>
<td>Order</td>
<td>Leave this field in its default setting.</td>
</tr>
<tr>
<td>Servers</td>
<td>Server for the profile. Select a server, or multiple servers to use for the sightings search. Select configured servers from the Available column and move them to the Selected column. Having the flexibility to choose and employ multiple servers broadens your search capability. Each server selected for the profile runs the associated search when this profile is used. By selecting more than one server, you broaden your search.</td>
</tr>
</tbody>
</table>
4. Click **Next**.

5. Enter the following details to complete the profile configuration. Configure these profile settings to define runtime parameters for the included search capabilities.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum wait time for sightings results (minutes)</td>
<td>Maximum time in minutes the search is gathering results. Default is five minutes.</td>
</tr>
<tr>
<td>Maximum sightings search results</td>
<td>Maximum search results returned for the wait time of the search that you selected in the preceding field. Default is 100 items.</td>
</tr>
<tr>
<td>Display Tag</td>
<td>Security tag. Default is selected. If the check box is selected and tagging is enabled, a security tag for</td>
</tr>
</tbody>
</table>
The associated SIR security incident record is automatically created. By default, the security tag name is the name you created for the profile, for example, *Sightings Search - Process hash*. If the check box is cleared and tagging is disabled, security tags are not displayed on the associated SIR security incident.

**Requires Approval**

Approvals. Default is disabled.

When the check box is cleared, the optional approval process for the sightings search is disabled. Verify this check box is cleared if you want to grant a user with the sn_si.analyst role permission to perform sightings searches without requesting prior permission.

Select this check box to enable the approval option if you want a user with the sn_si.analyst role to request permission prior to conducting sightings searches on your network.

After a request is submitted, only one approval is required from the group to complete the request. Any member of the approval group has approval authority. Requests are processed in *My Approvals* in the Now Platform instances of the approvers.

6. Click **Done**.

The configuration is complete and you can invoke sightings search from the Now Platform security incident.

Perform the following steps to verify the configuration and perform a sightings search.

7. Open a security incident, scroll to the bottom of the security incident, and click **Show all Related Lists**.
8. Select an item from either the CrowdStrike Falcon Insight Running Processes or Associated Observables related lists.

9. Expand the Action on rows list, and select Falcon Insight Sightings Search.

10. Select a sightings search profile and click Submit.

   If the tagging option is enabled in the Sightings Search Profile, a security tag is displayed in the SIR security incident, that the sightings search is initiated.

   If the approval option is enabled, a work note is posted that a request for approval is pending. After the request is approved, the flow for the search is launched.

11. Review the work notes section as the following snapshot illustrates.

12. You can review the sighting search results in the CrowdStrike Sightings Results and CrowdStrike Sightings Details related list tabs as the following snapshots illustrate.
CrowdStrike Falcon Sandbox for Security Operations integration

With the CrowdStrike Falcon Sandbox for Security Operations integration, you can submit files and URLs as part of the security incident response process to CrowdStrike Falcon Sandbox to perform a detailed malware and threat analysis.

The CrowdStrike Falcon Sandbox integration provides you with an on-demand, isolated virtual environment where you can perform the malware analysis and provide results to the ServiceNow security incident through the integration.

When you submit your malware incidents they are retained as part of the security incident record. You can use these records for further incident resolution and automate submission of files and URLs.

The integration supports automation of both phishing and malware response playbooks which allows your Security Operations center personnel to be more productive and efficient in responding to security incidents.

Key benefits

With this integration, you can do the following:

• Automate submission of files and URLs from user-reported phishing (URP), email messages, attachments, and other security incidents.

• Manually submit or resubmit previously analyzed files and URLs for updated analysis.

• Create multiple submission configurations that automatically apply CrowdStrike Falcon Sandbox submission parameters such as operating system, scan type, and runtime options.

• Analyze malware and threat results in an HTML formatted report within the SIR incident. You can view threat lookup results and the indicator history for files and URLs that have been analyzed multiple times.

• Tag ServiceNow incidents with the submission processing status, as well as threat finding results.

See also

<table>
<thead>
<tr>
<th>Document identifier</th>
<th>Document title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CrowdStrike Falcon Sandbox</td>
<td>CrowdStrike Falcon Sandbox FAQ</td>
</tr>
<tr>
<td>ServiceNow product documentation website</td>
<td>ServiceNow Product Documentation website</td>
</tr>
</tbody>
</table>
Get started with the CrowdStrike Falcon Sandbox integration

Activate and set up the CrowdStrike Falcon Sandbox to interface with your ServiceNow instance and Security Incident Response product.

Before you begin

Before you can use the CrowdStrike Falcon Sandbox for Security Operations integration, you must download it from the ServiceNow Store.

Role required:

- admin
- sn_si.admin

Review the following setup checklist and verify that you have completed all the tasks for a smooth CrowdStrike Falcon Sandbox integration.

Checklist

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Verify that you have assigned the required Now Platform and Security Incident Response roles. | The following roles are required for configuration and verification of the expected results:  
  - The administrator (admin) installs the sandbox integration from the ServiceNow app store and assigns the security incident administrator (sn_si.admin) role.  
  - The sn_si.admin creates and edits the configuration and global settings and then assigns the security incident analyst (sn_si.analyst) role.  
  - The security incident analyst (sn_si.analyst) responds to security incidents, such as submitting files and URLs to the sandbox and analyzing the submission results. |
| Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you configure this integration. | This integration is supported on Paris and Orlando releases. Ensure that these dependent plugins are installed. These plugins enable the execution of IntegrationHub actions and flows: |
Checklist (continued)

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• ServiceNow IntegrationHub Action Step - REST</td>
<td>(com.glide.hub.action_step.rest)</td>
</tr>
<tr>
<td>• ServiceNow IntegrationHub Runtime</td>
<td>(com.glide.hub.integration.runtime)</td>
</tr>
</tbody>
</table>

⚠️ **Note:** If you can’t find a plugin, you may have to request it from ServiceNow personnel. To request a plugin, follow the steps in Request a plugin.

The Security Incident Response plugin (com.snc.security_incident) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications that are required by the integration.

Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation.

1. Security Incident Response Dependency (com.snc.si_dep)
2. Security Integration Framework
3. Security Support Common
4. Security Support Orchestration
Checklist (continued)

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Threat Intelligence Support</td>
<td>Common (required to use the sandbox integration capabilities)</td>
</tr>
<tr>
<td>6. Trusted Security Circles</td>
<td></td>
</tr>
<tr>
<td>7. Security Operations Setup Assistant</td>
<td></td>
</tr>
<tr>
<td>8. Security Incident Response</td>
<td></td>
</tr>
<tr>
<td>For more information on setting up your Now Platform instance for the integration, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.</td>
<td></td>
</tr>
</tbody>
</table>

Verify that you are licensed for the Falcon Sandbox Private API key, and obtain the CrowdStrike Falcon Sandbox full API key.

This integration supports the Falcon Sandbox Private Cloud only.

Note: This release does not support Falcon X integration.

CrowdStrike Falcon Sandbox offers a self-signed restricted API key and an upgraded full API key. Use the full API key for this integration because it enables unrestricted access for automated submissions.

For more information, see CrowdStrike Falcon Sandbox Knowledge Base.

Procedure

1. **Download the CrowdStrike Falcon Sandbox for Security Operations integration from the ServiceNow Store.**

2. **When the installation is complete, navigate to Security Operations > Integrations > Integration Configurations.**

3. **Search for the CrowdStrike Falcon Sandbox integration tile, and click Configure.**
4. Enter the following details to complete the configuration:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Name of this integration, for example, <code>demo-1</code>. While this is a unique name to identify the sandbox configuration, you can only configure one integration per ServiceNow instance.</td>
</tr>
<tr>
<td><strong>CrowdStrike Falcon Sandbox Base URL</strong></td>
<td>Sandbox base URL. This URL is available after you configure the sandbox. For example, <code>https://servicenow.falcon-sandbox.com</code> is a base URL.</td>
</tr>
<tr>
<td><strong>API key</strong></td>
<td>Sandbox full API key.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.
After the sandbox is successfully validated and submitted, it is saved on the Security Integrations page as a tile. You can now view the Sandbox module in the application navigator.

What to do next
After you successfully complete the integration, the next step is to set up Sandbox submission configurations.

Set up Sandbox submission configurations
Set up the Sandbox configuration to define the analysis environment and runtime options for your security incident record submissions for the malware analysis.
Before you begin
Role required: sn_si.admin

About this task
Before you can submit files or URLs to the CrowdStrike Falcon Sandbox using the integration, you must configure at least one submission configuration. The submission configuration defines the Sandbox operating system, scan type, run time options, and other incident handling characteristics. You may want to create multiple configurations to use the different options that available in the CrowdStrike Falcon Sandbox environment.

Procedure
1. Navigate to CrowdStrike Falcon Sandbox > Configuration Settings.
2. Click New.

3. Complete the following fields to create a configuration for a Full Scan type.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the submission configuration. This name appears to analysts when they submit a file. It is important to ensure that the name is descriptive and easily distinguishable from the other configurations (example, Win 10 Full Scan). If the name is not unique, an error appears and duplicate configuration record names do not save.</td>
</tr>
<tr>
<td>Scan type</td>
<td>Scan type as Full. A Quick scan type provides a limited threat analysis.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Operating system</td>
<td>Analysis VM environment that the sandbox scans the file or URL in.</td>
</tr>
<tr>
<td>Active</td>
<td>Option that you select when manually submitting files or URLs.</td>
</tr>
<tr>
<td>Default configuration for automated submission</td>
<td>Option that is cleared by default. Selecting this option enables this configuration to be available for automating malware analysis submissions.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You can have only one active submission configuration as the default configuration for automated submissions.</td>
</tr>
<tr>
<td>Display tags</td>
<td>Option that is cleared by default. When you select this option, tags are displayed to provide the status of a file or URL submission. The analysis may take several minutes to process. The display tags are submission initiated, submission completed, or submission failed.</td>
</tr>
<tr>
<td>Additional runtime options</td>
<td>Option that is cleared by default. When you select this option, additional runtime parameters that Sandbox supports are available.</td>
</tr>
</tbody>
</table>
| Runtime action scripts                    | Option that enables you to use an action script that simulates human behavior and interacts with the file or URL during the analysis. 
<p>| Enable hybrid analysis                    | Option that enables you to do a unique process memory inspection. Using this option may slow down the                                                                                                          |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>analysis processing but improves behavior analysis. See CrowdStrike Falcon Sandbox documentation for more details.</td>
<td></td>
</tr>
<tr>
<td>Enable experimental anti-evasion</td>
<td>Option that enables you to improve the analysis performance for very evasive malware. Using this option may slow down the analysis processing. See CrowdStrike Falcon Sandbox documentation for more details.</td>
</tr>
<tr>
<td>Enable script logging</td>
<td>Option that provides deeper insights into the analysis of Javascript, VBA macros, and other similar scripting languages. See CrowdStrike Falcon Sandbox documentation for more details.</td>
</tr>
<tr>
<td>Allow input sample tampering</td>
<td>Option that enables sample process memory manipulation. Using this option may slow down the analysis processing. See CrowdStrike Falcon Sandbox documentation for more details.</td>
</tr>
<tr>
<td>Route network traffic via TOR</td>
<td>Option that enables you to route TCP (HTTP, HTTPS, DNS, TLS, and so on) based traffic through TOR to avoid external IP fingerprinting. See CrowdStrike Falcon Sandbox documentation for more details.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.
After you submit the configuration, it is saved on the Configuration Settings page as a record. The configuration must be **Active** to be used in sandbox submissions.

**What to do next**

After you configure sandbox submissions, the next step is to manually submit files or ULRs to Sandbox.

**Manually submit files or URLs to Sandbox**

You can manually submit a file or URL to a sandbox when certain incident criteria, such as category is phishing, are met. After reviewing the security incident and the file or URL, you can select the Submit to Sandbox option to perform a malware analysis.

**Before you begin**

Role required: sn_si.analyst

**Procedure**

1. Navigate to **Security Incident > Incidents > Show All Incidents** and open a security incident to which you want to submit a file or URL observable type record.

2. Click the **Show IoC** related link.

3. On the **Observables** tab, select a record or multiple records and click Submit to Sandbox.
4. When the File Submission filter appears, select your preferred sandbox configuration in **Submission configuration**, and click **Submit to Sandbox**.

5. (Optional) Select **Additional runtime options** if you want to provide further custom options.
After you initiate the submission, you can view the Work notes to see the status of your submission. For further information on the status of the submission or to analyze the results, view the **Sandbox Submission Results**.

**What to do next**

When you submit the observables to the sandbox for malware analysis, **view the Sandbox submission results** to take the next steps on potential threats.
Automate CrowdStrike Falcon Sandbox submissions using Flow Designer

The CrowdStrike Falcon Sandbox integration includes flow templates created using the Flow Designer that work with security incident records.

Before you begin

- Role required: sn_si.admin
- Verify that you have created a Sandbox submission configuration and have enabled one configuration as the Default configuration for automated submission. When the flow is triggered, the sandbox submission occurs on your default configuration.

About this task

These flows are primarily designed to get you started when you want to automate file or URL submissions as part of your incident response workflow. When you activate a sample flow, your phishing file attachments are automatically submitted if you define the security incidents as phishing in your sample flow. Alternatively, you can submit all .exe files when this file type is attached to an observable record.

You can modify these sample flows to trigger an automated submission under different conditions, categories, compound conditions, and so on.

The sandbox integration consists of two base system flows that are deactivated by default.

- **Submit file when category is phishing**: This flow submits a file to the sandbox for malware analysis when the security incident category is defined as phishing. You must attach a file to the observable record on the security incident. If you are using the User Reported Phishing (URP) functionality, any email attachment is automatically parsed and added to the SIR incident record as an observable record. No further action is required to automate the submission.

- **Submit when file type for observable is exe**: This flow submits a file to the sandbox for malware analysis when the security incident observable is an exe. Similar to the phishing category flow, you must attach a file to an observable record on the security incident. You can do this manually by uploading the file or automatically if a phishing email attachment, or other mechanism that is creating the incident, is associated with the observable records.

When the flows are configured and incident conditions satisfy the parameters, the sandbox submissions trigger automatically when you review the security incident. Review the Work note that indicates that a submission has been...
initiated, a tag appears if enabled in the configuration, and a pending submission results record.

The sandbox integration also contains multiple subflows. The subflows are internal components of the overall integration submission capabilities. You can customize and edit the subflows to suit your security criteria.

You can refer the subflows to troubleshoot issues with sandbox submissions. An Execution record is created every time you invoke a subflow. This record indicates where in the flow a particular error occurred and enables you to fix the problem.
Note:

- If you choose to customize the default flows, then you should verify that the Submit Observable for Automated submission subflow is included in your flow to trigger automatic submissions.
- You can customize and define your file extensions for an exe. Create a copy of the flow **Submit when file type for observable is exe**, and make changes to the copy. The content type and file extensions are mapped in the `SandboxUtils` script. To access script includes, navigate to **System Definitions > Script Includes** and search for `SandboxUtils`.

Procedure

1. Navigate to **Flow Designer > Designer > Flows**.
2. Filter the flows by the **Application** type. For example, `*crowd` filters the two CrowdStrike Falcon Sandbox flows.
3. Select a flow to view the details. The example below shows the Submit file when category is phishing flow.
4. Click **Activate** and then click **OK** when the confirmation message appears.

**What to do next**

After you configure automated submission flows, you can view the Sandbox submission results to analyze any threats.

**Monitor the submission results in the sandbox**

Results for all Sandbox submissions are shown in the **Sandbox Submission Results** tab for every security incident.

**Before you begin**

Role required: sn_si.analyst

**Procedure**

1. Open the security incident that you are working with and verify that the sandbox submission is successful.

2. Review the Work notes for more information and learn how to proceed if you can’t verify that the scan is successful.
3. Either click the complete results link in the Work notes or at the bottom of the security incident, navigate to **Show All Related Lists > Sandbox Submission Results**.

Results are displayed in the Sandbox Submission Results tab.

4. Click open any record to view the complete sandbox analysis.

5. (Optional) Click **Resubmit to Sandbox** to reprocess the observable.

**Results**

- The complete results are available as an HTML report that is attached at the top of the submission results. You can download the file to view the results. The format of this report is similar to the sandbox analysis report that you can view in the CrowdStrike Falcon Sandbox portal. This report contains all the available analysis information including related files, processes, screenshots, and artifacts that were collected as part of the sandbox analysis.
• The **Threat lookup results** tab provides the threat assessment, including malicious findings, threat scores, and additional details. These details are provided in the standard threat lookup format structure for all ServiceNow threat lookup integrations.

• The **Indicators of compromise** tab provides the malicious or suspicious sandbox results with the Confidence scores. The Confidence scores are similar to other Indicator information that is stored in the ServiceNow platform. Indicators that are classified as informational are not included in this tab but you can view them in the HTML report with the other details.

• Click **External link** to view the Sandbox HTML report in the CrowdStrike Falcon Sandbox portal.

    **Note:** This option requires that you have the CrowdStrike Falcon Sandbox role to view the results.

You can also monitor the sandbox submission results for all security incidents by navigating to **CrowdStrike Falcon Sandbox > Sandbox Submission Results**.
Tag security incidents with the Sandbox submission status

You can optionally tag security incidents with the Submission Initiated and Submission Complete tags.

When you select the **Display tags** option in the **Sandbox submission configuration**, tags are displayed to provide the status of a file or URL submission. Checking the status this way is useful because the sandbox analysis may take several minutes to process.

The display tags are called submission initiated, submission completed, and submission failed.

The following example shows a security incident where the submission has been initiated.

![Security incident with submission initiated](image)

The following example shows a security incident where the submission has been completed.

![Security incident with submission completed](image)

Review the sandbox global settings

If you experience issues with file or URL submission results, review and modify the global sandbox settings.

**Before you begin**

Role required: sn_si.admin
Procedure

1. Navigate to CrowdStrike Falcon Sandbox > Global Settings.
2. Review and modify the settings as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| File Size Limit (MB) | Sandbox upload file size limit in megabytes.  
  - **Note:** The file size limit of 100 MB is configured by default. Do not increase the value beyond 100 MB. However, you may want to reduce the maximum file size limit to avoid submitting large files. |
| Optional email notification for submission results available from CrowdStrike Falcon Sandbox | DL or email IDs that you enter to notify the sandbox submission results.  
  - **Note:** CrowdStrike Falcon Sandbox sends the notification and not the ServiceNow instance. The results may not be processed in the ServiceNow instance SIR incident. |
| Maximum time out for submission results (minutes) | Maximum timeout for submission results from the sandbox.  
  - **Note:** The default timeout is 30 minutes. If your results take longer than 30 minutes, you can increase the time. Also, you can view the results in the sandbox portal. |

3. Click Save.

**Elasticsearch Incident Enrichment integration**

The Elasticsearch - Incident Enrichment integration searches your logs and adds relevant sighting information to your security incidents.
<table>
<thead>
<tr>
<th>Explore</th>
<th>Set up</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Security Incident Response integrations</td>
<td>• Get started with the Elasticsearch - Incident Enrichment integration</td>
</tr>
<tr>
<td></td>
<td>• Create sightings search configuration records</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use</th>
<th>Develop</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Run a Sightings Search</td>
<td>• ServiceNow Security Operations integration development guidelines</td>
</tr>
<tr>
<td>• Security Operations Integration - Sightings Search workflow</td>
<td>• Tips for writing integrations</td>
</tr>
<tr>
<td>• Security Operations - Elasticsearch Sightings Search workflow</td>
<td>• Developer training</td>
</tr>
</tbody>
</table>

| Troubleshoot and get help | | |
|---------------------------|---------------------------|
| • Integration troubleshooting | • Developer documentation |
| • Ask or answer questions in the Security Operations community | • Find components installed with an application |
| • Search the Known Error Portal for known error articles | |
| • Contact Customer Service and Support | |

**Get started with the Elasticsearch - Incident Enrichment integration**

Elasticsearch is a distributed, RESTful search and analytics engine that easily integrates with Security Operations. Before you can use the Elasticsearch - Incident Enrichment integration, you must download it from the ServiceNow Store and add the appropriate API Base URL and login credentials.

**Before you begin**

Role required: sn_si_admin

**Procedure**

1. Download the integration from the ServiceNow Store.
2. When the installation is complete, access Elasticsearch and obtain the API Base URL under your Elasticsearch profile.
3. In your instance, navigate to **Security Operations > Integrations > Integration Configurations**. The available security integrations appear as a series of cards.

4. In the Elasticsearch - Incident Enrichment card, click **New**.

5. Fill in the fields, as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of this configuration.</td>
</tr>
<tr>
<td>Elasticsearch API Base URL</td>
<td>The base URL you acquired from the Elasticsearch site.</td>
</tr>
<tr>
<td>Link URL</td>
<td>[Optional] Links to a Kibana instance, when available</td>
</tr>
<tr>
<td>Username</td>
<td>Your Intel Elasticsearch username.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password</td>
<td>Your Intel Elasticsearch password.</td>
</tr>
<tr>
<td>Max Rows</td>
<td>The maximum number of rows you want to search.</td>
</tr>
<tr>
<td>Earliest Result (days)</td>
<td>The earliest results you want to see in number of days.</td>
</tr>
<tr>
<td>Include raw data samples in search results</td>
<td>Select this to include samples of raw data in your sightings search results. The amount of data returned depends on your setting in the number of rows of raw data property in Security Incident Response properties.</td>
</tr>
<tr>
<td>MID Server</td>
<td>Select Any to use any active MID Server, or select a specific MID Server name.</td>
</tr>
</tbody>
</table>

**Note:** Configuring this integration activates workflows. To manage the workflows, navigate to the **Workflow Editor**.

6. Click **Submit**.
   The integration configuration card displays.

7. When viewing the new configuration card, you can click **Configure** or **Delete** to change or delete the configuration, respectively.

8. To return to the original list of integration configuration cards, select **No** from the **Show Configurations** drop-down list.

**Have I been pwned? integration**

The Security Operations Have I been pwned? integration enables you to submit lookups on domain names and email addresses to determine whether user personal data has been compromised by data breaches.

**Explore**
- Security Incident Response integrations

**Set up**
- Security Operations Have I been pwned? integration setup
- Activate the Security Operations Have I been pwned? integration

**Use**

**Develop**
• Perform lookups on observables
• Threat Lookup - Have I been pwned? workflow

- ServiceNow Security Operations integration development guidelines
- Tips for writing integrations
- Developer training
- Developer documentation
- Find components installed with an application

<table>
<thead>
<tr>
<th>Troubleshoot and get help</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Integration troubleshooting</td>
</tr>
<tr>
<td>• Ask or answer questions in the Security Operations community</td>
</tr>
<tr>
<td>• Search the Known Error Portal for known error articles</td>
</tr>
<tr>
<td>• Contact Customer Service and Support</td>
</tr>
</tbody>
</table>

**Security Operations Have I been pwned? integration setup**

Have I been pwned? is a free resource used to assess if someone may have been put at risk due to their online account being compromised or "pwned" in a data breach. It easily integrates with Security Operations.

Before you can use the Have I been pwned? integration, you must activate the plugin. If necessary, you can also update your X509 SSL certification.

The Security Incident Response, Threat Intelligence, and Security Operations Have I been pwned? plugins are required to implement the Security Operations Have I been pwned? integration.

**Activate the Security Operations Have I been pwned? integration**

The Integration Configuration feature allows you to quickly activate and set up third-party security integrations, including the Security Operations Have I been pwned? integration. Before you can use the Have I been pwned? integration, you must download it from the ServiceNow Store.

**Before you begin**

The Threat Intelligence plugin must be installed and activated before you can use the Security Operations Have I been pwned? Integration.

Role required: sn_si_admin

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Procedure

Download the integration from the ServiceNow Store.
This integration supports an open API and does not require further configuration. Have I been pwned? can now be selected for performing lookups on observables in Threat Intelligence and on observables in security incidents.

Related information

Perform lookups on observables

Update your X.509 certificate

If you require an SSL connection for the integration, there are circumstances when the certificate provided by the third-party vendor is either not yet trusted in ServiceNow or has expired. This task is optional.

Before you begin
Role required: admin

Procedure

1. Acquire the SSL certificate from the third-party vendor. For example, you can import an X.509 Certificate (PEM) from an SSL endpoint in the Firefox browser, as follows.
   a. Enter the endpoint URL into the browser address bar. For example: https://<3rdparty>/.
   b. Click the lock icon in the address line.
   c. Click More Information and click the Security tab.
   d. Click View Certificate and click the Detail tab.
   e. Click Export to save the PEM into your local file system.
   f. Open the saved file in any text editor tool and copy the content to the clipboard. It must begin with -----BEGIN CERTIFICATE----- and end with -----END CERTIFICATE-----.
2. Navigate to System Definition > Certificates.
3. Click New and create a new record for the integration.
4. In PEM Certificate, paste in the certificate you downloaded and copied into the clipboard earlier.
5. Click Save.
   The other fields in the record are generated automatically.
Threat Lookup - Have I been pwned? workflow

The Threat Lookup - Have I been pwned? workflow performs a lookup on selected observables. If the observables are of a type recognized by Have I been pwned?, the observables are scanned for malware, and the results are returned.

About this task

This workflow is triggered by the Security Operations Integration - Threat Lookup capability when you perform a threat lookup on one or more observables, and the Have I been pwned? implementation is selected. For more information, see Perform lookups on observables.

For information on the activities used by this workflow, see Common integration workflow activities.

HPE Security ArcSight ESM - Email Parser integration

The HPE Security ArcSight ESM - Email Parser integration is supported using an email parser that consumes email notifications from ESM to create security incidents.

Configure HPE Security ArcSight ESM - Email Parser integration

HPE Security ArcSight ESM - Email Parser integration uses email notifications from ESM to drive enrichment, and response workflows.

Before you begin

Role required: sn_si_admin

About this task

An HPE Security ArcSight ESM - Email Parser template is provided to use for the integration. It must be configured and activated before the integration takes place. Updating the parser activates it.
Procedure


![HPE Security ArcSight ESM - Email Parser](image)

2. In the HPE Security ArcSight ESM - Email Parser card, click **Configure**.

3. In the **HPE Security ArcSight ESM - Email Parser Configuration** dialog box, click the **Configure Email Parser** link.

4. Click the **ArcSight ESM** link to edit the settings in the template email parser provided. At a minimum, fill in the **Email is from** field.
   
   To create your own email parser, see **Create email parsers in Security Operations**.

5. Check the **Active** box.

6. Click **Update** in the **Email Parser** form.
   
   The email parser is active. You do not need to return to **Integration Configurations**.

**HPE ArcSight Logger - Incident Enrichment integration**

The HPE ArcSight Logger - Incident Enrichment integration searches your logs and adds relevant sighting information to your security incidents.

<table>
<thead>
<tr>
<th>Explore</th>
<th>Set up</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Incident Response integrations</td>
<td>Get started with the HPE ArcSight Logger - Incident Enrichment integration</td>
</tr>
<tr>
<td>Create sightings search configuration records</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use</th>
<th>Develop</th>
</tr>
</thead>
</table>

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Get started with the HPE ArcSight Logger - Incident Enrichment integration

HPE ArcSight Logger streams real-time data and categorizes them into specific logs and easily integrates with Security Operations. Before you can use the HPE ArcSight Logger - Incident Enrichment integration, you must download it from the ServiceNow Store and add API URL and login credentials.

**Before you begin**
Role required: sn_si_admin

**Procedure**

1. Download the integration from the ServiceNow Store.

2. When the installation is complete, navigate to **Security Operations > Integrations > Integration Configurations**. The available security integrations appear as a series of cards.

3. In the HPE ArcSight Logger - Incident Enrichment card, click **New**.
4. Fill in the fields, as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of this configuration.</td>
</tr>
<tr>
<td>ArcSight Logger API URL</td>
<td>The base URL you acquired from the HPE Security ArcSight Logger site.</td>
</tr>
<tr>
<td>Link URL</td>
<td>[Optional] The Link URL that links to an HPE Security ArcSight Logger instance, when available.</td>
</tr>
<tr>
<td>Username</td>
<td>Your Intel HPE ArcSight Logger username.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password</td>
<td>Your Intel HPE ArcSight Logger password.</td>
</tr>
<tr>
<td>Earliest Result (days)</td>
<td>The earliest results you want to see in number of days.</td>
</tr>
<tr>
<td>Max Rows</td>
<td>The maximum number of rows you want to search.</td>
</tr>
<tr>
<td>All Peers</td>
<td>The default is unchecked and searches only the local logger you are connected to. When checked, it searches all the loggers that are connected to one another.</td>
</tr>
<tr>
<td>Include raw data samples in search results</td>
<td>Select this to include samples of raw data in your sightings search results. The amount of data returned depends on your setting in the <strong>number of rows of raw data</strong> property in Security Incident Response properties.</td>
</tr>
<tr>
<td>MID Server</td>
<td>Select <strong>Any</strong> to use any active MID Server, or select a specific MID Server name.</td>
</tr>
</tbody>
</table>

**Note:** Configuring this integration activates workflows. To manage the workflows, navigate to the **Workflow Editor**.

5. Click **Submit**.
   The integration configuration card displays.

6. When viewing the new configuration card, you can click **Configure** or **Delete** to change or delete the configuration, respectively.

7. To return to the original list of integration configuration cards, select **No** from the **Show Configurations** drop-down list.

**Hybrid Analysis integration**

The Hybrid Analysis application is part of an open online community in which users analyze files and URLs for threats. You share results and utilize research from the community for more effective incident responses. When integrated with the Now Platform Security Operations product, the shared threat intelligence provides you with additional insight into the severity of specific observables.

The Hybrid Analysis integration performs threat lookups on the following observables:

- File hashes
- IP addresses
- URLs
The workflow checks for new observables as they arrive in security incidents. If the observables are of a type recognized by the API integration, the observables are evaluated. Observables determined to be malicious are tagged.

This integration is compatible with the Kingston, London, Madrid, and New York releases of the Now Platform®.

**Install and configure Hybrid Analysis**

Before you run the integration on your instance, complete the installation and configuration steps so the Hybrid Analysis application properly integrates with Now Platform Security Operations.

**Before you begin**

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Verify that you have assigned the required Now Platform and Security Incident Response roles. | The following roles are required for installation, configuration, and verification of expected results:  
  • The System Administrator (admin) installs the app and assigns the Security Incident Administrator (sn_si.admin) role.  
  • The Security Incident Administrator (sn_si.admin) oversees the configuration and verifies the expected results. This role also has access to the Security Operations module and assigns the sn_si.analyst role. |
<p>| Obtain an API key and API Secret (user name and password). | Visit the Hybrid Analysis website for information on API keys and to create an account: Hybrid Analysis website. The configuration requires that you enter the API keys. |
| Verify that the ServiceNow core applications that are required to support the integration are installed | For the Madrid release and later family releases, the com.snc.si_dep plugin is required. This plugin automatically installs all the dependencies that |</p>
<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>and activated before you install the application for the integration.</td>
<td>are required to support the Security Incident Response product. Install and activate this plugin before installing and activating the other Security Operations applications. The following Security Operations applications must be installed and activated from the ServiceNow Store. Install and then activate one application at a time in the order listed below to ensure a smooth installation: 1. Security Integration Framework 2. Security Support Common 3. Security Support Orchestration 4. Security Incident Response For more information on setting up your Now Platform instance for the integration, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.</td>
</tr>
</tbody>
</table>

**Role required:** admin

**About this task**
Perform the following steps to update system properties and install and configure the integration.

**Procedure**
1. In the navigation filter, enter `sys_properties.list` and press Enter. The System Properties list is displayed.
2. Click New. A new record is displayed.
3. Fill in the fields, or select the values listed in the following table and click Submit.
<table>
<thead>
<tr>
<th>Field name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>glide.outbound.tls_sni.enabled</td>
</tr>
<tr>
<td>Type</td>
<td>Select <strong>true</strong></td>
</tr>
<tr>
<td>Value</td>
<td><strong>true</strong></td>
</tr>
</tbody>
</table>

4. If you have not installed the application for the integration, see Install a Security Operations integration and follow the steps to install it.

5. After the installation completes, navigate to Integrations > Integrations Configurations and locate the Hybrid Analysis tile.

6. Click **Configure**.
7. In the **Hybrid Analysis Configuration** dialog box, enter the API key and API user name and password (secret) you obtained from the Hybrid Analysis website and click **Submit**.

![Hybrid Analysis Configuration Dialog Box]

8. Verify successful configuration.
   Configuration is successfully completed unless an error message is displayed.

**Trouble?**
If an error message is displayed during the configuration, the Hybrid Analysis API key may be invalid.

**Verify expected results for Hybrid Analysis**
Observables are generated automatically by a security incident and scanned by the application. Locate the lookup results on the security incident to verify the threat lookup has run successfully. Also view raw data and run threat lookups on child observables.

**Before you begin**
Role required: sn_si.analyst

**Procedure**
1. Open the security incident record you are working with and verify that the lookup has run successfully.
After the application is configured, the workflow launches automatically upon incident creation. The execution and completion status of the lookup is then displayed in the work notes in the security incident.

2. Review the work notes for more information on how to proceed if you cannot verify that the lookup ran successfully.

3. Navigate to the bottom of the security incident record and click the **Show All Related Lists** related link to view results.

   <p>Note: The figures in the following steps are shown with the **Tabbed forms** setting active in the System Settings. In the upper-right corner of the banner frame, click the Settings gear icon. In the **System Settings** dialog box that is displayed, click **Forms** and verify that **Tabbed forms** and **With the Form** are selected.</p>

![Threat Lookup Results](image)

The **Threat Lookup Results** tab displays the lookup results at the bottom of the security incident record. Note the **Finding** column displays **Unknown** for records not determined to be malicious. For results matching malicious, the **Finding** column displays **Malicious**.

4. In the **Observable** column, click an observable to open the record.

![Observable](image)

For lookups matching malicious, the **Finding** field displays **Malicious**, and the observable is tagged with the Threat Intelligence source that found it to be malicious, in this case, the Hybrid Analysis integration.
5. **Optional:** Follow the steps to view raw data, view a list of child observables, and run a threat lookup on selected child observables.

   a. Navigate back to the security incident and on the **Threat Lookup Results** tab, click the blue information icon next to an observable.

   b. In the window that is displayed, click **Open Record** to view the data. From any observables viewable in the raw data that is displayed from the lookup, the Hybrid Analysis integration also creates child, or related observables.

   ![Threat Lookup Result](image)

   The link created by the API, the raw data, and other information are displayed.

   c. Navigate back to the security incident and click the **Show IoC** related link. The child observables are displayed on the **Child Observables** tab on the security incident, because the lookup has found an existing connection between these related observables and the observable initially submitted.

   d. Click the field next to an observable in the **Child** column to select it, followed by the **Run threat lookup** related link to perform a lookup.
e. In the dialog box that is displayed, verify that the Hybrid Analysis integration is selected and click **Submit**.

f. In the work notes, verify that the lookup has run successfully, and on the **Threat Lookup Results** tab in the security incident, locate lookup results for the child observables.

**Trouble?**
If you do not see results under the **Threat Lookup Results** tab, verify that the observable is a type that is supported for lookup by the integration.

**(Optional) Manually attach an observable for Hybrid Analysis**
You can manually attach observables when you want to perform threat lookups on observables that are not attached to a security incident on the initial event trigger. Also, you might perform this task when you want more information about a related observable.

**Before you begin**
Verify the observable is of a type supported by the integration. The integration performs lookups on the following types of observables:
- File hashes
- IP addresses
- URLs

Role required: sn_si.analyst

Procedure
1. Navigate to Security Incident > Incidents > Show All Incidents and open a security incident to which you want to attach the observable.
2. On the open security incident, click the Show IoC link in Related Links.
3. On the Observables tab, click New. The Observable form is displayed.
4. In the Value field, enter an observable (file hash, IP addresses, or URL).
5. Click the search icon and from the Observable Type Categories dialog box, click the desired observable type in the list to populate the field.
6. Click **Submit**. The workflow launches and checks for the new observable. The execution and completion status is displayed in the work notes section on the security incident record.

7. Navigate to your security incident and review the work notes.

8. At the bottom of the record, click the **Show All Related Lists** related link.

9. Click the **Threat Lookup Results** tab to view the results.
10. In the **Observable** column, click the blue information icon next to a given observable for more information and raw data.

11. In the dialog box that is displayed, click **Open Record** to view the raw data and more details.

12. **Optional:** Alternatively, you can also attach an existing observable to the security incident record. With the **Observables** tab selected, click **Edit.** In the **Edit Members** form that is displayed, move an existing observable from **Collection** to **Observables List** and click **Save.** You are returned to the security incident.

13. In the far left column, select the observables you want to run the lookup on, and from the **Actions on selected rows...** choice list, select **Run threat lookup.** A message is displayed across the top of the record that the request is being processed. Verify that the lookup has run successfully.

**Trouble?**
Review the work notes for more information and how to proceed if you cannot verify that the lookup ran successfully.

**IBM QRadar Offense Ingestion Integration**

The IBM QRadar Offense Ingestion integration allows you to automatically fetch IBM QRadar offenses and convert them into security incidents and enable automated response actions.

This integration supports the following:
- Discovery of IBM QRadar offenses that are candidates for security incidents.
- Fetching recent events or flows associated with an offense.
• Track key updates to offenses periodically.
• Mapping of offense, event, and flow fields to security incident fields.
• Preliminary view of the mapped fields.
• Setup scheduled ingestions of offenses to create security incidents periodically.
• Close the offenses when the security incidents are closed.

Install and configure the ServiceNow application for the IBM QRadar offense ingestion integration

Before you run the integration on your Now Platform® instance, complete these installation and configuration steps so the application properly integrates with the Security Incident Response and Security Operations products on your Now Platform instance.

Before you begin
Role required: sn_si.admin

Procedure
1. If you have not installed the IBM QRadar application from the ServiceNow Store for the integration, see Install a Security Operations integration and follow the steps to install it.

2. After you have successfully installed the application, navigate to Integrations > Integrations Configurations and locate the IBM QRadar tile.

3. To configure the application, click New.

4. Alternatively, if a Configure button is displayed on a tile, click it to edit an existing configuration.

5. In the Offense Ingestions Configuration dialog that is displayed, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the IBM QRadar console or the IBM QRadar instance used for the integration. Spaces are supported for names, but parentheses are not supported.</td>
</tr>
<tr>
<td>IBM QRadar API Base URL</td>
<td>Host URL for your IBM QRadar instance.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Note:</strong> You need to enter only the URL and the port number here. For example, <a href="https://ibm-qradar.com:8443">https://ibm-qradar.com:8443</a>. If the port number is 443, it need not be explicitly entered.</td>
<td></td>
</tr>
<tr>
<td>IBM QRadar Dashboard URL</td>
<td>The URL for the IBM QRadar dashboard or the console. This URL is used to auto construct the hyperlinks for offenses in the IBM QRadar dashboard. Enter only the host URL, for example, <a href="https://qradar.com">https://qradar.com</a>. Do not include the .jsp in the URL, for example, <a href="https://qradar.com/console/qradar/jsp/QRadar.jsp">https://qradar.com/console/qradar/jsp/QRadar.jsp</a> is an invalid format.</td>
</tr>
<tr>
<td><strong>Note:</strong> If the dashboard URL is not available, enter the IBM QRadar API Base URL here.</td>
<td></td>
</tr>
<tr>
<td>IBM QRadar API Version</td>
<td>Version 10 and above are supported.</td>
</tr>
<tr>
<td>IBM QRadar API Authorized Service Token (on premises)</td>
<td>The IBM QRadar authorized service token is used for authentication. The authorized service token must have Admin user role and Admin security profile. To generate the authorized service token, follow these steps:</td>
</tr>
<tr>
<td></td>
<td>• In the IBM QRadar console, navigate to the Admin tab and click Authorized Services.</td>
</tr>
<tr>
<td></td>
<td>• If a valid authorized service token exists, check the expiry date and use this token. If an authorized service token is not available, follow these steps:</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>IBM QRadar API Authorized Service Token (for QRoC)</td>
<td>If you are using IBM QRadar on Cloud (QRoC), use the self service application to generate the authorized service token with admin user role and admin security profile for authentication.</td>
</tr>
<tr>
<td>On Premises Deployment</td>
<td>Default is disabled. If this option is enabled, you must specify a MID Application Name. If you are using IBM QRadar on Cloud (QRoC), verify that the check box is cleared.</td>
</tr>
<tr>
<td>MID Application Name</td>
<td>Specify a MID Server Application that is set up in your environment. If you do not have a Mid Server Application configured, you must create a new MID Server application for this integration. <strong>Note:</strong> The MID Server Application can be configured only by users with system administrator role.</td>
</tr>
</tbody>
</table>

To create a new MID Server Application, follow these steps:

- Navigate to **Mid Server > Applications** and click **New**.
- Enter a name for the MID Server Application and select a MID Server to be used as the default.
- Deselect the Included in application ALL check box and click **Save**.
• Click **Edit**. In the **Edit Members** page, select all available MID Servers, move them to the MID Servers List, and click **Save**. Depending on the availability, one of the MID Servers configured with the MID Server Application will be used.

6. Enter the configuration details and specify the MID Server Application you have created.
The source that you configure on the IBM QRadar Offense Ingestion Configuration form can be reused for multiple Now Platform profiles as long as each profile ingests offenses.

7. Click **Submit**.
   After it is successfully validated and submitted, each IBM QRadar server configuration is saved on the Security Integrations page as a tile. If your saved configuration tiles are not displayed on the Security Integrations page, on the top right corner of the page, from the Show Configurations choice list, click **Yes**.

**Note:** If you encounter some issues with the IBM QRadar domain segmentation feature, contact IBM QRadar Customer Support for assistance.

**What to do next**
You have successfully installed and configured the application. The next step is to create the profile.

**Set up your Now Platform® instance for the IBM QRadar offense ingestion integration**
The following section lists the setup tasks that you are required to complete in your Now Platform® instance prior to installing the application from the ServiceNow Store.

**About this task**
Refer to the following table and verify that you have completed all the listed tasks before you download and install the application to ensure a smooth installation and configuration.
Role required: sn_si.admin

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Verify that you have assigned the required Now Platform® and Security Incident Response (SIR) roles. | The following roles are required for the installation, setup, and use of the integration in your Now Platform® instance.  
- A user with the Now Platform® administrator role (admin) installs the application from the ServiceNow Store and assigns the security incident administrator (sn_si.admin) role.  
- A user with the sn_si.admin role oversees the following tasks in the Now Platform®: |
### Setup task | Description
---|---
| | ◦ Names, creates, and edits offense profiles.  
| | ◦ Selects and maps IBM QRadar offense data fields to the security incident fields.  
| | ◦ Previews security incident details for accuracy prior to finalizing the configuration.  
| | ◦ Schedules on-going offense ingestion.  
| | ◦ Enables offense updates when a SIR incident is created and closed.  
| | ◦ Assigns the security incident analyst (sn_si.analyst) role.  
| | ◦ Users with the sn_si.analyst work with security incidents.  
| **Verify that you are using the following versions:** | **If you have access to the IBM QRadar console, you have access to the API that is required for this integration. There is no other special setup required for the API.**  
| • IBM QRadar version 7.3.2 or later.  
| • IBM QRadar API version 10 or later.  
| **Earlier versions are not supported.** | **Configured MID Server Application.**  
| | A MID Server in your Now Platform® instance is required to connect to the IBM QRadar service if the IBM QRadar server is deployed within your corporate network. See the ServiceNow Product Documentation website for information about MID Servers.  
| | If you are using the IBM QRadar Cloud service, a MID Server is not required.  

For more information about roles and assigning roles to users, see Roles on the ServiceNow Product Documentation website.
<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration. | Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation.  
1. Security Incident Response  
2. Event and Alert Ingestion for Security Operations: This application requires:  
   - com.glide.hub.integration.runtime => ServiceNow IntegrationHub Runtime  
   - com.glide.hub.action_step.rest => ServiceNow IntegrationHub Action Step - REST  
   
   **Note:** The Integration Hub components are installed along with the Event and Alert Ingestion plugin. If these are not installed, contact Customer Support for assistance.  

For more information about installing the Security Operations core applications, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application. |

**What to do next**  
You have successfully set up your Now Platform® instance for the integration. The next step is to install the IBM QRadar application from the ServiceNow Store for the integration.  

**Create a profile for IBM QRadar offense ingestion integration**  
As a user with the sn_si.admin role, you create an offense profile in your Now Platform instance and determine which offenses create security incidents. Before Now Platform Security Incident Response (SIR) security incidents are created from offenses, the field values from offenses are displayed on a layout of a Now Platform security incident so that you can preview how the actual security incident will be created.
About this task
From an integration perspective using available APIs, IBM QRadar offenses are automatically ingested into the Security Operations environment of your Now Platform instance depending on the profile type defined. The integration workflows ingest different types of offenses such as unauthorized access attempts and malware, for example. These offenses are ingested based on the profiles that you configure in the Security Operations environment of your instance. All offenses are initially ingested for a configured offense type in a profile. Ingested offenses can then be further filtered to specify which offenses create security incidents. For example, you may prefer filters that create security incidents only for offenses that are identified as high-risk. Before a profile is activated, and it creates security incidents from ingested offenses, individual field values on the offenses are mapped to corresponding fields on a layout of security incident for a preview.

Names for the offense profiles in your Now Platform instance must be unique. You can create multiple configurations for multiple sources and you can also create multiple profiles for a single source.

Create profiles for ingesting IBM QRadar offenses
You can set up a profile to ingest offenses.

Before you begin
Role required: sn_si.admin

Procedure
1. To create a profile for an offense in your Now Platform instance, navigate to IBM QRadar Integration > IBM QRadar Profile.
2. Click New.
3. Fill in the fields.
   An example of a completed form follows the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the profile. If names are not unique, an error will be displayed and duplicate profile names are not saved. Profile names in your Now Platform instance must be unique.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box is cleared by default. If this option is disabled, the profile is</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>not active and ingestion will not take place.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You should complete all sections in the profile before making it active.</td>
</tr>
<tr>
<td>Source</td>
<td>The IBM QRadar server that you configured to ingest offenses. If you have multiple IBM QRadar servers configured, select the appropriate server for the offense types that will be ingested for the profile. You are required to enter a value.</td>
</tr>
<tr>
<td>Order</td>
<td>Default is 100. If you have created multiple profiles, this value provides a run time execution priority when two or more profiles share the same triggering conditions. The workflow in the profile with the lowest number has the highest priority.</td>
</tr>
<tr>
<td>(Optional) Description</td>
<td>Additional text to help you distinguish this profile from other profiles.</td>
</tr>
</tbody>
</table>

The following figure is an example of a completed form.

What to do next
The next step is to select the offenses for ingestion.
Select offenses based on one or more IBM QRadar rules

Based on the IBM QRadar Source, select one or more IBM QRadar rules for the profile.

About this task

View the available IBM QRadar rules in your Now Platform instance so you know the active IBM QRadar rules for which you want to ingest and create security incidents.

In IBM QRadar, you can identify rules by their origin as System, Override, and User rules. By default, the origin of a rule is linked to a System rule. When you modify a System rule in IBM QRadar, its origin is set as Override.

Role required: sn_si.admin

Click the list in the IBM QRadar Rules List field. A list of active IBM QRadar rules that are present in the IBM QRadar Console is displayed. Select one or more rules from the list and move them to the Selected column. Offenses triggered by one or more of the IBM QRadar rules selected are ingested in this profile.

Rules with the same name: In the Now Platform instance, a list of active or enabled rules are displayed. If you modify an active or enabled System rule in IBM QRadar, a new Override rule is created. This results in two rules being displayed with the same name in the Now Platform. When this scenario occurs, select both the rules to ingest and create security incidents.

The following figure is an example of a completed form:

Click Continue to proceed to the next step in the wizard.

Mapping of offense fields for the IBM QRadar integration

After you have selected the rules, the next step is to map offense, event, or flow fields to the fields in the security incident form.
Overview

For the mapping step, you must first ingest sample offenses for one or more selected IBM QRadar rules. Then you must ensure that all relevant offense field data is mapped to the appropriate place on the SIR incident form and then visualize the SIR incident in the preview section.

Mapping of the sample offense fields involves the following:

• Fetching and populating of the sample data: See Ingesting the sample IBM QRadar offenses.

• Mapping the offense fields to the security incident: See Mapping IBM QRadar offense fields to security incident response fields.

Ingesting the sample IBM QRadar offenses

You can ingest sample offenses for one or more selected IBM QRadar rules.

Before you begin
Role required: sn_si.admin

Procedure

1. If the mapping form is not displayed, click Mapping on the progress bar.

2. You can either pull the three most recent sample offenses or provide the unique offense IDs for the specific offenses that you want to use for your mapping experience. From the Ingestion Preference choice list, select one of the following:
   - Retrieve most recent offenses: The three most recent offenses for the selected rules are retrieved.
   - Select offenses based on offenses ID: Specify the offense ID for the offenses to be retrieved. You can specify a maximum of 3 offense ids separated by commas.
3. Click **Fetch Sample Data** to pull the latest sample offense data from the IBM QRadar console for the selected offense rules. The offense fields and values results are displayed as individual tabs. An offense can be triggered by three types of rules:

- **Event**: In this rule, event logs are checked and if the specified criteria is met, an offense is created.
- **Flow**: Network data and traffic is checked and if certain conditions are met, an offense is created.
- **Common**: In this case, you can specify conditions for events or flows and either or both conditions are met, an offense is created.

The pull for sample offenses may take a few moments. A message indicating that the transaction is working is displayed at the top of the screen. Depending on the rule or rules that triggered the offense, along with the offense fields, the event or flow fields are populated as shown in the figure below:
Sample Offenses

<table>
<thead>
<tr>
<th>Offense Fields</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>33</td>
<td></td>
</tr>
<tr>
<td>rules(id)</td>
<td>100084, 100163</td>
<td></td>
</tr>
<tr>
<td>rules_contributing_to_offense</td>
<td>Multiple login failures</td>
<td></td>
</tr>
<tr>
<td>assigned_to</td>
<td></td>
<td></td>
</tr>
<tr>
<td>categories</td>
<td>Notice</td>
<td></td>
</tr>
<tr>
<td>category_count</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>close_time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>closing_reason_id</td>
<td></td>
<td></td>
</tr>
<tr>
<td>closing_user</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event Fields</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>category</td>
<td>8053</td>
<td></td>
</tr>
<tr>
<td>categoryname</td>
<td>Notice</td>
<td></td>
</tr>
<tr>
<td>destinationip</td>
<td>127.0.0.1</td>
<td></td>
</tr>
<tr>
<td>destinationport</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eventcount</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>eventdescription</td>
<td>Automatic updates successfully downloaded. See the...</td>
<td></td>
</tr>
<tr>
<td>eventname</td>
<td>Auto Update successful download</td>
<td></td>
</tr>
<tr>
<td>identifier</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>logsource</td>
<td>System Notification-2 :: ip-172.10.2-57</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1. **Note:** The event or flow fields displayed belong to the first event or flow field that triggered the offense based on the corresponding event or flow rule.

4. The following are custom offense fields created for this integration. Standard offenses fields in addition to these custom fields are available for mapping.
   - **rules_contributing_to_offense:** IBM QRadar rules that contributed to the offense based on the Rule ID.
   - **users:** User names for the offense.
   - **remote_destination_ip:** The remote destination IPs for the offense. Based on the local destination IDs for the offense, the following custom local destination address fields are available:
     - **local_destination_address (domain_id)**
     - **local_destination_address (event_flow_count)**
     - **local_destination_address (first_event_flow_seen)**
     - **local_destination_address (id)**
     - **local_destination_address (last_event_flow_seen)**
     - **local_destination_address (local_destination_address_ids)**
     - **local_destination_address (magnitude)**
     - **local_destination_address (network)**
     - **local_destination_address (offense_ids)**
     - **local_destination_address (local_destination_ip)**
   - The following source addresses are available based on the source IDs of the offense:
     - **source_addresses (domain_id)**
     - **source_addresses (event_flow_count)**
     - **source_addresses (first_event_flow_seen)**
     - **source_addresses (id)**
     - **source_addresses (last_event_flow_seen)**
     - **source_addresses (source_address_ids)**
     - **source_addresses (magnitude)**
     - **source_addresses (network)**
     - **source_addresses (offense_ids)**
     - **source_addresses (source_ip)**
• Select the **Fetch additional event and flow fields (Optional)** check box. You can fetch sample event and flow data from any active, valid custom event and flow fields. Specify the custom fields separated by commas as shown below:

![Offense Ingestion Settings](image)

- Ingestion Preference
- Retrieve most recent offenses
- Check box: Fetch additional event and flow fields (optional)
- Event Fields
  - sourcemac,File Hash,File Path,Filename,URL,Policy
- Flow Fields
  - Enter flow field names separated by commas
- Fetch Sample Data

• Click **Fetch Sample Data**. The specified event or flow fields along with their values (if available) are appended to the Event or Flow section as shown below:
After you fetch the sample data, the corresponding values for these fields are populated on the left side of the form.
What to do next
After you have fetched the sample data, the next step is to map the offense fields to the security incident.

Mapping IBM QRadar offense fields to security incident response fields
Map individual offense, event, and flow fields to fields on a Now Platform SIR security incident.

Offense field mapping
As a user with the sn_si.admin role, use the fields from the Sample Offenses section on the left and map them to the security incident fields in the SIR Incident Field Mapping column. Edit the mapping configuration by dragging offense, event, or flow fields from the left side and dropping them on the ServiceNow SIR incident mapping section on the right. The mapping on the right associates the incoming offense field with an outgoing security incident field.

1. After you have fetched the sample data, the next step is map the offense, event, or flow fields to the security incident. To map a field value from the left side of the form to a field on the security incident on the right side of the form, click-hold a blue field name on the left side of the form.
2. Drag the field name, for example, `description`, and drop it on a field in the Input Expression column next to a field name in the Security Incident column. The field value is displayed in the Input Expression column. In the following image, `description` is mapped to the Description field on the security incident.

**Note:** If you enter the event or flow field name manually in the Input Expression section, you must add a prefix as `{Event:eventfield}` or `{Flow:flowfield}` before the name of the field being mapped.
To help you ensure that no offense, event, or flow fields are overlooked or duplicated in the mapping process, fields are color-coded. Color-coding of the offense fields helps you keep track of the offense values that you have already mapped as they become greyed out while all remaining unmapped fields appear in blue. This helps you better visualize which field values have been added to the security incident and if any remaining important offense information remains unmapped.

Light blue fields on the left indicate that an offense field is not yet selected and mapped on the security incident. You may prefer to associate an incoming offense, event, or flow field with more than one field on a security incident. A gray field indicates that a field has been selected and mapped to a field on the security incident. This color-coding helps you track the mapping.

3. To add fields to the default fields displayed on the security incident on the right side of the form, follow these steps:
   
a. On the right of the form in the SIR Incident Field Mapping section, at the bottom of the grid, click the plus (+) icon. A new field is displayed.

b. In the Security Incident column, expand the choice list that is displayed, and select a field.

In the expanded choice list for the new field, some fields are shaded. In the following figure, Category has a gray background, because it has been mapped in the security incident. Similar to the color-coding for the offense fields on the left side of the form, this color-coding for the security incident fields on the right helps you track the already mapped SIR incident fields.
Note: As multiple observables can be displayed on the same security incident, the Observable field can be mapped multiple times with different values. Similarly, the Configuration Item and Work notes fields support multiple values. If you try to map two values to a field that cannot support multiple values, when you preview the incident, an error message is displayed that there is no value for the field. Similarly, if a field on a security incident has a choice list from which you can choose multiple options, and you try to map an option to that field that is not displayed on the choice list, the field is not populated on the security incident.

c. Alternatively, type a value in the Search field for the new row.

d. From the left side of the form, select the offense field and drag-and-drop it to an appropriate security incident field on the right.

4. Remove fields by using the - icon next to the field name in the SIR incident field mapping section.

5. Continue mapping by adding or removing field values to the mapping.

Offense fields with multiple values

- Security incident fields such as Category and User fields, (for example, Affected user, Assigned to) available with the base product do not support multiple values.

- The following IBM QRadar fields support multiple values:
  - categories
  - destination_networks
  - source_address_ids
  - local_destination_address_ids
  - remote_destination_ips
  - rules_contributing_to_offense
  - users

If you need to map the above fields to any Security Incident Response fields apart from CI and Observable type fields, you must create new Security Incident Response fields of type List and use them for mapping.

Note: By default, only non-reference List type fields are supported.

Format Field Translation
In certain cases, offense field values in IBM QRadar may not translate directly to the fields on the SIR security incident. For these values, you can use a script editor to format field values on the security incident during the mapping step. Use the script editor if you want to format values that are similar, but not identical. For example, with the script editor, a category value of Malware Alert and Virus Infection may have different field values for the source category but both values can be translated to a common Malicious Code Activity in the Category field on the SIR security incident using the Format Field Translation functionality.

To use the script editor, click the . The script editor is displayed.

Enter any changes to the script and click Update to save the changes and return to the Mapping page.

**Incident generation conditions**

Once the mapping section is complete, you can set filter conditions so that you can specify which offenses should create security incidents versus which offenses should be filtered out, for example, low priority offenses. You can use the same field values in the Incident Generation Conditions builder to define additional criteria that an incoming offense must satisfy to create a security incident. To set incident generation conditions, follow these steps.

1. Scroll to the **Incident Generation Conditions** section on the form and select the **Filter based on conditions** check box to enable the option.

   The Filter conditions builder is displayed. Use these filters to create security incidents that match the specific conditions described by the fields.

   The options in the choice lists for the first field in the Filter conditions builder match the fields that are displayed on the Sample QRadar Offense Ingestion section for the offenses you ingested. These fields are dynamic and change
depending on the offenses that you ingest. Criteria that you enter are case-sensitive, and they must match exactly the values of the IBM QRadar offense. If you are not sure about the values to enter in the filter fields, you may prefer to return to your IBM QRadar console and review your offenses for the keywords.

**Note:** The categories, destination_networks, source_address_ids, local_destination_address_ids, remote_destination_ips, rules_contributing_to_offense, and users offense fields can have multiple values (as the values are stored in arrays). As the filter condition can retrieve only strings, you must use the contains filter condition for these fields to ensure that the data is filtered correctly.

2. Using the choice lists and fields of the conditions builder, set filters for the first row.

3. To add more conditions, to the right of the fields, click **AND** or **OR**.
   - If **AND** is selected, all conditions must be matched.
   - If **OR** is selected, either condition can be matched.

4. (Optional) In the second row, set a second filter condition.
   The following image is an example with two conditions that must be matched before security incidents are created.

![Incident Generation Conditions](image)

You have set the incident generation conditions so that security incidents are created only when both of the filtering conditions that you entered are matched.

This type of incident generation condition filtering helps you narrow down the offenses, and limit the number of unnecessary security incidents that you create without modifying the underlying rule or filters in IBM QRadar. If
additional filtering criteria are set, only offenses that match all criteria are mapped to incidents.

Note: If any of the offense field names have special characters such as quotes ("), hyphens (-), or ampersands (@), these characters may need to be replaced for filtering purposes but a numerical suffix is appended to differentiate fields with duplicate offense names. For example, if the first offense field is alerts.alert and the second offense field is alerts@alerts, these fields cannot be uniquely identified as the remaining standard text characters are the same. In this case, a suffix is added to the second offense field and the field is renamed to alerts@alert(1) when displayed in the Filter Conditions list.

Offense aggregation criteria to handle similar offenses and prevent duplicate incidents
Define additional offense aggregation criteria that aggregates an incoming offense to an existing SIR security incident instead of creating similar, potentially duplicate incidents. Using field matching value criteria for each profile, this additional aggregation capability can reduce the number of active, overlapping security incidents by placing all related offense data on a single security incident. To set the criteria, follow these steps below:

1. Scroll to the Offense Aggregation Criteria section on the form and select the Aggregation Conditions check box to enable this option.

   The Incident Field Matching Values columns are displayed. These field names are the fields on the security incident that include any custom fields that are configured on the SIR security incident.

2. From the Available list, select the field values that you want to match on existing security incidents in your Now Platform and move them to the Selected list.

   All the field values that you select must be matched to append this incoming alert to an existing security incident. This includes fields, such as Observables and Configuration Items, that may have multiple offense field values mapped to them. All values must match. If only a subset of the values are matched, the offense aggregation conditions will not be met and a new security incident will be created. See screen shot below for multi-value field mapping.
If a new offense matches all the values that are selected in the aggregation field conditions in the mapping step, the new offense is automatically added to the most recently opened security incident with the same field values. As a user with the sn_si.analyst role working with security incidents, you can view all the added aggregated offenses on a related list on a security incident. This list details associated time stamps and aggregated field values. This information helps you understand why these offenses are being aggregated to existing security incidents. If this tab is not displayed, scroll to the left side of the record under Related Links and click the Show All Related Lists link.

3. (Optional) To log a work note for a new offense that is recently added on the security incident, select the check box to enable this option. The work note logs that a new offense has been added along with a link to the offense details and any other details that may have been added to the work note field in your mapping section.

You have successfully mapped values from an IBM QRadar offense to fields on a security incident. Also, you have configured additional conditions to limit the creation of security incidents with incident generation filtering criteria. You also appended offenses to existing security incidents when offense field values match the configured aggregation criteria.

4. Click Continue to continue with the profile configuration. The next step is to preview the fields you mapped on a SIR security incident

Preview the security incident for the IBM QRadar integration

After you complete the mapping step, preview the values that you mapped in a SIR security incident. This preview step permits you to verify that you have mapped all the offense fields that you want displayed on the security incident.
About this task
As a user with the sn_si.admin role, preview a security incident and edit the mapping again as required to fix fields with errors or to populate any missing data. If the preview is not successfully completed, you cannot proceed to the scheduling step. Previews of SIR security incidents are not saved as actual incidents in the Security Incident Response product.

Role required: sn_si.admin

Procedure
1. If the security incident preview is not displayed, click Preview in the progress bar.
2. From the Sample Offense IDs choice list, select an item. The security incident is displayed. This view is a read-only view, and a record of this security incident is not saved.
3. Review the field mapping of the offense values on the security incident.

The preceding image is an example of a preview with a mapping error of the samples that were ingested.

4. To resolve this error, click Mapping in the progress bar.
5. Edit the mapping to fix incorrect values or populate any missing data.
6. Preview the mapping again and continue to fix any errors that are described in error messages.

What to do next
If no error messages are displayed, and you are satisfied with the field mapping on the security incident, the next step is to define the schedule.

Define schedule for the IBM QRadar integration
You can define the schedule for the offense ingestion. During this step, you can verify the default settings for the offense retrieval or modify the scheduling as needed. This step also permits you to retrieve historical offenses using a date range.

About this task
You can choose whether you want to ingest any historical offenses during the Scheduling step. You also choose how often you will poll for future new offenses and updated offenses that match the profile configuration.

As a user with the sn_si.admin role, you configure these polling intervals on a per-profile basis. The performance of the IBM QRadar offense ingestion integration may be impacted by the different polling intervals. When scheduling, you may prefer to balance reducing polling overhead on the IBM QRadar server against a desire to be notified as soon as possible when an offense is created or updated. A five-minute default value is set for any profile, but you may prefer to modify this setting to as low as one minute if required.

Pulling new and updated offenses
When the polling schedule is set, the scheduled job pulls both new and updated offenses that were pulled previously but did not meet the incident filtering criteria. This provides you with the flexibility to create incidents based on criteria that may not be present when a offense is first created but becomes available after an update occurs, for example, during the investigation phase. Once an incident is created for a specific offense, its subsequent updates are ignored since it is expected that the offense is now being treated as an active ServiceNow security incident. However, all other offenses that have been previously ingested but failed to meet the incident generation criteria, will continue to be pulled and checked against the incident generation criteria until they become part of an active incident.
Procedure

1. If the Scheduling page on the progress bar is not displayed, select **Scheduling**.
2. Choose one to schedule how and when offenses are pulled from the IBM QRadar console.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>• Ongoing offense ingestion field selected</strong></td>
<td>On-going Offense</td>
</tr>
<tr>
<td></td>
<td>Based on the default setting, the Now Platform instance pulls from the IBM QRadar server for new and updated offenses every five minutes. Security incidents are created if offenses are found and incident generation filtering criteria are matched. To balance ingestion polling overhead desire to get the most current data, five minutes is the default setting. However, this value can be modified to as low as one minute if needed.</td>
</tr>
<tr>
<td><strong>• Ongoing offense ingestion selected</strong></td>
<td>Initial ingestion time</td>
</tr>
<tr>
<td><strong>• Set initial offense ingestion time</strong></td>
<td>If you want to schedule the initial ingestion at a specific time, follow these steps:</td>
</tr>
<tr>
<td></td>
<td>• Select the Ongoing offense ingestion and Set initial offense ingestion time fields.</td>
</tr>
<tr>
<td></td>
<td>• Specify the time in the Input initial offense ingestion time field.</td>
</tr>
<tr>
<td></td>
<td>The initial ingestion will take place at the time specified here. Subsequent ingestions will be based on the schedule defined in the Polling increment (minutes) field.</td>
</tr>
<tr>
<td></td>
<td>As an example for scheduling an initial offense ingestion time, if you have a daily IBM QRadar security check that runs once a day at 4 AM local time, you can set up the corresponding offense profile in your Now Plat-</td>
</tr>
</tbody>
</table>
Option | Description
---|---
form instance to run at 4:05 AM local time to capture the security failure right away and create a security incident.

Enter `<date> 04 05 00` in the **Initial offense ingestion** field. In the **Polling increment (Minutes)** field, enter `<date> 1440` (24 hours) to schedule the next offense ingestion for 24 hours from the initial offense ingestion. Both the initial offense ingestion time and next offense ingestion time are displayed in the fields.

The initial ingestion will take place at 4:05 am. The subsequent ingestions will be based on the polling interval. In this case, since the Polling increment is 24 hours, the next ingestion will take place on the next day at 4:05 am.

- **One Time Retrieval field selected**

**One-Time Retrieval**

Use this configuration if you want a one-time pull to ingest historical offenses.

When this setting is configured, a profile is used once to retrieve offenses from historical events that are based on a date range. To the right of the **Since date** field, click the calendar icon. In the calendar that is displayed, select the date that you want to start pulling offenses. Starting with the **Since date** value, offenses are retrieved up through the current date. Note that you can pull as far back as seven days from the current date. This functionality is not intended to retrieve significant amounts of historical offenses from IBM QRadar for archival reasons but rather a minimal
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>amount of in-flight offenses that are being actively worked at the time of profile activation.</td>
</tr>
<tr>
<td></td>
<td>After the offenses are pulled, this setting will not retrieve more offenses for this profile going forward from the current date. This setting populates the security incident with all the offenses that are found for the range you enter.</td>
</tr>
</tbody>
</table>

3. Click **Continue** to navigate to the Additional Options page.

**Automate offense updates and closure based on SIR incident status**

The IBM QRadar integration has a bi-directional interface that allows for both offenses to create security incidents, as well as an ability to update the offenses once the security incident is created and/or closed with relevant incident details such as security incident number, assignment group, security incident URL, and so on.

**Before you begin**

Role required: sn_si.admin
Procedure

1. If the Additional Options page on the progress bar is not displayed, select **Additional Options**.

2. Follow the instructions below to complete the configuration for updating offenses when the security incident is created:

<table>
<thead>
<tr>
<th>Option or Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Update Offenses upon SIR Incident Creation</strong></td>
<td>Select this option if you want to update the offense status and add additional comments when a security incident is created from the offense. This can occur for both the initial triggering offenses that create the security incident, as well as aggregated offenses.</td>
</tr>
<tr>
<td><strong>Initial Offense Status Update</strong></td>
<td>You can select:</td>
</tr>
<tr>
<td></td>
<td>• Open: The status of the offense is set to <strong>Open</strong> and a comment is added indicating that a security incident has been created for the offense.</td>
</tr>
<tr>
<td></td>
<td>• Hidden: The status of the offense is set to <strong>Hidden</strong> and this offense is hidden in the IBM QRadar dashboard.</td>
</tr>
<tr>
<td><strong>Initial Comments posted back to Offense</strong></td>
<td>Based on the stage you have selected, the initial comments as defined in the IBM QRadar console are displayed here.</td>
</tr>
<tr>
<td><strong>Close out offenses upon SIR Incident Closure</strong></td>
<td>Select this option if you want to use the automated offense closure option. When the security incident is closed in ServiceNow with a relevant close code, the offense status is updated in IBM QRadar to <strong>Closed</strong> with closure comments.</td>
</tr>
<tr>
<td>Option or Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Note:</strong> The close code specified for the security incident must correspond to the closing reason specified in the IBM QRadar dashboard. The offense is closed in IBM QRadar only if a corresponding closing reason is found. If a corresponding reason is not found, the offense is closed with a default close code.</td>
<td></td>
</tr>
<tr>
<td><strong>Closure Comments Posted back to Offense</strong></td>
<td>The closure comments as defined in the IBM QRadar dashboard are displayed here.</td>
</tr>
<tr>
<td><strong>Default closing reason when security incident closes</strong></td>
<td>The default reason to be used when a security incident is closed. When a security incident is closed, a close code (or the reason for closing) is specified in the security incident record. If the close code does not match the closing reason specified in the IBM QRadar dashboard, and you try to close the security incident, an error message is displayed. In such cases, the default closing reason specified here is used when the security incident is closed.</td>
</tr>
</tbody>
</table>
3. Click **Finish** to complete the configuration and move the profile to the **Waiting** state.

   A confirmation dialog is displayed. You have successfully completed the setup and configuration for the integration. Activate this profile to pull offenses from the IBM QRadar console based on your scheduling.

**IBM QRadar integration configuration settings**

Use this option to modify the IBM QRadar ingestion integration default system properties.

To modify the system properties, log in as a user with the `sn_si.admin` role and navigate to **IBM QRadar Integration > IBM QRadar Integration Settings**.

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce a limit on number of security incidents that can be created in 24 hour period.</td>
<td>Specifies the maximum number of security incidents that can be created in 24 hours.</td>
</tr>
<tr>
<td><code>sn_sec_qradar.max_si_per_day</code></td>
<td><strong>Type</strong>: integer</td>
</tr>
<tr>
<td></td>
<td><strong>Default value</strong>: 1000</td>
</tr>
</tbody>
</table>
IBM QRadar Integration Settings (continued)

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enforce a limit on number of offenses that can be aggregated to a single incident. sn_sec_qradar.max_aggregation_per_si | The offense aggregation limit for a security incident. For example, if there are 102 offenses, the first 100 offense are aggregated to security incident_1 and the remaining 2 to security incident_2.  
**Type:** integer  
**Default value:** 100 |
| This property sets the time period of AQL to fetch recent event/flows for a particular offense. sn_sec_qradar.on_demand_recent_days_limit | Specifies the number of days to fetch recent events or flows for a particular offense.  
**Type:** integer  
**Default value:** 7 |
| This property limits the number of recent events fetched for a particular offense. sn_sec_qradar.on_demand_event_limit | Specifies the number of events that are retrieved for an offense. The most recent events are retrieved first based on the event timestamp.  
**Type:** integer  
**Default value:** 100 |
| This property limits the number of recent flows fetched for a particular offense. sn_sec_qradar.on_demand_flow_limit | Specifies the number of flows that are retrieved for an offense. The most recent flows are retrieved first based on the flow timestamp.  
**Type:** integer  
**Default value:** 100 |
| This property sets the timeout value(seconds) for the AQL which fetches recent flows/events for a particular offense. sn_sec_qradar.on_demand_timeout |  
**Type:** integer  
**Default value:** 300 |
<p>| Search IDs timeout(seconds) for records in queue for polling AQLs of an offense. | The AQL's time out for an offense in the queue before creating a security incident. For example, if there are |</p>
<table>
<thead>
<tr>
<th>Property Name</th>
<th>Description</th>
<th>Type</th>
<th>Default value</th>
</tr>
</thead>
</table>
| `sn_sec_qradar.sid_ttl`                                                      | 90 offenses, the first 50 offenses are processed for AQL data in the first batch, and the remaining 40 offenses in the subsequent batch in the same polling interval. | **Type:** integer  
**Default value:** 300 |               |
| Threshold to control the number of searches that can be running in IBM QRadar at a time which is triggered by the integration scheduled job. |                                                                                                                                                                                                                                                              | **Type:** integer  
**Default value:** 50 |               |
| `sn_sec_qradar.records_threshold_in_queue_for_aql`                           | Specifies the number of offenses that you fetch in a single batch in a polling interval.                                                                                                                                                                       |           |               |
| This is the number of days for integration tables clean up.                  | The following are the integration tables:                                                                                                                                                                                                               |           |               |
| `sn_sec_qradar.queue_item_expire`                                            | • `sn_sec_qradar_events` - IBM QRadar Events  
• `sn_sec_qradar_flows` - IBM QRadar Flows  
• `sn_sec_qradar_offense_updates` - IBM QRadar Offense Updates  
• `sn_sec_qradar_offense_to_task` - IBM QRadar Offense to Task | **Type:** integer  
**Default value:** 30 |               |
| Offense limit per scheduled job runs per profile either in one-time retrieval or on-going ingestion. | Specifies the number of offenses that you fetch into the Now Platform in a single retrieval.                                                                                                                                                                  | **Type:** integer  
**Default value:** 1000 |               |
| `sn_sec_qradar.max_offense_limit_per_run`                                    |                                                                                                                                                                                                                                                              |           |               |
| Set this property to activate the Offense Updates feature.                  | **Note:** Enabling this setting may cause a delay in creating a security incident.                                                                                                                                                                          |           |               |
| `sn_sec_qradar.get_offense_updates`                                         |                                                                                                                                                                                                                                                              |           |               |
IBM QRadar Integration Settings (continued)

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type:</strong> true</td>
<td>false</td>
</tr>
<tr>
<td><strong>Default value:</strong> false</td>
<td></td>
</tr>
</tbody>
</table>

Any modified integration settings will be applied during the next polling interval as defined in the profile.

Optional: Copy a IBM QRadar profile

Copy an existing profile and its associated settings instead of creating new profiles. If you are creating multiple profiles, and you want to reuse the settings of an existing profile, you may prefer to copy profiles to save time.

Before you begin
Role required: sn_si.admin

About this task
As a user with the sn_si.admin role, if you copy a profile, the profile name is initially modified to avoid duplicate profiles. In addition, the copied profile is disabled (false) so it is not activated accidentally prior to completing the configuration. Copy profiles and use existing maps for security incidents that you have already previewed and verified.

Procedure
1. Navigate to IBM QRadar Integration > IBM QRadar Profile.
2. In the IBM QRadar Profiles list that is displayed, select a profile that you want to copy, and, from the Actions on selected rows choice list, click **Copy**.
The profile is copied and displayed on the list. The copy has all the settings of the original profile including the mapping and scheduling configuration. The name of the profile contains copy. Although the original profile is enabled (true), the copy is disabled at this point (false). You may prefer to edit values of the copied profile and rename it so the configuration settings apply to the new profile as required.

**Note:** If you select a different source for the profile, you must select new rules (Select offenses based on one or more IBM QRadar rules) for the profile. But if you use the same source and select new rules, the sample offenses will be cleared.

You have successfully copied the settings from an existing profile to a new profile. Note that the **Active** column status is set to false as the profile needs to be activated.

**What to do next**
You are prompted to activate (enable) the new profile after you complete the configuration steps.

**Domain separation and IBM QRadar Offense Ingestion**
This section provides information on domain separation support with IBM QRadar offense ingestion.

Follow these steps to achieve domain separation:

- **Create a user with the sn_si.admin role in the respective domain.**

  **Note:** When you create the profile, use the domain picker to select the specific domain. Do not create the user in the parent domain and later change the domain of the profile. You should have a specific user for each domain for your profile with the sn_si.admin role. Use this user to create or modify settings in the profile.

- **Disable existing scheduled jobs.**
• Replicate the IBM QRadar Process Polling Queue, the IBM QRadar Process Profiles, and the Offense Updates scheduled jobs for every domain.

• Change the **Run as** from the system user to the user with the `sn_si.admin` role in the respective domain and run the scheduled job.

---

**Security Incident Response form after offense ingestion**

After an IBM QRadar offense has been ingested, a security incident is created and the corresponding updates are made to the security incident record.

**Worknotes**

A worknote is posted with details of the offense that triggered the security incident.
Click the offense link to navigate to the internal security incident record. The **Click here** hyperlink takes you to the IBM QRadar dashboard where you can view the offense details.

If you had selected the **Log work note for new offense** option in the Offense Aggregation Criteria as described in the [Mapping IBM QRadar offense fields to security incident response fields](#), a worknote is posted when the offense is aggregated.
Aggregated offenses
Click Related Lists > Aggregated IBM QRadar offenses to view the offenses aggregated to the security incident. Click the QRadar offense hyperlink to view the offense in the IBM QRadar dashboard.

Create security incident: Select an offense from the list, click the Actions menu, and click Create security incident. This option creates a security incident for the offense and this offense is de-aggregated from the parent security incident.
Delete offense record: Select an offense from the list, click the **Actions** menu, and click **Delete**. This option deletes the offense record.

IBM QRadar offense updates

This shows the standard and custom offense fields and tracks changes to the offense during every polling interval. This is helpful as you can view any offense updates directly without navigating to the IBM QRadar dashboard. Any changes to the values are displayed in the Previous value and Current value fields.

To enable the offense updates feature navigate to **IBM QRadar Integration > IBM QRadar Integration Settings** and enable **Set this property to activate the Offense Updates feature**. By default, this setting is disabled.
Recent IBM QRadar events
Click the Fetch Recent IBM QRadar Events option under the Related Links to view the most recent IBM QRadar events.

By default, a maximum number of 100 events are displayed. You can modify this default setting in the IBM QRadar integration configuration settings.

Note: The above image shows the standard event fields associated with the offense. If you have configured and mapped any custom event fields (See Mapping IBM QRadar offense fields to security incident response fields), you can view them in the List View by clicking the Event Name link.
Recent IBM QRadar Flows

Using the Integration Hub and Flow Designer, several flows, subflows, actions are available with the IBM QRadar integration. When you click the Fetch Recent IBM QRadar Flows option under the Related Links, the most recent flows are retrieved. To view these flows, click Recent IBM QRadar Flows.

By default, a maximum number of 100 flows are displayed. You can modify this default setting in the IBM QRadar integration configuration settings.

ℹ️ Note: The above image shows the standard flow fields associated with the offense. If you have configured and mapped any custom flow fields (See Mapping IBM QRadar offense fields to security incident response fields), you can view them in the List View by clicking the Flow ID link.
Flow Designer and Integration Hub usage with IBM QRadar offense ingestion integration

Using the Flow Designer and Integration Hub functionality, several subflows and actions have been built as part of the IBM QRadar offense ingestion integration.

The following IBM QRadar subflows are available:

- **Connection and Credential Validation**: This is used in the configuration tile for validating the host and credentials in the initial setup.

- **IBM QRadar Rules Retrieval**: This is used in the Rules section of the profile setup to retrieve all active rules in IBM QRadar. This subflow is triggered asynchronously.

- **Fetch Sample Offenses Data From IBM QRadar**: This is used in the Mapping section of the profile setup to fetch sample data. This subflow is triggered asynchronously.

- **IBM QRadar Offense status updates**: This is triggered by a scheduled job every minute and updates the offense in IBM QRadar when the security incident is created or closed.

- **Process Profiles from Scheduled Job and Queue Offenses**: This is triggered by a scheduled job every minute to pull offenses per profile based on polling interval. This pulls offenses and queues them to the polling table for further processing.

- **Process Polling Queue and Poll in Batches**: This is triggered by a scheduled job every 30 seconds to process the Polling table Queue.

- **Fetch Recent IBM QRadar Flows**: This is triggered from the security incident form link to get latest flows of offense.

- **Fetch Recent IBM QRadar Events**: This is triggered from the security incident form link to get latest events of offense.

To view these subflows, login as a user with the `sn_si.admin` role and navigate to Flow Designer > Designer. Click on the Name link of any of the subflows listed above to view the subflow in detail.

Troubleshooting IBM QRadar offense ingestion integration

This section covers important troubleshooting tips and frequently asked questions related to IBM QRadar offense ingestion.

- **Integration run**: When a scheduled job starts executing, an integration run record with logs, errors, and warnings is displayed. The number of offenses pulled and the number of incidents created in a scheduled job run are also
displayed. Users with the sn_si.analyst role can see if any errors/profiles pulling failed during the integration run. Worknotes in the integration run provide links to the executed subflows. Users with the sn_si.analyst role can check the sn_event_ingestion_integration_run table for any errors that have occurred. To troubleshoot any integration issues, you must first check the integration run. Errors are logged as worknotes in the integration run records for every scheduled job run.

![Integration Run Records](image)

- **SSL issues**: When connecting to IBM QRadar cloud instances, ensure that the instance has a valid CA certificate which has not expired. You can import RSA or your own certificates into the platform and ensure that the common name of the certificate matches host name. See [https://support.servicenow.com/nav_to.do?uri=%2Fkb_view.do%3Fsys_kb_id%3D55ecefd61bf3774cada243f6fe4bcb44](https://support.servicenow.com/nav_to.do?uri=%2Fkb_view.do%3Fsys_kb_id%3D55ecefd61bf3774cada243f6fe4bcb44) for details.

- **Incomplete profile**: While configuring the profile, in the Additional Options (Automate offense updates and closure based on SIR incident status) section, you must click the **Finish** button to ensure that the profile is moved to Waiting state indicating that it is waiting for ingestion.

- **Validate profile**: To validate if the integration is working correctly, check the profile states, last pulled date of profile, offense import table, offense to task table records.

- **MID server configuration**: If you are installing the IBM QRadar application on-premise, after configuring the MID server, you must create a MID server application. The MID server application name should be used in integration configurations file instead of the MID server name.
Note: The default MID serve timeout is 30 seconds. To see instructions on disabling the timeout period, see <link>. Note that this is a system-wide change and may impact other integrations.

- **Offense Updates:** If you have enabled the `sn_sec_qradar.get_offense_updates` property and you notice a delay in the creation of security incidents, then disable the property. Do not enable this property when the polling interval is low and the offenses load on QRadar is high as this increases the queue load.

- **Missing event, flow data, remote_ip, or users data in a security incident:** If you observe that event, flow data, remote_ip, or users data is missing in a security incident, then increase the timeout (seconds) for `sn_sec_qradar.sid_ttl` parameter. Increasing the duration delays the creation of the security incident until the AQLs complete parsing each offense.

- **Timeouts:** If you view timeout errors in the application logs, review and modify the following flow designer actions:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fetch Sample Offenses</strong></td>
<td>Review and update the duration in milliseconds.</td>
</tr>
<tr>
<td><code>var flow_outputs =</code>&lt;br&gt;<code>sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses',</code>&lt;br&gt;<code>flow_inputs, 60000);</code></td>
<td></td>
</tr>
<tr>
<td><strong>Fetch Sample Offenses</strong></td>
<td>Add a parameter for the <code>executeAction</code> and enter the duration in milliseconds.</td>
</tr>
<tr>
<td><code>var flow_outputs =</code>&lt;br&gt;<code>sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses',</code>&lt;br&gt;<code>flow_inputs);</code></td>
<td></td>
</tr>
<tr>
<td><strong>Fetch Offenses for profile and queue records in polling table</strong></td>
<td>Review and update the duration in milliseconds.</td>
</tr>
<tr>
<td><code>var flow_outputs =</code>&lt;br&gt;<code>sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses',</code>&lt;br&gt;<code>flow_inputs, 180000);</code></td>
<td></td>
</tr>
<tr>
<td><strong>Wrapper for testing connection REST</strong></td>
<td>Add a parameter for the <code>executeAction</code> and enter the duration in milliseconds.</td>
</tr>
<tr>
<td><code>var rest_outputs =</code>&lt;br&gt;<code>sn_fd.FlowAPI.executeAction('sn_sec_qradar.test_connection_rest',</code>&lt;br&gt;<code>rest_inputs);</code></td>
<td></td>
</tr>
<tr>
<td><strong>Wrapper for validating API credentials REST</strong></td>
<td>Add a parameter for the <code>executeAction</code> and enter the duration in milliseconds.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Parameters | Action
--- | ---
`var rest_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.validate_credentials_rest', rest_inputs);` | REST step for IBM QRadar Offense updates
`var result = sn_fd.FlowAPI.executeAction('sn_sec_qradar.'+restStep, inputs,60000);` | Review and update the duration in milliseconds.

**IBM QRadar - Incident Enrichment Integration**

The IBM QRadar - Incident Enrichment integration searches your logs and adds relevant sighting information to your security incidents.

<table>
<thead>
<tr>
<th>Explore</th>
<th>Set up</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Security Incident Response integrations</td>
<td>- Get started with the IBM QRadar - Incident Enrichment integration</td>
</tr>
<tr>
<td>- Create sightings search configuration records</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use</th>
<th>Develop</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Run a Sightings Search</td>
<td>- ServiceNow Security Operations integration development guidelines</td>
</tr>
<tr>
<td>- Security Operations Integration - Sightings Search workflow</td>
<td>- Tips for writing integrations</td>
</tr>
<tr>
<td>- Security Operations - QRadar Sightings Search workflow</td>
<td>- Developer training</td>
</tr>
<tr>
<td>- View Sightings Search Details</td>
<td>- Developer documentation</td>
</tr>
<tr>
<td>- View Sightings Search Results</td>
<td></td>
</tr>
</tbody>
</table>

**Troubleshoot and get help**

- Integration troubleshooting
- Ask or answer questions in the Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support
Get started with the IBM QRadar - Incident Enrichment integration

IBM QRadar is an enterprise security information and event management (SIEM) product that integrates easily with Security Operations. Before you can use the IBM QRadar - Incident Enrichment integration, you must download it from the ServiceNow Store and add the appropriate API Base URL and API Key.

Before you begin
Role required: sn_si_admin

Procedure
1. Download the integration from the ServiceNow Store.
2. When the installation is complete, access IBM QRadar and obtain the API Base URL and API Key under your IBM QRadar profile.
4. In the IBM QRadar - Incident Enrichment card, click New.
5. Fill in the fields, as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of this configuration.</td>
</tr>
<tr>
<td>QRadar API Base URL</td>
<td>The base URL you acquired from the IBM QRadar site.</td>
</tr>
<tr>
<td>Link URL</td>
<td>[Optional] The Link URL that links to an IBM QRadar instance, when available.</td>
</tr>
<tr>
<td>Version</td>
<td>The IBM QRadar version; 5.0 is the default.</td>
</tr>
<tr>
<td>API Key</td>
<td>The API key you obtained from the IBM QRadar site.</td>
</tr>
<tr>
<td>Max Rows</td>
<td>The maximum number of rows you want to search.</td>
</tr>
</tbody>
</table>
### Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Earliest Result (days)</td>
<td>The earliest results you want to see in number of days.</td>
</tr>
<tr>
<td>Include raw data samples in search results</td>
<td>Select this to include samples of raw data in your sightings search results. The amount of data returned depends on your setting in the <strong>number of rows of raw data</strong> property in Security Incident Response properties.</td>
</tr>
<tr>
<td>MID Server</td>
<td>Select <strong>Any</strong> to use any active MID Server, or select a specific MID Server name.</td>
</tr>
</tbody>
</table>

**Note:** Configuring this integration activates workflows. To manage the workflows, navigate to the **Workflow Editor**.

6. Click **Submit**.
   
The integration configuration card displays.

7. When viewing the new configuration card, you can click **Configure** or **Delete** to change or delete the configuration, respectively.

8. To return to the original list of integration configuration cards, select **No** from the **Show Configurations** drop-down list.

### LogRhythm integration

The LogRhythm Enterprise integration with the Now Platform® Security Incident Response (SIR) product allows Security Operations Center (SOC) analysts to generate Security Incident Response (SIR) incidents automatically when certain configured LogRhythm alarms are triggered.

### Overview

The mapping flexibility of this integration provides an analyst with visibility to events and related alarm data that can be integrated into Now Platform security incidents for further investigation and remediation. Alarm profiles are created in your Now Platform instance to customize how different LogRhythm alarm fields are displayed on a Now Platform security incident. A default mapping of alarm fields is provided, which can be edited to meet customer-specific needs.

The following figure is an example of a customer environment. When an event triggers the creation of a security incident in the Now Platform® instance, a request is sent from your Now Platform® instance to pull alarms from the LogRhythm Client Console via a MID Server.
The SOAP API key is used by the Now Platform® to authenticate with the LogRhythm Client Console. This connection allows your Now Platform instance to pull individual LogRhythm alarms based on configured profiles.

The AI Engine Drilldown Cache API is used to gather message details not accessed by the SOAP API.

Key features
This integration includes the following key features:

- Flexibility to create multiple alarm profiles for different alarm types such as Phishing and Malware.
- Drag-and-drop mapping of LogRhythm alarm field values to associated SIR security incident fields.
- A Preview of the SIR security incident layout based on LogRhythm sample alarms.
- Ingest historical alarms as well as ongoing future alarms on configurable intervals.
- Automated LogRhythm alarm closure upon SIR incident closure. A URL to the SIR incident as well as an incident ID is provided for easy reference.

Supported releases of the Now Platform
This integration is compatible with the Kingston, London, Madrid, and New York releases of the Now Platform®.
Supported versions of LogRhythm

This integration is compatible with LogRhythm 7.3.2 or later. Earlier versions are not supported due to API limitations.

The images used in the following topics were generated for the Kingston release of the Now Platform. For information about the London user interface, see Managing security threats using the Security Analyst Workspace on the ServiceNow Product Documentation website.

⚠️ Note: The following topics are numbered. For a smooth installation and to help you verify expected results, follow the topics in the order they are presented.

Set up the SOAP API for LogRhythm

You use the SOAP API key to authenticate with the LogRhythm Client Console. This connection allows your Now Platform instance to pull individual LogRhythm alarms based on configured profiles.

Before you begin
Role required: LogRhythm Client Console/Platform Manager Administrator.

About this task
This task is performed on the LogRhythm Client Console. Set up the SOAP API prior to installing the application from the ServiceNow Store.

The images in this section are from the LogRhythm Client Console. Content is used by permission and is Privileged and Proprietary.

Procedure
1. Navigate to the LogRhythm Client Console on the host machine.
2. Select the Tools menu and navigate to Administrator > User Profile Manager.
3. In the User Profile Manager dialog, click the plus icon (+) and select **Allow Access** in the choice list that is displayed to create a new User Profile.

4. In the New User Profile Properties dialog, type a **User Profile Name**, for example, **SOAP API Profile**, and set the **Security Role** to **SOAP API Service Administrator**.
5. Click **OK** and close the Profile Manager dialog.

6. If the Entity Selection dialog is displayed, follow the steps to clear the dialog and select an entity.
a. Click **OK** to clear the Entity Selection dialog.

b. Click the **Entities** tab.  
The available entities are displayed.
c. Click **Primary Site**, and in the Grant column, select the check box.
d. Click **OK**.

7. Navigate to **Tools > Administration > Deployment Manager > People**.

8. In the upper left of the Deployment Manager, expand the File menu and click **New** to create a new user.
9. In the **Is Person an Individual?** dialog that is displayed, click **Yes**.

10. Enter user information in the Name fields for the SOAP API user and click **OK**.
11. In the list on the LogRhythm Client Console page, right-click to select the new user (SOAP, API) and select **Create User Account**.
12. In the **ADD LogRhythm User** dialog, enter the user name, select the newly created profile from the User Profile choice list, and enter a password.
13. Click **OK**.
   You have completed the setup for the SOAP API.

**What to do next**
The next step is to **Setup the AI Engine Drilldown Cache API**.

**Set up the AI Engine Drilldown Cache API for LogRhythm**
You use the AI Engine Drilldown Cache API key to gather additional event details for individual alarm fields. This API key provides details that are unavailable using the SOAP API.

**Before you begin**
Role required: LogRhythm Client Console/Platform Manager Administrator.

**About this task**
This task is performed on the LogRhythm Client Console. Set up the AI Engine Drilldown Cache API prior to installing the plugin from the ServiceNow Store.
The images in this section are from the LogRhythm Client Console. Content is used by permission and is Privileged and Proprietary.

Procedure

1. If not already displayed on the host machine, navigate to the LogRhythm Client Console and select the File menu.

2. Click **New** to create a new user.

3. In the **Is Person an Individual?** dialog that is displayed, click **Yes**.

4. In the Person Properties dialog that is displayed, fill in the Name fields.
   Use a different name for the AI Engine Drilldown Cache API than the one you used to create the SOAP API, for example, **REST API_2**.
5. Click **OK**.

6. Right-click the new listing in the Name column (**API_2_REST**) and, in the choice list, select **Create Case API Account**.
Note: The Case API is not used, but the credentials for the Case API Account and the AI Engine Cache Drilldown API are the same.

7. In the Service Account Properties dialog, click **Generate**.

8. Click **Copy**.
You have now set up the AI Engine Drilldown Cache API. You paste the string you copied in the previous step into your Now Platform instance in the AI Engine Cache Drilldown API Token field during the configuration steps listed in Install the plugin and configure LogRhythm.

What to do next
You are now ready to Install the plugin and configure LogRhythm.

Install the plugin and configure LogRhythm
Before you run the integration on your instance, complete the installation and configuration steps so the application properly integrates with Security Operations on the Now Platform®.

Before you begin
Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Verify that you have assigned the required Now Platform® and Security Incident Response (SIR) roles. | The following roles are required for installation, configuration, and verification of expected results:  
  - The system administrator (admin) installs the application plugin and assigns the security incident administrator (sn_si.admin) role.  
  - The (sn_si.admin) oversees the following tasks:  
    ◦ Names, creates, and edits alarm profiles.  
    ◦ Maps and filters alarms – identifies specific LogRhythm alarms that |
<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>create security incidents and configures how these alarm fields map to a</td>
<td>create security incidents and configures how these alarm fields map to a Now Platform® security incident.</td>
</tr>
<tr>
<td>Now Platform® security incident.</td>
<td>◦ Previews security incident details for accuracy prior to finalizing the configuration.</td>
</tr>
<tr>
<td>◦ Previews security incident details for accuracy prior to finalizing the</td>
<td>◦ Ingests historical alarms and schedules pulled alarms.</td>
</tr>
<tr>
<td>configuration.</td>
<td>◦ Assigns the security incident analyst (sn_si.analyst) role.</td>
</tr>
<tr>
<td>◦ This role also has access to the Security Operations module.</td>
<td>• The security incident analyst (sn_si.analyst) responds to security incidents that are created based on the alarm profile settings.</td>
</tr>
<tr>
<td>Obtain a LogRhythm API user name and password and verify that you are</td>
<td>Obtain a LogRhythm API user name and password and verify that you are using version LogRhythm 7.3.2 or later.</td>
</tr>
<tr>
<td>using version LogRhythm 7.3.2 or later.</td>
<td>Visit the product website for information on API keys and to create an account: LogRhythm Enterprise website. The user accounts, credentials, and certificates must be configured properly prior to installing the application.</td>
</tr>
<tr>
<td></td>
<td>The integration requires LogRhythm version 7.3.2 or later and the SOAP and AI Engine Drilldown Cache APIs.</td>
</tr>
<tr>
<td></td>
<td>See Set up the SOAP API for LogRhythm.</td>
</tr>
<tr>
<td></td>
<td>See Set up the AI Engine Drilldown Cache API for LogRhythm.</td>
</tr>
<tr>
<td>Verify that you have installed and configured a MID Server.</td>
<td>Verify that you have installed and configured a MID Server.</td>
</tr>
<tr>
<td></td>
<td>A MID Server is required in your Now Platform environment. See the ServiceNow Product Documentation website for information about how to set up and configure MID Servers.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration. | Madrid release and later release requirements  
For the Madrid release and later family releases, the Security Incident Response Dependency plugin (com.snc.si_dep) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications required by the integration.  
Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation. |

1. Security Incident Response  
2. Security Integration Framework  
3. Security Support Common  
4. Security Support Orchestration  

For more information on setting up your Now Platform instance for the integration, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application. |

Role required: admin
Procedure

1. If you have not installed the application for the integration, see Install a Security Operations integration and follow the steps to install it.

2. Once the installation completes, navigate to Integrations > Integrations Configurations and locate the LogRhythm tile.

3. Click Configure.

4. Click the New Configuration link.

5. In the new record, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>LogRhythm server name, for example, logrhythm-server-a.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LogRhythm API Base URL</td>
<td>Base URL hosting the LogRhythm SOAP API. The MID Server permits access to the network where the LogRhythm Client Console is hosted. This URL is where the LogRhythm server is hosted within that network. Follow these steps to enter the URL:</td>
</tr>
<tr>
<td></td>
<td>a. On the right side of the form, click the lock icon to edit the field and enter text for a URL, for example, <a href="https://logrhythm-soap.secops-snc.com">https://logrhythm-soap.secops-snc.com</a>.</td>
</tr>
<tr>
<td></td>
<td>b. Click the icon to display the active URL.</td>
</tr>
<tr>
<td></td>
<td>Note: Do not enter the API-specific URL. For example, if your SOAP Alarm WSDL is available at <a href="https://logrhythm-soap.secops-snc.com/LogRhythm.API/Services/AlarmServiceBasicAuth.svc?singleWsdl">https://logrhythm-soap.secops-snc.com/LogRhythm.API/Services/AlarmServiceBasicAuth.svc?singleWsdl</a>, enter, <a href="https://logrhythm-soap.secops-snc.com">https://logrhythm-soap.secops-snc.com</a>.</td>
</tr>
<tr>
<td>SOAP MID Server</td>
<td>Specific MID Server that is set up in your environment. Only MID Servers that are active and have been validated are available from this choice list.</td>
</tr>
<tr>
<td>SOAP API Account User Name</td>
<td>User name you created for the individual user account on the LogRhythm Client Console.</td>
</tr>
<tr>
<td></td>
<td>See Set up the SOAP API for LogRhythm.</td>
</tr>
<tr>
<td>SOAP API Password</td>
<td>User password you created for the individual user account on the Log-</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rhythm Client Console</td>
<td>See Set up the SOAP API for LogRhythm.</td>
</tr>
<tr>
<td>LogRhythm AI Engine Drilldown Cache API</td>
<td>The base URL hosting the LogRhythm AI Engine Cache Drilldown API. The MID Server permits you to access the network where LogRhythm Client Console is hosted. This URL is where the LogRhythm server is hosted within that network. Follow these steps to enter the URL:</td>
</tr>
<tr>
<td></td>
<td><em>a.</em> On the right side of the form, click the lock icon to edit the field and enter text for a URL for example, <code>https://logrhythm.secops-snc.com:8501</code>.</td>
</tr>
<tr>
<td></td>
<td><em>Note:</em> Do not enter the API-specific URL. For example, if your REST Case documentation is available at <code>https://logrhythm.secops-snc.com:8501/lr-case-api/docs</code>, enter, <code>https://logrhythm.secops-snc.com:8501</code>.</td>
</tr>
<tr>
<td></td>
<td><em>b.</em> Click the icon again to display the active URL.</td>
</tr>
<tr>
<td>Token Base URL</td>
<td>The base URL hosting the LogRhythm AI Engine Cache Drilldown API. The MID Server permits you to access the network where LogRhythm Client Console is hosted. This URL is where the LogRhythm server is hosted within that network. Follow these steps to enter the URL:</td>
</tr>
<tr>
<td>Requires separate mid server</td>
<td>Default is (cleared). Select the check box if access to your AI Engine Cache Drilldown API requires a different MID Server than your SOAP API. In the AI Engine Drilldown API Mid Server field that is displayed after you select the check box, select a specific MID Server in your environment. Only MID Servers that are active and have been validated are available in this choice list.</td>
</tr>
<tr>
<td>AI Engine Drilldown Cache Base API Token</td>
<td>Enter the token that is associated with your AI Engine Cache Drilldown API.</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
that you created on the LogRhythm Client Console.
See Set up the AI Engine Drilldown Cache API for LogRhythm.

The following figure is an example of a completed form.

6. Optional: If your SOAP API and AI Engine Drilldown Cache API are both deployed, but they cannot be accessed from the same Mid Server, select the Requires separate mid server check box and select one AI Engine Drilldown Cache API Mid Server from the choice list.
7. Click **Validate and save**.
   After validation is successfully completed, a message is displayed and the LogRhythm Configurations page is reloaded. The next step is to create an alarm profile.

**Trouble?**
You cannot proceed to the next configuration step until all entries on this form have been validated. An error message is displayed when an entry is invalid. If an error message is displayed, refer to the message text for more information and how to proceed to fix the problem. The SOAP API key or username and password may be invalid, or the MID Server URL may be incorrect. Verify your connection to the LogRhythm server and try validating again. For more information about testing your connectivity, see *(Optional) Verify connectivity for LogRhythm.*
**What to do next**
After you successfully complete the validation, the next step is to **Create an alarm profile for LogRhythm**.

**Create an alarm profile for LogRhythm**

In an alarm profile that you create and name, you specify which alarms you want to pull from the LogRhythm Client Console. You also define how they are mapped to fields on a Now Platform security incident.

**Before you begin**
Role required: sn_si.admin

**About this task**
Using available APIs, LogRhythm alarms are organized based on alarm rules, which define the conditions under which security events become alarms.

The Now Platform ingests specific LogRhythm alarms based on alarm rule associations such as *Unauthorized access attempts*, or *Malware*. Using this Now Platform integration, all alarms are initially ingested for a configured alarm rule. Alarm rules such as only high-risk level alarms can then be filtered to specify which alarms should create security incidents. Before security incidents are created, individual field values on the filtered alarms are mapped to...
corresponding fields on the Now Platform security incident. This configuration is done via an alarm profile within your Now Platform instance.

**Procedure**

1. Navigate to LogRhythm Integration > Alarm Profiles.

2. Select the Alarm Profiles module to display the Alarm Profiles list and click New to create a new alarm profile.

A new alarm profile form is displayed. At the top of the page in the progress bar, **Name** is selected. This bar tracks your progress during the configuration.

3. Fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the alarm profile. This name helps you identify the alarm types such as Unauthorized access (VPN), malware, or phishing.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
**Source** | Source server from the choice list. The list consists of LogRhythm configurations you have already set up, for example, logrhythm-server-a. See Install the plugin and configure LogRhythm.

**Active** | Default is cleared. After you complete all alarm profile setup steps and click Finish, you are prompted to select this check box to activate the alarm profile. When the alarm profile is active, it pulls alarms from the LogRhythm Client Console automatically.

**Optional) Description** | Text for additional information about the alarm profile, which may include the type of alarms, or an alarm category. An example description is *All alarms associated with unauthorized Powershell and Sudo access attempts.*

4. Choose one option to continue the configuration.

| Option   | Description |
---|---|
**Click Continue.** | Save your data and the Alarm Rules Selection form is displayed. **Alarm Rule Selection** is selected on the progress bar. The next step is to select LogRhythm alarm rules. |
**Click Update.** | Leave this page and the **Alarm Profiles** list is displayed. |
**Click Delete.** | Delete this alarm profile and the **Alarm Profiles** list is displayed. |

If validation is successful, the page reloads and the **Alarm Rule Selection** form is displayed. You cannot proceed with the configuration until you have successfully validated your connection and credentials.
Trouble?
If you cannot connect to the server, or your credentials are incorrect, a validation error message is displayed. Verify that your credentials are correct and try again.

What to do next
The next step is to **Select LogRhythm alarm rules**.

Related information
(Optional) Copy an alarm profile for LogRhythm

**Select LogRhythm alarm rules**
Select the LogRhythm alarms you want to map to a Now Platform security incident.

**Before you begin**
Role required: sn_si.admin

**About this task**
With this record in the Now Platform, you select LogRhythm alarm rule types you want to include in a specific alarm profile. Depending upon on how LogRhythm alarm fields are mapped to the security incident fields, and how the alarms are filtered, you can create an individual profile for each alarm rule. You can also combine multiple alarm rules into a single alarm profile. If there is consistency among alarms with different alarm rules, you can create a single profile for several alarm rules, or, you can create separate alarm profiles for distinct LogRhythm alarm rules.
Procedure

1. If the Alarm Profile form is not displayed, click **Alarm Rule Selection** on the progress bar.

2. In the Alarm Rule List section of the form, choose one to select LogRhythm alarms and move them to the Selected column.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the Alarm Rule List search field, enter text.</td>
<td>The column below the search field is filtered with available options based on the text you enter. With the arrow keys, move the selected alarm from <strong>Available</strong> to <strong>Selected</strong>.</td>
</tr>
<tr>
<td>In the Alarm Rule list, double-click an Alarm rule.</td>
<td>The <strong>Selected</strong> column is populated with your alarm rule.</td>
</tr>
<tr>
<td>In the Alarm Rule list, single-click an alarm rule.</td>
<td>The alarm is selected. With the arrow keys, move the selected alarm from <strong>Available</strong> to <strong>Selected</strong>.</td>
</tr>
</tbody>
</table>
3. Add any other alarm rules you want to include for this alarm profile.

4. Choose one to continue the configuration.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click Continue, or alternatively, click Mapping in the progress bar.</td>
<td>The Mapping form is displayed. Mapping is selected on the progress bar. The next step is to map alarm rules.</td>
</tr>
</tbody>
</table>
What to do next
The next step is to map LogRhythm alarms. For more information on mapping before you begin this step, see Overview for mapping LogRhythm alarms to the security incident.

Overview for mapping LogRhythm alarms to the security incident
After you have identified and selected the LogRhythm alarms you want to ingest, the next step is to map individual LogRhythm alarm fields to the Now Platform security incident fields.

Mapping alarms includes the following tasks:

- Map LogRhythm alarms. For this step, you list and ingest (pull) sample alarm IDs from the LogRhythm Client Console. Available alarm fields and their corresponding values are displayed.

- On the tabs that are displayed for each alarm ID you pulled, verify that all critical alarm fields from the Alarm Sample Ingestion section on the left of the form are mapped to the SIR Incident Field Mapping section on the right of the form.

- Edit the configuration by adding or removing fields on the security incident. Track overlooked or duplicated fields with the color coding that is provided.

- Filter alarms so you can specify which alarms are ingested into the SIR application.

- Use the script editor if you want to format values for the Priority and Category fields on the security incident.

The next step is to Map LogRhythm alarm fields to security incident fields.
Related information

Map LogRhythm alarm fields to security incident fields
(Optional) Use the script editor to format LogRhythm values
Filter alarms for LogRhythm

Map LogRhythm alarm fields to security incident fields

You map individual alarm fields to the security incident fields. The preconfigured mapping can be edited, and color coding provided for the fields helps you monitor alarms you have already mapped. This step helps you visualize how your edits impact the fields on the security incident.

Before you begin
Role required: sn_si.admin
If you are unfamiliar with the LogRhythm alarms, navigate to the LogRhythm Client Console and review a few sample Alarm IDs. For the following example, LogRhythm alarms 9468 and 9474 were used to map the alarms to the security incident.

About this task
Using this form, you map the LogRhythm alarm rules on the left to the security incident fields on the right.

The following figure shows the default mapping of alarms that is preconfigured for each alarm profile. This default mapping can be edited, and with this form, you customize the fields that populate the security incident. After you complete this mapping, you can see how adding or removing alarm fields potentially impacts the field values on the security incident.

On the left side of this form in the following figure, the LogRhythm alarm rules are outlined. The values of these alarm rules are mapped to the security incident fields on the right side of the form.
Procedure

1. If this form is not displayed, click **Mapping** on the progress bar.

2. In the **Alarm Sample Ingestion** field, enter up to five sample LogRhythm Alarm IDs separated by commas (9468, 9474).

3. Next to the alarm field, click **Pull Alarms**.
   
   The pull for sample alarms may take a few moments. A message indicating that the transaction is working is displayed at the top of the screen.
After the sample Alarm IDs are submitted and successfully pulled from the LogRhythm server, the alarm fields and their corresponding values are displayed in tabs.

**Note:** After an alarm ID is successfully pulled, the Now Platform may return the following message: The following new fields will be available for filtering shortly. Please reload this profile in a few minutes if filtering based on these fields is required. itemspacketsin, itemspacketssout.

This message occurs when the single alarm that has been pulled contains field names not previously processed by the Now Platform. These fields are available for mapping, however, if this message is displayed, reload the form so that these fields are displayed and available in the filter choice lists of the conditions builder when you are ready to set filtering conditions.

Ingesting these sample alarms in the alarm profile configuration helps you prevent mapping alarm fields to the security incident that contain no values. It also aligns alarm fields with values to the appropriate fields in the security incident. This step ensures that all critical alarm fields are mapped and that there are no missing field values on the security incident.

To help you ensure that no alarms are overlooked or duplicated in the mapping process, alarm fields are color-coded. A light blue alarm field (Account, AlarmRuleID, AlarmStatus, etc.) indicates that a field is not yet selected for mapping to a security incident.
A gray field (AlarmDate, AlarmID, and AlarmRuleName) indicates that a field has already been selected and has been mapped to a field on the security incident. This color coding helps you track the mapping, because in certain cases, an alarm field can be mapped to more than one field on a security incident. For instance, the Observables and Work Note fields can have more than one value.

4. To edit the default configuration on the security incident, follow these steps to add a field.
a. On the lower right of the form, click the plus icon. A new field is displayed.

b. In the Security Incident column, select an available field from the choice list. In the expanded choice list, some of the fields are shaded. For example, Category has a gray background, which indicates it has been mapped in the security incident. Similar to the color coding for LogRhythm alarm fields, this color coding for the security incident fields ensures that values from the alarm fields are not inadvertently mapped to the same security incident field.

In the illustration above, the alarm rule ${ClassificationName}$ is already mapped to the Category field in the security incident in this profile. Also note the Observable field in the security incident can accept more than one alarm rule, as shown by $(OriginIP)$ and $(OriginHostName)$ in the Input Expression column.
Note: The Observable field can be mapped to more than one field on the same security incident so that multiple observables can be displayed. Similarly, the Configuration Item and Work notes fields can be mapped to display multiple values.

On the Alarm Sample Ingestion side of the form, blue indicates that an alarm rule field has not been mapped. Gray indicates that it has been mapped. In the choice list on the SIR Incident Field Mapping side of the form, white indicates that a field has not been mapped. Gray indicates that a field has been mapped. Use this color coding to help you track your field mapping.

In the above illustration, Affected user has been selected from the choice list as a new field on the security incident.

c. From the Alarm Sample Ingestion section on the left side of the form, left-click to select the Alarm ID you want in the Input Expression field.

In the above illustration, Login has been selected.

d. Drag it to the cleared field and release it.

In the left column in the SIR Incident Field Mapping section, the new value for the Affected User field is displayed. In this case, the Login value from the LogRhythm alarm is displayed in the Affected user field on the security incident.

5. Alternatively, to manually enter a value for fields in the Input Expression column, place your cursor in the input expression field, and enter a desired alarm value.

For example, in the above illustration another field has been added (Assignment group) to the security incident form, and Security Incident Assignment has been entered manually in the field.

6. Continue editing the preconfigured mapping as required.

If you need to translate values from LogRhythm alarm fields to values that are supported by the fields on the security incident, you can use the script editor. See (Optional) Use the script editor to format LogRhythm values.

What to do next
After you complete the field mapping, the next step is to Filter alarms for LogRhythm.
Filter alarms for LogRhythm

Setting filtering criteria for alarms after you have mapped fields helps you determine which alarms should be ingested into the SIR application. Filtering alarms helps you significantly reduce the number of alarms you ingest when the alarm profile is activated.

Before you begin
Role required: sn_si.admin

About this task
Use the filtering conditions at the bottom of the mapping form to filter out specific alarms or limit ingestion to only alarms that meet certain field-level criteria. Filtering significantly reduces the number of alarms you ingest once the alarm profile is activated. Use filtering to ingest a manageable quantity of alarms that your Security Operations Center (SOC) staff can support.

Note: The following example shows a default filter setting in which Alarm status-does-not-contain-Closed is the default setting. This filter only pulls active alarms, and this setting reduces the number of pulled alarms. The following steps illustrate how to add another useful filter which includes only alarms with the highest severity or priority values.

Procedure

1. To edit the filtering criteria, select the Filter based on conditions check box.

2. To the right of the filter fields of the conditions builder, click OR or AND.
3. In the new line that is displayed, select the filtering conditions from the choice lists.

The following image shows an additional filter added to the criteria in which risk-based priority (\(RBP_{\text{max}}\)) is greater than 50. With this filter setting, only LogRhythm alarms with a risk-based priority value that is greater than 50 are pulled.

![Filter Conditions Image]

4. After you have verified that all critical LogRhythm alarm fields are mapped to the Now Platform security incident, and you have set filtering criteria to limit alarm ingestion, choose one to continue the configuration.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click Continue or Preview on the progress bar.</td>
<td>The Preview form of the security incident with your mapping configuration is displayed.</td>
</tr>
<tr>
<td></td>
<td><strong>Preview</strong> is selected on the progress bar. The next step is to view the security incident with your mapped alarms.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click Update.</td>
<td>Save your data and return to the Alarm Profiles list.</td>
</tr>
<tr>
<td>Click Previous.</td>
<td>The alarm profile record is displayed.</td>
</tr>
<tr>
<td>Click Delete.</td>
<td>Delete this alarm profile and the Alarm Profiles list is displayed.</td>
</tr>
</tbody>
</table>

**What to do next**

The next step is to preview your mapped fields on the security incident. See Previewing the security incident with mapped LogRhythm alarm values.

**Previewing the security incident with mapped LogRhythm alarm values**

After you have completed the mapping step, preview the values that you mapped to the fields on the security incident. This preview step permits you to verify that you have mapped all the critical LogRhythm alarm fields you want displayed on the security incident.

Role required: sn_si.admin

**Security incident**

If the security incident preview is not displayed, click Preview in the progress bar.

An example of the preview for the entire Now Platform security incident is displayed in the two following figures. This example of the preview of the security incident is populated with the LogRhythm alarms fields mapped from sample alarm 13663.

In the following figure, the Configuration item, Affected user, Priority, Assignment Group, and Short description fields of the security incident are populated.
Upper half of the security incident

To test and verify the transform field mapping and alarm filter criteria configured, you can select a previously ingested sample alarm and preview how the field mapping will display on the Security incident synopsis incident.

The following mapped fields do not have an input value: "Category", "Configuration item", "Observable"

On the lower half of the security incident, the Description field is populated. Under the Related Items section, the Configuration item, Observable, and Work note fields are populated with values. If multiple values for these fields are mapped, each value is displayed on the security incident, because each of these fields can accept more than one value.
Lower half of the security incident

Error conditions in preview

The following warning messages may be displayed when previewing the security incident. If a sample alarm does not pass the filtering criteria, the entire security incident is not populated.

Alarm is not in the profile Alarm rule List

A warning message is displayed if a sample alarm is pulled for an alarm rule other than those alarms selected in the alarm rule selection step. For example, as shown in the following figure, Alarm rule “AIE Suspicious Process –Carbon Black –Unknown Binary Running” was selected during the Alarm Rule Selection step, but the alarm rule ID for mapping and preview is not in the profile’s Alarm Rule List. If this error is displayed, navigate back to the Alarm Rule Selection step, verify that the correct alarm rules have been selected, and try pulling the alarms again.
Input value not found

If the alarm ID is included within the filtering conditions, a warning message may still be displayed if specific input values are not found for certain mapped fields. For the sake of the following example, in the preview of the record, assume that there is no value in the Assigned to field, although it was mapped.

For this type of message, in the Mapping record, verify that the input value is correct. In this case, the person in the Assigned to field in security incident is incorrect in the Now Platform instance. When this alarm is ingested and it creates a security incident with this condition, fields with this input value (Abel Tuter) are left blank in the security incident.
The remaining messages in blue are informational, and they indicate that these fields have no value to display in the preview. This preview permits the security incident administrator configuring the alarm profile to verify that these fields should have no value at the initial creation stage, because in certain cases, security incident fields may be populated later automatically. Other mapping errors are also displayed.

After you are satisfied with the mapping and the security incident preview, choose one to continue the configuration.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click <strong>Continue</strong> or <strong>Scheduling &amp; Alarm Retrieval</strong> in the progress bar.</td>
<td>Advance to the <strong>Scheduling &amp; Alarm Retrieval</strong> form.</td>
</tr>
<tr>
<td><strong>Scheduling &amp; Alarm Retrieval</strong> is selected on the progress bar. The next step is to schedule alarm retrieval.</td>
<td></td>
</tr>
<tr>
<td>Click <strong>Previous</strong>.</td>
<td>Return to the alarm profile and continue mapping.</td>
</tr>
<tr>
<td>Enter another alarm ID in the <strong>Sample Alarm ID</strong> choice list at the top of the preview form.</td>
<td>The <strong>Sample Alarm ID</strong> choice list is displayed for every alarm ID you have entered. You can select up to five alarms.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>This option permits you to preview another LogRhythm alarm ID on a security incident.</td>
<td></td>
</tr>
</tbody>
</table>

After you preview the security incident and are satisfied with the results, the next step is to **Schedule and retrieve LogRhythm alarms**.

**Schedule and retrieve LogRhythm alarms**

After you preview the security incident with the LogRhythm alarms that you have selected and mapped, you are ready to schedule alarm retrieval. After you complete this step, the alarm profile is ready to be activated.

**Before you begin**

Role required: sn_si.admin

**About this task**

Scheduling and alarm retrieval permits you to modify the scheduling and the types of alarms selected for retrieval. You filter the alarms you ingest based on a date range or on specific alarm IDs. With this step, you determine whether you want to ingest historical alarms, and how often you poll for future alarms that match the alarm profile configuration.

**Procedure**

1. If the scheduling form is not displayed, click the **Scheduling and Alarm Retrieval** step on the progress bar.

2. Choose from the following options to configure your alarm retrieval.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Ongoing Alarm Ingestion Polling.** | Default is selected.  
The Now Platform instance pulls from the LogRhythm Client Console for new alarms every five minutes. If mapped alarms are found, and filtering criteria are matched, security incidents are created.  
This setting can be changed, however, the default setting balances alarm ingestion against server load and retrieves the most current data. |
| **Historical alarm Retrieval.**  | Default is cleared. No historical data is pulled.  
If selected, the following fields are displayed. Choose one to configure retrieval either by date or alarm ID.  
**Since the following date**  
Click the calendar icon to enter a date. Alarms are pulled from the date you enter to the current date.  
**Ingest specific alarm based on Alarm ID**  
Enter specific alarm IDs. You pull the specified alarms, and you can enter multiple alarm IDs separated by commas.  
**Note:** After a historical, one-time pull of alarms is completed, this check box is cleared. You will need to select this check box again before you execute another one-time pull of historical alarms. |
3. To edit Historical alarm retrieval, follow these steps to enter a date for alarm retrieval or a specific Alarm ID.

   a. Select **Since the following date**, and, in the calendar that is displayed, select the date followed by the green check mark to save your entry.

   ![Historical alarm retrieval screenshot](image1)

   The date is displayed.

   ![Historical alarm retrieval screenshot](image2)

   b. Alternatively, select **Ingest specific alarm based on Alarm ID** and enter specific Alarm IDs for the historical data.

   You may enter up to five alarms separated by commas.
c. Click **Update**.

4. Choose one to continue editing or complete the configuration.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Click Update.</strong></td>
<td>Save your data and remain on the form.</td>
</tr>
<tr>
<td><strong>Click a step along the progress bar.</strong></td>
<td>Return to the selected step.</td>
</tr>
<tr>
<td><strong>Click Previous.</strong></td>
<td>Return to Preview.</td>
</tr>
<tr>
<td><strong>Click Finish.</strong></td>
<td>Save the configuration of the alarm profile. You are prompted to activate the alarm profile.</td>
</tr>
<tr>
<td><strong>Click Delete.</strong></td>
<td>Delete this alarm profile and the Alarm Profile list is displayed.</td>
</tr>
</tbody>
</table>

5. To complete the configuration, click **Finish**. The **Confirmation** dialog box is displayed.
6. Choose one in the Confirmation dialog box.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click Cancel</td>
<td>Return to the form. The form is not saved and it is inactive.</td>
</tr>
<tr>
<td>Click Finish</td>
<td>Save the alarm profile. The alarm profile is saved, but it is still inactive. The next step is to activate the alarm profile.</td>
</tr>
</tbody>
</table>

7. Follow these steps to activate the alarm profile so it pulls alarms automatically from the LogRhythm Client Console as configured.

a. In your Now Platform instance, navigate to LogRhythm Integration > LogRhythm Configurations.

b. Select the LogRhythm Configurations module, and, in the Name column, click the name of the alarm profile to open the record.

c. Select the Active check box and click Submit to activate the alarm profile.
When you complete the configuration and activate the alarm profile, the value in the **Active** column on the **Alarm Profiles** list changes to **true**. When the alarm profile is activated, it pulls alarms automatically. You have now completed the configuration of the alarm profile and activated it.

![Alarm Profile List](image.png)

**What to do next**
The next step is to **Verify alarm closure for LogRhythm**.

**Verify alarm closure for LogRhythm**
The LogRhythm Enterprise integration automatically closes out LogRhythm alarms when the Now Platform security incident is closed (or canceled). This closure permits the security incident analyst to simultaneously monitor the status of LogRhythm alarms and Now Platform security incidents.

**Before you begin**
Role required: sn_si.analyst

**About this task**
The LogRhythm alarm ID is connected to the Now Platform security incident ID throughout the course of the incident’s life cycle. This correlation permits a simultaneous and automated security incident/alarm closure to occur. When the Security Incident Response (SIR) security incident record is closed, there is a comment posted in the alarm on the LogRhythm Web Console. This comment indicates that the alarm was closed out based on the closure of the Now Platform security incident. The incident number and a URL that links back to the security incident for reference are also included in the comment section in the LogRhythm alarm.

**Procedure**
1. Navigate to **Security Incident > Show all Incidents** to locate a security incident created by the LogRhythm alarm ingestion.
2. On the Security Incidents list that is displayed, click the filter icon.
3. Using the filter fields that are displayed, create a filter (**Active-is-false**) as shown in the following figure and click **Run**.

The results of the search are displayed. In the **Short Description** column, note the LogRhythm alarm number and name used during the mapping step are displayed.

4. In the **Number** column, click an item with a short description with a familiar alarm name to open the security incident.

   In the following figure, for example, the alarm ID (**2790**) is displayed, and the work notes indicate the LogRhythm alarm status is **Closed_Resolved**.

5. Log on to the LogRhythm Web Console and locate and click the alarm ID tile on the console page.
The following image is from the LogRhythm Web Console. Content is used by permission and is Privileged and Proprietary.

A pane expands and indicates the security incident number (SIR0010118) is closed, and a URL is displayed. On the tile, the alarm ID (Id: 2790) is displayed and the status is Closed: with a Resolved Comment.

Trouble?
If you do not see notes indicating the alarm has closed successfully in the security incident, review the work notes for more information about how to proceed to fix the problem. Also, check your server connection. If you confirm the Now Platform security incident has been closed and the server has not timed out, you may have to manually close the alarm on the LogRhythm Web Console.

More options and troubleshooting for the LogRhythm integration
The following topics are optional and are not required for the setup and configuration of the integration. These topics assist you with customizing your configuration and troubleshooting connectivity and alarm ingestion problems.

Refer to the following topics for troubleshooting:

- Verify connectivity for LogRhythm
- Verify alarms with the LogRhythm AlarmEvent table
- Script execution and system log for LogRhythm

Refer to the following topics if you want more options for the basic setup and configuration:
• Use the script editor to format LogRhythm values
• Copy an alarm profile for LogRhythm
• Disable automated alarm closure for LogRhythm

(Optional) Verify connectivity for LogRhythm

Verify your connection to the LogRhythm Client Console by sending curl requests to test the SOAP and AI Drilldown Cache APIs.

Before you begin
Role required: admin

About this task
To verify the connection to the LogRhythm Client Console is working properly after you set up the SOAP and AI Engine Drilldown Cache APIs, send two curl requests from the computer hosting the MID Server you configured in Install the plugin and configure LogRhythm.

The SOAP API uses WSSE for authentication, which requires some outside scripting to work with Curl and Postman. The SOAP API requires port 443. This port number should be included in the URL that you plan to use for the test.

The Drilldown Cache API uses a token for authentication, so you can make the actual validation call that the integration uses. The “0” at the end of the URL is a LogRhythm Alarm ID. The Cache Drilldown API with a default configuration requires port 8501. This port number should be included in the URL that you plan to use for the test.

Procedure

1. Update the `<soap api url>` in the following curl request and send it from the computer hosting MID Server to validate the SOAP API:
   ```
curl -k -i -v --trace-time -o /dev/null -H "Content-Type: text/xml" "https://<soap api url>/LogRhythm.API/Services/LookupServiceBasicAuth.svc?wsdl"
   
   For a successful connection to the SOAP API, you should receive an HTTP 200 response code, and the body of the response is a WSDL (an XML file describing a SOAP web service).
   ```

2. Update the URL `<cache drilldown url>` and token `<api token>` in the following curl request and send it to validate the AI Drilldown Cache API:
   ```
   
   For a successful connection to the Cache Drilldown API, you should receive an HTTP 404, but the response body contains Alarm ID: 0 not found.
Related reference

More options and troubleshooting for the LogRhythm integration

(Optional) Use the script editor to format LogRhythm values

In addition to the directly mapped fields from the pulled alarm values, and the alarm values you enter manually, you can use the script editor to format field values on the security incident during the mapping step. The script editor changes the values of a LogRhythm alarm so the values that are mapped to the Priority and Category fields on the security incident are supported.

Before you begin
Role required: sn_si.admin

About this task
In certain cases, if LogRhythm alarm values are mapped to the Priority and Category fields on the security incident, you may want to edit the mapped values. If you want to translate the value of a LogRhythm alarm to a value that is supported by the Priority or Category fields on the security incident, use the script editor.

Procedure
1. With the mapping form displayed, in the SIR Incident Field Mapping section, click the bracket icon \[\{(\}\] to open the script editor.

The default values are included for the Priority and Category fields on the security incident. You can edit these values.
For this example, in the open editor, verify that **Priority** is displayed in the **Destination Field** choice list, as shown in the following figure. Note that this field is the security incident *priority*, not the LogRhythm risk-based *priority*.

In certain instances, a script include may be appropriate for the **Priority** field. For a LogRhythm alarm, for example, a risk-based priority score is assigned a value between 0-100. However, in the Now Platform, the priority field on a security incident supports values between 1-5. As illustrated in the preceding figure, a script include translates the LogRhythm alarm field values to the appropriate values supported by the field on the security incident in the Now Platform.

In this example for the **Priority** field, if the LogRhythm alarm value is 80 or greater, 1 is displayed in the security incident field (**Priority**). This value translates to a **Critical** priority in the security incident. If there is no value for the alarm, the field on the security incident is set to null.

2. Enter any changes, and click **Update** to save your changes.
   The LogRhythm Field Translations table is displayed.

3. Close the table to return to the Mapping form.
   The following figure shows the script editor with **Category** selected in the Destination Field choice list.
4. If you want to add a new field to the Field Translations list, follow these steps to add a new record.

a. With the mapping form displayed, in the SIR Incident Field Mapping section, click the **Click here** link. The LogRhythm Field Translation list with the **priority** and **category** destination fields are displayed.

b. Click New.
A new record is displayed.

c. From the Destination Field choice list, select a destination field on the security incident that you want to display your scripted values.

d. Click Submit.
   The script editor is displayed.

e. Enter any changes into the editor, and click Submit to save your changes.
   The LogRhythm Field Translations table with your new record is displayed.

5. Close the table to return to the Mapping form.

What to do next
After you have edited any values with the script editor and completed the mapping step, the next step is to filter alarms. For instructions on how to filter alarms, see Filter alarms for LogRhythm.

Related reference
More options and troubleshooting for the LogRhythm integration
(Optional) Copy an alarm profile for LogRhythm

Copy an existing profile and its associated settings instead of creating a new alarm profile. If you are creating multiple alarm profiles for different types of alarms and you want to reuse the settings of an existing profile, you can copy alarm profiles to save time.

Before you begin
Role required: sn_si.admin

About this task
If you copy a profile, the profile name is initially modified to avoid duplicate profiles. In addition, the copied profile is set to inactive so it is not activated accidentally prior to completing the configuration.

Procedure
1. Navigate to LogRhythm Integration > LogRhythm Alarm Profiles.

   In the list that is displayed, note the Active column indicates if the profile is active (true).

2. In the field to the left of the Name column, select the name of the record.

3. From the Actions on selected rows choice list, select Copy.

   In the Alarm Profiles list, both the copy and the original profile are displayed. Although the original record is active, the copy is inactive at this point (false). After you have configured it, you activate this copied profile.
You can edit values of the copied profile and rename it so alarm rules you pull apply to the new profile. You are prompted to activate the new profile once the configuration steps are completed.

**Related reference**

More options and troubleshooting for the LogRhythm integration

**(Optional) Verify alarms with the LogRhythmAlarmEvent table**

To verify that a given alarm or set of alarms is ingested into the Now Platform, you can view the alarms in the LogRhythmAlarmEvent table. Use this table for general troubleshooting if your alarms do not create security incidents as expected.

**Before you begin**

Role required: sn_si.admin

**About this task**

Before incidents are created, all alarms associated with alarm rules that are configured in the alarm profiles are pulled into the Now Platform Security Incident Response (SIR) application. Based on filtering conditions applied in the alarm profiles, some alarms may be filtered out and prevented from becoming security incidents.

If you confirm that alarms are displayed in the LogRhythmAlarmEvent table, verify that your filtering conditions are set correctly if the expected security incidents are not created. If the alarms are displayed in the LogRhythmAlarmEvent table, your alarm rule selection or other profile settings for scheduling the ongoing alarm polling may be incorrect. You can also verify if there are issues with pulling information into the Now Platform, or, if there is a problem processing the alarm data within the Now Platform Security Incident Response application.
Procedure

1. Navigate to **System Definition > Tables** and select the **Tables** module.

2. In the **Tables** list that is displayed, click the **LogRhythmAlarmEvent** link.

3. In the list that is displayed, click the **Show List** Related Link.
4. Confirm that alarms are displayed in the table that is displayed.

Related reference

More options and troubleshooting for the LogRhythm integration

(Optional) Disable automated alarm closure for LogRhythm

Disable the automated alarm closure capability if you no longer want to view the security incident closure information on the LogRhythm Web Console. Once deactivated, the Now Platform no longer closes alarms within the LogRhythm Web Console.

Before you begin

Role required: sn_si.admin
About this task
Once disabled, the status notes and other closure information on the security incident are no longer displayed on the LogRhythm Web Console.

Procedure
1. Navigate to **System definition > Business Rules** and select the **Business Rules** module.

2. If not displayed in the **Business Rules** list, enter `closeLogRhythmAlarm` in the search field and press **Enter**.

3. In the **Name** column, click the **closeLogRhythmAlarm** link to open the record.
4. In the record that is displayed, clear the **Active** check box.

5. Click **Update**.
   The automated alarm closure capability is now disabled.

**Related reference**

More options and troubleshooting for the LogRhythm integration
(Optional) Script execution and system log for LogRhythm

If you are troubleshooting an alarm ingestion issue, you can override the default five-minute polling interval to view results immediately. In this scenario, call the script execution manually to execute polling.

**Before you begin**

Role required: sn_si.admin

**Procedure**

1. Navigate to **Scheduled job > Scheduled Jobs** and select the **Scheduled Jobs** module.

2. Click the Process LogRhythm integrations job record.

3. In the Scheduled Script Execution record that is displayed, click **Execute Now**.
If you require more troubleshooting help, you can access the system log for the LogRhythm queries.

4. For other general troubleshooting issues, follow these steps to access the system logs.

a. Navigate to **System log > All** and select **All**.

b. Set the filter (Go to) to **Source** and enter **sn_sec_logrhythm**.
c. Press **Enter**.

Any messages generated by the integration are displayed in this table. The messages listed can provide insight into the running processes of the integration, and they may assist you with further troubleshooting.

**Related reference**

More options and troubleshooting for the LogRhythm integration

**View LogRhythm drilldown events**

View the related raw or base events for a LogRhythm alarm in the security incident.

**Before you begin**

Role required: admin

**About this task**

As a security analyst you can view the related raw or base events for a LogRhythm alarm without having to go back to the LogRhythm console. You can do this by going to a related list that contains all the drill-down events on the SIR incident.

**Procedure**

Navigate to LogRhythm Integration > LogRhythm Drilldown Events.

The following illustration shows how to navigate to the LogRhythm Drilldown Events module, sort the list of events by Group By Alarm ID, and click the associated security incident. In the security incident, you can find the LogRhythm Drilldown Events tab in the related links.
McAfee ePO integration

When the McAfee ePO capabilities are integrated with the Security Incident Response (SIR) product of your Now Platform® instance, security operations center (SOC) analysts are provided with an endpoint detection and response (EDR) capability that helps them identify cyber threats and repair the damage caused by malicious files.

Overview

As a security incident analyst from your Now Platform® instance, you request certain actions, or capabilities, on your endpoints (assets) from the McAfee ePO console in your environment. These requests are based on security event information found in Now Platform® security incidents. From your Now Platform® instance, you select and group McAfee ePO capabilities and define when and under what conditions these capabilities are invoked. You preview how the returned data are displayed on a Now Platform® security incident to confirm the returned results match your expected search criteria.

There are two types of McAfee ePO capabilities used in this integration, the capabilities that invoke actions, such as isolating a host machine or initiating an on-demand malware scan, and the capabilities that run queries to gather system details, threat events, and system compliance. Both types of capabilities, the actions and the queries, are invoked from your Now Platform® instance. You can group these capabilities together so that they automatically run when a specific type of security event occurs, or, you can invoke them manually from a Now Platform® security incident.
The following McAfee ePO capabilities are available for this integration.

**Get system details**
- Gather system details that include operating system details.

**Initiate malware scan**
- Based on scan configuration and scheduling, initiate a scan of an impacted endpoint.

**Isolate host**
- Remove a system from network access for investigation and restore access to the network.

**List threat events**
- Gather compliance status and the most current threat events.

**Key features**
This integration includes the following key features.

- Supports automated triggering of McAfee ePO queries that are based on incident conditions.
- Supports launching McAfee ePO capabilities manually from Now Platform® Security Incident Response (SIR) security incidents that perform on-demand actions.
- The flexibility to create multiple profiles for triggering different types of McAfee ePO and Now Platform® Security Operations capabilities. These profiles gather threat event information or perform actions based on the conditions of specific incident categories such as malware.
- Validate your profile configuration with a preview of the McAfee ePO results on SIR security incidents.
- If tagging is enabled, security tags identify which McAfee ePO capabilities are initially launched by a workflow and when the queries or actions are successfully completed.
- A complete audit trail of the McAfee ePO queries and actions is posted in the work notes on SIR security incidents, and commands from the Now Platform® are logged in the McAfee ePO console.
- Supports multiple McAfee ePO consoles so that you can apply different policies to user groups and regions.
Supported versions of the Now Platform


ServiceNow Plugins

Madrid and later release requirements

The com.snc.si_dep plugin is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before installing and activating the other Security Operations applications.

The following Security Operations applications must be installed and activated from the ServiceNow Store. Install and then activate one application at a time in the order listed below to ensure a smooth installation:

1. Security Integration Framework
2. Security Support Common
3. Security Support Orchestration
4. Security Incident Response

For more information on setting up your Now Platform instance for the integration, see Set up your Now Platform instance for the McAfee ePO integration.

The ServiceNow extension plugin

The ServiceNow Security Operations Extension for McAfee ePO extension plugin is required for this integration. You install this ServiceNow plugin in your McAfee ePO console. For more information, see Set up your Now Platform instance for the McAfee ePO integration.

MID Server

This integration requires an installed and configured MID Server in your Now Platform® instance to connect to the McAfee ePO server (console). See the ServiceNow Product Documentation website for more information about MID Servers.

Supported versions of McAfee

The integration supports version 5.9.1 & 5.10 of McAfee ePO. It supports McAfee Agent: MA 5.5.1.388 For more information about McAfee products and the ePolicy Orchestrator, see the McAfee product website.
The integration supports the version 10.5 of the McAfee Endpoint Security Threat Prevention product. If you are not running version 10.5, consult with your McAfee ePO administrator to see if your version can support on-demand scans via tag actions.

McAfee ePO security tags are used in this integration. You are required to create these tags in your McAfee ePO console. For more information on these tags, see Set up your McAfee ePO console to integrate with Security Incident Response (SIR).

References

<table>
<thead>
<tr>
<th>Reference</th>
<th>Document Identifier</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>McAfee product website</td>
<td>McAfee product website</td>
</tr>
<tr>
<td>2</td>
<td>McAfee Business Product Documentation for ePolicy Orchestrator Cloud</td>
<td>McAfee Product Documentation</td>
</tr>
<tr>
<td>3</td>
<td>ServiceNow Product documentation website</td>
<td>ServiceNow Product Documentation website</td>
</tr>
</tbody>
</table>

The images used in the following topics were generated for the Kingston release of the Now Platform. For information about the London user interface, see Managing security threats using the Security Analyst Workspace on the ServiceNow Product Documentation website.

For a checklist to track your progress with setting up, installing, and verifying results for the integration, see Checklist for the McAfee ePO integration.

For a smooth installation of the application and to help you verify expected results, follow the topics in the order they are presented.

Related information

Integration architecture for McAfee ePO

Set up your Now Platform® instance for the McAfee ePO integration

The following section lists the setup tasks that you are required to complete in your Now Platform® instance prior to installing the application for the McAfee ePO integration.

About this task

The following table is a list of setup requirements for the application.

Role required: Now Platform administrator (admin)
Procedure

1. Verify that you have completed these tasks before you install the application for the integration from the ServiceNow Store.

<table>
<thead>
<tr>
<th>Set up task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have assigned the required Now Platform® and Security Incident Response (SIR) roles.</td>
<td>The following roles are required:</td>
</tr>
<tr>
<td></td>
<td>• A user with the system administrator (admin) role installs the application and assigns the security incident administrator (sn_si.admin) role.</td>
</tr>
<tr>
<td></td>
<td>• A user with the security incident administrator (sn_si.admin) role configures the application, and creates, activates, and removes profiles. Users with this role also assign the sn_si.analyst role.</td>
</tr>
<tr>
<td></td>
<td>• A user with the security incident analyst (sn_si.analyst) role works with security incidents. Tasks include manually launching profiles from security incidents. If the approval option is selected in a profile during the configuration step, users with this role also submit requests for isolating hosts and returning them to the network.</td>
</tr>
<tr>
<td>Verify that you are using version 5.9 of McAfee ePO.</td>
<td>The integration supports version 5.9 of the McAfee ePolicy Orchestrator.</td>
</tr>
<tr>
<td>Verify that you have installed the ServiceNow extension plugin in your McAfee ePO console.</td>
<td>Install the ServiceNow plugin in your McAfee ePO console.</td>
</tr>
<tr>
<td></td>
<td>For more information and to obtain the plugin file, in your Now Platform instance, navigate to Knowledge &gt; Articles &gt; All and, in the Search field, enter, ServiceNow Security Operations Extension for McAfee ePO.</td>
</tr>
<tr>
<td>Set up task</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration. | Madrid and later release requirements  
For the Madrid release and later family releases, the Security Incident Response Dependency plugin (com.snc.si_dep) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications required by the integration.  
Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation.  
**a.** Security Incident Response  
**b.** Security Integration Framework  
**c.** Security Support Common  
**d.** Security Support Orchestration  
For more information about installing the Security Operations core applications, see [Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application](#). |
<p>| Verify that you have installed and configured a MID Server.                | An installed and configured MID Server is required in your Now Platform® instance. See the <a href="#">ServiceNow Product Documentation website</a> for more information about MID Servers. |</p>
<table>
<thead>
<tr>
<th>Set up task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you want to enable the approval process for profiles, verify that you</td>
<td>There is an optional approval process available for isolating host machines and restoring them to the network.</td>
</tr>
<tr>
<td>have created an approval group to process requests.</td>
<td>If this option is enabled, prior approval is required before host machines are isolated and restored to your network.</td>
</tr>
<tr>
<td></td>
<td>If your organization wants an extra level of control over these actions, enable the <strong>Require approval</strong> option during the configuration step for a profile.</td>
</tr>
<tr>
<td></td>
<td>By default, approval authority is assigned to the Now Platform® security incident administrator (sn_si.admin). This authority can be reassigned to an approval group. Within the group, any member has permission to approve or reject requests.</td>
</tr>
<tr>
<td></td>
<td>Follow the steps below to create an approval group to process requests.</td>
</tr>
<tr>
<td></td>
<td>You select an active approval group during the configuration step of your profile setup. For more information, see <a href="#">Configure a profile for system enrichment queries for the McAfee ePO integration</a>.</td>
</tr>
</tbody>
</table>

Approval requests submitted by the security incident analyst to isolate host machines and initiate malware scans are assigned to the user with the sn_si.admin role by default. As a user with this role, you can reassign this approval authority during the configuration step for a profile. Before you can reassign authority to an approval group, an approval group must be available on the Groups list in your Now Platform instance.

2. If you want to enable the approval option for profiles, follow these steps to create an approval group.
a. Navigate to **User Administration > Groups**.

b. In the Groups list that is displayed, click **New**.

c. Fill in the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the group that is displayed when an approval request is submitted, for example, Approvers McAfee host isolation.</td>
</tr>
<tr>
<td>Group email</td>
<td>Group email distribution list or the email address of the point of contact, such as the group manager, <a href="mailto:McAfeeapproval@servicenow.com">McAfeeapproval@servicenow.com</a></td>
</tr>
<tr>
<td>Manager</td>
<td>Name of group manager. Click the search icon to view the list.</td>
</tr>
<tr>
<td>Parent</td>
<td>(Optional) Other group of which this group is a member, if this group has a parent.</td>
</tr>
<tr>
<td>Type</td>
<td>Category for this group. Click the search icon to open the list.</td>
</tr>
<tr>
<td>Description</td>
<td>Additional information about the group.</td>
</tr>
</tbody>
</table>

d. Click **Submit**.
The new group is displayed in the Groups list.
You have successfully created an approval group. You can add users to this group who can approve the requests submitted by the security analyst. A user inherits roles from all groups to which the user belongs. You can also assign roles directly to a user. For more information about assigning approval roles to groups and users, see Roles on the ServiceNow product documentation website.

If the Require approval option is enabled during configuration step for this profile, a group is available to process requests. In the preceding example, each user in the Approvers McAfee host isolation group has approval authority.

Each member of the approval group navigates to My Approvals to monitor and process requests.

Set up your McAfee ePO console to integrate with Security Incident Response (SIR)

The following section lists the setup steps that you are required to complete in your McAfee ePO console prior to installing the application from the ServiceNow Store for the integration.

Before you begin
As a user with the McAfee ePO administrator permission, verify that you have installed the Servicenow.zip extension plugin in your McAfee ePO console. This extension plugin is required for the integration. For more information and to obtain the plugin, in your Now Platform instance, navigate to Knowledge > Articles > All. In the Search field, enter, ServiceNow Security Operations Extension for McAfee ePO.

About this task
The ServiceNow extension plugin connects your Now Platform instance to your McAfee ePO console. This connection allows you to reference the security tags
you that create in your McAfee ePO console for the isolate host and initiate malware scan actions to the capability profiles in your Now Platform instance. The security tags in your McAfee ePO console must match the security tags in the capability records in your Now Platform instance.

The following steps show you how to install the extension plugin, create a security tag in your McAfee ePO console, and assign an action to the tag. For more information about the security tags in the McAfee ePO console, see the McAfee Product Documentation website.

Note: The figures in the following section are from the McAfee ePO console. Content is used by permission.

Role required: McAfee ePO administrator

Procedure

1. If you have not installed the ServiceNow extension plugin on your McAfee ePO console, follow these steps to install it.

   a. Log in to your McAfee ePO console with your McAfee user name and password.

   ![McAfee ePolicy Orchestrator Login](image)

2. If the page shown in the following figure is not displayed, in the top left of banner of the home page, click the menu icon to display it.
3. On the page that is displayed, in the Software section, click the Extensions link.

4. On the Extensions page that is displayed, click Install Extension.
5. In the Install Extension dialog, click **Choose File**, navigate to the *Servicenow.zip* file on your system, and click **OK** to download it.

After the download is completed, the Software Extensions page is displayed with the ServiceNow Extension plugin listed.

You have successfully installed the ServiceNow plugin Extension on your McAfee ePO console.
6. If you have not created security tags in McAfee ePO console for the initiate malware scan and isolate host actions, follow these steps.

a. Navigate to the home page and click the Tag Catalog link.

![Tag Catalog link](image)

b. On the Tag Catalog page that is displayed, click New Tag.

![New Tag button](image)

c. With the Description step selected in the progress bar that is displayed, enter a name and description for the tag.

For this example, a tag with a name and description for the Initiate Malware Scan capability is displayed. This tag name is what is matched and referenced in your Now Platform instance.

![Tag editor](image)
d. To advance to the Criteria step, click **Criteria** in the progress bar. The messages that are displayed indicate that no actions are currently assigned to this tag, and that the tag can only be applied manually.

e. Click **Evaluation** in the progress bar to continue.

f. With the Tag Catalog page of the Evaluation step displayed, leave the settings on this page in their defaults, and, in the progress bar, click **Preview**.

g. With the Preview page displayed, in the lower right of the page, click **Save** to save the record.
The new tag is displayed in the Tag catalog as shown in the following figure.

7. Create a security tag for the host isolation action by repeating the previous steps.
   After you have created both tags, you are ready to assign actions to the new tags.

8. To add an action to your new tag, follow these steps.
a. Navigate to the home page and in the Policy section, click the **Client Task Assignments** link.

b. In the System Tree page that is displayed, at the bottom of the page, expand the **Actions** menu and select **New Client Task Assignment**.
c. On the page that is displayed, navigate to **Endpoint Security Threat Prevention > Policy Based On-Demand Scan > On-Demand Scan - Full Scan** by selecting the path as shown in the following figure.

d. In the Tags section, under the radio button and next to **Has any of these tags:**, click the **edit** link to edit the criteria for the tag.

e. In the dialog that is displayed, select the **Initiate Malware Scan ServiceNow** tag that you created in the preceding steps and click **OK**.
The ServiceNow Initiate Malware Scan tag you created is assigned to the On-Demand Scan action.

f. Click **OK**.
   In the Tags section, under the radio button and next to **Has any of these tags**, the Initiate Malware Scan tag is displayed.
g. Click **Save**.
   On the System Tree page, the task is displayed on the Assigned Client Tasks list (tab).
h. If you have not assigned an action to the Isolate Host action, repeat the previous steps to assign it.

You have successfully installed the extension plugin, created security tags, and assigned tasks to your tags. You have completed the setup for the integration in your McAfee ePO console. The next step is to configure a server in your Now Platform instance.

**Install the application and configure a server for the McAfee ePO integration**

Before you invoke the workflows for the integration, install and configure the McAfee ePO application from the ServiceNow Store on your Now Platform instance. The configuration is required to connect to the McAfee ePO console.

**About this task**
Role required: Now Platform administrator (admin)
Procedure

1. If you have not installed the McAfee ePO application for the integration from the ServiceNow Store, see Install a Security Operations integration and follow the steps to install it.

2. After you have successfully installed the application, follow these steps to configure the application on your Now Platform instance.

   a. Log in to the Now Platform instance that you want to configure the application for.

   b. In the left navigation panel, navigate to Security Operations > Integrations and click the Integrations module.

   ![Integration Module Screenshot]

   A list of various application tiles available for installation and configuration is displayed.

   c. Locate the McAfee ePO Integration tile and click Configure.
d. In the McAfee ePO Configuration dialog that is displayed, in the lower right, click the **Create new configuration** link.

3. Fill in the form.
Note:

The integration supports multiple servers, however, to avoid conflicts in profiles that share the same triggering conditions, you cannot share a McAfee ePO capability with multiple profiles that use the same McAfee ePO server. For example, as shown in the following figure, you can have capability 1 in more than one profile as long as each McAfee ePO server is mapped to a unique profile that has capability 1.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ePO Server Name</td>
<td>Name for the McAfee ePO server. If you use one server, an example is, McAfee HQ (McAfee Head Quarters). This name is how the server and related credentials are recognized. If your organization requires support for multiple servers, enter names for each server. Example names might be McAfee HQ, McAfee Global, and McAfee EMEA. These names help you distinguish the credentials and accounts and identify each server to avoid conflicts with profiles.</td>
</tr>
<tr>
<td>API account username</td>
<td>Unique account username, for example, ServiceNow API.</td>
</tr>
<tr>
<td>API account password</td>
<td>Unique password for the API account.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>McAfee ePO REST API URL</strong></td>
<td>Base URL hosting the McAfee ePO REST API. Enter the URL with the https:// protocol, for example, https://corp.epo_server:8443.</td>
</tr>
<tr>
<td><strong>Mid server</strong></td>
<td>Select the name of the MID Server that you configured during the setup of your Now Platform instance. Only MID Servers that are active and validated are available from this choice list. An example name is, secops_local_midserver.</td>
</tr>
</tbody>
</table>

The following figure is an example of a completed configuration form.

![Completed Configuration Form](image)

4. In the lower left of the page, click **Validate and Save**. The McAfee ePO Configurations list is displayed with your new configuration record. You have successfully completed the configuration for a McAfee ePO server. The next step is to create a profile.

**Trouble?**
If you cannot connect to the server, or your credentials are incorrect, a validation error message is displayed as shown in the following figure. Verify that your credentials are correct and try again.
Edit security tags in the Now Platform for the McAfee ePO integration

As part of the setup for the integration, edit the security tag names that you created in your McAfee ePO console in your Now Platform instance. Edit the tag names in your Now Platform instance so that they match the names of the tags in your McAfee ePO console.

About this task
The security tag names in your McAfee ePO console for the initiate malware scan and isolate host actions must match the security tag names in the records for these capabilities of your Now Platform instance.

Before you create a capability profile to run your capabilities, view the list of available McAfee ePO capabilities and edit the security tags in your Now Platform instance so that they match the security tag names in your McAfee ePO console.

For more information about creating the security tag names in your McAfee ePO console, see Set up your McAfee ePO console to integrate with Security Incident Response (SIR).

Role required: Now Platform security incident administrator (sn_si.admin)
Procedure

1. In the left panel, navigate to McAfee ePO Integration > McAfee ePO Capabilities and click the McAfee ePO Capabilities module to open the list.

2. To edit the security tag name for the initiate malware scan capability, in the Name column, click Initiate Malware Scan to open the record.

3. In the record that is displayed, in the upper right, click the link to open the record.

The record is refreshed and you can edit the EPO Tag Name field.
4. **In the EPO Tag Name field**, enter the name for the security tag that you created in your McAfee ePO console for the initiate scan action.  

For this example, the security tag name in the McAfee ePO console for the on-demand malware scan action is, **ServiceNow - Initiate Malware Scan**. This name was created as an example of a security tag name in **Set up your McAfee ePO console to integrate with Security Incident Response (SIR)**.

5. **If the Active check box is not selected, select it so this capability is available for a profile.**

6. **Click Update.**  
The EPO Tag Name is updated and displayed on the McAfee ePO Capabilities list. The security tag name for the on-demand malware scan action in your Now Platform instance matches the name for the scan in your McAfee ePO console.

7. **Optional:** In the Name column, click **Initiate Malware Scan** to view the updated record.
8. Repeat the preceding steps to edit the EPO Tag Name for the Isolate Host capability.

You have successfully edited the EPO Tag Names for the malware scan and the isolate host capabilities in your Now Platform instance. The next step is to create a profile for your capabilities.

For more information about editing the colors for the security tags, see (Optional) Edit the start and completion tag names and colors in your Now Platform instance.

Related information

McAfee Product Documentation

Creating profiles for the McAfee ePO integration

As a user with the security incident administrator (sn_si.admin) role, you create profiles for the McAfee ePO capabilities in your Now Platform® instance. You group queries or actions in profiles and determine which McAfee ePO capabilities you want to run when a new security incident is created.

Capability profiles

You create profiles so you can group McAfee ePO capabilities and configure the settings for these capabilities from your Now Platform® instance. You have the flexibility to create multiple profiles for these capabilities, which allows you to determine which actions or queries are invoked when a Security Incident Response (SIR) incident is created. To fit the needs of your organization, you can create a single profile that runs queries for system details, initiates malware
scans, and isolates host machines, for example, or, you can create multiple profiles, each with its own, single McAfee ePO capability.

Capability types for profiles

There are two types of McAfee ePO capabilities available for profiles. Capabilities such as List Threat Events and Gather System Details run queries and gather system data. The Isolate Host and Initiate Malware Scan capabilities invoke actions. In most cases, you configure the profiles that gather system data so that they run automatically when a security incident is created. These profiles are launched based on the triggering conditions that you specify during the configuration step for the profile, and they gather system data. Alternatively, you can launch profiles manually from security incidents. You usually launch profiles manually that isolate hosts and initiate malware scans directly from security incidents. If a profile is inactive, it is no longer available to launch manually, and it is not triggered automatically upon incident creation.

Isolate host capability

If your research determines that a host machine is infected or otherwise compromised, you may want to remove it temporarily from your network. Since host isolation and restoring machines to your network directly and significantly impacts your users, your organization may want you to submit approval requests for these actions. An optional process is available for the host isolation and host restoration actions during the profile setup.

Initiate malware scan capability

Malware scans search your assets for threats. These scans may take some time to complete. To verify when a scan starts and when it is successfully completed, an optional tagging feature is available. If this feature is enabled, a security tag is displayed when a scan is scheduled on related security incidents. This tag helps you verify that a scan is scheduled, because even on-demand scans may occur during off-hours. On the security incident, after the scan is successfully completed, the scheduled tag is automatically replaced by a completed tag.

All the capabilities grouped into a single profile share the settings that you select during the profile configuration step. Multiple capabilities can be mapped to a single profile as long as they have the same triggering conditions.

The next step is to Create a profile for the McAfee ePO integration.

Create a profile for the McAfee ePO integration

Create a profile and select the McAfee ePO capabilities that you want the profile to run.
About this task
For this step of the configuration, you create a profile for the McAfee ePO capabilities. When you create profiles, consider the intention of the profile before you add McAfee ePO capabilities to it. Refer to the following table when you create profiles.

The following table lists the capabilities that you are required to add to a profile if you want the profile perform certain queries or actions. Create a single profile that runs queries for system details, initiates malware scans, and isolates host machines, or, create multiple profiles, each with its own, single capability.

<table>
<thead>
<tr>
<th>Primary purpose of your profile</th>
<th>Set up requirements</th>
<th>McAfee ePO capabilities required for this profile type</th>
</tr>
</thead>
</table>
| Gather system details and threat enrichment data. | None | • List Threat Events  
| | | • Get System Details |
| Isolate Host | Verify with your McAfee ePO administrator that you have created the security tags for the isolate host action in your McAfee ePO console. For more information, see Set up your McAfee ePO console to integrate with Security Incident Response (SIR). | Isolate Host |
| Initiate malware scan | Verify with your McAfee ePO administrator that you have created the | Initiate Malware Scan |
Profile types and required McAfee ePO capabilities (continued)

<table>
<thead>
<tr>
<th>Primary purpose of your profile</th>
<th>Set up requirements</th>
<th>McAfee ePO capabilities required for this profile type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>security tags for the initiate malware scan action in your McAfee ePO console. For more information, see Set up your McAfee ePO console to integrate with Security Incident Response (SIR).</td>
<td>Note: As part of the McAfee ePO malware scan, the List Threat Events capability is invoked automatically. However, you are not required to add the List Threat Events capability to the profile with the malware scan capability. Results of the malware scan are displayed on the Threat Event Details tab on the security incident.</td>
</tr>
</tbody>
</table>

Role required: Now Platform® Security incident administrator (sn_si.admin)

Procedure

1. To create a new capability profile, follow these steps.
   a. Navigate to McAfee ePO Integration > McAfee ePO Capability Profiles.

      ![McAfee ePO Capability Profiles list displayed.

      The McAfee ePO Capability Profiles list is displayed.

   2. Click New.
The form for the new profile is displayed.

3. Fill out the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the McAfee ePO capability profile. This name helps you identify the profile type and describe it. An example for a profile that runs queries is, System and Threat Details. This name is also the name for the security tag for this profile by default.</td>
</tr>
<tr>
<td>Description</td>
<td>Additional information about the profile that further describes the activities of the profile. An example description</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Source</strong></td>
<td>Name of the McAfee ePO server. Only configured servers are available from the choice list.</td>
</tr>
<tr>
<td><strong>McAfee ePO Capability</strong></td>
<td>Capabilities of the McAfee ePO profile. Select the capabilities you want for this profile from the Available column and move them to the Selected column. In the figure below, the Get System Details and List Threat Events capabilities are selected for threat enrichment queries for this profile.</td>
</tr>
<tr>
<td><strong>Order</strong></td>
<td>Workflow priority. Default is 100. The value of this field indicates the order that workflows are executed when two or more profiles share triggering conditions. The workflow with the lowest number has the highest priority. To set the order of operation, enter a value. For example, 100, 200, 300, 400.</td>
</tr>
<tr>
<td><strong>Active</strong></td>
<td>The check box is selected by default to indicate that the profile is active. When selected, the profile is active and triggers automatically when a security incident is created that matches the filtering conditions that you specify during the configuration step. When inactive, the profile will not run, and it is not available to invoke from a list.</td>
</tr>
</tbody>
</table>
The following figure is an example of a completed form for a profile with the List Threat Event and Get System Details capabilities.

4. To save and validate the profile, in the lower right on the page, click **Continue**. If validation is successful, the page reloads and the **Configuration** form is displayed.

On the McAfee ePO Capability Profile list, your new profile is displayed.

**Trouble?**
If error messages are displayed as shown in the following figure, the capabilities you have assigned to this profile exist in another profile. In the following figure, this profile failed validation because a profile with the Get System Details or the List Threat Events capabilities already exists on the server (McAfee HQ) that you selected for this profile. This error message prevents you from creating profiles that share capabilities on the same server inadvertently.

Clear this error and navigate to **McAfee ePO Integration > McAfee ePO Capability Profiles** and select an item in Name column to view a profile. Verify the capabilities that you want for the new profile are not shared by existing profiles that are mapped to the server you want to use.
What to do next

The next step is to configure your profile. Before you configure the settings for the profile, you may prefer to review the concepts for configuring profiles and triggering conditions. See Creating profiles for the McAfee ePO integration and Defining triggering conditions with a Configuration item (CI) field for a McAfee ePO profile for more information.

Defining triggering conditions with a Configuration item (CI) field for a McAfee ePO profile

After you create a profile and select the McAfee ePO capabilities that you want the profile to run, you configure the settings of the profile so that it runs only when a set of specific conditions are met. You have the flexibility to set these triggering conditions so the profile runs automatically based on the default field values that are matched on a Now Platform® Security Incident Response security incident. Alternatively, you can set up a profile so it searches for matches on field values you specifically identify on the security incident.

One of the keys to the functionality of the integration and how a profile works is the Configuration Item (CI) field on the Now Platform® Security Incident Response (SIR) security incident. The value of this field is the principle value on a security incident. This value is used to match the IDs of your assets with the information stored in the Now Platform® database. When a SIR security incident is created by a security event, and a profile is activated, your assets are scanned for a matching value for a Fully Qualified Domain Name (FQDN), a host name, or an IP address based on the value of the Configuration Item field.

In an ideal case, a matching value is found in the database, and data can be gathered from the McAfee ePO console for the matching asset, pulled into your Now Platform® instance, and displayed on the related lists of a security incident. The following figure shows an example of the Configuration Item field populated with a host name on a SIR security incident.
In cases when the Configuration item (CI) field is not populated on the security incident, or a match cannot be found for a FQDN, a host name, or an IP address that matches the database, you can select an alternate field on the security incident to display any matching CI enrichment data found during the scan of your assets.

During the configuration step of the profile setup, you can select an alternate CI trigger field for endpoint identification to ensure that the CI enrichment data from the McAfee ePO lookup is populated on the associated security incident. You can select any field on the security incident as an alternate CI trigger field including custom fields that you create. By selecting this alternate CI field as a backup, you ensure that your profiles run even if the CI field is not populated on the associated security incident upon incident creation.

As an example, as a security operations center (SOC) analyst, you create a custom field for a security incident called, *IP Address on my security incident*. If you do not think that the value of this custom field will be displayed in the Configuration Item field on the security incident upon incident creation, you can set up the profile so it scans for this IP address. If matched, the IP address is displayed on the security incident in the field of your choice. In the following figure, the *Identified CI* field is selected as the alternate field for the IP Address for this example.
The following figure illustrates how the first search of the workflow scans for matches for Configuration Items. If the Alternate CI trigger field is enabled, the second search scans for matches for alternate values.
If matching IDs are not found for the CI field or the alternate CI field, a work note is logged and a message is displayed on the security incident. When no matches are found, no enrichment data are populated on the security incidents related to the event.

You enable the alternate CI trigger field and select the field you want to display the matching ID during the configuration step for a profile. This step for enabling the alternate CI field is described along with the other profile configuration requirements in Configure a profile for system enrichment queries for the McAfee ePO integration.

**Configuring profiles and testing security incidents for the McAfee ePO integration**

After you create a profile and select the McAfee ePO capabilities that you want the profile to run, configure the settings so that the profile is invoked only under the specific conditions that you define.
Configuring a profile

In this step, you configure a capability profile so that it runs only when the conditions you specify are fulfilled. You define which conditions on security incidents automatically trigger the McAfee ePO capabilities that you selected for the profile. You also have the option to select an alternate input field for the Configuration Item (CI) field and set filtering conditions so that only those security incidents that are related to your triggering event automatically launch the profile. The configuration step includes the following settings on the configuration form for the profile.

Alternate configuration item (CI) trigger field

In cases when the Configuration item (CI) field on the Now Platform® Security Incident Response (SIR) security incident is not populated with a value, or a match cannot be found in the database, you can select an alternate field on the security incident to display any matching CI enrichment data found during the scan of your assets. For more information about the Configuration item and the Alternate configuration item fields on a security incident, see Defining triggering conditions with a Configuration item (CI) field for a McAfee ePO profile.

Security tags

To help you track the status of isolated host machines and when malware scans are initiated, an optional tagging feature is available. By default, this option is disabled on the configuration form for profiles. If this option is enabled during the configuration step, security tag names are displayed on the configuration form. These are the names of the tags that are displayed on related security incidents. These tags inform you when a host isolation action is successfully initiated and when it is approved. After a host is successfully returned to the network, the security tag is automatically removed from the security incident. For malware scans, a tag is displayed on the related security incident when a scan is scheduled. After the scan is finished, the scheduled tag is automatically replaced by a tag that indicates that the scan is successfully completed.

Auto-trigger based on incident

When the Auto-trigger based on incident option is enabled, the filter condition builder is available, and you are required to set filtering conditions that specify when the profile runs automatically. A common filter is Category is malicious code activity and Business impact is 1 - Critical. With these filters, only security incidents that are related to malicious code and that have a critical business impact launch the profile. Using the Auto-trigger option can reduce the number of security incidents that automatically invoke the profile.
Approvals

If your organization wants an extra level of control over actions such as isolating host machines and initiating malware scans, you can enable the Require approval option during the configuration step for a profile.

For example, if both the approval and tagging features are enabled for a profile, after a request to isolate a host machine or to return it to the network is submitted for approval, the associated security incident is tagged automatically that the action is initiated. Requests are sent for approval to a user with the sn_si.admin role by default, but this approval can be reassigned to another individual or an approval group to fit the needs of your organization. Approvers process requests in My Approvals in their Now Platform® instances. Security tags are displayed on related security incidents. All workflow activities are also logged in work notes to create an audit trail.

Testing security incidents

During the Test Incident step of the configuration, you can verify that your McAfee ePO search results match your expectations with a preview of the results displayed on the related lists of a SIR security incident.

Select up to five incidents from a filtered list of incidents to preview during the test and preview step. You can preview the incidents that match the auto trigger conditions that you configured for a profile.

ServiceNow audit log in the McAfee ePO console

In version 5.10.0 of McAfee ePO, a ServiceNow tab is displayed with a log of commands that are initiated from your Now Platform® instance. After an action or a query is invoked from a profile in your Now Platform® instance on a host machine (endpoint) in the McAfee ePO console, an audit log of ServiceNow commands is created in the McAfee ePO console. This log is displayed in the System tree in the McAfee ePO console and helps you audit the times of the commands that are sent to specific endpoints. To view logged ServiceNow events on specific machines in a McAfee ePO console, follow these steps.

1. Navigate to the System tree in your McAfee ePO console and locate the ServiceNow tab.
2. Click the tab to open a list of host machines.
3. In the Name column, click a host name to open the audit log.

In the following image, an example of a log for a host (PODCLIENT1) is displayed.
The events initiated from the profiles in your Now Platform® instance are recorded and displayed in the log. Verify by checking the status of the host machine that the events listed in the log are successfully completed on the host.

Example profiles

The following topics include examples for how to configure profiles and test security incidents. These examples include profiles for all of the McAfee ePO capabilities that are available for this integration.

Configure a profile for system enrichment queries for the McAfee ePO integration

After you create a profile and select the List Threat Events and Gather System Details McAfee ePO capabilities for enrichment queries, the next step is to configure the settings so that it is invoked under the specific conditions that you define.

About this task

In this step, you configure the settings of a capability profile so it runs only when the conditions you specify are fulfilled. You define which conditions on Now Platform Security Incident Response (SIR) security incidents trigger the McAfee ePO capabilities that you selected for the profile. The following example shows the configuration steps for the profile created in the preceding section that submits queries, gathers system details, and lists threat events on your assets. The Enable alternate CI trigger field and Auto-trigger based on incident options are enabled for this example. Approvals and tagging options are disabled for this example.
Role required: Now Platform® security incident administrator (sn_si.admin)

Procedure

1. If the Configuration page is not displayed, click Configuration on the progress bar.

2. With the Configuration page displayed, fill out the form.

   The image following the table is an example of a completed form for the configuration step for this enrichment profile. The steps that follow the image show you how to fill in the fields on the form.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable alternate CI trigger field</td>
<td>Alternate configuration item (CI) trigger field. Default is cleared. When this check box is cleared, and the alternate CI trigger field option is disabled, an alternate for the CI field is not identified. If disabled, a value for the CI field must be populated on a SIR security incident, and the value in the field must be recognized by the McAfee ePO console before the profile gathers enrichment data. Select this check box if you believe the CI field will not be populated upon incident creation, but CI information will be populated in another field on the security incident. When this</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>option is enabled, the Alternate CI trigger field choice list is displayed. Choose an alternate field from the choice list to check for your CI search criteria.</td>
<td>For more information on the alternate CI trigger field, see Defining triggering conditions with a Configuration item (CI) field for a McAfee ePO profile.</td>
</tr>
<tr>
<td>Security tags are displayed on security incidents. Default is cleared.</td>
<td>When this check box is cleared, and the tagging option is disabled, no security tag names are displayed on the configuration form, and tags are not displayed on related security incidents. For this example, the security tags option is disabled.</td>
</tr>
<tr>
<td>Filter conditions. Default is cleared.</td>
<td>When the check box is cleared, and the option is disabled, the profile must be invoked manually from a security incident. When this option is enabled, the Filter condition builder is displayed. You are required to set the filtering conditions to specify when the profile runs automatically upon incident creation. A common example of a filter for a profile that runs enrichment queries is Category is Malicious code activity and Business impact is 1-Critical. These filter conditions help you locate the incidents that are related to specific types of security events, and they help you limit the number of security incidents you have to review. These filter settings remain saved until you change them, and they are</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Require approval</td>
<td>available for editing during the preview and test incident step of the configuration.</td>
</tr>
<tr>
<td>Require approval</td>
<td>Request approval option. Default is cleared. This approval option is available for any profile. Usually, approvals are used for capabilities that invoke actions such as host isolation and malware scans. When the check box is cleared, and this option is disabled, no approval requests are submitted. For this example, no prior permission is required for system enrichment queries.</td>
</tr>
</tbody>
</table>

3. To enable the alternate CI field option and set the filtering conditions that automatically invoke this profile, follow these steps.
a. Select the **Enable alternate CI trigger field** check box.

![Screenshot of the ServiceNow interface](image)

The Alternate CI trigger field is displayed. For this example, as a user with the `sn_si.admin` role, you believe that the CI field will not be populated on the security incident upon incident creation. Alternatively, you think CI information for a FQDN, host name, or IP address will be populated in the **Identified CI** field on the security incident, and you select the **Identified CI** field as an alternate. The **Identified CI** is selected for this example, but you can use any field on the security incident for the alternate CI.

b. From the **Alternate CI trigger** field choice list that is displayed, select the **Identified CI** field.

All the available fields on the security incident are displayed in the list including any custom fields.
In the Alternate CI trigger field, Identified CI is displayed.

When this profile is invoked, and the CI field is not populated on the associated security incident upon the initial event trigger, the profile alternatively uses the value from the Identified CI field in the search.

c. Select the Auto trigger based on incident check box.
The filter conditions builder is displayed. With this option, set filtering conditions and specify when the profile is invoked automatically upon creation of a security incident.
d. To set the first condition, in the most left field, click the arrow to expand the choice list.

e. In the search field that is displayed, start to type **Category** and select the highlighted text that is displayed to populate the field.

For this example, **Category** is displayed.

f. If not displayed in the second field, select **is** from the choice list.

g. In the third field, from the choice list, select **Malicious code activity**.
The first filter condition is displayed (Category is Malicious code activity).

h. To add a second filter condition that identifies only those incidents that have a critical impact to your organization, the right of the filter fields, click AND.

i. In the second row of filter fields that is displayed, repeat the previous steps and create a filter for Business impact is Critical as shown in the following figure.

You have successfully set the triggering conditions so that this profile is invoked automatically only when the following conditions are fulfilled.

- The Configuration item field is populated or the Identified CI field is populated.
- The category is Malicious code activity.
- The business impact is critical.
After you save your edits, the profile is displayed on the McAfee ePO Capability Profiles list with your settings displayed. In the Alternate CI trigger field column, your alternate field selection is identified (identified_ci). In the Enable alternate CI trigger field column, the status is active (true). In the Require Approval column, the option is cleared (false), because it was not selected for this example.

4. Choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Previous</td>
<td>Return to the Name step if you want to edit the profile.</td>
</tr>
<tr>
<td>Save</td>
<td>Save your changes and remain on this page. To save your changes, in the gray banner at the top of the screen, right-click and in the menu that is displayed, click <strong>Save</strong>.</td>
</tr>
<tr>
<td>Continue or Test Incident</td>
<td>Proceed to the Test Incident and Preview step. This step lets you verify that your McAfee ePO search results match what is expected before you activate the profile. If you select <strong>Continue</strong> or <strong>Test Incident</strong> prior to saving your changes, your edits are not saved if you leave the profile. If you try to exit the profile, a warning message is displayed.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete this profile from the McAfee ePO Capability Profiles list.</td>
</tr>
</tbody>
</table>

You have successfully configured the profile so it is triggered automatically upon incident creation, and an alternate field is used to populate matching CI results. The next step is to and preview and test security incidents fir this enrichment profile.

**Test security incidents for system enrichment queries for the McAfee ePO integration**

After you configure the settings for the system enrichment profile, test the profile and view the security incidents that match the settings of your profile. The preview permits you to validate that CI enrichment results are returned as expected for the profile.

**About this task**

As user with the a security incident administrator (sn_si.admin) role, you verify that your McAfee ePO search results match what is expected by getting a preview of the results displayed on the related lists of a security during this step. Similarly, if an incident is triggered by an external source, you may want to gather the security events related to the matching endpoint for additional context.

Select up to five incidents from a filtered list of incidents to preview. You can preview the incidents that match the auto trigger conditions that you set up for this profile. For this example, the System and Threat Details profile created in Create a profile for the McAfee ePO integration is used. The triggering conditions include security incidents with the Category field populated with Malicious code activity, Business impact is 1-Critical, and an alternate CI value for the Identified CI field.

By default, the filter criteria you enter during the profile configuration step are used to filter out and display only those security incidents that are related to your triggering event. As an option during this test incident step, you can add extra
filtering criteria so that incidents that are outside of the auto-trigger criteria are selected. This filtering permits you to validate that no workflow action is taken for incidents that fall outside of your triggering conditions for the profile.

To verify the workflow started and completed successfully, all workflow actions are written to work notes on the security incident to create an audit trail.

Role required: sn_si.admin

**Procedure**

1. If the Test Incident page is not displayed, click **Test Incident** in the progress bar. The Test Incident step for the System and Threat Details profile is displayed.

2. To the right of the top field on the page, click the search icon to view and select a security incident.
Only security incidents that match the profile criteria are displayed in the list.

3. In the Number column of the list that is displayed, select a security incident for the first field.

In the first field, the security incident number is displayed.
4. Repeat steps 2 and 3 until all the incidents you want to preview are displayed in the fields. Select up to five security incidents for the preview.

5. Click McAfee ePO Preview.

The incidents you selected are displayed in tabs after the page has loaded.
6. On the security incident preview, select a tab for a security incident and scroll to view the work notes.

```
Workflow Security Operations McAfee EPO Integration - List Threat Events execution completed.
```

```
Workflow Security Operations McAfee EPO Integration - List Threat Events execution started.
Data Inputs for this action: SIR0010034
```

```
Workflow Security Operations McAfee EPO Integration - Identify Endpoint execution completed.
```

```
Workflow Security Operations McAfee EPO Integration - Identify Endpoint execution started.
Data Inputs for this action: SIR0010034
```

The work notes for this security incident (SIR0010034) list when the workflows started and are successfully completed. For this example, the List Threat Events and the Identify Endpoint (the Get System Details capability) workflows started and completed successfully.

7. To view the returned enrichment results, scroll to Related Links and click **Show all Related Lists**.

```
Related Links
View Manual Redbook
Add Multiple Observables
Alert Orchestration
Show All Related Lists
Show Related Items
Show HC
Show Enrichment Data
Tanium Capabilities
Show Response Tasks
McAfee EPO Capabilities
```

The related lists are displayed in tabs. The returned enrichment data for the Get System Details and List Threat Events capabilities are displayed in the Threat Events Results, Threat Event Details, and System Details tabs of the security incident in the preview.

8. If no results are displayed on these tabs as shown in the following figure, anywhere in the gray banner below the tabs, right-click and select **Refresh List**.
9. Click the **Threat Event Details** tab.
The enrichment data that is displayed includes the following information.

- In the Actions taken column, a list of actions taken on files on the asset (podclient2).

- The alternate CI field value that was matched for an asset during the scan (podclient2).

- The empty Configuration item column that indicates this field was left blank on the security incident upon incident creation, because the example was configured with the assumption that the CI field would remain unpopulated.

10. Click the System Details tab, and, in the Alternate CI value column, click an item (podclient2) to open the record.
The raw data are displayed along with other information including the Alternate CI value and Last Check-in Date, which refers to when in local time the most current data were pulled from the McAfee ePO console.

11. To view the compliance status of the asset, click **Threat Events Results**.

As of the Last Check-in Date, that is, when the most current data were pulled, this asset is **Compliant**.

You have successfully tested and previewed the enrichment profile.

12. Choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Previous</strong></td>
<td>Return to the Configuration step for the profile. If you are not satisfied with the test and preview results, continue configuring the profile settings.</td>
</tr>
<tr>
<td><strong>Finish</strong></td>
<td>Complete the configuration and exit the profile.</td>
</tr>
</tbody>
</table>
Configure a profile to isolate host for the McAfee ePO integration

After you create a profile with the isolate host capability as a user with the security incident administrator (sn_si.admin) role, configure the profile.

About this task
In this step, as a user with the sn_si.admin role, configure the profile so it is invoked under the specific conditions that you define. You can also invoke the host isolation profile manually from a security incident. For more information about launching a profile manually, see Submit a request to isolate host manually from a security incident for the McAfee ePO integration.

 Usually, you invoke the host isolation request manually from a related security incident. Alternatively, you can select an alternate input field for the Configuration Item (CI) field and set filtering conditions so that only those security incidents that are related to your triggering event automatically invoke a profile with the isolate host capability. When the profile is active, you can launch it manually from a related list on the security incident. When the profile is inactive, it is not available to launch from a security incident.

Role required: sn_si.admin

Procedure

1. If the Configuration page is not displayed, on the progress bar click Configuration.

   ![Configuration Form](image)

   The Configuration form is displayed.

2. With the Configuration form displayed, fill out the form.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable alternate CI trigger field</strong></td>
<td>Alternate configuration item (CI) trigger field. Default is disabled. When the check box is cleared, and this option is disabled, an alternate field for the CI field is not identified. Enable this option for this example so an alternate field for the CI field is populated on the security incident. When this check box is selected, and this option is enabled, the Alternate CI trigger field choice list is displayed and you can choose any field from this list. For this example, the Identified CI field is selected. For more information on the alternate CI trigger field, see <a href="#">Defining triggering conditions with a Configuration item (CI) field for a McAfee ePO profile</a>.</td>
</tr>
<tr>
<td><strong>Display Tags</strong></td>
<td>Security tags are displayed on security incidents. Default is disabled. When the check box is cleared, and the tagging option is disabled, no security tag names are displayed on the configuration form. Leave this check box cleared if you do not want security tags displayed on related security incidents. When this check box is selected, and tagging is enabled, security tag names are displayed on the configuration form. These are the security tags that are displayed on related security incidents. These tags inform you when workflows are initiated and successfully completed. When the tagging option is enabled along with the <strong>Require approval</strong> option for a profile with the isolate host...</td>
</tr>
</tbody>
</table>
Field

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capability, security tags and work notes are displayed on the security incident. These tags and work notes indicate when a request for host isolation is initiated, when it is pending approval, and when it is approved. After a host is successfully returned to the network, the security tag is automatically removed.</td>
</tr>
</tbody>
</table>

Tag names and colors can be edited. For more information, see [Optional] Edit the start and completion tag names and colors in your Now Platform instance.

Auto trigger based on incident

Filter conditions. Filters are disabled by default.

When the check box is cleared, you are required to invoke the profile with the host isolation action manually from a security incident.

When the check box is selected, and this option is enabled, host isolation requests for assets that match the conditions of this profile are automatically submitted for approval if the Require approval option is also selected.

**Note:** If you enable the auto-triggering conditions and disable the approval option for host isolation for this profile, assets that match the profile configuration are automatically isolated from the network without prior approval.

If this option is enabled, the Filter condition builder is available and you are required to set filtering conditions that specify when the profile runs auto-
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto trigger based on incident</td>
<td>matically. A common filter is Category is malicious code activity, and Business impact is 1 - Critical. If the Auto trigger based on incident and the Require Approval options are enabled for this profile, these settings locate only those security incidents related to your event filtering. Requests for host isolation are submitted for approval automatically. For this example, only incidents related to malicious code activity and a critical business impact are displayed during the preview and test incident step of the configuration.</td>
</tr>
<tr>
<td>Require Approval</td>
<td>Require approval option for the isolate host action. Default is disabled. When the check box is cleared, the optional approval process for host isolation and undo host isolation for this profile is disabled. Verify that this option is disabled if you want to grant a user with the sn_si.analyst role permission to isolate host machines and return them to your network without requesting prior permission. When the check box is selected, and this option is enabled, a user with the sn_si.analyst role submits an approval request to isolate a host machine or restore it to the network. Enable this option if you want your security analyst to request permission prior to isolating a host machine or restoring it to the network. After a request is submitted, only one approval is required from the group to complete the request. Any member of the approval group has approval authority. Requests are</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>processed in <strong>My Approvals</strong> in the Now Platform instances of the approvers. Having a group with more than one person with approval permission ensures that these requests are processed in a timely manner.</td>
<td></td>
</tr>
</tbody>
</table>

For this example, the **Display Tags** option is enabled. The **Alternate CI trigger field** is enabled and **Identified CI** is the alternate field. **Auto trigger based on incident** is enabled. The auto-trigger filters are **Category is malicious code activity** and **Business impact is 1 - Critical**. For information about using the Filter conditions builder, see Configure a profile for system enrichment queries for the McAfee ePO integration.

3. With the approval process for the profile enabled, follow these steps to select an approval group.

   a. If not selected, on the form, enable the **Require Approval** option.

   ![Form with Require Approval option enabled]

   On the form, the Approver field is displayed.

   b. To the right of the Approver field, click the search icon.
The Groups list is displayed. The list contains the groups that you created to approve host isolation requests sent from the user with the sn_si.analyst role. For this example, Approvers McAfee host isolation is the approval group.

c. From the list, select the group that you want to process approval requests.

![Groups list screenshot]

In the Approver field, the group is displayed.

As an approver, after requests are submitted, you navigate to My Approvals in your instance to approve or reject requests.

d. Click Save to save your changes.

e. Navigate to McAfee ePO Integration > McAfee Capability Profiles.

In the Approver column of the McAfee ePO Capability Profiles list, the group you selected to process approval requests for this profile is displayed. The Alternate CI trigger field is identified_ci, the approval option is active (true) with a group identified (Approvers McAfee host isolation). The Enable alternate CI trigger field is enabled (true). The filtering conditions for invoking the profile automatically upon incident creation are also active (true).

![McAfee ePO Integration and McAfee Capability Profiles screenshot]

You have successfully completed the configuration step for the isolate host profile. The next step is to test and preview security incidents.
4. Choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Previous</td>
<td>Return to the Name step if you want to edit the profile.</td>
</tr>
<tr>
<td>Save</td>
<td>Save your changes and remain on this page. To save your changes, in the gray banner at the top of the screen, right-click and in the menu that is displayed, click <strong>Save</strong>.</td>
</tr>
<tr>
<td>Continue or select Test Incident in the progress bar</td>
<td>Proceed to the Test Incident and Preview step. If you leave the page without first saving your changes, your edits to the profile settings are not saved.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete this profile from the McAfee ePO Capability Profiles list.</td>
</tr>
</tbody>
</table>

**Test security incidents and approve requests for isolate host for the McAfee ePO integration**

The test and preview step permits you to validate that the host isolation and remove host isolation workflow results are returned as expected for the profile.

**About this task**

During this step of the configuration, as a user with the sn_si.admin role, verify that the profile you configured with the isolate host capability returns security incidents and matching asset IDs as expected. View the actual Now Platform Security Incident Response (SIR) security incidents that are created when security event conditions occur that match the settings of your profile.

After a request to isolate a host machine is submitted, as a user with an approver role, process the request.

Role required: sn_si.admin
Procedure

1. If the Test Incident page is not displayed, click **Test Incident** in the progress bar.

The Test Incident page is displayed for your profile. For this example, the *Isolate Host* profile you created and configured in the preceding sections is displayed.

2. To the right of the top field, click the search icon to select a security incident to preview.
3. In the Number column of the list that is displayed, select an item that you want to display in the preview.

Only security incidents that match the criteria you set for the profile are displayed.

The security incidents are displayed on the page.
4. Repeat steps 2 and 3 until all the incidents that you want to preview are displayed in the fields. Select up to five security incidents for the preview.

5. Click **McAfee ePO Preview** to view the security incidents.

The incidents created for the security event conditions that match your profile are displayed in tabs.

ℹ️ **Note:** If you leave the Test Incident page at this point, your security incidents are cleared from these fields.

6. Select a tab, and, on the security incident, scroll to view the work notes.
For this example, SIR0010021 from the preceding image is selected. The work notes list that the isolate host workflow is started. Because the **Require Approval** option is enabled for this profile, the work notes indicate that the request is **pending approval**.

On the top of the incident, the security tag is displayed that indicates the request is initiated (**Isolate Host - Initiated**).

You have successfully located security incidents that match your profile for the Isolate Host capability and viewed a security incident.

**7. If you are a user in an approval group, follow these steps to process a request.**

   **a. Navigate to My Approvals in your instance.**

   For this example, the user name of the approver is **Mary admin**.
The approvals list is displayed.

**b.** In the State column, click an item to open the approval record.

**c.** In the Approval record that is displayed, click **Approve** or **Reject**.

After you process the request, the workflow may take a few moments to run. On the record at the top, a message is displayed as shown in the following figure if the transaction takes more than a few seconds.
After a few moments, in the approval record that is displayed, the State column changes from Requested to Approved. No additional approvals are required to isolate the host machine for this request. If the request is rejected, the host is not isolated and the request remains pending. As a user with the sn_si.analyst role, if the request is rejected, you are required to submit a new request if you still wish to isolate the endpoint.

The request to isolate the host machine in the preceding figure is approved.

d. Navigate to Security Incident > Incidents > Show All Incidents and, in the Number column, click an entry to open the security incident that you are working with.
On the security incident that is displayed, the Isolate Host - Completed tag replaces the Isolate Host - Initiated tag. The host isolation workflow for this example is successful.

Work notes on the security incident also indicate that the host isolation is completed, and the approver, Mary admin, is listed.

Note: Although the security tag and work notes on the security incident indicate that a successful isolate host workflow is completed, return to your McAfee ePO console and verify that the host machine is isolated from your network.

After you have completed your investigation on the asset, launch the Remove Isolation workflow from the Host Isolation Entries table in your Now Platform® instance to return the host to the network.

8. To remove the host from quarantine and return it to the network, follow these steps.
a. If the McAfee ePO Isolate Host Entries table is not displayed, navigate to McAfee epO Integration > McAfee epO integration Isolate Host Entries.

The Isolate Host Entries list is displayed. At the top of the list in the Status column, search for the asset you isolated.

b. In the Added date column, click the item to open the record. The Isolate Host Entries record is displayed. An audit trail for all the actions associated with the security incident is displayed in the work notes. In the following figure, the last entry in the work notes is a successful host isolation. The date the quarantine is completed is displayed in the Added date field (2019-01-03 14:04:17).
c. Click **Remove Isolation** to launch the workflow to restore the machine to the network. The Isolate Host Entry record is displayed. On the top of the record, a message indicates that the request was submitted. The Status changes from **Isolated** to **Pending Approval**, and a work note is logged. In this case, the System Administrator has requested that the machine is restored to the network.

![ServiceNow interface](image)

**Note:**
- **Active** status of the task is set to **true**.
- **Request action** is set to **Add**.
- **Status** is set to **Pending Approval**.
- **Task** is set to **$R00(001)**.
- **Reference** is set to **$R00(001)**.
- **Requestor** is set to **System Administrator**.
- **Added date** is set to **2019-03-01 14:04:17**.
- **Submission note** contains the message: "**System Administrator** submitted the request on 2019-03-01 14:04:17.

**Actions:**
- **Add**
- **Approve**
- **Reject**

**Notes:**
- "**System Administrator** submitted the request on 2019-03-01 14:04:17."
- "**Pending Approval**

**Status Changes:**
- **Isolated**
- **Pending Approval**
- **Approved**

**Comments:**
- "The status changes from **Isolated** to **Pending Approval**.
- A work note is logged.
- The System Administrator has requested that the machine is restored to the network.

**Pending Approval Actions:**
- **Approve**
- **Reject**

**Notes:**
- "After you are notified of the request, as a user with approval permission for host isolation, navigate to **My Approvals** in your instance and open the record for the remove isolation request.
- **Click Approve** to approve the request and return the asset to the network. Alternatively, **click Reject** to keep the request in the pending approval state.
- **If a request is rejected, a new request must be submitted to isolate the host.**
- **After you approve the request to remove the host isolation, the tag on the security incident is removed.** Work notes create an audit trail for the remove isolation request. For this example, the system administrator initiated and approved the request.

![ServiceNow interface](image)
The security tag and work notes on the security incident indicate that the remove host isolation workflow is successfully completed. To verify that the host is back on the network, return to your McAfee ePO console and verify that the host machine is now active.

9. Choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Previous</td>
<td>Return to the Configuration step for the profile. If you are not satisfied with the test and preview results, continue configuring the profile settings.</td>
</tr>
<tr>
<td>Finish</td>
<td>Complete the configuration. You are prompted to confirm activation.</td>
</tr>
</tbody>
</table>

Submit a request to isolate host manually from a security incident for the McAfee ePO integration

Submit an on-demand request to isolate a host machine from the network directly from a Now Platform Security Incident Response (SIR) security incident.

Before you begin
As a user with the sn_si.admin role, if you want a user with the sn_si.analyst role to request approval prior to isolating a host machine, verify that the Require Approval option is enabled in the profile with the McAfee ePO isolate host capability.

About this task
As shown in the preceding sections, you can invoke a request to isolate a host machine automatically if the triggering conditions you specify in the profile...
match the conditions on security incidents. Alternatively, if you want to submit a request to isolate a host manually, submit the request directly from a security incident. You may prefer to submit an on-demand request manually after the initial incident is created and you need more time to research the event. Role required: sn_si.analyst

**Procedure**

1. If the security incident you are working with is not displayed, navigate to **Security Incident > Show all Incidents**.

2. In the list that is displayed, locate and click the incident in the Number column (SIR0010021) to open the record. The record is displayed.

3. Scroll to the Related Links section and click the **McAfee ePO Capabilities** link.

   The McAfee ePO Profiles dialog is displayed.

4. To the right of the field, click the search icon.
5. Click the profile in the **Name** column that has the isolate host capability.

6. With the profile displayed in the McAfee ePO Capability Profile field, click **Submit**.
   The security incident is displayed. If tagging and approvals are enabled for the profile, at the top of the record, the **Isolate Host - Initiated** security tag is displayed.
The work notes verify that the workflow is started, and the request is submitted and pending.

You have successfully submitted a request to isolate a host machine from a security incident. To approve the request, as a user with an approval role, navigate to **My Approvals** in your Now Platform instance and process the request. For more information, see **Test security incidents and approve requests for isolate host for the McAfee ePO integration**.

**Configure a profile for initiate malware scan for the McAfee ePO integration**

After you create a profile with the Initiate Malware Scan capability and any other McAfee ePO capabilities that you want the profile to run, configure the settings of the profile so that it is invoked under the specific conditions that you define.

**About this task**

As a user with the sn_si.admin role, configure the profile so it schedules a scan only when the conditions that you specify are fulfilled on Now Platform Security Incident Response (SIR) security incidents. You define which conditions on security incidents trigger the scan. Any other McAfee ePO capabilities that you select for the profile share the triggering conditions. The options to select...
an alternate input field for the Configuration Item (CI) field and set filtering conditions are available. You may prefer to set filtering so that only those SIR security incidents that are related to your triggering event automatically invoke the profile.

As with the isolate host action, you can initiate an on-demand scan directly from a SIR security incident. For more information about launching a scan manually, see Submit a request to isolate host manually from a security incident for the McAfee ePO integration.

Role required: sn_si.admin

**Procedure**

1. If the Configuration page is not displayed, click **Configuration** on the progress bar.

![Configuration form](image)

The Configuration form is displayed.

2. Fill out the form.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable alternate CI trigger field</td>
<td>Alternate configuration item (CI) trigger field. Default is disabled. For this example, the check box is cleared. When this check box is cleared, and the alternate CI trigger field option is disabled, an alternate for the CI field is not identified. If disabled, a value for the CI field must be populated on a SIR security incident, and the value</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>in the field must be recognized by the McAfee ePO console before the profile runs.</td>
</tr>
<tr>
<td></td>
<td>When this check box is selected, and this option is enabled, the Alternate CI trigger field choice list is displayed. Choose any field from this list as an alternate field for the CI.</td>
</tr>
<tr>
<td></td>
<td>For more information about the alternate CI trigger field, see Defining triggering conditions with a Configuration item (CI) field for a McAfee ePO profile and Create a profile for the McAfee ePO integration.</td>
</tr>
<tr>
<td></td>
<td>Security tags on security incidents. Default is disabled.</td>
</tr>
<tr>
<td></td>
<td>When this check box is cleared, and the tagging option is disabled, no security tag names are displayed on the security incident. Leave this check box cleared if you do not want security tags displayed on related security incidents.</td>
</tr>
<tr>
<td></td>
<td>When the check box is selected, and the tagging option is enabled, security tag names are displayed on the configuration form. These are the tag names that are displayed on related security incidents.</td>
</tr>
<tr>
<td></td>
<td>Malware scans may be scheduled during off-hours and take time to complete. On the top of the security incident, when tagging is enabled, a security tag is displayed that indicates that the scan is scheduled. After the scan is successfully completed, the scheduled tag is automatically replaced by a tag that indicates that the scan is successfully completed.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Tag names and colors can be edited. For more information, see <em>(Optional)</em> Edit the start and completion tag names and colors in your Now Platform instance.</td>
</tr>
<tr>
<td></td>
<td>Filter conditions. Default is disabled.</td>
</tr>
<tr>
<td>Auto trigger based on incident</td>
<td>When the check box is cleared, and the option is disabled, the profile does not automatically launch a malware scan. The profile must be launched manually from a security incident.</td>
</tr>
<tr>
<td></td>
<td>When the check box is selected, and the auto trigger option is enabled, the Filter condition builder is displayed on the form. You are required to set the filtering conditions to specify when the profile runs automatically upon incident creation.</td>
</tr>
<tr>
<td></td>
<td>For this example, filters for <code>Category is Malicious code activity</code> and <code>Business impact is 1 - Critical</code> are used. For more information about the filter condition builder, see <em>Create a profile for the McAfee ePO integration</em>.</td>
</tr>
<tr>
<td>Require Approval</td>
<td>Require approval prior to initiating the scan. Default is disabled.</td>
</tr>
<tr>
<td></td>
<td>When the check box is cleared, and the approval option is disabled, a user with the sn_si.analyst role initiates a malware scan without requesting prior approval.</td>
</tr>
<tr>
<td></td>
<td>Select this check box and enable this option if you want a user with the sn_si.analyst role to request approval prior to initiating a malware scan.</td>
</tr>
<tr>
<td></td>
<td>For more information about the approval option, see <em>Configure a profile</em>.*</td>
</tr>
</tbody>
</table>
For this example, the approval and tagging options are enabled for the profile. For more information about how to configure the Enable alternate CI trigger field and the Auto trigger based on incident options, see Configure a profile for system enrichment queries for the McAfee ePO integration.

3. Choose one option to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Previous</td>
<td>Return to the Name step if you want to edit the profile.</td>
</tr>
<tr>
<td>Save</td>
<td>Save your changes and remain on this page. To save your changes, in the gray banner at the top of the screen, right-click. In the menu that is displayed, click Save.</td>
</tr>
<tr>
<td>Continue or select Test Incident in the progress bar</td>
<td>Proceed to the Test Incident andPreview step. If you leave the page without first saving your changes, your edits are not saved.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete this profile from the McAfee ePO Capability Profiles list.</td>
</tr>
</tbody>
</table>

You have successfully configured the profile so a malware scan is triggered automatically upon incident creation. An alternate CI field is used to populate matching CI results from the scan. The next step is to and preview and test security incidents for this profile.

Test security incidents for initiate malware scan for the McAfee ePO integration

After you configure a profile for the malware scan, test the profile and view the security incidents that match the settings of your profile. Preview the scan results on the related lists of a Now Platform Security Incident Response (SIR) security incident.

About this task

As a user with the sn_si.admin role, verify that the profile with the malware scan capability is invoked and that the scan search results match what is expected with a preview of the related lists on a Now Platform Security Incident Response
(SIR) security incident. The preview permits you to validate that scan results are returned as expected for the profile.

Role required: sn_si.admin

Procedure

1. If the Test Incident page is not displayed, click **Test Incident** in the progress bar. The Test Incident page is displayed for your profile. For this example, the *Initiate Malware Scan* profile you created and configured in the preceding sections is displayed.

2. To the right of the top field, click the search icon to select a security incident to display on the preview.

3. In the Number column of the list that is displayed, select an item that you want to display in the preview.
The security incident number is displayed in the field.

4. Repeat steps 2 and 3 until all the incidents that you want to preview are displayed in the fields. Select up to five security incidents for the preview.

5. Click McAfee ePO Preview.
The security incidents that match the event conditions of your profile are displayed. After the page has loaded, on the bottom of the page, tabs are displayed for each security incident.

6. Scroll to view the work notes.

**Note:** The list threat events workflow is part of the scan. For more information about creating a profile with the malware scan capability, see Create a profile for the McAfee ePO integration.
Scans are sometimes scheduled to run during after peak working hours to minimize their impact to users on the network. The scan may not complete immediately. In this case, on the top of the security incident, a security tag is displayed indicating that the scan is scheduled. Refer to the work notes for status on the workflow. The work notes list when workflows start and are successfully completed. For this example, the work notes in the following figure show that the scan started, and that it successfully completed. The List Threat Events capability was also started and successfully completed as part of the scan.

The following figure shows an example of a security tag on the related security incident.
On the security incident, after the scan is successfully completed, the scheduled tag is automatically replaced by the completed tag.

7. After you verify that the scan is successfully completed, on the security incident, scroll to view the Related Links and click **Show all Related Lists**.
The Threat Event Results and Threat Event Details list are displayed as tabs.

8. If the Threat Event Details list is not selected, select it to view the results.

9. Click an item in the Source column to open a record and view the enrichment data.

The enrichment data includes the following information.

- The CI field value that was matched during the scan.
- Last Check-in Date with time zone. This data refers to when in local time the most current data was from pulled from the McAfee ePO console.
- Raw data

You have successfully verified that the scan workflow successfully completed for security incidents that matched the auto-trigger criteria that you set for this profile.

10. Choose one to continue.
Option | Description
--- | ---
Previous | Return to the Configuration step for the profile. If you are not satisfied with the test and preview results, continue configuring the profile settings.
Finish | Complete the configuration. You are prompted to confirm activation.

Integration architecture for McAfee ePO

The following topic is an overview of the system architecture and lists key features of the integration. This section also provides information about the setup steps that you are required to complete in your Now Platform instance and in the McAfee ePolicy Orchestrator (McAfee ePO) console prior to installing the application from the ServiceNow Store.

Key terms for the McAfee ePO integration

The following terms are used throughout the installation and configuration documentation for the integration.

Now Platform

An enterprise ServiceNow product. The Now Platform is the base upon which individual components, such as Security Incident Response (SIR), IT Service Management, (ITSM), and other products are built.

Security Incident Response (SIR)

A Now Platform application that tracks the progress of security incidents from discovery and initial analysis, through containment, eradication, and recovery, and into the final post incident review and closure.

Plugin

Plugins are software components that provide specific features and functionalities within your Now Platform instance. For more information on the installation and configuration of the integration plugins, see Install the application and configure a server for the McAfee ePO integration.

ePolicy Orchestrator (McAfee ePO)

The user console where you manage the McAfee services, products and settings.
**McAfee extension plugin**

This ServiceNow extension plugin is required for this integration. This plugin resides on your McAfee ePO console and connects your McAfee ePO console to your Now Platform instance.

**Capability**

An automatic activity initiated from your Now Platform instance that is run in the McAfee ePO console to conduct enrichment queries and perform actions on your assets.

**Profile**

Settings for McAfee ePO capabilities that you configure to specify when and under what conditions capabilities conduct enrichment queries and perform actions on your assets.

**MID server**

An application that facilitates communication and the movement of data between the Now Platform and external applications, data sources, and services.

**ServiceNow administrator (admin)**

A user with this role downloads and installs the SIR and McAfee ePO plugins to your Now Platform instance. A user with this role also assigns the security incident administrator role as required.

**ServiceNow Security incident administrator (sn_si.admin)**

A user with this role performs the configuration of the McAfee ePO integration with the Security Incident Response (SIR) product in your Now Platform instance as required. A user with this role also assigns the security incident analyst role as required.

**ServiceNow security incident analyst (sn_si.analyst)**

A user with this role interacts with and analyzes security incidents in the SIR product.

**System connection and data flow**

The following figure is an example of a customer environment. A Now Platform MID server is required so that your Now Platform instance can connect to a McAfee ePO server (console) via a ServiceNow extension plugin. After you are connected, you invoke capabilities from your Now Platform to initiate malware scans, isolate host machines and restore them to your network, retrieve last scan results, and gather system details on your assets. When these capabilities return results from your assets that match your search criteria, data is pulled via the MID server into your Now Platform instance. Data is displayed on the related lists of...
a Now Platform Security Incident Response (SIR) security incident. The following figure illustrates the data flow for one group of endpoints managed by one McAfee ePO console.

As shown in the following figure, this integration can support more than one McAfee ePO console. You can have one group of endpoints managed by one McAfee ePO console, and another group of endpoints managed by another McAfee ePO console. Data from multiple McAfee ePO consoles is pulled via a single MID server. However, you also may prefer to configure multiple MID servers if required by your organization.
Workflows for the McAfee ePO integration

This integration includes the following workflows. These workflows are pre-configured and are designed specifically for this integration. You can edit these workflows to meet the needs of your organization as required. For more general information about workflows and using the workflow editor, see Getting started with workflows on the ServiceNow Product Documentation website.

- Security Operations McAfee EPO integration - Identify Endpoint
- Security Operations McAfee EPO integration - Initiate Malware Scan
- Security Operations McAfee EPO integration - Isolate Host
- Security Operations McAfee EPO integration - List Threat Events
- Security Operations McAfee EPO integration - Queue Isolate Host

External systems connection

The integration requires that the MID server communicates via HTTPS protocol connection to the McAfee ePO console.
(Optional) Edit the start and completion tag names and colors in your Now Platform® instance

You may prefer to edit the names and colors of the start and complete tags for the initiate malware scan and isolate host capabilities. The start and complete tags help you quickly identify which capabilities are invoked from Now Platform Security Incident Response (SIR) security incidents.

About this task
As a user with the sn_si.admin role, you may prefer to edit the colors and names of the security tags that are displayed on SIR security incidents. You may also assign tags to security tag groups to help you organize them in your Now Platform® instance. For example, you can change the colors of tags so the start tag of a capability is one color, and the completion tag is another color. These different colors can help you quickly identify when scans start and are successfully completed. For more information on how to set up security tag groups and tags, see Set up security tag groups and tags on the Servicenow Product Documentation website.

Procedure
1. To edit the names and colors of the security tags, navigate to McAfee EPO Capabilities, and, in the Name column, click an item in the list.

The record for the capability is displayed.
2. To edit a tag, to the right of a tag name, click the information icon, and open the tag record.

In the record that is displayed, edit the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the security tag.</td>
</tr>
<tr>
<td>Color</td>
<td>Security tag color. Select a color from the choice list.</td>
</tr>
<tr>
<td>Security Tag Group</td>
<td>Enter a name of the security tag group. Click the information icon to view the available groups. Default is Metatag group.</td>
</tr>
<tr>
<td>Enforce restricted access</td>
<td>Select this check box to assign read and write roles needed by users to read or write to records that have this security tag. Default is cleared.</td>
</tr>
<tr>
<td>Order</td>
<td>Specify the order the tag appears on forms or within a list. Default is 100.</td>
</tr>
<tr>
<td></td>
<td>To set the order on the list, enter a value. For example, 100, 200, 300, 400. The tag with the lowest the number is displayed first on the list. The profile with the highest number is displayed last.</td>
</tr>
<tr>
<td>Active</td>
<td>Turn the tag on or off.</td>
</tr>
<tr>
<td>Description</td>
<td>A description for the tag.</td>
</tr>
</tbody>
</table>

3. Choose one to continue.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update</td>
<td>Update the page with new changes.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete this tag record from the McAfee ePO capability.</td>
</tr>
</tbody>
</table>

(Optional) Copy a profile for McAfee ePO

Copy an existing profile and its associated settings and triggering conditions instead of creating a new alarm profile. As a user with the sn_si.admin role, you may prefer creating multiple alarm profiles for different types of alarms. Copy the settings of existing alarm profiles to save time.

**Before you begin**

Role required: sn_si.admin

**Procedure**

1. Navigate to **McAfee ePO Integration > McAfee ePO Capability Profiles**.
2. In the check box field to the left of the Name column, select the profile that you want to copy.
3. From the Actions on selected rows choice list, select **Copy**.

   In the **Alarm Profiles** list, both the copy and the original profile are displayed. Although the original record is active, in the Inactive column, the copy of the profile is inactive (false). After you have configured the copy, activate the copied profile.

   As a user with the sn_si.admin role, you may prefer to edit the copied profile and rename it so that the capabilities apply to the new profile. You are prompted to activate the new profile after the configuration steps are completed.

**Checklist for the McAfee ePO integration**

Use this checklist to guide you through all the tasks of the integration. The following checklist includes setup and installation tasks and examples of use cases that include expected results for the integration.

**About this task**

Track your progress with the setup, installation, and configuration of the integration with the following table. Complete all the tasks for a step before moving on to the next step. Each row of the table lists tasks and identifies the roles that are required to perform the tasks. Numbered topics of the installation and configuration guide are also referenced.
Roles required: Roles are listed for each step.

**Procedure**

Follow the steps in the table in the order that they are presented.

<table>
<thead>
<tr>
<th>Checklist</th>
</tr>
</thead>
<tbody>
<tr>
<td>0. As a user with the Now Platform® administrator role, set up your Now Platform® instance.</td>
</tr>
<tr>
<td>b. Verify that any ServiceNow Security Incident Response and other plugins that support the integration are installed and activated for your release of the Now Platform.</td>
</tr>
<tr>
<td>c. Install and configure a MID server in your Now Platform® instance.</td>
</tr>
<tr>
<td>d. Create an approval group if you want to process requests submitted from the security incident analyst for the isolate host and initiate malware scan actions.</td>
</tr>
<tr>
<td>For more information, see <a href="#">Set up your Now Platform instance for the McAfee ePO integration</a>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Checklist</th>
</tr>
</thead>
<tbody>
<tr>
<td>0. As McAfee ePO administrator, set up your McAfee ePO console.</td>
</tr>
<tr>
<td>a. Verify that you are using version 5.9 of McAfee ePO.</td>
</tr>
<tr>
<td>b. Install the ServiceNow extension plugin in your McAfee ePO console.</td>
</tr>
<tr>
<td>c. Verify you have created security tags in your McAfee ePO console for the isolate host and initiate malware scan actions.</td>
</tr>
<tr>
<td>For more information, see <a href="#">Set up your McAfee ePO console to integrate with Security Incident Response (SIR)</a>.</td>
</tr>
<tr>
<td>For more information and to obtain the extension plugin file, in your Now Platform instance, navigate to <strong>Knowledge &gt; Articles &gt; All</strong> and, in the Search field, enter, <strong>ServiceNow Security Operations Extension for McAfee ePO</strong>.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
|   | As a user with the security incident administrator role, configure a profile and test security incidents. 
  a. Review the information about triggering conditions and settings. 
  b. Configure a profile. 
  c. Test and preview security incidents. 
  d. Locate search results and other details on the related lists on the security incident. 
  e. Create and Configure different types of profiles and test security incidents for each type. For information about triggering conditions and the alternate CI field, see Defining triggering conditions with a Configuration item (CI) field for a McAfee ePO profile. For information about triggering conditions and settings, see Configuring profiles and testing security incidents for the McAfee ePO integration. For the steps required to configure a profile, test, and preview security incidents and examples of profile types, see the examples that follow Configuring profiles and testing security incidents for the McAfee ePO integration. |
|   | As a user with the Now Platform security incident analyst role, submit on-demand requests for host isolation and malware © 2021 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
scans. For more information, see Submit a request to isolate host manually from a security incident for the McAfee ePO integration.

In the Now Platform, as a user with an approval role, or, as a member of an approval group, approve requests for host isolation and malware scans.

For more information on processing approval requests, see Test security incidents and approve requests for isolate host for the McAfee ePO integration.

You have successfully completed the set up steps, installed and configured the application, and verified expected results for the integration.

**McAfee ESM - Email Parser integration**

The ESM - Email Parser integration is supported by an email parser that consumes email notifications from ESM to create security incidents.

**Configure McAfee ESM - Email Parser integration**

McAfee ESM - Email Parser integration uses email notifications from ESM to drive enrichment, and response workflows.

**Before you begin**

Role required: sn_si_admin

**About this task**

A McAfee ESM email parser template is provided to use for the integration. It must be configured and activated before the integration takes place. Updating the parser activates it.

**Procedure**

2. In the McAfee ESM - Email Parser card, click **Configure**.

3. In the **McAfee ESM - Email Parser Configuration** dialog box, click the **Configure Email Parser** link.

4. Click the **McAfee ESM** link to edit the settings in the template email parser provided. At a minimum, fill in the **Email is from** field.
   To create your own email parser, see **Create email parsers in Security Operations**.

5. Check the **Active** box.

6. Click **Update** in the **Email Parser** form.
   The email parser is active. You do not need to return to **Integration Configurations**.

---

**McAfee ESM - Incident Enrichment Integration**

McAfee ESM - Incident Enrichment integration searches your logs and adds relevant sighting information to your security incidents.

<table>
<thead>
<tr>
<th>Explore</th>
<th>Set up</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Security Incident Response integrations</td>
<td>• Get started with the McAfee ESM - Incident Enrichment integration</td>
</tr>
<tr>
<td></td>
<td>• Create sightings search configuration records</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use</th>
<th>Develop</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Run a Sightings Search</td>
<td>• ServiceNow Security Operations integration development guidelines</td>
</tr>
<tr>
<td>• Security Operations Integration - Sightings Search workflow</td>
<td>• Tips for writing integrations</td>
</tr>
</tbody>
</table>
Get started with the McAfee ESM - Incident Enrichment integration

McAfee ESM protects endpoints against viruses, spyware, Trojan horses, and other malware threats and integrates easily with Security Operations. Before you can use the McAfee ESM - Incident Enrichment integration, you must download it from the ServiceNow Store and add the appropriate API Base URL and login credentials.

Before you begin
Role required: sn_si_admin

Procedure
1. Download the integration from the ServiceNow Store.
2. When the installation is complete, navigate to Security Operations > Integrations > Integration Configuration. The available security integrations appear as a series of cards.
3. In the McAfee ESM - Incident Enrichment card, click New.
4. Fill in the fields, as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of this configuration.</td>
</tr>
<tr>
<td>McAfee ESM API Base URL</td>
<td>The base URL you acquired from the McAfee ESM site.</td>
</tr>
<tr>
<td>Link URL</td>
<td>[Optional] The Link URL that links to an McAfee ESM instance, when available.</td>
</tr>
<tr>
<td>Username</td>
<td>Your McAfee ESM username.</td>
</tr>
<tr>
<td>Password</td>
<td>Your McAfee ESM password.</td>
</tr>
<tr>
<td>Max Rows</td>
<td>The maximum number of rows you want to search.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Earliest Result (days)</td>
<td>The earliest results you want to see in number of days.</td>
</tr>
<tr>
<td>Include raw data samples in search results</td>
<td>Select this to include samples of raw data in your sightings search results. The amount of data returned depends on your setting in the number of rows of raw data property in Security Incident Response properties.</td>
</tr>
<tr>
<td>MID Server</td>
<td>Select Any to use any active MID Server, or select a specific MID Server name.</td>
</tr>
</tbody>
</table>

**Note:** Configuring this integration activates workflows. To manage the workflows, navigate to the **Workflow Editor**.

5. Click **Submit**. The integration configuration card displays.

6. When viewing the new configuration card, you can click **Configure** or **Delete** to change or delete the configuration, respectively.

7. To return to the original list of integration configuration cards, select **No** from the **Show Configurations** drop-down list.

### Microsoft Exchange Online integration

For the Microsoft Exchange Online integration application by ServiceNow, the Now Platform® Security Incident Response (SIR) product is integrated with the Microsoft Exchange Online service, one of the cloud-based services in the Microsoft Office 365 suite of products. Your Security Operation Center (SOC) analyst can search your corporate email environment for security-related threats and remove and remediate phishing emails with email search and delete capabilities.

### Overview

As the security incident analyst, you execute the integration from the security analyst interface, and the workflow returns email message details that match search criteria. Email searches are based on criteria that include subject lines as well as sender and recipient email addresses. After the email search is complete, you can delete suspicious emails from the Microsoft Exchange Online service, and, an optional approval process can be configured to request approval prior to deleting emails.
This email search and delete integration can be used with a broader phishing response incident workflow or runbook. After a corporate user or employee receives a suspicious email and reports it to the company’s phishing response team or inbox, the reported email is forwarded to the Now Platform and categorized as a security incident. After you have verified that an email is a phishing attack, as the analyst responsible for investigating phishing incidents, you can initiate an email search to determine if other corporate users have received this phishing email. The search allows you to locate related emails from the same phishing campaign and identify other potential victims who may have received the email, read it, and also potentially clicked a malicious URL or opened an attachment.

**Key features**

The integration includes the following key features:

- Configure search criteria for phishing threats in Security Incident Response based on combinations of the sender, recipient, and subject fields on email messages.
- For large and lengthy email searches, the security incident analyst is notified via email when the search has successfully completed, along with the number of matched messages.
- Status for individual messages informs you if recipients have read or deleted suspicious emails.
- If configured, optional approval processes ensure that suspicious emails are not deleted without prior approval.
- A complete audit trail for delete requests that includes the number of deleted emails is logged in the work notes of security incidents.
- If tagging is configured, security tags record when email search and delete workflows are initiated and successfully completed on security incidents.

**Supported Microsoft Exchange Online versions**

This integration supports Microsoft Exchange Online services, which are part of the Microsoft Office 365 suite. The integration does not support hosted Microsoft Exchange environments. Microsoft runs Microsoft Exchange Online services on the Exchange 2016 version.

**Supported Now Platform versions**

This integration supports the Kingston, London, Madrid, and NY releases for the Now Platform.

Madrid and later release requirements
For the Madrid release and later family releases, the com.snc.si_dep plugin is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before installing and activating the other Security Operations applications.

The following Security Operations applications must be installed and activated from the ServiceNow Store. Install and then activate one application at a time in the order listed below to ensure a smooth installation:

1. Security Integration Framework
2. Security Support Common
3. Security Support Orchestration
4. Security Incident Response

Integration architecture and systems connection

For more information about the architecture of the integration, including key terms and external systems connection details, see Integration architecture and external systems connection for the Microsoft Exchange Online integration.

Checklist

The following topics are numbered. Follow the topics that are listed below in the order that they are presented for a smooth installation and configuration of the application.

For a printable checklist of these steps, see Checklist for the Microsoft Exchange Online integration. You can use this list to monitor your progress as you work through the end-to-end tasks of the integration set up, configuration, and verification of results.

Set up your Microsoft Office 365 account for the ServiceNow Microsoft Exchange Online integration

Complete the following setup tasks in your Microsoft Office 365 account prior to installing the ServiceNow application for this integration. This account permits access to the Security and Compliance center in the Microsoft Office 365 product.

Before you begin
Role required: Microsoft Office 365 Global administrator

About this task
The integration requires an account in the Microsoft Office 365 service. Follow these steps to create this administrative account. At a minimum, you are required to have an account that permits access to the Security and
Compliance center in the Microsoft Office 365 product. Access to the Security and Compliance center grants this account permission to perform searches across mailboxes of users on the Microsoft Exchange Online server. There are two options for creating this account.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a new account with the Global administrative role.</td>
<td>This account has access to all areas on the Microsoft Office 365 product including the Security and Compliance center. With this option, you can assign the Global administrator role when you create a new user. You can also use an existing user with the Global administrative permission.</td>
</tr>
<tr>
<td>Create a customized role group and assign an existing user to this group with the Compliance Search role.</td>
<td>This account does not have access to the other areas of Microsoft Office 365 product outside of the Security and Compliance center. If you want to limit user access to only the Security and Compliance center, follow the steps to create a custom role group. You are required to assign the Compliance Search role to an existing user when you create the role group.</td>
</tr>
</tbody>
</table>

The images in the following tasks are privileged and proprietary and are used with permission from Microsoft. This content is subject to updates by Microsoft. To verify that you have access to the most current content, see the Microsoft doc website.
Procedure

1. Follow these steps to create a new user account with Global administrative permission on the Microsoft Office 365 service.

   a. Log in to your Microsoft Office 365 account, and, on the Office 365 page that is displayed, click the Admin icon ( ).

   ![Admin Icon](image)

   b. In the left navigation panel on the Microsoft 365 admin center page that is displayed, click Users.

   ![User Panel](image)

   c. On the Home > Active users pane that is displayed, click Add a user.

   ![Add a User](image)
d. Fill in the New User form that is displayed.

An example of a completed form follows the table.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) First name and Last name</td>
<td>First name and last name for your Microsoft account for the ServiceNow application for the integration. The names that you enter auto-fill the Display name and Username fields. If you choose to enter names in these fields, enter the names that you want for this account.</td>
</tr>
<tr>
<td>Display name</td>
<td>If you do not enter names in the First name and Last name fields as described in the preceding step, enter unique names as required for the new user record. The example name shown in the following figure is Service Account.</td>
</tr>
</tbody>
</table>
| Username                              | The user name that you want for the login credentials for this user account. The example shown is ExchangeIntegration. This value is the user name for the new account in the Microsoft Office 365 service. Enter this user name in the API account field during the configuration step in your Now
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform instance</td>
<td>Platform instance. The steps for the configuration in your Now Platform® instance are described in <a href="#">Configure the Microsoft Exchange Online integration with your Now Platform instance</a>.</td>
</tr>
<tr>
<td>Domain</td>
<td>Unique name that appears after @ for email addresses for your organization. For this example, nowsecopslab.onmicrosoft.com is the domain. The domain is automatically displayed for your account on the form. If more than one domain is available in the list, verify that the domain you want to perform emails searches on with the ServiceNow application is displayed.</td>
</tr>
<tr>
<td>Location</td>
<td>Location of your organization. Select the location from the list.</td>
</tr>
<tr>
<td>Password</td>
<td>For this account, click <strong>Let me create the password</strong>. Enter a unique password for this service account so that you can set this password later in your Now Platform instance. Enter this password in the API password field for the Microsoft Office 365 account during the configuration step of your Now Platform instance. For this integration, verify that the <strong>Make this user change their password</strong> check box is cleared.</td>
</tr>
<tr>
<td>Roles</td>
<td>The role for this user. For this example, <strong>Global administrator</strong> is selected.</td>
</tr>
<tr>
<td>Product licenses</td>
<td>The first option for a licensed user should be selected. The default setting is displayed with both options <strong>off</strong> (cleared). You are required to have a licensed user selected</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>to log in to the account. See your Microsoft subscription for more information on licenses.</td>
</tr>
</tbody>
</table>
New user

First name

Last name

Display name *
Service Account

Username *
Domain
ExchangeIntegrationNowsecopslab.onmicrosoft.com

Location
United States

Contact information

Password
Admin-created

Auto-generate password

Let me create the password
Password *

Make this user change their password when they first sign in

Roles
Global administrator

You can assign different roles to people in your organization. Learn more about administrator roles

User (no administrator access)

This user won't have permission to the Office 365 admin center or any admin tasks.

Global administrator

This user will have access to all features in the admin center and can perform all tasks in the Office 365 admin center.

Customized administrator

You can assign this user one or many roles so they can manage specific areas of Office 365.

Alternative email address

Product licenses *
Decision required

Office 365 Enterprise E3

1 of 1000 licenses available

Not Recommended:
Create user without product license
They may have limited or no access to Office 365 until you assign a product license.

Add Cancel
e. At the bottom of the form, click Add.
You have successfully added a new user record and assigned the Global administrator role to the user in your Microsoft Office 365 account. This role permits access to all areas of the Microsoft Office 365 service including the Security and Compliance center.

2. Alternatively, you can create a new, customized role group and assign a user to this group who only has access to the Security and Compliance search permission. This user performs security and compliance searches across mailboxes of users with this permission. The Compliance Search role that you assign to this group is limited to Security and Compliance. The user (member) does not have the broad permissions that are granted to the Global administrator role described in the preceding steps. Follow these steps to create an account that is limited to the Security and Compliance center.

**Before you begin:** Verify that you have created a user account (member) that you can assign to the role group that you create with the Compliance Search permission. For more information on creating users in Microsoft Office 365, see the Microsoft docs website.

a. Log in to your Microsoft Office 365 account, and, on the Office 365 page that is displayed, click the Admin icon.

![Office 365 Admin icon](https://www.office.com/auth=2)

b. In the left navigation panel, navigate to Admin centers > Security & Compliance.
c. On the Security & Compliance pane that is displayed, in the left navigation panel, click Permissions > Create.
d. On the form that is displayed, verify that the **Name your role group** option is selected and enter the name for your role group in the **Name** field.

This name is the name of the group that has access to the Security and Compliance center in your Microsoft Office 365 account. In this example, **Compliance Center Search Group** is entered. Creating this group is required, because it is the only way to relate a user to the compliance search role. This role has access to the Security and Compliance center but not global access to the other areas of your Microsoft Office 365 account.
e. Click **Next**.

f. On the Choose roles pane that is displayed, verify that the **Choose roles** option is selected and click the **Choose roles** link.

g. On the Choose roles pane that is displayed, click **Add**.
h. On the Choose roles pane that is displayed, in the Choose which roles to add from the list below field, enter compliance.

i. Expand the Roles list and select **Compliance Search**.
   This role permits email searches in the Microsoft Exchange Online tenant.

j. At the bottom of the pane, click Add.

k. On the Choose roles pane that is displayed, verify that **Compliance Search** is displayed, and click **Done**.
I. On the Choose roles pane that is displayed, click **Next**.

m. On the Choose members pane that is displayed, click the **Choose members** link.
n. On the Choose members pane that is displayed, click **Add**.

o. On the Choose members pane that is displayed, expand the Members list.

p. From the list of users that is displayed, select the user account that you want to assign to the role group.
q. At the bottom of the pane, click **Add**.

r. On the Choose members pane that is displayed, review the user information and click **Done**.

s. On the Choose members pane that is displayed, click **Next**.

t. On the Review your settings pane that is displayed, verify that the name of the group you created (**Compliance Search**), and the user you selected in the preceding steps are displayed, and click **Create role group**.
You have successfully created a role group that has access to the Security and Compliance center and assigned a user to the group. In the preceding example, secopstest22@nowsecopslab.onmicrosoft.com (the email address), is the user account name assigned to the Compliance Search role. This name is the user name that you also enter in the API account user name field on the configuration page in your Now Platform instance. The password for this user account is the password that you originally set up with the account for secopstest22@nowsecopslab.onmicrosoft.com. Enter the same password in the API Password field on the configuration page in your Now Platform instance. The fields of the configuration form in your Now Platform instance for this integration are described in Configure the Microsoft Exchange Online integration with your Now Platform instance.

What to do next
Create an application ID for OAUTH authentication in the Microsoft Azure portal.

Set up your Microsoft Azure account for the ServiceNow Microsoft Exchange Online integration

Complete the following setup tasks in your Microsoft Azure portal prior to installing the ServiceNow application for this integration. This account permits access to the Microsoft Exchange Online tenant for email message details.

Before you begin
Role required: Microsoft Azure portal administrator

This account is required to access the Microsoft Exchange Online tenant to gather additional email message details and to delete email messages. This account is set up in the Microsoft Azure portal.
The images in the following tasks are privileged and proprietary and are used with permission from Microsoft. This content is subject to updates by Microsoft. To verify that you have access to the most current content, see the Microsoft doc website.

In the following images, ServiceNow Inc. is displayed for the account name in the examples for the Azure portal. In your Azure portal account, the company name for your account in the Azure portal is displayed.

Procedure

If you have not created an application ID for OAUTH authentication in the Microsoft Azure portal, follow these steps.

a. Log in to the Microsoft Azure portal using your Azure portal administrator credentials.

b. In the left navigation panel on the Home pane, click Azure Active Directory.

c. In the Overview pane that is displayed, click App Registrations (Preview).
d. In the App registrations (Preview) pane that is displayed, click **New Registration**.

e. Fill in the Register an application form that is displayed.

An example of a completed form is shown after the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the application. In this example, ServiceNow Exchange Online Integration is entered.</td>
</tr>
<tr>
<td>Supported account types</td>
<td>For this account, in Supported account types, click <strong>Accounts in this organizational directory only</strong></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Redirect URL (optional)</strong></td>
<td>If you enter a value for this field, it is not used by the integration.</td>
</tr>
</tbody>
</table>

f. Click **Register**. An Application ID is created. This ID is similar to a user name. You enter this value on the configuration page in the **OAUTH Application ID** field during the configuration step in your Now Platform instance that is described in Configure the Microsoft Exchange Online integration with your Now Platform instance.

g. With the Application (client) ID displayed in the ServiceNow Exchange Online Integration pane, click **View API Permissions**.
h. In the Request API permissions pane that is displayed, click **Microsoft Graph**.

i. In the ServiceNow Exchange Online Integration - API permissions pane that is displayed, click **Add a Permission**.
j. In the Request API permissions pane that is displayed, click **Application permissions**.

![Request API permissions pane](image)

k. In the Select Permissions field that is displayed, enter **Mail.ReadWrite** and select the **Mail.ReadWrite** check box.

![Select Permissions field](image)

l. Click **Add Permissions**.

m. In the ServiceNow Exchange Online Integration - API permissions pane that is displayed, click **Grant Admin Consent for <your organization name>**.
n. To confirm the previous API selection (Microsoft Graph API) that you entered, click **Confirm**.

o. In the ServiceNow Exchange Online Integration - Certificates & Secrets pane, click **Certificates & secrets** followed by **New Client secret** (password).

p. In the form that is displayed on the ServiceNow Exchange Online Integration - Certificates & Secrets pane, enter the name for the application in the **Description** field, click an option for expiration, and click **Add**.
In the Certificates & Secrets pane that is displayed, in the **Client secrets** section, under **Value**, the row is populated with the new client secret (password). Save this password in a secure location. After you leave this page, this password value is no longer visible. You enter this password in the **OAUTH Client Secret** field on the configuration page during the configuration step for the integration in your Now Platform instance. The configuration steps for the integration are described in **Configure the Microsoft Exchange Online integration with your Now Platform instance**.

You have successfully created an application ID for OAUTH authentication in the Microsoft Azure portal.

**What to do next**

You are ready to set up your Now Platform® instance for the integration.
Set up your Now Platform® instance for the Microsoft Exchange Online integration

The following section lists the setup tasks that you are required to complete in your Now Platform® instance prior to installing the Microsoft Exchange Online application. Review the checklist and verify that you have completed these tasks before you download and install Microsoft Exchange Online application for the integration to ensure a smooth installation and configuration.

Before you begin
Role required: admin

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have assigned the required Now Platform® and Security Incident Response (SIR) roles.</td>
<td>The following ServiceNow roles are required:</td>
</tr>
<tr>
<td></td>
<td>• The system administrator (admin) installs applications and assigns the security incident administrator (sn_si.admin) role.</td>
</tr>
<tr>
<td></td>
<td>• The security incident administrator (sn_si.admin) configures the application for the integration. If required, the security incident administrator role also assigns the security incident analyst (sn_si.analyst) the email read and write roles (sn_sec_cmn.cap_email_write and sn_sec_cmn.cap_email_read). The (sn_sec_cmn.cap_email_read) and (com.snc.security_incident) roles are installed with the Security Incident Response product. They are assigned to the security incident administrator by default and can be reassigned as required.</td>
</tr>
<tr>
<td></td>
<td>• The security incident analyst (sn_si.analyst) performs email searches and deletes emails. This role also verifies that emails have been deleted and works with security incidents.</td>
</tr>
<tr>
<td>Setup task</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| ◦ The write role permits the sn_si.analyst to edit, create, and perform email searches and to delete messages. There is no separate role that is required to delete messages.  
◦ The read role permits the sn_si.analyst to view results on related lists on security incidents.  
Note: The sn_si.analyst must have the (sn_sec_cmn.cap_email_read) and (sn_sec_cmn.cap_email_write) roles to view email search results and create and perform email search queries. | If not assigned, the following the steps describe how to assign the (sn_sec_cmn.cap_email_read) and (sn_sec_cmn.cap_email_write) roles to the security incident analyst.  
For more information about assigning roles in Security Incident Response, see Roles installed with Security Incident Response on the ServiceNow Product Documentation website. |
<p>| Verify that you have setup a Windows MID Server in your Now Platform instance. | The MID Server is required in your Now Platform environment. Although both the Microsoft Exchange Online product and the Now Platform are cloud offerings, a MID Server is required for this integration. The PowerShell script runs from a Windows server in the customer environment to connect to the Microsoft Exchange Online server via a MID server. |</p>
<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>An outbound HTTPS connection from the MID server is necessary for the integration to retrieve information from the Microsoft Exchange Online service tenant. For more information on MID servers and MID server set up, see MID Servers on the ServiceNow Product Documentation website. You test the connection between your instance and the Windows MID Server after installing the application during the configuration step of the integration.</td>
<td></td>
</tr>
<tr>
<td>Set up the Windows MID Server to handle Microsoft Exchange Online queries</td>
<td>• Set up Windows Remote Management (RM) Basic Authentication on the designated MID Server(s). • Assign WinRM Basic Authentication and PowerShell capabilities to the designated MID Server(s).</td>
</tr>
<tr>
<td>Set up Windows Remote Management (RM) Basic Authentication on the designated MID Servers.</td>
<td>• Configure Windows Remote Management (RM) Basic Authentication: To allow the Now Platform instance to invoke Windows Powershell based cmdlet queries, you must configure the Windows Remote Management (RM) Basic Authentication on the designated MID Servers. This allows you to maintain security for communication between these endpoints by supporting standard methods or authentication and message encryption. The Microsoft recommended procedures for enabling Window Remote Management Basic Authentication can be found here: <a href="https://">https://</a></td>
</tr>
<tr>
<td>Setup task</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Validate that Windows Remote Management (RM) Basic Authentication is Enabled: To validate that basic authentication is enabled, run the following command:</td>
<td>docs.microsoft.com/en-us/windows/win32/winrm/authentication-for-remote-connections</td>
</tr>
<tr>
<td>Assign WinRM Basic Authentication and PowerShell capabilities to the designated MID Server(s).</td>
<td>After you have configured the designated MID Server(s) with the Windows Remote Management Basic Authentication functionality, you must update the MID Server configuration to selectively route the Microsoft Exchange Online queries to the designated MID Servers. For example, if you decide to configure Windows Remote Management on a subset of your MID servers, only those MID Servers can be used to process the integration queries. Configure the New WinRM Basic Authentication capability on the designated MID Server(s): After the MID Server has been configured, a new MID Server capability called <strong>WinRM Basic Authentication</strong> is added to the list of available MID Server capabilities. Use this new capability to tag the MID Servers to which the email searches are routed. When you access your MID server by typing MID Server in the left navigation search, you will see a list of your configured MID Servers. When you access a particular MID server record, you will see a list of configured capabilities. Select the...</td>
</tr>
</tbody>
</table>
In your current MID Server environment, if you have set the Capabilities to **ALL** for every MID Server, the **WinRM Basic Authentication** is added automatically for all the MID Servers. In this case, any of the MID Servers in your environment may receive Microsoft Exchange Online integration search requests.

To ensure that the search requests are sent only to the designated MID Servers and to prevent incorrect search routing, click **Edit** and follow these steps:

- Remove the **ALL** Capability from any MID Server that does not have the required **WinRM Basic Authentication** functionality.
- Select the required capabilities as shown below and click **Save**.
<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration.</td>
<td>For the Madrid release and later family releases, the Security Incident Response Dependency plugin (com.snc.si_dep) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications required by the integration. Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation. 1. Security Incident Response 2. Security Integration Framework</td>
</tr>
<tr>
<td>Setup task</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>3. Security Support Common</td>
<td>For more information on setting up your Now Platform instance for the integration, see <a href="#">Get entitlement for a Security Operations product or application</a> and <a href="#">Activate a ServiceNow Store application</a>.</td>
</tr>
<tr>
<td>4. Security Support Orchestration</td>
<td></td>
</tr>
</tbody>
</table>

If your organization plans to use Now Platform emails notifications, verify that the email send/receive capability is enabled.

<table>
<thead>
<tr>
<th>If your organization plans to use Now Platform emails notifications, verify that the email send/receive capability is enabled.</th>
<th>Follow these steps to verify that email send and receive capability is enabled in your Now Platform® instance. This capability notifies users via email when searches and delete requests have been initiated and successfully completed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Navigate to <strong>Email properties &gt; Administration &gt; Email Properties</strong>.</td>
<td></td>
</tr>
<tr>
<td>2. In Outbound Email Configuration, verify that Email sending enabled and Email receiving enabled are selected.</td>
<td></td>
</tr>
<tr>
<td>This email send/receive capability is required so that your security incident analyst receives email notifications sent by the Now Platform®. If the delete approval feature is enabled, requests to delete emails are also sent to approvers via email. Other than enabling this email property, there is no other setup required to send and receive emails in the Now Platform®.</td>
<td></td>
</tr>
</tbody>
</table>
Setup task

About this task
As a Now Platform security incident administrator (sn_si.admin), the email read and write (sn_sec_cmn.cap_email_read) and (sn_sec_cmn.cap_email_write) roles are automatically assigned to you when you download the Security Incident Response (SIR) product. As security incident administrator, you assign these roles to the security incident analyst (sn_si.analyst) or another role. If you have not assigned these roles to the security incident analyst, or to another role, follow these steps to assign them.

Role required: admin

Procedure
1. Navigate to Organization > Users.
2. Click the Users module.

If the user is a new user, follow these steps to add the user.
a. On the Users list that is displayed, click **New**.

![Image of the Users list display](image)

b. On the new user form that is displayed, fill out the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserID</td>
<td>User ID for the Now Platform security incident analyst role, for example, <code>jferguson</code>.</td>
</tr>
<tr>
<td>Email</td>
<td>Company email address. The notifications for email search results and email delete confirmations are sent to this email address. For this example, <code>jferguson@servicenow.com</code> is used, but any company email address can be used to receive these email notifications as required by your organization.</td>
</tr>
<tr>
<td>First name</td>
<td>First name</td>
</tr>
<tr>
<td>Last name</td>
<td>Last name</td>
</tr>
<tr>
<td>Title</td>
<td>Security incident analyst, or Security Analyst, or Security Operations Center (SOC) Analyst, for example.</td>
</tr>
</tbody>
</table>
c. Click Submit.  
The new user is displayed on the Users list.

3. In the Users list in the User ID column, click the name of the user you want to assign the `sn_sec_cmn.cap_email_read` and `sn_sec_cmn.cap_email_read` roles to.

4. On the open record in the Related Links section, click Edit.
5. On the Edit Members form that is displayed, enter `sn_sec_cmn.cap_email_read` in the collection field.

**Note:** The column below the field auto-populates. If the user has not been assigned the `sn_si.analyst` role, enter `sn_si.analyst` in the Collection field as well. In the following figure, the `sn_si.analyst` role already has been assigned to Joe Ferguson.
6. In the Collection column, select then move `sn_sec_cmn.cap_email_read` and `sn_sec_cmn.cap_email_read` and `sn_si.analyst` (if not already assigned) to the Roles List.
7. Click **Save**.
   The `sn_sec_cmn.cap_email_read` and `sn_sec_cmn.cap_email_read` roles are assigned to the security analyst (jferguson).

8. Add users and assign roles as required for your organization.

9. If you want to enable the optional approval capability for email delete requests, follow these steps to create an approval group.
   Role required: admin

   a. Navigate to **User Administration > Groups**.

   ![User Administration Groups](image)

   b. In the Groups list that is displayed, click **New**.

   ![User Administration New Group](image)
c. Fill in the form.

An example of a completed form follows the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the group that processes an approval when an email delete request is submitted, for example, Exchange Online Approvers.</td>
</tr>
<tr>
<td>Group email</td>
<td>Enter an email address if you want a Group email distribution list or the email address of the point of contact, such as the group manager. Leave this field blank if you want email notifications sent to the individual email addresses for each user in the group.</td>
</tr>
<tr>
<td>Manager</td>
<td>(Optional) Name of group manager. Click the search icon to view the list.</td>
</tr>
<tr>
<td>Parent</td>
<td>(Optional) If this group has a parent, the other group this group is a member of.</td>
</tr>
<tr>
<td>Type</td>
<td>(Optional) Define categories of groups.</td>
</tr>
<tr>
<td>Vendors</td>
<td>(Optional) Assign the vendor manager role to users who are involved with the vendor management process of your organization.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Additional information about the group.</td>
</tr>
</tbody>
</table>
For more information about creating groups and assigning roles, see Create a user group on the ServiceNow Product Documentation website.

d. Click Submit.
In the Name column, the new group is displayed on the Groups list.

You can add more users to this group. A user inherits roles from all groups to which the user belongs. You can also assign roles directly to a user. For more information about assigning roles to groups and users, see Roles on the ServiceNow Product Documentation website. Each user can approve email delete requests submitted by the security analyst. Only one user is required to approve or reject the request.

If your organization wants an extra level of control over deleting emails with this integration, enable the optional approval capability. Select the Enable check box on the Additional Settings tab during the configuration step.
to enable approvals. In the preceding example, each user of the Exchange Online Approvers group is available to process delete requests via email notification.

Install the Microsoft Exchange Online application for the ServiceNow Microsoft Exchange Online integration

Before you run the integration on your instance, install the Microsoft Exchange Online application for the integration from the ServiceNow Store.

Before you begin
Before you install the application from the ServiceNow Store on your Now Platform instance, complete all the tasks listed in the prerequisite checklists.

Role required: admin

Note: If you install demo data, a demo configuration without credentials is automatically created. This can cause errors. For details, see KB0755880.

Procedure
If you have not installed the application for the integration, see Install a Security Operations integration and follow the steps to install it.

Related information
Set up your Microsoft Office 365 account for the ServiceNow Microsoft Exchange Online integration
Set up your Microsoft Azure account for the ServiceNow Microsoft Exchange Online integration
Set up your Now Platform instance for the Microsoft Exchange Online integration

Configure the Microsoft Exchange Online integration with your Now Platform instance

After you have installed the application from the ServiceNow Store, configure it to connect to your Now Platform instance. This activation activates the search and delete workflows.

Before you begin
Role required: sn_si.admin
Procedure

1. In your Now Platform instance, navigate to Security Operations > Integrations > Integration Configurations.
2. Locate the Microsoft Exchange Online tile.
3. Click Configure.

4. In the Microsoft Exchange Online Configuration dialog that is displayed, click Configure Exchange Online.

   An example of a completed and validated form follows the table.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection Settings tab</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Tenant</strong></td>
<td>The Microsoft Exchange Online tenant that you want to perform searches on. This text is the unique name that appears after @ for email ad-</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>API account</td>
<td>User name of the API account. This text is the user name for the API account that you created in Microsoft Office 365 during the set up for the integration. This account provides access to the Security and Compliance center, and it is used to search across mailboxes for matching emails. For more information, see Set up your Microsoft Office 365 account for the ServiceNow Microsoft Exchange Online integration.</td>
</tr>
<tr>
<td>API password</td>
<td>API password. This value is the password for the API account that you created in Microsoft Office 365 during the set up for the integration. This password provides access to the Security and Compliance center account that is used to search across mailboxes for matching emails. For more information, see Set up your Microsoft Office 365 account for the ServiceNow Microsoft Exchange Online integration.</td>
</tr>
<tr>
<td>OAUTH Application ID</td>
<td>The Application (client) ID that was generated for the account that you created in the Microsoft Azure portal. For more information, see Set up your Microsoft Azure account for the ServiceNow Microsoft Exchange Online integration.</td>
</tr>
<tr>
<td>OAUTH Client Secret</td>
<td>Password (client secret) for the account that you created in the Microsoft Azure portal. For more information, see Set up your Microsoft Exchange Online integration.</td>
</tr>
</tbody>
</table>
### Option

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td><strong>Azure account for the ServiceNow Microsoft Exchange Online integration.</strong></td>
</tr>
<tr>
<td><strong>Additional Settings tab</strong></td>
<td>The email search history range in number of days. The integration searches for email messages that have been sent or received in the Microsoft Exchange Online server for the number of calendar days that you enter. You are required to enter a value between 1-30. 30 days is the default and the maximum number of days you can enter for a search. Entering a low number of days in the search window range improves response time, but you may not capture all matched messages as a result. This global setting is for all searches. Prior to executing the email search, there are no parameters that permit you to modify this value for individual searches.</td>
</tr>
<tr>
<td><strong>Email Search Window (days)</strong></td>
<td>Use this option to set the search timeout threshold. If the timeout threshold is reached, the search ends and no results are displayed. You can specify a default value of 90 minutes and a maximum value of 240 minutes. By setting this threshold, you can avoid endless search loops that could cause performance issues on the Microsoft Exchange Online tenant and the ServiceNow instance.</td>
</tr>
<tr>
<td><strong>Maximum Search Duration</strong></td>
<td>Security tag. Default is selected. When enabled, security tags are automatically applied to related security incidents when search and delete</td>
</tr>
<tr>
<td><strong>Tagging</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Recover Deleted Emails</td>
<td>Default is selected. This item only applies to emails that you have deleted using this integration. If you do not want users in your organization to have access to the emails that you have deleted, verify that this check box is cleared. If the check box is cleared, the emails that you delete using the workflow of this integration are permanently deleted and placed in the Purges folder. This folder is a sub folder within the Recoverable Items folder on Microsoft Exchange Online that a user normally cannot access. If you want users to recover the emails you delete, select this check box. If this check box is selected, depending on how the user's account is configured in Microsoft Exchange Online, the emails you delete using the workflow of this integration are placed in the Deleted Items folder in the mailbox of the user. If an account is configured so that the user can view the Deleted Items folder in their mailbox, the user can recover the emails you delete from their Microsoft Exchange Online account. For more informa-</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Recover deleted items or email in Outlook Web App.</td>
<td>Select this option to enable notifications when the search is completed. If the <strong>Enable</strong> check box is selected, you will receive notifications if any matching emails are found. If the check box is cleared, search completion notifications are not sent.</td>
</tr>
<tr>
<td>Search Completion Notification</td>
<td>Request approval to delete emails. Default is cleared. When the check box is cleared, the optional approval process for requesting prior permission before deleting emails from the Microsoft Exchange Online service is disabled. Verify that this check box is cleared if you want to grant your security incident analyst permission to delete emails without requesting prior permission. If enabled, a request is submitted via email to each member of an approval group. From the choice list, select an approval group from the list. For more information about creating an approval group, see <a href="#">Set up your Now Platform instance for the Microsoft Exchange Online integration</a>. After a request is submitted to an approval group, only one approval is required from the group to complete the request. Any member of the approval group has approval authority. Having a group with more than one person with approval permission ensures that these requests are processed in a timely manner.</td>
</tr>
<tr>
<td>Approvals</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Failure Notiﬁcations</strong></td>
<td>Select the checkbox to enable failure notifications when the search or delete action fails due to invalid OAUTH credentials. If Enabled, failure notifications are sent via email to each member of failure notifications group when OAUTH credentials are invalid. If the check box is cleared, no failure notifications are sent.</td>
</tr>
<tr>
<td><strong>Email Result Threshold</strong></td>
<td>Starting with version 10.3, you can specify an email delete threshold for approvals. If the number of emails being deleted is greater than or equal to the value specified here, the Delete request must be approved before the Delete action is invoked. If the threshold value is set to 1, every Delete request must be approved.</td>
</tr>
</tbody>
</table>

The following image is an example of a completed form that is validated.
5. Choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Save</strong></td>
<td>Save your edits. This action does not verify your connection.</td>
</tr>
<tr>
<td><strong>On the Connection Settings tab, click Validate.</strong></td>
<td>This action validates your API and OAUTH credentials and your MID server connection. If your credentials are valid, the Validate button and both small colored icons are green.</td>
</tr>
</tbody>
</table>

**Trouble?**

If an error message is displayed, or one or more of the colored icons to the right of the Validate button are red, verify that the user account credentials you entered are valid. Enter your credentials and click **Save** again.

Refer to the following table for more information about the Validate button and the colored icons.
<table>
<thead>
<tr>
<th>State of Validate button and icons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validate button is green and all the small colored icons are green.</td>
<td>Indicates that the MID Server connection and the credentials (API and OAUTH) are valid.</td>
</tr>
<tr>
<td>Validate button is light red with a blue border and one or all the small colored icons are orange.</td>
<td>The validation is in process. Validation may take a few more moments to complete.</td>
</tr>
</tbody>
</table>
| Validate button is light red and one or all of the small colored icons are red. | • API or OAuth Credentials button is red: Indicates that the API or OAuth credentials are invalid.  
• API Credentials and MID Server Ready buttons are red: Indicates that the MID Server is not reachable and therefore, API authentication through the MID Server has failed.  
• API Credentials button is red but MID Server Ready button is green: Indicates that the MID Server is active and configured correctly, but the API credentials are incorrect. |

**Define email search criteria and request a search on the Microsoft Exchange Online service**

As a user with the sn_si.analyst role, define search criteria and submit an email search request based on incident details on a security incident record. The status of individual messages that match the search query and the results of the search are reported on the security incident record. If email notifications are enabled, you can view the search results from an email message.

**Before you begin**

This procedure shows results in the UI format that is available in the Kingston release. For information about the London and Madrid user interfaces, see Managing security threats using the Security Analyst Workspace on the ServiceNow Product Documentation website.

The figures in this procedure are shown with Tabbed forms selected in System Settings. For more information about selecting and clearing tabbed forms, see the section titled, Display tabbed forms in Configuring the form layout on the ServiceNow Product Documentation website.
About this task
Search criteria may include message sender addresses, recipient addresses, or subject names. The following combinations of message Subject, Sender, and Recipient search parameters are often used for finding phishing-related email messages that may be part of a single phish campaign:

- Find all original emails sent by a phishing account: Search by sender.
- Find all original emails for a single phishing campaign: Search by subject and sender.
- Find all emails received for a single phishing campaign (original and forwarded, any sender): Search by subject.
- Find all forwarded emails for a single phishing email from a single user: Search by recipient + subject.
- Find all phishing-related emails sent to a single user: Search by sender + recipient.

Note: Searches are conducted on emails sent or received within last 30 calendar days, unless a shorter search window is configured during the initial setup. A successful email search is required before you can delete emails.

The following example shows you how to initiate a search from a Now Platform security incident. A security incident is created based on the original email of a suspected phishing attack in the Microsoft Exchange Online server of your organization. For this example, the search criteria is Sender (From) plus Subject, where From is phisher@cbazyx.com, and the Subject is log in to your account.

Results for searches on subjects are returned when the search finds text strings that contain key words that match the entered search criteria. In this example, the subject is log in to your account. Use the AND operator to separate the From and Subject search conditions to return results for all the email messages that contain these given search criteria. The following steps describe how to set up a search that finds only emails that contain subject line text sent by a specific phishing account.

Role required: sn_si.analyst

Procedure
1. Navigate to Security Incident > Show All Incidents and locate the security incident that you are working with.
2. Alternatively, follow these steps to set and run a filter so that only security incidents created by phishing events are displayed.
a. Navigate to **Security Incident > Show All Incidents** to open the Security Incidents list.

b. In the upper-left corner of the list that is displayed, click the filter icon.

c. In the fields that are displayed, select **Short description > contains** from the choice lists, then enter **user reported phishing** and click **Run**.

The phishing-related security incidents are displayed.
d. Use the text in the Short description column to help you locate the security incident that you are working with.

e. In the Number column, click a security incident to open a record.

3. Scroll to the bottom of the Security Incident record and click the Email Search related list.

If the Email Search related list is not displayed, click the **Show All Related Lists** related link to display this related list.

4. In the Email Search related list, click **New** to create a new email search record. The Email Search form is displayed. If you determine that you want to rerun this search query for the same phishing-related incident with minor modifications, you can use this search query record again. However, it is unlikely that you would use this search for a different phishing-related incident, because phishing campaigns are dynamic and the sender and message fields often change.

5. **Optional:** To edit an existing search query record, click **Edit**.

6. On the Email Search form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Information to describe the type of search. For this example, a name for a From + Subject search is <strong>Phish &quot;log in to your account&quot;.</strong></td>
</tr>
<tr>
<td>Description</td>
<td>Information about the search in the email server. An example for this</td>
</tr>
</tbody>
</table>
7. Click **Submit**.
   The security incident is displayed and the name of the email search is displayed in the Email search column in the Email Search related list. Before you can use this new search query, search criteria must be defined for the search record.

8. To define search criteria, with the Email Search related list selected, in the Email search column, click **Phish "log in to your account"**.
9. On the Email search record that is displayed, click the Email Search Criteria related list, and click **New**.

![Email Search Criteria form](image)

10. On the Email Search Criteria form, fill in the fields.

   An example of a completed form follows the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email search</td>
<td>Field is populated automatically with the name that you entered for the Email Search record.</td>
</tr>
<tr>
<td>Search icon</td>
<td>Lookup using list. A list of saved searches. Click the icon to open a list of saved email searches. Click an item in this list to remove the current search and select a previously saved email search.</td>
</tr>
<tr>
<td>Information icon</td>
<td>Icon used to view the Email Search record. Click the icon to view the email search record.</td>
</tr>
<tr>
<td>Search field</td>
<td>Search criterion (<strong>Subject</strong>, <strong>From</strong>, or <strong>Recipient</strong>). Select the search criterion from the choice list and define a value that you want to search for in the text field. For this example, start with <strong>From <a href="mailto:phisher@cbazyx.com">phisher@cbazyx.com</a></strong> (the email address of the phisher).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>address of the sender of the phishing email).</td>
<td></td>
</tr>
<tr>
<td>Active</td>
<td>Option for activating the search. The search is activated by default. If you clear this option, this record is not included in a search.</td>
</tr>
<tr>
<td>Operator</td>
<td>Operators (AND, OR) to further define your search. <strong>AND</strong>: The system searches for the conditions separated by <strong>AND</strong> and returns results only if all the conditions are met. For the sender-plus-subject search, use the <strong>AND</strong> operator so that both search conditions are met during the email search. For this example, use the <strong>AND</strong> operator so that the query is From (Sender) = <a href="mailto:phisher@cbazyx.com">phisher@cbazyx.com</a> <strong>AND</strong> Subject = log in to your account. <strong>OR</strong>: The system searches and returns results if any of the conditions separated by <strong>OR</strong> are met. An example is From (Sender) = <a href="mailto:phisher@cbazyx.com">phisher@cbazyx.com</a> <strong>OR</strong> From (Sender) = <a href="mailto:phisher-2@cbazyx.com">phisher-2@cbazyx.com</a>.</td>
</tr>
<tr>
<td>Order</td>
<td>If you enter more than two search conditions, use Order to prioritize the conditions. 100 is the default. Enter a value between 1 and 100 for each condition, for example, 100, 95, 90, 80. The condition with the lowest number assigned has the highest search priority within a group of conditions.</td>
</tr>
<tr>
<td>Search text</td>
<td>The text values (key words) for the search (email addresses or subject lines).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>The search field contains the text used in the search, for example, <a href="mailto:phisher@cbazyx.com">phisher@cbazyx.com</a>. For the search to return results accurately for Sender (From) and recipient searches, the search strings must match exactly. For subject searches, the search string can contain key words that are part of a larger string. For example, a subject may contain the exact search string that is matched in a forwarded or a response message header such as FW: log in to your account and change your password immediately. For example, Log in to your account are exact key words in the string log in to your account and change your password immediately. No wildcard (*) designation is required to support a contains type of search. Currently, no filtering method exists for matching an exact search string that is not part of a larger text string.</td>
</tr>
</tbody>
</table>

11. Click **Submit**. The Email Search record is displayed. In the **Query from criteria** field, the search criteria you added for the Sender (From) is displayed.
12. To update this email search criteria with more information so that the query includes the subject-plus-sender condition that you want, follow the steps to add another search condition.

a. In the Email Search Criteria related list, click **New**.

b. From the **Search field** list on the Email Search Criteria record that is displayed, select **Subject**.

c. From the **Operator list**, select **AND** or **OR**.

If you select **OR**, the search returns results if either key words in the subject line text string are matched, or the email address condition is matched. **AND** is selected for this example so that the search returns results only for emails that contain the key words of the subject text string and that match the email address of the sender.
d. In the Search text field, enter the value for subject line text, log in to your account.

![Screenshot of the ServiceNow interface showing the Search text field and the log in to your account option.]

e. Click Submit. The new condition is displayed in the Email Search Criteria related list, and both conditions are displayed in the Query from criteria field separated by the AND operator.

![Screenshot of the ServiceNow interface showing the Query from criteria field with AND operator.]  

f. Optional: If you have more than two search conditions, and you select AND to separate each condition, set the order value to prioritize them.

![Screenshot of the ServiceNow interface showing the order value for the search conditions.]  

g. Continue to add, modify, or remove search criteria as desired and click Update to save your changes to the record.
13. Choose one option to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Update</strong></td>
<td>Update and save your changes to the record.</td>
</tr>
<tr>
<td><strong>Search on Email Server(s)</strong></td>
<td>Initiate a search on the servers with the criteria that you saved on the Email Search Criteria record.</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Delete this Email Search record from your Now Platform instance. This action does not delete the actual email messages. It only deletes the search record used for finding messages. A dialog box is displayed. If you click <strong>Delete</strong>, the email search results and email search criteria for this search record are deleted. If a record has search results, the following warning is displayed.</td>
</tr>
</tbody>
</table>

14. To initiate an email search, on the email search record, click **Search on Email Servers(s)**.
A message is displayed that indicates the search request is submitted.

On the Security Incident record, a work note is displayed indicating that a search has been initiated.

If tagging is enabled, at the top of the Security Incident record, the Email Search - Initiated security tag is displayed.
After the search is successfully completed, if email notifications are enabled, an email is sent to the email address of the individual who initiated the search. In this example, the user with the sn_si.analyst role, Hans SecAnalyst, submitted this search. The following image shows that this notification is sent to an account in Microsoft Exchange Online. However, these notifications can be sent to a different email service, as required.

This notification lets you view any matched results that require follow-up and deletion. The following example shows that there is one email that matched the search criteria. An Email search result link to the email search result record in your Now Platform instance is also provided. If you want to view the search record, click this link.

15. From this email, to view the search results, click the Email search result link.
The email search result record is displayed. On this record, you can verify and review the following data.

- In the **Raw data** field, the email count for the number of emails that matched the search criteria 
  "count":1, and the mailbox addresses where the emails were found are displayed
  ["JuanCustomer@nowsecopslab.onmicrosoft.com"].

- In the **Recipients** column, the recipient is
  (JuanCustomer@nowsecopslab.onmicrosoft.com)

- In the **Sender** column, the source of the email is displayed.

- In the **Email date received** column, the date and time the email was received is displayed to help you track phishing campaign time lines.

- In the **Email read status** column, the email in this example has not been read (false). If an email has been read, true is displayed.

- In the **Was deleted** column, the email in this example has not been deleted. If an email has been deleted, true is displayed.

16. Alternatively, to view the search results from the security incident, follow these steps.
a. Navigate to **Security Incident > Incidents** and open the security incident that you are working with.

At the top of the record, when the search is successfully completed, the **Email Search - Completed** security tag replaces the **Email Search - Initiated** security tag.

Work notes are displayed that the search is successfully completed and that one matching email was found.
b. Scroll to the bottom of the Security Incident record and click the Email Search related list. If the Email Search related list is not displayed, click the **Show All Related Lists** related link to display this related list.

The Email Search related list is displayed.

c. With the Email Search related list selected, in the Email search column, click the name of your search.
d. In the Email Search record, click the Email Search Results related list.

e. In the Search date column, click the date of your search to display the data.
The email search result record is displayed.

After an email search is successfully completed, evaluate the results. If you determine that emails require remediation, you are now ready to delete emails, or request delete approval.

Request delete approval for emails on the Microsoft Exchange Online service

After an email search is successfully completed and matching messages are identified, as a user with the sn_si.analyst role, you can permanently delete all the suspicious emails from the Microsoft Exchange Online service that are related to the security incident and phishing campaign. If the approvals and email notifications are enabled, send a request to delete emails to an approval group prior to email removal.

Before you begin
The system performs deletions on your latest successful search results.
Role required for requesting delete approval: sn_si.analyst

About this task
Email search results are displayed with any messages that have been received. To ensure that phishing emails are successfully deleted, the delete results are posted to the work notes of the associated security incident. If tagging is enabled, a security tag is also displayed on the related security incident. If the email is not successfully deleted, you are also notified in the work notes. Depending on your organizational policies, you may need to request approval prior to deleting phishing emails. The delete approval process requires
information on the number of emails to be deleted and, potentially, access to other message details. For processing the delete request, in an email notification, an approver is provided with the matching email message count, the security incident link for access to complete message details, and approve or reject links. The links in this email permit an approver to accept or reject the delete request from the email notification. A full audit trail with a time stamp is also available that tracks when the approval status changed in work notes. If an approval group is assigned, one user in the group may process the request for the entire group. Each member of the approval group receives an email notification for the request.

As a user with the sn_si.analyst role, if you determine that emails require remediation, follow the required steps to delete emails. If approvals are enabled, request approval to delete emails from the Microsoft Exchange Online service.

Procedure
1. Navigate to Security Incident > Show All Incidents.
2. Click the Email Search related list.

3. With the Email Search related list selected, in the Email search column, click the name of your search.
The search results are displayed in the Email Search Results related list.

For this example, this search has found emails that match your search criteria. There are two search actions listed on the record. One search has no matches (0), and the other search has one matching email (1).

4. To delete email items associated with a search, to the left of the Search Date column, select the check box of a search result set. You can select a single result set, or multiple result sets from the list.

5. Select the result sets that you want to delete.
6. At the bottom of the Email Search Results related list, from the Actions on selected rows list, select **Delete Emails from Exchange Online** to delete all the email items associated with one or more result sets from the Exchange Online server.

If a result set contains more than one email, you are not required to open the Email Search Result record and select individual emails to delete them. All emails items with a status of **false** in the Was deleted column in the Email Search Result record are deleted after you select **Delete Emails from Exchange Online**.

If an email item in a result set has already been deleted, the status in the Was deleted column in the Email Search Result record is **true**. These items are not deleted again.

If the approval option is disabled during the configuration step, after you select **Delete Emails from Exchange Online**, the emails associated with the result set are deleted. The result set itself is not deleted. However, the status of all the deleted email items of the result set is updated to **true** in the Was deleted column of the Email Search Result record. For more information on the approval feature, see Configure the Microsoft Exchange Online integration with your Now Platform instance.
These emails are deleted from the Microsoft Exchange Online tenant that you performed the searches on. A work note is displayed if the emails are successfully deleted.

On the security incident record, the **Email Delete - Completed** security tag is displayed.

If approvals are disabled for delete requests, you have successfully deleted emails from the Microsoft Exchange Online tenant.

If approvals are enabled for delete requests during the configuration step, after you select **Delete Emails from Exchange Online**, an email notification is sent to each member of the approval group that you selected during the configuration step.
If tagging is enabled during the configuration step, the Email Delete - Initiated security tag is displayed on the related security incident record. For more information on tagging, see Configure the Microsoft Exchange Online integration with your Now Platform instance.

Work notes are displayed that a request to delete emails is submitted by the user with the sn_si.analyst role (Hans SecAnalyst).

If approvals are enabled, the next step is to process the delete request.
7. Alternatively, if you want to view the details and individual email items of a search record prior to deleting it or submitting a delete request, follow these steps.

a. With the Email Search Results related list selected, in the Search date column, click the date of a search that you want to review.

![Image of Email Search Results](image)

The following information about the emails is displayed:

- Recipients
- Sender
- Email date received
- Email read status (true or false)
- Was deleted (true or false)
- Deleted By Integration (true or false)

⚠️ Note:

Value is set to true when the email is deleted when the analyst initiates the Delete from Email Server(s).

The work notes is updated with the total number of deleted records which includes the records deleted by integration and user.

For this example, the matching email has not been read (false) or deleted (false).
b. After you have reviewed the data, to delete all the emails, or send a request to delete all the emails, click **Delete from Email Server(s)**.

As described in the previous example, if there is more than one email listed on the search result record, you do not need to select the individual emails to remove them. The delete request removes any emails associated with the search when `false` is displayed in the Was deleted column from the latest search results.

If approvals are enabled, you have successfully submitted a request to delete emails. The security tags and work notes are displayed on the related security incident record as described in the previous example. As an approver, the next step is to process the delete request.
Approve delete email requests for the Microsoft Exchange Online integration

If the approval option is enabled in your Now Platform instance, requests to delete emails are sent to each member of the approval group via email. You select the approval group during the configuration step. Approvals provide your organization with an additional level of control over the deletion of emails.

Before you begin

Verify that you have the Approvals option selected on the Additional Settings tab of the Exchange Online Search and Delete Emails Configuration Settings form.

Verify that you have enabled the email Email sending enabled and Email receiving enabled options in your Now Platform instance for approval requests. For more information, see Set up your Now Platform instance for the Microsoft Exchange Online integration.

When the user with the sn_si.analyst role submits delete email requests, by default, these requests are sent via email to the sn_si.admin. If you have created an approval group, each member of the group receives a notification. Approvers can process email delete requests directly from the email notification. Alternatively, requests can be processed from the email search result records in Now Platform instances. This topic shows both approval methods.

The following information describe the request in the email notification:

**Email Search Result record number**

Unique number assigned to the search record by the Now Platform as part of the audit trail.

**Name of the analyst who submitted the request**

Name of the person who submitted the request as part of the audit trail.

**Link to the security incident**

A link to the security incident related to the phishing event. View the security incident with the work notes, email searches, and email search results directly from the email.

**Approve or Reject links**

Links to approve or reject the request from the email notification. After you click either link, the system automatically initiates the related workflow and a work note is posted to the security incident record.

Role required: sn_si.admin or all members of an assigned approval group.
**Procedure**

1. To process the delete request from the email notification, follow these steps.

   a. As an approver, locate the notification email in the email account that you configured in your Now Platform user account.

      In this example, the user with the sn_si.analyst role (Hans SecAnalyst) submits a request to delete one email. Johann SecAdmin is a member of the approval group.

      ![Email notification image]

      A phishing deletion approval request has been submitted for Email Search Result ESR0001002

      A phishing deletion approval request has been submitted by Hans SecAnalyst. The request is to delete 1 email(s) that are part of a phishing campaign. Please review and approve this request as soon as possible. Additional details on the phishing emails can be found on the security incident located here - SRBO101002

      Click here to approve

      ![Click here to approve image]

      The status of all the email items of the result set is updated to **true** in the Was deleted column of the Email search result record.

      A work note is posted to the security incident record with the number of successfully deleted emails. If tagging is enabled, the Email Delete - Com-
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Completed tag replaces the Email Delete - Initiated tag.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Reject the delete request. A work note is posted with the name of the person who rejected the request.</strong></td>
<td>After a request is rejected, as the user with the sn_si.analyst role, you are required to submit a new delete request if you determine that the emails should be deleted.</td>
</tr>
<tr>
<td><strong>Click the link to the security incident record (SIR0010002)</strong></td>
<td>Review the related security incident and any related search data prior to processing the request.</td>
</tr>
</tbody>
</table>

The following image shows an example of the audit trail created by the work notes on the related security incident record for this example. When the request is rejected from the email notification by an approver, a work note is posted with by the person who rejected the request. Johann SecAdmin rejects this request.

<table>
<thead>
<tr>
<th>JS</th>
<th>Johann SecAdmin</th>
<th>Automation activity • 2019-01-22 14:35:27</th>
<th>Request to approve deletion of emails from Office 365 (sender=<a href="mailto:phisher@cbazyx.com">phisher@cbazyx.com</a> AND subject=log in to your account) rejected by Johann SecAdmin</th>
</tr>
</thead>
<tbody>
<tr>
<td>HS</td>
<td>Hans SecAnalyst</td>
<td>Automation activity • 2019-01-22 14:24:39</td>
<td>Request to approve deletion of emails from Office 365 (sender=<a href="mailto:phisher@cbazyx.com">phisher@cbazyx.com</a> AND subject=log in to your account) submitted by Hans SecAnalyst</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Automation activity • 2019-01-22 14:19:39</td>
<td>1 emails were found in search Phish &quot;log in to your account&quot;.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Automation activity • 2019-01-22 14:18:32</td>
<td>Email search Phish &quot;log in to your account&quot; initiated. An updated message will be posted when the search completes.</td>
</tr>
</tbody>
</table>
In the Now Platform instance of the person who rejected the request (Johann SecAdmin), in Self-Service > My Approvals, Rejected is displayed in the State column.

![ServiceNow Self-Service > My Approvals](https://via.placeholder.com/150)

After a request is rejected by any single member of the approval group, as the user with the sn_si.analyst role, you are required to submit a new request to delete these emails if you determine that they should be deleted.

For this example, after the request is rejected, the user with the sn_si.analyst role submits a new request.

Another member of the approval group, John Approver, receives an email similar to the one shown in the preceding example. John Approver can also process this request.

2. Alternatively, approvers can navigate to Self-Service > My Approvals in their Now Platform instances to view and process delete requests. To process a request from My Approvals, follow these steps.

**a.** Navigate to Self-Service > My Approvals.

![ServiceNow Self-Service > My Approvals](https://via.placeholder.com/150)

**b.** In the State column, click the requested item.

In the approval record that is displayed, data about the search, the search request, and the search results are listed.
c. On this record, click **Approve** to approve the request.

After the request is approved, the system initiates the delete workflow to remove the emails. The following image shows an example of the audit trail created by the work notes on the related security incident record for this example. After this delete request is submitted again, it is approved. Regardless of which method is used to approve a request, the number of successfully deleted emails is posted in a work note.

After the emails are successfully deleted, on the related security incident record, if tagging is enabled, the **Email Delete - Completed** tag replaces the **Email Delete - Initiated** tag.
In **Self-Service > My Approvals** for the approver (John Approver), the state changes from *Requested* to *Approved*.

In **Self-Service > My Approvals** for other members of the approval group, for example, Johann SecAdmin, the state changes to *No Longer Required* after the request is approved.

3. Alternatively, to confirm that emails are deleted in the Email Search Result record on the related security incident record, follow these steps.

   a. Navigate to **Security Incidents > Show All Incidents** and locate the phishing-related security incident.
      At the bottom of the record, the related lists are displayed.

   b. Click the Email Search related list.
c. Click the name of the search in the Email search column (Phish "log in to your account"). The Email Search record is displayed. If the Email Search related list is not visible, click the Show All Related Lists link.

d. Click the Email Search Results related list. In the Search date column, the email search and delete actions are displayed with corresponding dates.

e. In the Search date column, click the item that corresponds to the delete action. In the Email Search Result record that is displayed, the Was deleted column status shows that the email is deleted (true).

You have successfully approved email delete requests from both an email notification and an approval record and confirmed that emails are deleted. For more information about locating the Email Search Result record, see Define email search criteria and request a search on the Microsoft Exchange Online service.

Integration architecture and external systems connection for the Microsoft Exchange Online integration

The Microsoft Exchange Online integration architecture was developed to support the search and delete capabilities for email threats in the Microsoft Exchange Online service. This introduction explains why there are setup steps
that you are required to complete in your Microsoft accounts prior to installing the ServiceNow application.

The integration architecture is based on evaluations of currently available application programming interfaces and with the consultation of Microsoft integration personnel. This information, as well key terminology about the Now Platform and the Microsoft Exchange Online service, is provided to clarify the conceptual operation of the integration.

Key terms used for this integration

The following key terms are used during the installation and configuration. For more information about the following terms, see the ServiceNow Product Documentation website and the Microsoft docs website.

**Now Platform**

An enterprise ServiceNow product. The Now Platform is the base upon which individual components, such as Security Incident Response (SIR), IT Service Management, (ITSM), and other products are built.

**Security Incident Response (SIR)**

A Now Platform application that tracks the progress of security incidents from discovery and initial analysis, through containment, eradication, and recovery, and into the final post-incident review and closure.

**Microsoft Exchange Online**

The mail service offering for Microsoft Exchange Online, which is part of the Office 365 suite of Microsoft products.

**Global Graph API**

The API provided by Microsoft that is used for accessing mailbox information in Microsoft Exchange Online.

**OAUTH authentication**

An ID created in the Microsoft Azure portal used to gather additional mail message details and to delete emails in Microsoft Exchange Online.

**Windows host**

The specific type of virtual machine used in this integration.

**MID Server**

A Now Platform application that facilitates communication and movement of data between the Now Platform and external
applications, data sources, and services. A MID Server is typically required for integration with on-premises technologies, but a MID Server may be deployed in certain cases between the Now Platform and a cloud-based offering when a customer-provided component is required for the integration. For this Microsoft Exchange Online services integration, the MID Server facilitates communication between the Now Platform and the PowerShell server.

PowerShell server

The PowerShell server is a Microsoft application that requires your Microsoft account credentials.

Security incident admin (sn_si.admin)

The user with the sn_si.admin role oversees the configuration of the integration with the SIR product in your Now Platform instance. The user with this role also approves delete requests for emails by default and assigns the sn_si.analyst role as required. The user with this role also has full control over all Service Management data.

Security incident analyst (sn_si.analyst)

The user with the sn_si.analyst role interacts with and analyzes security incidents in the SIR product.

External systems connection for email search and delete

This application uses the Office 365 Security and Compliance Center PowerShell service and the Global Graph API service to retrieve information from the Office 365 Exchange Online service tenant. An outbound HTTPS connection from the MID Server to this environment is necessary for the integration to work properly.

The integration architecture supports an email search and delete capability in the Microsoft Exchange Online service. The integration architecture targets phishing emails as well as other email threats that can compromise the security of your organization. To obtain emails that match a given search query criteria, the Now Platform connects to a Microsoft Exchange Online service tenant using a MID Server that runs PowerShell on a Windows server.

After the Now Platform is connected to the Microsoft Exchange Online service, the integration supports the following levels of email searches:

- The matched messages: This search is conducted through the Microsoft PowerShell cmdlet via a Windows MID Server that is a component of the Now Platform. This search is based on criteria that you configure in the Now Platform from a security incident. The first component of the search returns all email messages that match the search criteria you configured in addition
to the specific mailbox addresses where these messages can be found in Microsoft Exchange Online. The supported search parameters are email message Subject, Sender, and Recipient (the value displayed in the To field in an email message).

- The message details: After the initial PowerShell cmdlet-based search identifies the matched messages, this search retrieves additional message information using the Microsoft Global Graph API. The returned email results include the following message details:
  - Read status: True or false status tracks when users have read emails.
  - Sender address.
  - Recipient address: These addresses include individuals, a group, and individuals that are cc’d and bcc’d on messages.
  - Delete status: True or false status tracks deleted emails.
  - Message ID: The alpha-numeric identifier of email messages.

The basic data flow of the email searches for the number of messages and the message details is illustrated in the following figure.

For email delete, the integration uses the Global Graph API. The recovery of deleted emails is available as an option during the configuration step and is
described in more detail in *Configure the Microsoft Exchange Online integration with your Now Platform instance*.

The data flow for email delete with the preconfigured approval process is illustrated in the following figure.

---

Workflows

The Microsoft Exchange Online application for email search and delete includes the following workflows:

- Exchange online-Emails delete
- Get Exchange Online email details.
- Microsoft Exchange Online-Email search and delete.

For more information about workflows, see *Getting started with workflows* on the ServiceNow Product Documentation website.
You are now ready to set up the accounts that are required for the integration.

(Optional) Recover deleted emails on the Microsoft Exchange Online service

As a Microsoft Exchange Administrator, you can recover deleted emails if your incident remediation requires that you to recover the emails deleted by the workflow of this integration.

Before you begin

For more information about how this integration deletes emails, see Configure the Microsoft Exchange Online integration with your Now Platform instance.

For more information about the administrative role in the Microsoft Office 365 product, including information about recovering deleted items in a user mailbox, see About the Exchange Online admin role.

About this task

If you select the Recover Deleted Emails option in the Additional Settings tab during the configuration step, you enable the recovery of deleted emails in your Microsoft Exchange Online tenant. Emails deleted using the delete workflow of this integration are placed in the Deleted Items sub folder of the Recoverable items folder in the mailbox of the user on the Microsoft Exchange Online service. If the user's account is configured in Microsoft Exchange Online tenant so that the user can view the Deleted Items folder, the user can recover these emails by using the Microsoft Outlook service on the web. Alternatively, the Microsoft Exchange Online administrator can recover deleted emails from a Deleted Items folder of a user. See Recover deleted items or email in Outlook Web App for more information.

Role required: Microsoft Exchange Online administrator or Microsoft Global administrator to recover deleted emails.

Role required: sn_si.admin in the Now Platform to enable the Recover Deleted Emails option.

Role required: sn_si.analyst in the Now Platform for completing a successful search for emails and verifying that emails are successfully deleted prior to recovery.

Procedure

To enable the email recovery option, follow these steps.


b. Locate the Microsoft Exchange Online tile.
c. Click **Configure**.

d. In the Microsoft Exchange Online Configuration dialog box that is displayed, click **Configure Exchange Online**.

e. On the **Additional Settings** tab under **Recover Deleted Emails**, select the **Enable** check box.
f. Verify any other settings and click **Submit**.

g. To verify that a search and delete of email messages are successfully completed for the email messages you want to recover, navigate to the security incident that logged the email search and delete workflows.

h. Locate the work notes and verify that the system successfully deleted the messages.

i. As a Microsoft Exchange Online administrator or Global administrator, log in to your Microsoft Office 365 account.

j. Follow the steps described in **Recover deleted items or email in Outlook Web App** on the Microsoft documentation website.
(Optional) Edit security tags in the Now Platform for the Microsoft Exchange Online integration

You can edit the names and colors of the security tags in your Now Platform® instance for the Microsoft Exchange Online integration. These security tags help you quickly identify when email search either completes or fails. They also identify when requests to delete emails are initiated and when the email items are successfully deleted.

Before you begin
By default, the security tags are enabled in your Now Platform® instance if you select the Display Tags option during the configuration step. You can edit tag colors and names, and assign tags to security tag groups to help you organize them in your Now Platform® instance. For example, you can change the colors of tags so that the start tag of a capability is one color, and the completion tag is another color to match the other security tags that are enabled in your Now Platform® instance. These different colors can help you quickly identify when workflows start and are successfully completed. If you decide that you do not need a specific tag, without disabling tagging for the integration, you can also disable a single tag from the tag record. If disabled, this tag is no longer displayed on the related security incidents. For more information on how to set up security tag groups and tags, see Set up security tag groups and tags on the Servicenow Product Documentation website.

Role required: sn_si.admin

Procedure
2. Click the Additional Settings tab to select it.
3. On the tab that is displayed, if the Display Tags option is cleared, select it to display tag names.
4. With the tag names displayed, to the right of a tag, click the information icon.
5. In the Security Tag dialog that is displayed, click **Open Record**.
6. In the record that is displayed, edit the fields.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the security tag.</td>
</tr>
<tr>
<td>Color</td>
<td>Security tag color. Select a color from the choice list.</td>
</tr>
<tr>
<td>Security Tag Group</td>
<td>Name of the security tag group. Click the information icon to view the available groups. Default is Metatag group.</td>
</tr>
<tr>
<td>Enforce restricted access</td>
<td>Select this option to assign read and write roles needed by users to read or write to records that have this security tag. Default is cleared.</td>
</tr>
<tr>
<td>Order</td>
<td>Specify the order the tag appears on forms or within a list. Default is 100.</td>
</tr>
<tr>
<td></td>
<td>To set the order on the list, enter a value. For example, 100, 200, 300, 400. The tag with the lowest the num-</td>
</tr>
</tbody>
</table>
Option | Description
--- | ---
ber is displayed first on the list. The profile with the highest number is displayed last.
Active | Turn this tag on or off. Default is selected (active)
Description | Description for the tag.

7. Click **Update** to save your changes.

You have now successfully edited the tag record for a security tag.

**Checklist for the Microsoft Exchange Online integration**

Use this checklist to guide you through the end-to-end tasks of the integration. The following checklist includes set up and installation tasks and examples of use cases and expected results for the application.

**Before you begin**

Track your progress with the setup, installation, and configuration of the integration with the following table. Complete all the tasks for a step before moving on to the next step. Each step identifies the roles that are required to
perform the tasks and references the numbered topics of the installation and configuration guide for this integration.

Roles required: Roles are listed for each step in the following table.

**Procedure**

To track your progress for the integration, follow the steps in the table in the order that they are presented

<table>
<thead>
<tr>
<th>Checklist</th>
</tr>
</thead>
</table>
| ☐ As Microsoft Office 365 administrator, set up your Microsoft Office 365 account.  
Create an API account that permits access to the Security and Compliance center in Microsoft Office 365. For steps to set up the account, see [Set up your Microsoft Office 365 account for the ServiceNow Microsoft Exchange Online integration](#). |
| ☐ As Microsoft Azure administrator, set up your Microsoft Azure account.  
Create an account that uses an Application ID to gather additional email message details and delete email messages. For steps to set up the account, see [Set up your Microsoft Azure account for the ServiceNow Microsoft Exchange Online integration](#). |
| ☐ As Now Platform admin, set up your Now Platform instance for the integration.  
For tasks and more information, see [Set up your Now Platform instance for the Microsoft Exchange Online integration](#).  
- b. Set up a MID Server in your Now Platform instance.  
- c. Install Now Platform (SIR) and Security Operations applications from the ServiceNow Store and activate them on your instance.  
- d. Enable the email send and email receive capabilities.  
- e. Assign the email read and write role to the sn_si.analyst.  
- f. Create an approval group. |
| ☐ As Now Platform admin, install the application for the integration from the ServiceNow Store. |
For installation steps, see Install the Microsoft Exchange Online application for the ServiceNow Microsoft Exchange Online integration.

- As sn_si.admin, complete the configuration settings tabs to establish connectivity and activate the search and delete workflows. For connection and configuration settings, see Configure the Microsoft Exchange Online integration with your Now Platform instance.

- As sn_si.analyst, set up email search criteria and request a search for matching emails on the Microsoft Exchange Online server. For an example, see Define email search criteria and request a search on the Microsoft Exchange Online service.
  
  a. Locate security incidents related to phishing events.
  
  b. Set up email search criteria.
  
  c. Request a search for emails.
  
  d. Locate search results and message details on the related lists on the security incident.

- As sn_si.analyst, delete emails from the Microsoft Exchange Online server. For an example, see Request delete approval for emails on the Microsoft Exchange Online service.
  
  a. Locate security incident with search results.
  
  b. Delete emails or request approval to delete emails.
  
  c. Verify that emails are deleted from results posted to the work notes and related lists on the security incident.

- As sn_si.admin, or, as a member of an Approval group, process email delete requests via email notifications. For an example, see Approve delete email requests for the Microsoft Exchange Online integration.

You have successfully completed the set up steps and verified expected results for the integration.

**Troubleshooting Microsoft Exchange Online integration**

After you have successfully configured the Microsoft Exchange Online application (see Configure the Microsoft Exchange Online integration with your...
Now Platform instance) and set up your Now Platform instance, if you run into any email search issues, you can run diagnostics tests based on specific criteria.

About this task
The results of these tests can help ServiceNow Customer Support identify and troubleshoot the issues.

Procedure
1. Navigate to Exchange Online Diagnostics > Initiate Diagnostic Tests.
2. Enter the following details:
   • Enter the Sender and one or more Recipient email addresses to narrow down the search criteria and provide more accurate results.
   • Specify the Subject for which the diagnostics tests is being performed. This is a mandatory field.
3. Click Submit.
4. To view the results of the diagnostics tests, navigate to Exchange Online Diagnostics > View Diagnostic Test Results.
   The Status column shows the following statuses:
   • Complete - Pass: The tests have been successfully completed.
   • Complete - Failures: The tests have been completed with some errors.
   • In Progress: The tests are still running and have not been completed.
5. Click on the Diagnostic Test Suite Execution to see the test execution details.

The following types of diagnostics tests are run:
• Diagnose Compliance Search: Generates a list of recipient email mailboxes by performing compliance search.

• Diagnose Simple Email Search – Searches email mailboxes by making separate REST calls to search each folder of the recipient.

• Diagnose Batch Search – Searches mailboxes in a batch query, by combining multiple searches in one REST call.

To perform tests 2 and 3, you must specify the Recipient email addresses in the Initiate Diagnostic Tests page. If they are not specified, the tests will not be performed.

6. Click on the Created link in the Diagnostic Test Suite Execution page to view the test results in detail.

![Diagnostic Test Step Execution](image)

The above image shows detailed result of the Diagnose Compliance Search Test step execution and shows the count of mailboxes found in the search.

**Microsoft Exchange On-Premises integration**

The Microsoft Exchange On-Premises integration provides tools for security analysts to contain and eradicate phishing and spear phishing email threats in on-premises instances.

<table>
<thead>
<tr>
<th>Explore</th>
<th>Set up</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Security Incident Response integrations</td>
<td>• Get started with the Microsoft Exchange On-Premises integration</td>
</tr>
</tbody>
</table>
### Use
- Search for and delete phishing emails

### Develop
- ServiceNow Security Operations integration development guidelines
- Tips for writing integrations
- Developer training
- Developer documentation
- Find components installed with an application

### Troubleshoot and get help
- Integration troubleshooting
- Ask or answer questions in the Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

---

**Get started with the Microsoft Exchange On-Premises integration**

The Microsoft Exchange On-Premises integration provides tools for security analysts to contain and remediate phishing and spear phishing email threats in on-premises instances. Before you can use the Microsoft Exchange On-Premises integration, you must download it from the ServiceNow Store and identify the appropriate Exchange and MID servers.

**Before you begin**
Role required: sn_si_admin

**Procedure**

1. Download the integration from the ServiceNow Store.
2. When the installation is complete, navigate to **Security Operations > Integrations > Integration Configuration**. The available security integrations appear as a series of cards.
3. In the Microsoft Exchange On-Premises card, click **New**.
4. Fill in the fields, as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of this configuration.</td>
</tr>
<tr>
<td>Delete Recovery</td>
<td>Select this option to remove the ability to recover deleted emails in Exchange.</td>
</tr>
<tr>
<td>Exchange Server</td>
<td>Specify the Exchange server to be used.</td>
</tr>
<tr>
<td>MID Server</td>
<td>Select Any to use any active MID Server, or select a specific MID Server name.</td>
</tr>
</tbody>
</table>

**Note:** Configuring this integration activates workflows. To manage the workflows, navigate to the **Workflow Editor**.

5. Click **Submit**.
   The integration configuration card displays.
6. When viewing the new configuration card, you can click Configure or Delete to change or delete the configuration, respectively.

7. To return to the original list of integration configuration cards, select No from the Show Configurations drop-down list.

**Microsoft Exchange - Perform Email Search and Deletion workflow**
When the Microsoft Exchange - Perform Email Search and Deletion workflow is executed, it searches the Exchange server using the search query provided, and returns the details to the on-premises instance.

**Before you begin**
Role required: sn_si.analyst

**About this task**
The Microsoft Exchange - Perform Email Search and Deletion workflow is executed when email searches are set up and the Delete from Email Server(s) or Search on Email Server(s) button are pressed.

Activities specific to this integration are described here. For more information on other activities, see Common integration workflow activities.

**Get Email Details from Exchange Server activity**
The Get Email Details from Exchange Server activity performs a search for emails in the designated Exchange server(s) using the search queries defined, and returns details from the subject, recipient, and sender parameters.
Input variables
Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>targetId</td>
<td>Mandatory target host identifier field where the Exchange Server is located.</td>
</tr>
<tr>
<td>search_query</td>
<td>Mandatory search query used to find emails in the Exchange Server across all mailboxes.</td>
</tr>
</tbody>
</table>

Output variables
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>response</td>
<td>Email details retrieved for each email found for the given search query.</td>
</tr>
</tbody>
</table>

Exit Conditions
Possible exit conditions for this activity are:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No emails found</td>
<td>When the email count is zero, no emails were found for the given search query.</td>
</tr>
<tr>
<td>Threat emails found</td>
<td>When the email count is greater than zero, and email details were returned for the given search query.</td>
</tr>
<tr>
<td>Error executing at exchange</td>
<td>When an error occurred while executing the powershell script in the Exchange Server.</td>
</tr>
</tbody>
</table>

Search/Delete Threat Email in Exchange activity
The Search/Delete Threat Email in Exchange activity performs a search for emails in the designated Exchange server(s) using the search queries defined, and returns the details.
**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>Mandatory target host identifier field where the Exchange Server is located and the powershell script will be executed.</td>
</tr>
<tr>
<td>search_query</td>
<td>Mandatory search query used to find emails in the Exchange Server across all mailboxes.</td>
</tr>
<tr>
<td>operation</td>
<td>Operation to be executed on the Exchange server. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• search</td>
</tr>
<tr>
<td></td>
<td>• delete</td>
</tr>
<tr>
<td>delete_from_recovery</td>
<td>Choose to delete emails from the recovery folder on the Exchange server. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• true</td>
</tr>
<tr>
<td></td>
<td>• false</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>emailCount</td>
<td>The total number of emails found during the search/delete operations for the given search query.</td>
</tr>
</tbody>
</table>

**Exit Conditions**

Possible exit conditions for this activity are:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No emails found</td>
<td>When the email count is zero, no emails were found for the given search query.</td>
</tr>
</tbody>
</table>
Exit Conditions (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat emails found</td>
<td>When the email count is greater than zero, and email details were returned for the given search query.</td>
</tr>
<tr>
<td>Error executing at exchange</td>
<td>When an error occurred while executing the powershell script in the Exchange Server.</td>
</tr>
</tbody>
</table>

**Microsoft Azure Sentinel integration**

Microsoft Azure Sentinel is a cloud-based security information event management (SIEM) and security orchestration automated response (SOAR) solution. You can use the Microsoft Azure Sentinel integration to ingest Azure Sentinel incidents and automatically create security incidents in Security Incident Response.

**Request apps on the Store**

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

**Overview**

See the following diagram to learn how Microsoft Azure Sentinel integrates with the Now Platform Security Operations applications.
Key features
This integration includes the following key features:

- Discover Microsoft Azure Sentinel incidents that are candidates for security incidents and automate the creation of security incidents.
- Mapping of Microsoft Azure Sentinel incident and entity fields to SIR security incident fields.
- Filtering of Microsoft Azure Sentinel incidents.
• Aggregation of similar incidents to existing open security incidents so that you don't have to create duplicate security incidents.

• Automatic Microsoft Azure Sentinel incident status update for SIR security incident creation and closure.

• Scheduled ingestion of incidents that create security incidents periodically.

• Synchronization of Microsoft Azure Sentinel incident comments with SIR Work notes.

Learn about this integration

<table>
<thead>
<tr>
<th>Document identifier</th>
<th>Document title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft product documentation website</td>
<td>Microsoft Product Documentation website</td>
</tr>
<tr>
<td>ServiceNow product documentation website</td>
<td>ServiceNow Product Documentation website</td>
</tr>
</tbody>
</table>

Get started with Microsoft Azure Sentinel integration

You can activate and set up the Microsoft Azure Sentinel - Incident Ingestion for Security Operation plug-in to interface with your Now Platform instance and Security Incident Response product.

Before you begin

Before you can use the Microsoft Azure Sentinel integration, you must download it from the ServiceNow Store.

Review the following setup checklist and verify that you have completed all the tasks for a smooth integration.

Checklist

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Assign and verify the required Now Platform and Security Incident Response roles. | These roles are required for configuration and verification of the expected results:  
• The admin role installs the integration from the ServiceNow Store and assigns the sn_si.admin role. |
Checklist (continued)

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The sn_si.admin role performs the following tasks: ◦ Configures the integration. ◦ Creates incident profiles. ◦ Maps Microsoft Azure Sentinel incident data fields to the security incident fields. ◦ Schedules on-going incident ingestion. ◦ Enables incident updates when a Security Incident Response incident is created or closed. ◦ Assigns the security incident analyst (sn_si.analyst) role.</td>
<td></td>
</tr>
</tbody>
</table>

Assign the Microsoft Azure required roles. The following roles are required in Microsoft Azure to register and configure your application: • Application developer for registering the application. • Tenant administrator for granting permissions to the application by calling the admin consent endpoint.

Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you configure this integration. The ServiceNow IntegrationHub Starter Pack Installer [com.glide.hub.integrations] plugin is required. The Security Incident Response plugin (com.snc.security_incident) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations
### Checklist (continued)

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>applications that are required by the integration.</td>
</tr>
<tr>
<td></td>
<td>Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If these applications are not already installed, you must install and activate each application one at a time in the following order to ensure a smooth installation:</td>
</tr>
<tr>
<td></td>
<td>1. Security Incident Response</td>
</tr>
<tr>
<td></td>
<td>2. Security Incident Response UI</td>
</tr>
<tr>
<td></td>
<td>3. ServiceNow IntegrationHub Runtime (com.glide.hub.integration.runtime)</td>
</tr>
<tr>
<td></td>
<td>4. ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest)</td>
</tr>
</tbody>
</table>

Register and configure your application in the Microsoft Azure portal.

Register your application in the Microsoft Azure portal and grant the read and write access to the application.

### Register and configure the Microsoft Azure portal

Register your application in the Microsoft Azure portal and grant the read and write access to the application.

**Before you begin**

Role required: Microsoft Azure application developer, Microsoft Azure tenant administrator

**Procedure**

1. Sign in to the Azure portal.
2. Search for and select **App registrations**.
3. Click **New registration**.
4. On the form, fill in the fields.
### Register an application form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>User-facing display name for the application. For example, LogAnalyticsAPI.</td>
</tr>
<tr>
<td>Supported account types</td>
<td>Account type that can use this application or access the API.</td>
</tr>
<tr>
<td>Redirect URI</td>
<td>Redirect URI. The authentication response is directed to this URI after successfully authenticating a user.</td>
</tr>
</tbody>
</table>

5. Click **Register**.

After you successfully register the application, you see the Overview page.

6. Navigate to **Manage > Certificates & secrets**.

7. In the Client secrets section, click **New client secret**.

You can't view the client secret later, so make sure that you copy and save the client secret now at this step. If you forget the client secret, you can generate a new one by following the instructions in steps 4 and 5.

8. Navigate to **Manage > API permissions**.

9. Click **Add a permission**.

10. In the Request API permissions window, search and select the application that you created in step 4.
11. Do the following actions:

   a. Select Application permissions.
      Enabling this permission ensures that the application runs as a background service or daemon without a signed-in user.

   b. Under the Data section, select Data.Read.

12. Enable the Grant admin consent for Default Directory option for the Data.Read API permission that you enabled in step 11.

13. Search for and select Log Analytics workspaces.

14. Select your Sentinel Log Analytics workspace. You now see the Sentinel Log Analytics workspace Overview page.

15. Navigate to Access control (IAM) > Role assignments.

16. Click Add, and select Add role assignment.

17. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Add role assignment form</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
</tr>
<tr>
<td>Role</td>
</tr>
<tr>
<td>Assign access to</td>
</tr>
<tr>
<td>Select</td>
</tr>
</tbody>
</table>

18. Click Save.

**Install and configure the Microsoft Azure Sentinel integration**

Install and configure the Microsoft Azure Sentinel integration from the ServiceNow Store on your Now Platform instance to start ingesting Azure Sentinel incidents.

**Before you begin**
Role required: sn_si.admin
Procedure
1. Download the Microsoft Azure Sentinel integration from the ServiceNow Store and install it.
3. Search for the Microsoft Azure Sentinel tile and click Configure.
4. On the form, fill in the fields.

Microsoft Azure Sentinel - Incident Ingestion Configuration form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the Microsoft Azure Cloud instance configuration.</td>
</tr>
<tr>
<td>Tenant ID</td>
<td>Microsoft Azure Sentinel Tenant ID. This is the instance from which all the incidents in the Microsoft Azure portal are retrieved.</td>
</tr>
<tr>
<td>Client ID</td>
<td>Client ID for the application that you have registered in the Microsoft Azure portal.</td>
</tr>
<tr>
<td>Client Secret</td>
<td>Client secret for your registered application.</td>
</tr>
<tr>
<td>Subscription ID</td>
<td>Subscription ID for your registered application.</td>
</tr>
<tr>
<td>Resource Group Name</td>
<td>Resource group name for your registered application.</td>
</tr>
<tr>
<td>Workspace Name</td>
<td>Workspace name for your registered application.</td>
</tr>
</tbody>
</table>

5. Click Submit.

Results
After you successfully validate and submit the configuration, each incident ingestion server configuration is saved on the Security Integrations page as a tile.

Create a profile for Microsoft Azure Sentinel
Create an incident profile in your Now Platform instance and determine the Microsoft Azure Sentinel incidents that are suitable for creating security incidents.
Before you begin
Role required: sn_si.admin

About this task
The integration enables you to create different types of incidents, such as unauthorized access attempts and malware. These incidents are created based on the profiles that you configure in the Now Platform instance. All incidents are initially created for a configured incident type in a profile. Created incidents can then be further filtered to specify which incidents create security incidents.

All incidents that meet the selection criteria in your Microsoft Azure tenant and are available over the Microsoft Azure Sentinel API are initially ingested into your Now Platform instance.

Procedure
1. Navigate to Microsoft Azure Sentinel Integration > Azure Sentinel Incident Profile.
2. Click New.
3. On the form, fill in the fields.

Microsoft Azure Sentinel - Incident Ingestion Configuration form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the profile. This name helps you to identify the profile type and is also the default name for the security tag that is associated with this profile.</td>
</tr>
<tr>
<td>Active</td>
<td>Indicator that the profile is active. When the profile is active, it implies that the Now Platform is actively polling Azure Sentinel incidents and corresponding security incidents are created in SIR when the filtering conditions are matched.</td>
</tr>
<tr>
<td>Source</td>
<td>Microsoft Azure tenant that you configured to ingest incidents. If you have multiple tenants configured, select the appropriate tenant for the incident types that you are planning to ingest for the profile.</td>
</tr>
</tbody>
</table>
4. To move to the Mapping section, click Continue.

What to do next
Map individual Microsoft Azure Sentinel incident fields to the fields on the Now Platform SIR security incident.

Map Microsoft Azure Sentinel incident fields
Map individual Microsoft Azure Sentinel incident fields to the fields on the SIR security incident so that you can create incidents with the mapped data.

Before you begin
Role required: sn_si.admin

Procedure
1. On the mapping page, in the Azure Sentinel Field Mapping section, select one of the Sample Ingestion Methods.

Sample Ingestion Methods

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All default Incident and entity fields</td>
<td>Use this ingestion method to view the static list of all the incidents and entity fields. This method contains only default field names without any values. You can use this information to map with the SIR fields.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Retrieve Recent Azure Sentinel incidents</td>
<td>Use this ingestion method to import the most recent incidents and entities data. If the Azure Sentinel incident contains the entity data, then the entity data is retrieved and it is available for mapping in the Azure Sentinel Source Fields section. Sometimes the Azure Sentinel incident may not contain the entity data, and hence the entity fields are not available for mapping in such a scenario. You can ingest 5 sample incidents by default and a maximum of 20 sample incidents. The sample incident field values populate when the profile ingests the sample incidents. You can map these incidents to the <strong>SIR Incident Target Fields</strong>. The incident fields and values appear as individual tabs.</td>
</tr>
<tr>
<td>Import Sample Data</td>
<td>Click <strong>Import Sample Data</strong> to import sample incidents from Azure Sentinel. This button appears when you select the Retrieve Recent Azure Sentinel incidents ingestion method. Retrieving sample incidents from Microsoft Azure Sentinel server may take a moment. Map these retrieved incidents to the <strong>SIR Incident Target Fields</strong>. The incident fields and values appear as individual tabs.</td>
</tr>
</tbody>
</table>

The following illustration shows, how to navigate to the Mapping page, viewing the All default Incident and entity fields ingestion method which shows all the static list of incidents and entity fields. The illustration then shows selecting the Retrieve Recent Azure Sentinel incidents ingestion method which imports the most recent incidents and entities data.
2. To add fields to the default fields that are displayed on the security incident, do the following actions:
a. On the SIR Incident Target Fields section, click the **Map another field** button. It shows a list of SIR fields, from which you can select a field for a new field to be displayed.

b. In the Security Incident column, expand the list that is displayed and then select a field.

> **Note:** Multiple observables can be displayed on the same security incident. For example, the **Observable** field can be mapped multiple times with different values. Similarly, the **Configuration Item** and **Work notes fields** support multiple values. If you try to map two values to a field that can’t support multiple values, you see an error message that this field does not support multiple values. Similarly, if a field on a security incident has a list from which you can choose multiple options, and you try to map an option to that field that is not displayed on the list, the field does not populate on the security incident.

c. From the Azure Sentinel Source Fields section, drag and drop your field to map it to your new field.

3. To remove a field, use the **Remove item** button next to the input expression field in the SIR Incident Target Fields section.

4. To map a field value from the Azure Sentinel Source Fields section to a field on the SIR Incident Target Fields section, use one of the following actions:

a. Drag the field name (for example, id) and drop it next to a field name in the SIR Incident Target Fields column.

You can match any value from the Azure Sentinel Source Fields section to a field on the SIR Incident Target Fields section. Fields are color-coded so that you do not overlook or duplicate incident fields in the mapping process. Light blue fields indicate that an incident field is not yet selected and mapped on the security incident. You may prefer to associate an incoming incident field with more than one field on a security incident. A gray field indicates that a field has been selected and mapped to a field on the security incident. This way, you can visualize which field values have been added to the security incident and if any remaining important incident information remains unmapped.

b. You can add a combination of text and field.
For example, *Incident name is* \${name}\$. Here *Incident name is* can be manually entered while \${name}\$ is mapped from the Azure Sentinel Source Fields section.

c. You can directly manually enter and map a source incident or entity field to a target field.

- To manually map a source incident field use the \${field name}\$ format. For example, to map an incident field Severity, the format is \${properties(severity)}\$.
- To manually add a source entity field, use the \${entity name: entity field}\$ format. For example, to map an entity field Description of entity Security Alert, the format is \${SecurityAlert: properties(description)}\$.

This integration classifies certain observable sub-types. When you map an Azure Sentinel field with the SIR observable field, the Now Platform auto-classifies the observable. If you want to generically map the incoming Azure Sentinel observable to the observable type in SIR, then drag and drop the Azure Sentinel field in the Observable field. However, if you aware of the observable type for the incoming Azure Sentinel observable in SIR, then map specifically to the SIR Observable type field. Some examples of specific observable types in SIR include Observable(Domain name), Observable(Email address), Observable(IP address (V4)), and Observable(Host name).

If your incoming Azure Sentinel fields contain any MITRE-ATT&CK information, then map it to the MITRE-ATT&CK Technique field. Ensure that the incoming Azure Sentinel field contains the MITRE-ATT&CK technique ID or technique name.

The following illustration shows how to map a field value from the Azure Sentinel Source Fields section to a field on the SIR Incident Target Fields section. A combination of drag and drop, and manual field entries have been added for source incident fields and source entity fields.
5. Sometimes, incident field values in Microsoft Azure Sentinel may not translate directly to the fields on the SIR security incident. For these values, you can use a script editor to format field values on the security incident during the mapping step. Use the script editor if you want to format values that are similar, but not identical. To format a field translation for a new field from an Azure sentinel incident to match a field value on a Security Incident, click the **Click here** link in the SIR Incident Target Fields header.
6. To modify the fields which support field translation, click the script format field translation button. The script editor is displayed. Enter any changes to the script and click Update to save the changes and return to the Mapping page.

7. Continue your mapping by adding or removing field values.
   You can use the same field values in the Incident Generation Conditions builder to define additional criteria that an incoming incident must satisfy to create a security incident.

8. To move to the Filtering and Aggregation section, click Continue.

What to do next
Define and set filter conditions so that you can specify which incidents should create security incidents. You can use the same field values (defined in the Mapping section) in the Incident Generation Conditions builder (in the Filtering and Aggregation section) to define additional criteria that an incoming incident must satisfy to create a security incident.

Define filter and aggregation criteria
Define and set filter conditions so that you can specify which incoming Microsoft Azure Sentinel incidents should create security incidents. You can also define additional incident field criteria that allows an incoming incident to be appended to an open security incident instead of creating an incident.

Filtering conditions
Set filtering conditions so that security incidents are created only when the filtering conditions match.

Before you begin
Role required: sn_si.admin

About this task
This type of filtering helps you isolate security incidents, and it limits the number of security incidents that you create. If additional filtering criteria are set, only incidents that are required are ingested without having to change the query or the triggered incident configuration.

Procedure
1. To define the criteria that an incoming Microsoft Azure Sentinel incident must satisfy so that a security incident is created, select Filter based on conditions.

   The options in the first field in the Filter Conditions match the fields that are displayed on the Azure Sentinel Sample Incident Ingestion section for the incident that you ingested. These fields are dynamic and change depending...
on the incident that you ingest. The criteria that you enter is case-sensitive. Verify that the criteria you define matches the values of the incident.

Use the filter condition `contains` for the following fields with multiple values:

- `properties(labels)`
- `properties(additionalData(alertProductNames))`
- `properties(relatedAnalyticRuleIds)`
- `properties(additionalData(tactics))`

Because the filter condition can retrieve only strings, you must use the `contains` filter condition for the above fields to ensure that the data is filtered correctly.

2. Using the lists and fields of the conditions builder, set the filters for the first row.

3. To add more conditions, click **AND** or **OR**.
   - If **AND** is selected, all conditions must be matched.
   - If **OR** is selected, either condition can be matched.

4. To set a second filter condition, click **New Criteria**.

**Aggregation conditions**

Define additional incident aggregation criteria that aggregates an incoming incident to an existing SIR security incident instead of creating similar, potentially duplicate incidents. Using field matching value criteria for each profile, this additional aggregation capability can reduce the number of active, overlapping security incidents by placing all related incidents data on a single security incident.
Before you begin
Role required: sn_si.admin

About this task
If a new incident matches all the values that are selected in the aggregation field conditions in the mapping step, the incident is automatically added to the most recently opened security incident with the same field values. As a user with the sn_si.analyst role working with security incidents, you can view all the added aggregate incidents on a related list on a security incident.
All the aggregated incidents on a security incident are displayed on the Azure Sentinel Aggregated Incidents related list. This list details the associated timestamps and aggregated field values. This information helps you understand why incidents are added to the existing security incidents.

Procedure
1. To define additional incident field criteria that allows an incoming Microsoft Azure Sentinel incident to be appended to an open security incident instead of creating a new incident, select the Aggregation Conditions option.

2. In the Incident fields with matching values field, enter the field values that you want to match on existing security incidents in your Now Platform instance. All field values that you selected in the multi-selection input field must be matched so that the aggregation criteria is met and that this incoming incident can be appended to an existing security incident. This selection
implies it is an **AND** condition where fields, such as Observables and Configuration Items, that may have multiple field values, are mapped to them. All values must match. If only a subset of the values is matched, the Azure Sentinel Incident aggregation conditions are not met and a new security incident is created.

3. To add multiple field matching conditions, click **Add New Criteria**
   The aggregation occurs if any one of the multi-selection field conditions defined are met. This selection implies the **OR** condition.

4. Select **Log work note for new Incident** to update the work note for a new incident when it is added to a security incident.
   The work note logs that a new incident is added and includes a link to the incident details. The log work note also updates more details that you add to the work note field in your mapping section.

5. To configure the schedule, click **Continue**.

**What to do next**
Set a schedule to retrieve the incident data and ingested incidents that match the criteria in the profile.

**Schedule Microsoft Azure Sentinel incident retrieval**
Set a schedule to retrieve incident data and ingest Microsoft Azure Sentinel incidents that match the criteria in the profile.

**Before you begin**
Role required: sn_sni.admin

**About this task**
You can plan how often you will poll for future Microsoft Azure Sentinel incidents that match the incident profile configuration.

To enable automated incident ingestion, you must configure the scheduling and incident retrieval before you activate the profile. To define a specific date and time for the initial ingestion, enable 'set incident ingestion time.' Subsequent ingestion is based on the polling interval period.

The polling interval is configured for each profile individually. The different polling intervals may impact the performance of the Microsoft Azure Sentinel incident integration. When scheduling, plan to balance the system load against the urgency of an incident. A one-minute default value is set for all profiles. You can modify this setting based on the urgency of the incident and the anticipated load on your system.
Procedure

1. On the scheduling form, fill in the fields.

Configure the schedule to define how and when you pull incidents from the Microsoft Azure tenant.

<table>
<thead>
<tr>
<th>Scheduling form</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Ongoing incident ingestion</td>
<td>Ongoing incident ingestion that theNow Platform instance pulls from the Microsoft Azure tenant for new incidents. Security incidents are created if triggered incidents are found and the incident generation filtering criteria matches.</td>
</tr>
<tr>
<td>Polling increment (minutes)</td>
<td>Polling frequency that is defined in minutes.</td>
</tr>
<tr>
<td>Set incident ingestion time</td>
<td>(Optional) Incident ingestion that is based on the configured date and time. You can use this option to define a specific date and time for the initial ingestion. Subsequent ingestions are based on the polling interval period.</td>
</tr>
<tr>
<td>Input incident ingestion time</td>
<td>(Optional) Date and time that you specify for the incident ingestion.</td>
</tr>
</tbody>
</table>

2. To navigate to the Additional Options page, click **Continue**.
Automate incident updates and closure based on the SIR incident status

The Microsoft Azure Sentinel integration has a bi-directional interface that enables for both incidents to create security incidents, and an ability to update the incidents once the security incident is created or closed. Relevant incident details such as the SIR incident number, assignment group, and SIR incident URL are updated in the incident.

Before you begin
Role required: sn_si.admin

Procedure
1. On the form, fill in the details.
   Follow the instructions to complete the configuration for updating incidents when you create or close a security incident in SIR.

   Automating Incident Updates form

<table>
<thead>
<tr>
<th>Category</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Creation Updates</td>
<td>Update Azure Sentinel Incidents Status upon SIR Incident creation</td>
<td><strong>Update Azure Sentinel incident status upon SIR Incident Creation</strong> option that enables you to use the automated incident update functionality. The Microsoft Azure Sentinel incident status is updated in Microsoft Azure incident with the comments after the SIR incident is created in the Now Platform.</td>
</tr>
<tr>
<td></td>
<td>Initial incident status update</td>
<td>Initial incident status is updated in Microsoft Azure Sentinel. You can select <strong>New</strong> or <strong>Active</strong> as the status.</td>
</tr>
<tr>
<td></td>
<td>Initial comments posted back to Incident</td>
<td>Initial comments that are posted to the incident in Microsoft Azure Sentinel. Edit the default text that is displayed in the comments section by adding or modifying the substitution variables using format ${{field}}</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Category</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Closure Updates</td>
<td>Close Azure Sentinel incidents upon SIR Incident Closure</td>
<td><strong>Close Azure Sentinel incident upon SIR Incident Closure</strong> option that enables you to use the automated incident status update functionality. Microsoft Azure Sentinel incidents are closed in the Microsoft Azure incident with the comments given after the SIR incident is closed in the Now Platform.</td>
</tr>
<tr>
<td></td>
<td>Closure incident status update</td>
<td>Status update in the Microsoft Azure Sentinel incident when the incident is closed in SIR.</td>
</tr>
<tr>
<td></td>
<td>Closure Comments Posted back to incident</td>
<td>Comments that are posted to the incident in the Microsoft Azure Sentinel incident when the incident is closed in SIR. Edit the default text that is displayed in the comments section by adding or modifying the substitution variables using format <code>${field name}</code> for any field on the SIR incident form.</td>
</tr>
<tr>
<td></td>
<td>Incident classification and closing reason</td>
<td>Method for the incident classification and closing reason that is used to close the incident in Microsoft Azure Sentinel. Select the <strong>Default incident classification and closing reason</strong> method to close the incident in Microsoft Azure Sentinel. When you select this method, you must further define the <strong>Default incident</strong></td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Category</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>classification and closing reason</td>
<td></td>
<td>When you close an incident in SIR, the incident status in Azure Sentinel is also closed with the specified Default incident classification and closing reason. Select the Incident classification and closing reason-SIR close code mapping method to close the incidents and to map the classification reasons with the SIR close codes. You can map multiple SIR close codes to a single classification reason. Once you close an incident in SIR using the close code, the incident status in Azure Sentinel is also closed with the mapped incident classification and closing reason. If the classification reason and SIR close codes are not mapped, or a match is not found, then the incident is closed using the default classification reason as 'Undetermined' in Microsoft Azure Sentinel.</td>
</tr>
<tr>
<td>Update SIR work notes with Azure Sentinel incident comments</td>
<td></td>
<td>Option that you can select to update your Microsoft Azure Sentinel comments in the SIR work notes. The comment in the SIR work notes appears with the prefix Comment from Sentinel.</td>
</tr>
</tbody>
</table>
| Update Azure Sentinel incident               |                                            | Option that you can select to update your SIR work notes in
<table>
<thead>
<tr>
<th>Category</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>comments with SIR work notes</td>
<td>the Microsoft Azure Sentinel incident comments. The comment in Microsoft Azure Sentinel appears with the prefix Comment from ServiceNow.</td>
<td></td>
</tr>
</tbody>
</table>

The following example shows the configuration options that are available for automating incident updates.

2. Click Finish.

What to do next

The profile moves to the Waiting state. Once the confirmation message shows that the setup and configuration is complete, you can activate the profile.
Copy an Microsoft Azure Sentinel Profile

Copy an existing profile and its associated settings instead of creating profiles. When you are creating multiple profiles, you can also reuse the settings of an existing profile, by copying these profiles to save time.

Before you begin
Role required: sn_si.admin

About this task
When you copy a profile, the profile name is initially modified to avoid creating duplicate profiles. In addition, the copied profile is disabled (set to false) to ensure that you do not accidentally activate it before you complete the configuration. You can copy the profiles and use existing maps for security incidents that you have already previewed and verified.

Procedure
1. Navigate to **Microsoft Azure Sentinel Integration** > **Azure Sentinel Profile**.
2. In the Azure Sentinel Profiles list, select a profile that you want to copy, and then from the Actions on selected rows list, click **Copy**.

The profile is copied and displayed on the list. The copy has all the settings of the original profile including the mapping and scheduling configuration. The name of the profile contains copy. Although the original profile is enabled (true), the copy is disabled at this point (false). You may prefer to edit values of the copied profile and rename them so the configuration settings apply to the new profile as required.
You have successfully copied the settings from an existing profile to a new profile. The Active column status is set to false, which means that the profile must be activated.

**SIR form after an incident ingestion**

After the Now Platform ingests the Microsoft Azure Sentinel incident, a security incident is created and the corresponding updates are made to the security incident record.

**Work notes**

A work note is posted when an incident is aggregated and if you have configured the **Log work note for new incident** option in the incident Aggregation Criteria. The following example shows the work notes in SIR.
When you click the incident number, you can view the internal incident import record that contains the raw incident data. The following example shows the raw incident data in SIR.

When you click the **Click here** link, you can view the record in Microsoft Azure Sentinel. The following illustration shows the record in Microsoft Azure Sentinel.

**Aggregated incidents**

**View incidents**: View the incidents that are aggregated to the security incident. Navigate to **Related List > Aggregated Microsoft Azure Sentinel incidents**.
Create security incident: Select an incident from the list, click the Actions menu, and then click Create security incident. This option creates a new security incident for the incident and this incident is de-aggregated from the parent security incident.

Delete security incident: Select an incident from the list, click the Actions menu, and then click Delete. This option deletes the incident record.

Microsoft Azure Sentinel integration settings

Modify the Microsoft Azure Sentinel integration default system properties.

Before you begin
Role required: sn_si.admin
**Procedure**

1. Navigate to **Microsoft Azure Sentinel Integration > Azure Sentinel Integration Settings**.
2. Modify the following settings as required.

### Microsoft Azure Sentinel Integration Settings

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sn_sec_sentinel.max_num_of_days_for_sample_data</td>
<td>Maximum number of days for which you can fetch sample data from Microsoft Azure Sentinel server. Type: integer Default value: 7</td>
</tr>
<tr>
<td>sn_sec_sentinel.max_num_of_sample_incident_per_call</td>
<td>Maximum number of sample incidents that you fetch from the Microsoft Azure Sentinel server for ingestion. Type: integer Default value: 5 Sample maximum value: 20</td>
</tr>
<tr>
<td>sn_sec_sentinel.max_aggregations_per_si</td>
<td>Incident aggregation limit for a security incident. For example, if there are 102 incidents, the first 100 are aggregated to security incident_1 and the remaining 2 to security incident_2. Type: integer Default value: 100</td>
</tr>
<tr>
<td>sn_sec_sentinel.max_si_per_day</td>
<td>Maximum number of security incidents that can be created in a 24-hour period in theNow Platform. Type: integer Default value: 1000</td>
</tr>
<tr>
<td>Maximum pagination limit for fetching the incident data in one REST call</td>
<td>Pagination limit for fetching incident data in one REST call from Microsoft Azure Sentinel.</td>
</tr>
<tr>
<td>Property Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>sn_sec_sentinel.max_page_size</td>
<td>Type: integer</td>
</tr>
<tr>
<td></td>
<td>Default value: 100</td>
</tr>
</tbody>
</table>

3. Click **Save**.  
Your modified integration settings are applied in the next polling interval as defined in the profile.

**Domain separation and the Microsoft Azure Sentinel integration**

Domain separation is supported for this application. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can then control several aspects of this separation, including which users can see and access data.

**Support level: Basic**

- Business logic: Ensure that data goes into the proper domain for the application’s service provider use cases.
- The application supports domain separation at run time. This includes domain separation from the user interface, cache keys, reporting, rollups, and aggregations.
- The owner of the instance must set up the application to function across multiple tenants.

Use case: When a service provider (SP) uses chat to respond to a tenant-customer’s message, the client must be able to see the SP’s response.

**How domain separation works in the Microsoft Azure Sentinel integration**

Follow these steps to achieve domain separation:

- Create a user with the sn_si.admin role in the respective domain.

  **Note:** When you create the profile, use the domain picker to select the specific domain. Do not create the user in the parent domain and later change the domain of the profile. You should have a specific user for each domain for your profile with the sn_si.admin role. Use this user to create or modify settings in the profile.

- Disable existing scheduled jobs.
• Replicate the Azure Sentinel comments and Status update and Azure Sentinel Profile Process on scheduled jobs for every domain.

• Change the Run as from the system user to the user with the sn_si.admin role in the respective domain and then run the scheduled job.

The following illustration shows replicating the Azure Sentinel comments and Status update job and running as a system user.
Scheduled Script Execution
Azure Sentinel comments and Status update.

Name: Azure Sentinel comments and Status update

Active: ☑

Application: Microsoft Azure Sentinel Incident Ingestion Integration For Security Operations

Conditional: 

For scheduled jobs that require an entered time, you have the option to enter an associated time zone. If no time zone is selected, the job will run at the entered time in the time zone of the user who entered the time. If ‘Use System Time Zone’ is selected, the entered time will run in the time zone of the instance running the job.

Run: Periodically

Repeat interval: Days: 0, Hours: 00, Minutes: 00

Starting: 2022-04-07T08:55:58

Run this script:
```java
REM AzureSentinelScheduledJobExecution(current.getUniqueValue()); InvokeCommentSynchronization();
```
The following illustration shows replicating the Azure Sentinel Profile Process job and running as a system user.
Scheduled Script Execution
Azure Sentinel Profile Process

Name: Azure Sentinel Profile Process

Active: Yes

Application: Microsoft Azure Sentinel Incident Ingestion Integration For Security Operations

Conditional: No

For scheduled jobs that require an entered time, you have the option to enter an associated time zone. If no time zone is selected, the job will run at the entered time in the time zone of the user who entered the time. If "Use System Time Zone" is selected, the entered time will run in the time zone of the instance running the job.

Run: Periodically

Repeat interval: Days: 0, Hours: 00, Minutes: 00, Seconds: 00

Starting: 2023-09-27 23:59:59

Run this script:

```javascript
var atf = new AzureSentinelScheduledJobExecution(current.getUniqueValue()).ingestIncidents();
```
Related information

Domain separation for service providers

Comparing Microsoft Azure Sentinel and Microsoft Graph Security API integrations with SIR

You can view the differences between Microsoft Azure Sentinel and Microsoft Graph Security API integrations and choose the right integration with your Now Platform instance.

Microsoft Azure Sentinel - Incident Ingestion overview

Microsoft Azure Sentinel is a cloud-based security information event management (SIEM) and security orchestration automated response (SOAR) solution. Microsoft Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise. It provides a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Microsoft Graph Security API overview

The Microsoft Graph Security API is an intermediary service (or broker) that provides a single programmatic interface for connecting multiple security providers (Native to Microsoft as well as ServiceNow Partners).

The Microsoft Graph Security API integration addresses these issues by using the Microsoft Graph Security API to connect with different Microsoft security technologies like Azure Sentinel, Microsoft Defender Advanced Threat Protection, and Azure Advanced Threat Protection. Alerts from Microsoft Security providers are ingested and security incidents are automatically created in Security Incident Response.
Summary of feature differences

Azure Sentinel and Graph Security API (Microsoft architecture)

ServiceNow SIR integration with Microsoft Azure Sentinel for ingesting *incidents* & creation of security incidents in SIR

ServiceNow SIR integration with Microsoft Graph Security API for ingesting *alerts* & creation of security incidents in SIR

Azure Sentinel Management API
- GET / UPDATE Incidents
- GET Entity Info

Microsoft Graph Security API
- GET Alert Info
- POST Alert Info
Microsoft Azure Sentinel vs Microsoft Graph Security API

<table>
<thead>
<tr>
<th>Microsoft Azure Sentinel</th>
<th>Microsoft Graph Security API</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingests Microsoft Azure Sentinel incidents along with entity information (when available) and automates security incident creation in SIR.</td>
<td>Ingests alerts from multiple Security providers (including Azure Sentinel) in a standard schema and automates security incident creation in SIR.</td>
</tr>
<tr>
<td>Supports bi-directional updates which include incident closure, incident status change (New), and synchronizing comments.</td>
<td>Supports alert updates (alert status change and alert closure) for selected security providers.</td>
</tr>
</tbody>
</table>

**Note:** For more information on the Microsoft Graph Security API supported security providers, view the Microsoft documentation.

Use this integration if your scenario includes the following conditions:
- Preliminary incident investigation is in Microsoft Azure Sentinel and subsequent investigation is in SIR
- Ingest Microsoft Azure Sentinel incidents to SIR

Use this integration if your scenario includes the following conditions:
- Perform incident investigation in SIR.
- Ingest Microsoft Azure Sentinel alerts in SIR.
- Incidents are not created in Microsoft Azure Sentinel.

Alert is an entity in Microsoft Azure Sentinel. You cannot retrieve standalone or specific alerts using the Microsoft Azure Sentinel Management API. You can only retrieve the alert data associated with an incident. The alert data available using this integration is richer than the alert data available using the Microsoft Graph Security API.

The Microsoft Azure Sentinel normalized alert data is available. The Microsoft Azure Sentinel alert fields that are mapped internally in Microsoft Graph Security API, and are available in Microsoft Graph Security API, are available for use in this integration.

You cannot update alerts in Microsoft Azure Sentinel using this integration.

Microsoft Graph Security API alert ingestion integration

Use the Microsoft Graph Security API integration to ingest alerts from Microsoft Graph security providers and automatically create security incidents.
Overview

The Microsoft Graph Security API is an intermediary service (or broker) that provides a single programmatic interface for connecting multiple security providers (Native to Microsoft as well as ServiceNow Partners).

The Microsoft Graph Security API integration addresses these issues by using the Microsoft Graph Security API to connect with different Microsoft security technologies like Azure Sentinel, Microsoft Defender Advanced Threat Protection, and Azure Advanced Threat Protection. Alerts from Microsoft Security providers are ingested and security incidents are automatically created in Security Incident Response.

Key features

This integration includes the following key features:

• Discovery of Microsoft Graph Security API alerts that are candidates for security incidents and automate the creation of security incidents.

• Mapping of alert fields to security incident fields.

• Aggregation of similar alerts to existing open security incidents instead of creating duplicate security incidents.

• Preview alert field values and validate their mappings in the security incident.

• Automatic alert status update for security incident creation and closure.

• Set up scheduled ingestion of alerts to create security incidents periodically.

Set up your Now platform instance for the Microsoft Graph Security API integration

The following section lists the setup tasks that you are required to complete in your Now Platform® instance prior to installing the application from the ServiceNow Store.

About this task

Refer to the following table and verify that you have completed all the listed tasks before you download and install the application to ensure a smooth installation and configuration.

Role required: admin

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have assigned the required Now Platform® and Security Incident Response roles.</td>
<td>The following roles are required for the installation, setup, and use of the integration in your Now Platform® instance.</td>
</tr>
<tr>
<td>Setup task</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>• A user with the Now Platform® administrator role (admin) installs the application from the ServiceNow Store and assigns the security incident administrator (sn_si.admin) role.</td>
<td></td>
</tr>
<tr>
<td>• A user with the sn_si.admin role oversees the following tasks in the Now Platform®:</td>
<td></td>
</tr>
<tr>
<td>◦ Names, creates, and edits alert profiles.</td>
<td></td>
</tr>
<tr>
<td>◦ Selects and maps Microsoft Graph Security API alert data fields to the security incident fields.</td>
<td></td>
</tr>
<tr>
<td>◦ Previews security incident details for accuracy prior to finalizing the configuration.</td>
<td></td>
</tr>
<tr>
<td>◦ Schedules on-going alert ingestion.</td>
<td></td>
</tr>
<tr>
<td>◦ Enables alert updates when a Security Incident Response incident is created and closed.</td>
<td></td>
</tr>
<tr>
<td>◦ Assigns the security incident analyst (sn_si.analyst) role.</td>
<td></td>
</tr>
<tr>
<td>◦ Users with the sn_si.analyst role work with security incidents.</td>
<td></td>
</tr>
</tbody>
</table>

For more information about roles and assigning roles to users, see Roles on the ServiceNow Product Documentation website.

<p>| Register your application in the Microsoft Azure portal. | Before you can ingest alerts, you must configure your application in the Microsoft Azure portal. See Configure the Microsoft Azure portal for details. |
| Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you | Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation. |</p>
<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
</table>
| install the application for the integration. | 1. Security Incident Response
2. Event and Alert Ingestion for Security Operations: This application requires:
   • com.glide.hub.integration.runtime => ServiceNow IntegrationHub Runtime
   • com.glide.hub.action_step.rest => ServiceNow IntegrationHub Action Step - REST

ℹ️ Note: The Integration Hub components are installed along with the Event and Alert Ingestion plugin. If these are not installed, contact Customer Support for assistance.

For more information about installing the Security Operations core applications, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.

**Configure the Microsoft Azure portal**

To retrieve security alerts for an application available in the Microsoft Azure tenant using the Microsoft Graph Security API, you must register the application in the Microsoft Azure portal and grant security event read and write access to the application.

**Before you begin**

Role required:
- Application Developer: Required for registering the application.
- Tenant Administrator: The Microsoft Azure tenant administrator must grant permissions to the application by making a call to the admin consent endpoint.
Procedure

1. Log into the Microsoft Azure portal. Enter App registrations in the Search box.

2. Click New registration. Enter a name for your application and the redirect URI, for example http://localhost and click Register. The Redirect URI is used while providing admin consent for the application.

3. In the App registrations page, select the application you have registered, for example Graph Security Demo.

4. Under Manage, select Certificates & secrets.

5. Select New client secret to create a client secret. Copy the client secret and save it as it will not be visible later. In case you forgot the client secret you can generate a new client secret.

   Note: If you forget the client secret, you can generate a new one by following the instructions in steps 4 and 5.

6. 2. Click View API Permissions in the Overview page.

7. Add new Application level API permissions for SecurityEvents.ReadWrite.All security events.
8. Grant admin consent for the newly added API permissions. See the Microsoft Graph Permissions reference for more information about the Microsoft Graph permission model.

9. Login as a tenant administrator and provide consent for the application. The steps are given below:
a. Navigate to the following URL: https://login.microsoftonline.com/common/adminconsent?client_id=APPLICATION_ID&state=12345

Enter the APPLICATION_ID of the application that you have registered.

10. Click **Accept** to accept permissions requested by the application created above. You can then use the application to read security events. See the Microsoft Graph Security Authorization documentation for more details.

**Install and configure the Servicenow application for Microsoft Graph Security API alert ingestion integration**

Before you run the integration on your Now Platform® instance, complete these installation and configuration steps so the application properly integrates with the Security Incident Response and Security Operations products on your Now Platform instance.

**Before you begin**
Role required: sn_si.admin

**Procedure**

1. If you have not installed the Microsoft Graph Security API application from the ServiceNow Store for the integration, see **Install a Security Operations integration** and follow the steps to install it.

2. After you have successfully installed the application, navigate to **Integrations > Integrations Configurations** and locate the Microsoft Graph Security API - Alert Ingestion tile.
3. To configure the application, click **Configure**.

4. In the **Alert Ingestions Configuration** dialog that is displayed, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Name of the Microsoft Azure Cloud instance.</td>
</tr>
<tr>
<td></td>
<td>You can enter only alphanumeric values and hyphens (-) in this field.</td>
</tr>
<tr>
<td><strong>Tenant ID</strong></td>
<td>The Microsoft Azure Tenant ID. This is the instance from which all the alerts in the Microsoft Azure portal are retrieved.</td>
</tr>
<tr>
<td><strong>Client ID</strong></td>
<td>The Client ID for the application that you have registered in the Microsoft Azure portal. See <a href="#">Configure the Microsoft Azure portal</a> for details.</td>
</tr>
<tr>
<td><strong>Client Secret</strong></td>
<td>The password for your registered application.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

After it is successfully validated and submitted, each alert ingestions server configuration is saved on the Security Integrations page as a tile. If your saved
configuration tiles are not displayed on the Security Integrations page, on the top right corner of the page, from the Show Configurations choice list, click Yes.

What to do next
You have successfully installed and configured the application. The next step is to create an alert profile.

Create a profile for the Microsoft Graph Security API alert ingestion integration
As a user with the sn_si.admin role, you create an alert profile in your Now Platform instance and determine which alerts create security incidents. Before security incidents are created from ingested alerts, the field values from alerts are displayed on a layout of a Now Platform security incident so that you can preview how the actual security incident will be displayed.

About this task
The integration allows you to ingest different types of alerts such as unauthorized access attempts and malware, for example. These alerts are ingested based on the profiles that you configure in the Security Operations environment of your instance. All alerts are initially ingested for a configured alert type in a profile. Ingested alerts can then be further filtered to specify which alerts create security incidents.

For example, you may prefer filters that create security incidents only for alerts that are identified as high-risk. Before a profile is activated, and it creates security incidents from ingested alerts, individual field values on the filtered alerts are mapped to corresponding fields on a layout of security incident for a preview. All alerts that meet the selection criteria in your Microsoft Azure tenant and are available over the Microsoft Graph Security API are initially ingested into your Now Platform instance.

Identify the source for the profile
Specify the name and source for the profile.

Before you begin
Role required: sn_si.admin

Procedure
1. To create a profile for an alert in your Now Platform instance, navigate to Microsoft Graph Security API Integration > Microsoft Graph Security API Profile.
2. Click New.
3. Fill in the fields.
An example of a completed form follows the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the profile. If names are not unique, an error will be displayed and duplicate profile names are not saved. Profile names in your Now Platform instance must be unique.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box is cleared by default. If this option is disabled, the profile is not active.</td>
</tr>
<tr>
<td>Note:</td>
<td>You should complete all sections in the profile before making it active.</td>
</tr>
<tr>
<td>Source</td>
<td>The Microsoft Azure tenant that you configured to ingest alerts. If you have multiple tenants configured, select the appropriate tenant for the alert types that you are planning to ingest for the profile. You are required to enter a value.</td>
</tr>
<tr>
<td>Order</td>
<td>Default is 100. If you have created multiple profiles, this value provides a run time execution priority when two or more profiles share the same triggering conditions. The lower the order value, higher the priority.</td>
</tr>
<tr>
<td>(Optional) Description</td>
<td>Additional text to help you distinguish this profile from other profiles.</td>
</tr>
</tbody>
</table>

The following figure is an example of a completed form.
What to do next
The next step is to map the alert fields.

Mapping of alert fields for Microsoft Graph Security API alert ingestion integration

After you identify the sources for scheduled alert ingestion, the next step is to map individual alert fields to the fields on a Now Platform SIR security incident. For the mapping step, you must first ingest sample alerts from the Microsoft Azure tenant. Then you must ensure that all relevant alert field data is mapped to the appropriate place on the SIR incident form and then visualize the SIR incident in the preview section.

Mapping of the sample alert fields involves the following:

- Ingest sample Microsoft Graph Security API alerts
- Mapping alerts to security incident response fields

Ingest sample Microsoft Graph Security API alerts
Ingest sample alerts from your Microsoft Azure tenant.

Before you begin
Role required: sn_si.admin
Procedure

1. You can either pull the 5 most recent sample alerts or provide the unique alert IDs for the specific alerts that you want to use for your mapping experience. From the Ingestion Preference choice list, select one of the following:
   - Retrieve most recent alerts: The 5 most recent alerts are retrieved.
   - Select alerts based on alerts ID: Specify the alert ID for the alerts to be retrieved. You can specify a maximum of 5 alert ids separated by commas.

2. Click Fetch Sample Data to pull the latest sample alert data from the Microsoft Azure tenant. The pull for sample alerts may take a few moments.

   The sample alert field values are populated on the left side of the form when sample alerts are ingested by the profile. These are the alerts that you map to the SIR security incident fields. The alert fields and values results are displayed as individual tabs.
What to do next
After you have fetched the sample data, the next step is map the alert fields to the security incident.

Mapping alerts to security incident response fields
Map individual alert fields from triggered alerts to fields on a Now Platform security incident.
Alert field mapping

As a user with the sn_si.admin role, use the fields from the Sample Alerts section on the left and map them to the security incident fields in the SIR Incident Field Mapping column on the right panel. Edit the mapping configuration by dragging alert fields from the left side and dropping them on the SIR incident mapping section on the right. The mapping on the right associates the incoming alert field with an outgoing security incident field.

1. After you have fetched the sample data, the next step is map the alert fields to the security incident. To map a field value from the left side of the form to a field on the security incident on the right side of the form, click-hold a blue field name on the left side of the form.

2. Drag the field name, for example, category, and drop it on a field in the Input Expression column next to a field name in the Security Incident column.

The field value is displayed in the Input Expression column. In the following image, category is mapped to the Category field on the security incident.

However, you can match any value from the left side to a field on the right. Verify that the value is mapped correctly on the security incident during the preview step.

To help you ensure that no alert fields are overlooked or duplicated in the mapping process, fields are color-coded. Color-coding of the alert fields helps you keep track of the alert values that you have already mapped as they become grayed out while all remaining unmapped fields appear in blue. This
helps you better visualize which field values have been added to the security incident and if any remaining important alert information remains unmapped.

Light blue fields on the left indicate that an alert field is not yet selected and mapped on the security incident. You may prefer to associate an incoming alert field with more than one field on a security incident. A gray field indicates that a field has been selected and mapped to a field on the security incident. This color-coding helps you track the mapping.

**Note:**

a. To manually enter a value in the Input Expression field, enter it in the format `${fieldname}`. The alert field is mapped to the security incident field.

b. You cannot map ingested alerts to the MITRE-ATT&CK Framework fields in the security incident mapping section. If you still map the fields, the information will not be available as part of the MITRE-ATT&CK card in the MITRE-ATT&CK framework section in the security incident form. To associate the MITRE-ATT&CK Techniques, use the Auto Extraction Feature available as part of the MITRE-ATT&CK Framework in the Threat Intelligence Module.

3. To add fields to the default fields displayed on the security incident on the right side of the form, follow these steps.

a. On the right of the form in the SIR Incident Field Mapping section, at the bottom of the grid, click the plus (+) icon. A new field is displayed.

b. In the Security Incident column, expand the list that is displayed, and select a field.

In the expanded list for the new field, some fields are shaded. In the following figure, Category has a gray background, because it has been mapped in the security incident. Similar to the color-coding for the alert fields on the left side of the form, this color-coding for the security incident fields on the right helps you track the already mapped SIR incident fields.
Note: As multiple observables can be displayed on the same security incident, the Observable field can be mapped multiple times with different values. Similarly, the Configuration Item and Work notes fields support multiple values. If you try to map two values to a field that cannot support multiple values, when you preview the incident, an error message is displayed that there is no value for the field. Similarly, if a field on a security incident has a list from which you can choose multiple options, and you try to map an option to that field that is not displayed on the list, the field is not populated on the security incident.

c. Alternatively, type a value in the Search field for the new row.

d. From the left side of the form, left-click to select the Alert ID that you want in the Input Expression field. With the drag-and-drop feature, map it next to your new field.

4. Continue mapping by adding or removing field values to the mapping.

5. After you have completed the preceding field-mapping steps, you can use the same field values in the Incident Generation Conditions builder to define additional criteria that an incoming alert must satisfy to create a security incident. To set incident generation conditions, follow these steps.
Format field translation

In certain cases, alert field values in Microsoft Graph Security API may not translate directly to the fields on the SIR security incident. For these values, you can use a script editor to format field values on the security incident during the mapping step. Use the script editor if you want to format values that are similar, but not identical. For example, with the script editor, a category value of Malware Alert and Virus Infection may have different field values for the source category but both values can be translated to a common Malicious Code Activity in the Category field on the SIR security incident using the Format Field Translation functionality.

To use the script editor, click the {} icon. The script editor is displayed.

Incident generation conditions

Once the mapping section is complete, you can set filter conditions so that you can specify which alerts should create security incidents versus which alerts should be filtered out, for example, low-priority alerts. You can use the same field values in the Incident Generation Conditions builder to define additional criteria that an incoming alert must satisfy to create a security incident. To set incident generation conditions, follow these steps.

1. Scroll to the Incident Generation Conditions section on the form and select the Filter based on conditions option. The Filter conditions builder is displayed. Use these filters to create security incidents that match the specific conditions described by the fields.

The options in the lists for the first field in the Filter conditions builder match the fields that are displayed on the Alert Sample Ingestion section for the alert you ingested. These fields are dynamic and change depending on the alert that you ingest Criteria that you enter are case-sensitive, and they must match exactly the values of the alert. If you are not sure about the values to enter
in the filter fields, you may prefer to return to your Microsoft Azure tenant and review your alerts for the keywords.

2. Using the lists and fields of the conditions builder, set filters for the first row.

3. To add more conditions, to the right of the fields, click **AND** or **OR**.
   - If **AND** is selected, all conditions must be matched.
   - If **OR** is selected, either condition can be matched.

4. In the second row, set a second filter condition

The following image is an example with two conditions that must be matched before security incidents are created.

You have set the triggering conditions so that security incidents are created only when both of the filtering conditions that you entered are matched.

This type of filtering helps you isolate security alerts, and it limits the number of security incidents that you create. If additional filtering criteria are set, only alerts that are required are ingested without having to change the query or the triggered alert configuration.

**Alert aggregation criteria to handle similar alerts and prevent duplicate incidents**

Define additional alert aggregation criteria that aggregates an incoming alert to an existing SIR security incident instead of creating similar, potentially duplicate incidents. Using field matching value criteria for each profile, this additional aggregation capability can reduce the number of active, overlapping security incidents by placing all related alert data on a single security incident. To set the criteria, follow these steps below:

1. Scroll to the **Alert Aggregation Criteria** section on the form and select the Aggregation Conditions option. The Incident Field Matching Values columns are displayed. These field names are the fields on the security incident that include any custom fields that are configured on the SIR security incident.
2. From the Available list, select the field values that you want to match on existing security incidents in your Now Platform and move them to the Selected list. All the field values that you select must be matched to append this incoming alert to an existing security incident. This includes fields, such as Observables and Configuration Items, that may have multiple alert field values mapped to them. All values must match. If only a subset of the values are matched, the alert aggregation conditions will not be met and a new security incident will be created. See screen shot below for multi-value field mapping.

If a new alert matches all the values that are selected in the aggregation field conditions in the mapping step, the alert is automatically added to the most recently opened security incident with the same field values. As a user with the sn_si.analyst role working with security incidents, you can view all the added aggregate alerts on a related list on a security incident. All of the aggregated alerts on a security incident are displayed on the Aggregated Microsoft Graph Alerts related list. This list details associated time stamps and aggregated field values. This information helps you understand why alerts are added to existing security incidents. If this tab is not displayed, scroll to the left side of the record under Related Links and click the Show All Related Lists link.

3. Optional: To log a work note for a new alert that is recently added on the security incident, select the check box to enable this option. The work note logs that a new alert has been added along with a link to the alert details and any other details that may have been added to the work note field in your mapping section.

You have successfully mapped values from an alert to fields on a SIR security incident. Also, you have configured additional conditions to limit the creation of security incidents with filtering criteria. You also appended alerts or events to existing SIR security incidents.

4. Click Continue to continue with the profile configuration. The next step is to preview the fields you mapped on a SIR security incident.
Preview the security incident for the Microsoft Graph Security API integration

After you complete the mapping step, preview the values that you mapped in a Now Platform SIR security incident. This preview step permits you to verify that you have mapped all the alert fields that you want displayed on the security incident.

About this task
As a user with the sn_si.admin role, preview a security incident and edit the mapping again as required to fix fields with errors or to populate any missing data. If the preview is not successfully completed, you cannot proceed to the scheduling step. Previews of SIR security incidents are not saved as actual incidents in the Security Incident Response product.

Role required: sn_si.admin

Procedure
1. If the security incident preview is not displayed, click Preview in the progress bar.
   All the ingested alerts and the field mappings defined in the Mapping page are displayed.

2. Click on an Alert ID to see a preview of the security incident.
   This view is a read-only view, and a record of this security incident is not saved.

3. Review the field mapping of the alert values on the security incident.

   The preceding image is an example of a preview with a mapping error of the samples that were ingested.

4. To resolve this error, click Mapping in the progress bar.
5. Edit the mapping to fix incorrect values or populate any missing data.
6. Preview the mapping again and continue to fix any errors that are described in error messages.

What to do next
If no error messages are displayed, and you are satisfied with the field mapping on the security incident, the next step is to define the schedule.

Define schedule for Microsoft Graph Security API integration
Verify the default settings for alert retrieval or modify the scheduling as needed. This step permits you to filter your alert retrieval based on a date range.

About this task
You also choose how often you will poll for future alerts that match the alert profile configuration. For automated alert ingestion profiles, before the profile is activated, you verify and modify the scheduling and alert retrieval. This step is needed for scheduled alert profiles.

As a user with the sn_si.admin role, you configure these polling intervals on a per-profile basis. The performance of the Microsoft Graph Security API alert ingestion integration is impacted by the different polling intervals. When scheduling, you may prefer to balance system load against incident urgency. A five-minute default value is set for any profile, but you may prefer to modify this setting based on the urgency of the incident and the anticipated load on your system.

Procedure
1. If the Scheduling page on the progress bar is not displayed, select Scheduling.
2. Choose one to schedule how and when alerts are pulled from the Microsoft Azure tenant.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ongoing Alert Ingestion selected</td>
<td>Based on the default setting, the Now Platform instance pulls from the Microsoft Azure tenant for new alerts every five minutes. Security incidents are created if triggered alerts are found and incident generation filtering criteria are matched. To balance alert ingestion against server load, and to pull the most current data, five minutes is the setting you may prefer.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>• Ongoing Alert Ingestion selected</td>
<td>However, this value can be modified as needed.</td>
</tr>
</tbody>
</table>
| • Set initial alert ingestion time | Initial ingestion time  
If you want to schedule the initial ingestion at a specific time, follow these steps:  
• Select the Ongoing Alert Ingestion and Set initial alert ingestion time fields.  
• Specify the time in the Input initial alert ingestion time field.  
The initial ingestion will take place at the time specified here. Subsequent ingestions will be based on the schedule defined in the Polling increment (minutes) field.  
As an example for scheduling, if you have a daily alert job that runs once a day at 4 AM local time, you can set up the corresponding alert profile in your Now Platform instance to run at 4:05 AM local time to capture the alert right away and create a security incident.  
Enter 04 05 00 in the Initial alert ingestion field. In the Increment (Minutes) field, enter 1440 (24 hours) to schedule the next alert ingestion for 24 hours from the initial alert ingestion.  
Both the initial alert ingestion time and next alert ingestion time are displayed in the fields.  
To configure the settings in this example, follow these steps:  
• Select the **Ongoing Alert Ingestion** option.  
• In the Polling Increment (minutes) field, enter 1440 (24 hours).
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Click the <strong>Set Initial alert ingestion time</strong> option to enable editing for the Initial alert ingestion time and Next alert ingestion (estimated) time fields.</td>
<td></td>
</tr>
<tr>
<td>• In the Initial alert ingestion time field, enter 04 05 00. In the Next alert ingestion (estimated) time field, the time of the next alert ingestion is displayed.</td>
<td></td>
</tr>
<tr>
<td>One-Time Retrieval</td>
<td>Use this configuration if you want a one-time pull to ingest historical alerts.</td>
</tr>
<tr>
<td></td>
<td>When this setting is configured, a profile is used once to retrieve alerts from historical events that are based on a date range. To the right of the Since date field, click the calendar icon. In the calendar that is displayed, select the date that you want to start pulling alerts. Starting with the Since date value, alerts are retrieved up through the current date. Note that you can pull as far back as seven days from the current date. This functionality is not intended to retrieve significant amounts of historical alerts but rather a minimal amount of in-flight alerts that are being actively worked at the time of profile activation. After the alerts are pulled, this setting will not retrieve more alerts for this profile going forward from the current date. This setting populates the security incident with all the alerts that are found for the range you enter.</td>
</tr>
</tbody>
</table>

3. Click **Continue** to navigate to the Additional Options page.
Automate alert updates and closure based on SIR incident status

The Microsoft Graph Security API alert ingestion integration has a bi-directional interface that allows for both alerts to create security incidents, as well as an ability to update the alerts once the security incident is created and/or closed with relevant incident details such as SIR incident number, assignment group, SIR incident URL, and so on. This section is the final portion of the profile configuration set-up that provides optional capabilities to update the alerts.

Before you begin
Role required: sn_si.admin

Note: The initial and closure alert statuses are updated only if this functionality is supported by the service provider. For details, see the Microsoft Graph Security API documentation and the security provider documentation.

Procedure

1. If the Additional Options page on the progress bar is not displayed, select Additional Options.

2. Follow the instructions below to complete the configuration for updating alerts when the security incident is created:

<table>
<thead>
<tr>
<th>Option or Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Update alerts upon SIR Incident Creation</strong></td>
<td>Select this option if you want to update the alert status and add additional comments when a security incident is created from the alert. This can occur for both the initial triggering alerts that create the security incident, as well as aggregated alerts.</td>
</tr>
<tr>
<td><strong>Initial Alert Status Update</strong></td>
<td>Select an initial alert status from the list. This status will be set for all alerts when a security incident is created for an ingested alert. This includes alerts that create new incidents and alerts that are ingested and aggregated to an existing open incident.</td>
</tr>
<tr>
<td>Option or Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><img src="image.png" alt="Image" /></td>
<td><img src="image.png" alt="Image" /></td>
</tr>
</tbody>
</table>

Note: Based on the alert status selected here, the alert status used by the security providers will be correspondingly updated.

Initial Comments posted back to Alert

- Based on the stage you have selected, default comments are displayed. You can modify the default text and use the `$(field name)` format to add or modify any fields available in the security incident form.

Close out alerts upon SIR Incident Closure

- Select this option if you want to use the automated alert closure option. This can occur for both the initial triggering alerts that create the security incident, as well as aggregated alerts. Alert status will be updated in the security provider with the status and closure comments after SIR incident is closed in the Now Platform.

Closure Alert Status Update

- Select an alert status from the list. Select the status value to be set for all alerts when a security incident is closed for an ingested alert.

Closure Comments Posted back to Alert

- The default closure comments are displayed here. You can edit the default text and use the `$(field name)` format to add or modify any fields available in the security incident form.

3. Click **Finish** to complete the configuration and move the profile to the **Waiting** state.

A confirmation dialog is displayed. You have successfully completed the setup and configuration for the integration. Activate this profile to pull alerts from the Microsoft Azure tenant based on your scheduling. A maximum of 1000 security incidents can be created within a 24 hour period.
Microsoft Graph Security API integration configuration settings

Use this option to modify the Microsoft Graph Security API ingestion integration default system properties.

About this task

Modify the default configuration properties to limit the number of security incidents that can be created during a 24 hour period or the number of alerts that can be aggregated in one security incident.

To modify the system properties, log in as a user with the `sn_si.admin` role and navigate to **Microsoft Graph Security API Integration > Microsoft Graph Security API Integration Settings**.

The default configuration settings are displayed. You can modify these settings if required.

<table>
<thead>
<tr>
<th>Microsoft Graph Security API Integration Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>All properties used in Microsoft Graph Security API Alert Ingestion Integration.</td>
</tr>
<tr>
<td>Enforce a limit on number of security incidents that can be created in 24 hour period.</td>
</tr>
<tr>
<td>1000</td>
</tr>
<tr>
<td>Enforce a limit on number of alerts that can be aggregated to a single incident.</td>
</tr>
<tr>
<td>100</td>
</tr>
<tr>
<td>Maximum number of alerts per vendor that can be fetched in one REST call</td>
</tr>
<tr>
<td>50</td>
</tr>
</tbody>
</table>

Any modified integration settings will be applied during the next polling interval as defined in the profile.

Security Incident Response form after alert ingestion

After a Microsoft Graph Security API alert has been ingested, a security incident is created and the corresponding updates are made to the security incident record.
Worknotes

If you had selected the **Log work note for new alert** option in the alert Aggregation Criteria as described in the **Mapping alerts to security incident response fields**, a worknote is posted when the alert is aggregated.

Click on the alert link to navigate to the internal alert import record that contains raw alert data.
Aggregated alerts

Click Related Lists > Aggregated Microsoft Graph Security alerts to view the alerts aggregated to the security incident.

- **Create security incident**: Select an alert from the list, click the Actions menu and click Create security incident. This option creates a new security incident for the alert and this alert is de-aggregated from the parent security incident.

- **Delete alert record**: Select an alert from the list, click the Actions menu and click Delete. This option deletes the alert record.

**Optional: Copy a Microsoft Graph Security API profile**

Copy an existing profile and its associated settings instead of creating new profiles. If you are creating multiple profiles, and you want to reuse the settings of an existing profile, you may prefer to copy profiles to save time.

**Before you begin**

Role required: sn_si.admin

**About this task**

As a user with the sn_si.admin role, if you copy a profile, the profile name is initially modified to avoid duplicate profiles. In addition, the copied profile is disabled (false) so it is not activated accidentally prior to completing the configuration. Copy profiles and use existing maps for security incidents that you have already previewed and verified.
Procedure

1. Navigate to Microsoft Graph Security API Integration > Microsoft Graph Security API Profile.

2. In the Microsoft Graph Security API Profiles list that is displayed, select a profile that you want to copy, and, from the Actions on selected rows choice list, click Copy.

The profile is copied and displayed on the list. The copy has all the settings of the original profile including the mapping and scheduling configuration. The name of the profile contains copy. Although the original profile is enabled (true), the copy is disabled at this point (false). You may prefer to edit values of the copied profile and rename it so the configuration settings apply to the new profile as required.

You have successfully copied the settings from an existing profile to a new profile. Note that the Active column status is set to false as the profile needs to be activated.

What to do next

You are prompted to activate (enable) the new profile after you complete the configuration steps.

Domain separation and Microsoft Graph Security API alert ingestion

This section provides information on domain separation support with Microsoft Graph Security API alert ingestion.

To achieve domain separation, replicate the Microsoft Graph Security API Profile Process and SIR Process Alert Updates scheduled jobs and change the Run as users. By default these scheduled jobs are executed by the system user. Change the Run as to a user with the sn_si.admin role in the respective domain and run the scheduled job.
Flow Designer and Integration Hub usage in Microsoft Graph Security API integration

Using the Flow Designer and Integration Hub functionality, several subflows and actions have been built as part of the Microsoft Graph Security API integration.

The following subflows are available:

- **Microsoft Graph Security API Configuration Validation**: This is used in the configuration tile to validate the credentials in the initial setup.
- **REST Call For Microsoft Graph Security API**: This is used for any interactions with Microsoft Graph security API using REST calls.
- **Retrieve Sample Alerts**: This is used in the Mapping section of the profile setup to fetch sample data. This sub-flow is triggered asynchronously.

Troubleshooting Microsoft Graph Security API integration

This section covers important troubleshooting tips and frequently asked questions related to the Microsoft Graph Security API alert ingestion integration.

- **Integration run**: When a scheduled job starts executing, an integration run record with logs, errors, and warnings is displayed. The number of alerts pulled and the number of incidents created in a scheduled job run are also displayed. Users with the `sn_si.analyst` role can see if any errors/profiles pulling failed during the integration run. Users with the `sn_si.analyst` role can check the `sn_event_ingestion_integration_run` table for any errors that have occurred. To troubleshoot any integration issues, you must first check the integration run. Errors are logged as worknotes in the integration run records for every scheduled job run.
Incomplete profile: While configuring the profile, in the Additional Options (Automate alert updates and closure based on SIR incident status) section, you must click the Finish button to ensure that the profile is moved to Waiting state indicating that it is waiting for ingestion.

Validate profile: To validate if the integration is working correctly, check the profile states, last pulled date of profile, alert import table, alert to task table records.

SSL issues: When connecting through the Microsoft Graph Security API, ensure that the instance has a valid CA certificate which has not expired. You can import RSA or your own certificates into the platform and ensure that the common name of the certificate matches host name. See KB0778285 for details.

Palo Alto Networks - AutoFocus integration

The Palo Alto Networks - AutoFocus integration base system includes a workflow and a series of workflow activities you can use to integrate Palo Alto Networks - AutoFocus with your instance.
Activate and configure Palo Alto Networks AutoFocus integration

The Integration Configuration feature allows you to quickly activate and set up third-party security integrations, including Palo Alto Networks - AutoFocus. Before you can use the Palo Alto Networks - AutoFocus, you must download it from the ServiceNow Store.

Before you begin
Role required: sn_si_admin

Procedure

1. Download the integration from the ServiceNow Store.

2. When the installation is complete, access Palo Alto Networks support site and obtain the API Key.


4. In the Palo Alto Networks AutoFocus card, click Configure.

5. Enter (or paste) the API Key you acquired from the Palo Alto Networks support site.

6. Click Submit.
Get AutoFocus Session Info Enrichment workflow

When the Security Operations Palo Alto Networks - Get AutoFocus Session Info Enrichment workflow is executed, it queues a search query with AutoFocus for gathering information about a specified source IP. If AutoFocus has knowledge about previous sessions originating from that IP address, a JSON-formatted report is returned.

Before you begin
Role required: sn_si.analyst

About this task
The Security Operations Palo Alto Networks - Get AutoFocus Session Info Enrichment workflow is executed when the Source IP field in a security incident is modified and the record is updated. The workflow fetches the IP address and submits a query request to AutoFocus. If AutoFocus has previously identified sessions originating from the IP address, a JSON-formatted report is returned.

Procedure
1. Navigate to Security Incident > Show Open Incidents.
2. Click the Indicators of Compromise tab and populate the Source IP field.
3. Click Update.
AutoFocus scans the information from the IP address and a text file in JSON format is attached to the security incident.

Activities specific to this integration are described here. For more information on other activities, see Common integration workflow activities.

**AutoFocus Search Session activity**

The **AutoFocus Search Session** workflow activity uploads information from an IP address assigned to a security incident to AutoFocus and queues it for a search query. When the activity executes, it queues a search query with AutoFocus for gathering information for a specified source IP. If AutoFocus has previously identified sessions originating from that IP address, a JSON-formatted report is returned.

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>searchSessionQuery [string]</td>
<td>The search query for session information.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>requestStatus [Boolean]</td>
<td>True if a search query was scheduled for execution in AutoFocus.</td>
</tr>
<tr>
<td>error [string]</td>
<td>The error, if any, that occurred in the activity.</td>
</tr>
<tr>
<td>afcookie [string]</td>
<td>An identifier for the AutoFocus search query used by the Fetch Search Results activity to retrieve the search results.</td>
</tr>
</tbody>
</table>

**Fetch Search Results activity**

The **Fetch Search Results** workflow activity fetches search results identified by a cookie to the search query initiated by the **AutoFocus Search Session** activity.
**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>afcookie [string]</td>
<td>The AutoFocus cookie for the search request generated by the AutoFocus Search Session activity.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>searchPending [Boolean]</td>
<td>True if the search request is still processing in AutoFocus.</td>
</tr>
<tr>
<td>result [string]</td>
<td>The search results data.</td>
</tr>
<tr>
<td>status [Boolean]</td>
<td>True if the search is completed and results have been successfully generated.</td>
</tr>
<tr>
<td>error [string]</td>
<td>The error, if any, that occurred in the activity.</td>
</tr>
</tbody>
</table>

**Write content to record as attachment activity**

This activity writes the content passed in from an input and creates a designated attachment to a given record.

The *Write content to record as attachment* activity can be used with any workflow to write content and attach it to a record.

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tablename [string]</td>
<td>The table name for the record. This input field is mandatory.</td>
</tr>
</tbody>
</table>
Input variables (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sysid [string]</td>
<td>The system identifier (sys_id) of a task record. This input field is mandatory.</td>
</tr>
<tr>
<td>payload</td>
<td>The plain text content to be written as an attachment. This input field is mandatory.</td>
</tr>
<tr>
<td>filename</td>
<td>The attachment file name.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result [string]</td>
<td>Indicates whether the update was successful.</td>
</tr>
</tbody>
</table>

Palo Alto Networks - Firewall integration

To perform Palo Alto Networks - Firewall integration, ensure that you have a MID Server set up with SSH credentials. If a firewall is not already set up, add one.

<table>
<thead>
<tr>
<th>Explore</th>
<th>Set up</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Security Incident Response integrations</td>
<td>- Activate and configure the Palo Alto Networks Firewall Integration</td>
</tr>
<tr>
<td>- Security Operations Integration Palo Alto Networks Firewall Launcher workflow</td>
<td>- Set up SSH credentials to the MID Server</td>
</tr>
</tbody>
</table>

Troubleshoot and get help

- ServiceNow Security Operations integration development guidelines
- Tips for writing integrations
- Developer training
- Developer documentation
- Find components installed with an application
Set up SSH credentials to the MID Server

Palo Alto Networks Firewall sends API calls to the MID Server. As such, ensure that SSH credentials have been created for the MID Server.

Before you begin
Role required: admin
The Orchestration plugin must be activated.

Procedure
1. Navigate to **Orchestration > Credentials & Connections > Credentials**.
2. Click **New**.
3. In the Interceptor screen, click **SSH Credentials**.
4. Fill in the fields, as needed.

### SSH Credentials

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the credential.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to activate this credential.</td>
</tr>
<tr>
<td>Applies to</td>
<td>Select <strong>All MID servers</strong> or <strong>Specific MID servers</strong>.</td>
</tr>
<tr>
<td>MID Servers</td>
<td>If you selected <strong>Specific MID servers</strong>, click the lock icon and select the MID Servers you want to apply these credentials to.</td>
</tr>
<tr>
<td>Order</td>
<td>Select the order to which the credentials are tried by the server. Smaller numbers are tried first.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the user name of the user associated with these credentials, if any.</td>
</tr>
</tbody>
</table>
Activate and configure the Palo Alto Networks Firewall Integration

The Integration Configuration feature allows you to quickly activate and set up third-party security integrations, including Palo Alto Networks - Firewall. Before you can use the Palo Alto Networks - Firewall, you must download it from the ServiceNow Store.

Before you begin
Role required: sn_si_admin

Procedure

1. Before activating and configuring the integration, access the Palo Alto Networks Firewall dashboard. Take note of the names of the IP Dynamic List, URL Dynamic List, or Domain Dynamic List you are using for firewall blocking.

2. Download the integration from the ServiceNow Store.

3. When the installation is complete, navigate to Security Operations > Integration Configuration. The available security integrations appear as a series of cards.

4. In the Palo Alto Networks Firewall card, click Configure.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>If you entered a <strong>User name</strong>, enter the user’s password.</td>
</tr>
<tr>
<td>Tag</td>
<td>Enter a tag to be used for search criteria. The <strong>Tag</strong> field should contain the same value as the <strong>Name</strong>.</td>
</tr>
</tbody>
</table>
5. Click **Configure firewalls**.
6. In the Firewall Configurations screen, click **New**.
7. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewalls</td>
<td>Click the lock icon and select the firewall to be configured.</td>
</tr>
<tr>
<td>Firewall Version</td>
<td>Select the Palo Alto Networks Firewall version. <strong>PAN-OS-7.1</strong> is the recommended version. Selecting earlier versions may return inconsistent results.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username to use when connecting to the firewall via REST endpoints.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the connecting user.</td>
</tr>
<tr>
<td>IP Dynamic List</td>
<td>Enter the name of the External Dynamic List or Dynamic Block List you use for IP addresses.</td>
</tr>
<tr>
<td>URL Dynamic List</td>
<td>Enter the name of the External Dynamic List or Dynamic Block List you use for URLs.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Domain Dynamic List</td>
<td>Enter the name of the External Dynamic List or Dynamic Block List you use for domains.</td>
</tr>
</tbody>
</table>

8. Click **Submit**.

**Security Operations Integration Palo Alto Networks Firewall Launcher workflow**

*Security Operations Integration Palo Alto Networks Firewall Launcher* workflow is the Palo Alto Networks Firewall implementation launched by the *Security Operations Integration - Block Request* capability workflow.

**Before you begin**
Role required: sn_si.analyst

**About this task**
Workflow process activities include:

- **Security Operations Palo Alto Networks - Check and Block Value workflow**

![ Workflow diagram ]

**Security Operations Palo Alto Networks - Check and Block Value workflow**

As security incidents are created and triaged to identify potential threats, you can use the *Security Operations Palo Alto Networks - Check and Block Value* workflow to automatically check and update IP addresses, URLs, and domains using External Dynamic Lists defined in Palo Alto Networks - Firewall.

**Before you begin**
Role required: sn_si.analyst

**About this task**
The *Security Operations Palo Alto Networks - Check and Block Value* workflow is executed when Firewall Block Requests are submitted. The block request specifies the firewall to be used, the type of observable to be checked and blocked (if needed), and the block value. That is, the IP address, URL, or domain in question.
During workflow execution, commands defined under **Palo Alto Networks Integration > Firewall > Commands** are run. The Show type commands (for example, Show-IP-ExternalDynamicList) determine whether the value exists on the firewall. The Refresh type commands (for example, Refresh-IP-ExternalDynamicList) add value that do not exist on the firewall to the block list.

After the **Blocked Status** activity executes, approval by a system administrator is required before the workflow can proceed.

**Security Operations Palo Alto Networks - Check and Block Value workflow**

**Procedure**
1. Navigate to **Palo Alto Networks Integration > Firewall > Block Requests**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>Select the firewall to be used.</td>
</tr>
<tr>
<td>Block Type</td>
<td>Select the type of value to be checked:</td>
</tr>
<tr>
<td></td>
<td>• IP</td>
</tr>
<tr>
<td></td>
<td>• URL</td>
</tr>
<tr>
<td></td>
<td>• DOMAIN</td>
</tr>
<tr>
<td>Block Value</td>
<td>Enter the value of the selected type to be checked on the firewall.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**Palo Alto Firewall: Block Request Status activity**

This activity is called by other activities to set the Firewall block request status to success or failure.

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>firewallBlockRequestSysid [string]</td>
<td>The system id of the firewall block request. This input variable is mandatory.</td>
</tr>
<tr>
<td>status [string]</td>
<td>Indicates whether the refresh job ran: success or failure.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities. The output consists of data from the firewall configuration, as well as dynamically generated data.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result [string]</td>
<td>Indicates whether the success or failure of the refresh job.</td>
</tr>
</tbody>
</table>
Palo Alto Firewall: Block Value activity

After the workflow has identified a value that is not on the firewall, the record is routed for approval. Upon approval, this activity connects to the MID Server via your SSH credentials and invokes a script that adds the value to the firewall External Block List.

Input variables
Input variables determine the initial behavior of the activity.

Note: You must manually enter the input variables for this activity and then publish the workflow. If the workflow is not published, the input variables will not be saved for non-admin users.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>toBeBlockedValue [string]</td>
<td>The value to be added to the EDL if not already present. This input variable is mandatory.</td>
</tr>
<tr>
<td>typeToBeBlocked [string]</td>
<td>The type of value to be blocked: IP, URL, or Domain. This input variable is mandatory.</td>
</tr>
<tr>
<td>targetHost [string]</td>
<td>The MID Server on which the script is executed.</td>
</tr>
<tr>
<td>SSHCredentialTag [string]</td>
<td>The SSH credential tag defined on the MID server.</td>
</tr>
<tr>
<td>scriptCommand [string]</td>
<td>The AppendValueToList.sh script used to add the value to the EDL. It requires the full path to the MID Server.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result [string]</td>
<td>The result passed to the EDL.</td>
</tr>
</tbody>
</table>

Palo Alto Firewall: Blocked Status activity

This activity checks if the value (IP, URL, or domain) is included in its respective External Dynamic List/Dynamic Block List (EDL/DBL) on firewall. The EDL/DBL
details are obtained from the firewall using an operational command, and a routine is performed to check if the value is blocked on the firewall.

**Input variables**

Input variables determine the initial behavior of the activity. All input variable entries listed are mandatory.

### Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>valueToBeChecked [string]</td>
<td>The value in the block request.</td>
</tr>
<tr>
<td>showEDLDetailsCommand [string]</td>
<td>The External Dynamic List command being used to determine whether the value exists on the firewall.</td>
</tr>
<tr>
<td>FirewallIpAddress [string]</td>
<td>The IP address of the firewall used.</td>
</tr>
<tr>
<td>FirewallApiKey [string]</td>
<td>The firewall API key.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities. The output consists of data from the firewall configuration, as well as data dynamically generated using the Palo Alto Firewall Operational Command API message.

### Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>commandResult [string]</td>
<td>The results from the firewall for the show EDL Details command.</td>
</tr>
<tr>
<td>commandResponse [string]</td>
<td>The response status obtained from the firewall for the show EDL Details Command.</td>
</tr>
</tbody>
</table>

**Palo Alto Firewall: Get API Key activity**

This activity retrieves the API key from the firewall.
**Input variables**

Input variables determine the initial behavior of the activity. All input variable entries listed are mandatory.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username [string]</td>
<td>The user name of the firewall administrator.</td>
</tr>
<tr>
<td>Password [string]</td>
<td>The firewall administrator password.</td>
</tr>
<tr>
<td>FirewallIpAddress [string]</td>
<td>The IP address of the firewall.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities. The output consists of data from the firewall configuration, as well as dynamically generated data.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APIKey [string]</td>
<td>The firewall API key.</td>
</tr>
</tbody>
</table>

**Palo Alto Firewall: Get Firewall Config activity**

The **Palo Alto Firewall: Get Firewall Config** workflow activity gets all the related firewall configuration information from the database, and makes it available for use by the subsequent activity.

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>firewallSysid [string]</td>
<td>The system id of the firewall. This input variable is mandatory.</td>
</tr>
<tr>
<td>typeOfValueToBeBlocked [string]</td>
<td>The type of value to be blocked on the firewall: IP, URL, or Domain.</td>
</tr>
<tr>
<td>firewallIPAddress [string]</td>
<td>The IP address of the firewall.</td>
</tr>
</tbody>
</table>
Output variables

The output variables contain data that can be used in subsequent activities. The output consists of data from the firewall configuration, as well as dynamically generated data.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipEDLName [string]</td>
<td>The External Dynamic List name for IP addresses.</td>
</tr>
<tr>
<td>urlEDLName [string]</td>
<td>The External Dynamic List name for URLs.</td>
</tr>
<tr>
<td>domainEDLName [string]</td>
<td>The External Dynamic List name for domains.</td>
</tr>
<tr>
<td>firewallVersionSysId [string]</td>
<td>The system id for the firewall version.</td>
</tr>
<tr>
<td>refreshEDLCommand [string]</td>
<td>The command to be used to refresh the EDL from the source.</td>
</tr>
<tr>
<td>ShowEDLDetailsCommand [string]</td>
<td>The command to be used to get the EDL details.</td>
</tr>
<tr>
<td>error [string]</td>
<td>The error, if any, that occurred in the activity.</td>
</tr>
<tr>
<td>endpoint [Encrypted]</td>
<td>The encrypted endpoint from the database.</td>
</tr>
</tbody>
</table>

Palo Alto Firewall: Refresh EDL/DBL activity

This activity executes an operational command on the firewall to refresh the External Dynamic List from the source configured on the firewall. The output of this activity indicates whether the Refresh job has been queued up.

Input variables

Input variables determine the initial behavior of the activity. All input variable entries listed are mandatory.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FirewallIPAddress [string]</td>
<td>The IP address of the firewall being refreshed.</td>
</tr>
</tbody>
</table>
Input variables (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FirewallApiKey</td>
<td>The refreshed firewall API key.</td>
</tr>
<tr>
<td>FirewallCommand</td>
<td>The operational command to be executed to queue up the refresh job.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities. The output consists of data from the firewall configuration, as well as dynamically generated data.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>activity.Output.result</td>
<td>A text string to indicate whether refresh job was queued to run: success or failure.</td>
</tr>
</tbody>
</table>

Get Log Data workflow

If Security Incident Response, Threat Intelligence, and Palo Alto Networks - Firewall are activated, the **Security Operations Palo Alto Networks - Get Log Data** workflow automatically executes when the Source IP for observables in a security incident is changed.

**Before you begin**

Role required: sn_si.analyst

**About this task**

During workflow execution, firewall configuration information is retrieved from the database and the API Key is retrieved from the firewall. The Get Log activity queues up a search query on the firewall. When the query runs, it returns a Job ID that is used to retrieve threat logs data from the firewall. It attaches the log data as an XML file to the security incident.
Procedure

1. Navigate to a security incident that contains observables.
2. Click the **Security Incident Observables** tab.
3. In **Source IP**, add or modify the IP address.
4. Click **Update**.

   The **Security Operations Palo Alto Networks - Get Log Data** workflow executes and enriched threat log data is attached to the security incident. The information is also parsed and displayed in the **Firewall Logs** section under the **Enrichment Data** tab.

**Palo Alto Firewall: Get API Key activity**

This activity retrieves the API key from the firewall.
Input variables

Input variables determine the initial behavior of the activity. All input variable entries listed are mandatory.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username [string]</td>
<td>The user name of the firewall administrator.</td>
</tr>
<tr>
<td>Password [string]</td>
<td>The firewall administrator password.</td>
</tr>
<tr>
<td>FirewallIpAddress [string]</td>
<td>The IP address of the firewall.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities. The output consists of data from the firewall configuration, as well as dynamically generated data.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APIKey [string]</td>
<td>The firewall API key.</td>
</tr>
</tbody>
</table>

Palo Alto Firewall: Get Firewall Config activity

The **Palo Alto Firewall: Get Firewall Config** workflow activity gets all the related firewall configuration information from the database, and makes it available for use by the subsequent activity.

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>firewallSysid [string]</td>
<td>The system id of the firewall. This input variable is mandatory.</td>
</tr>
<tr>
<td>typeOfValueToBeBlocked [string]</td>
<td>The type of value to be blocked on the firewall: IP, URL, or Domain.</td>
</tr>
<tr>
<td>firewallIPAddress [string]</td>
<td>The IP address of the firewall.</td>
</tr>
</tbody>
</table>
Output variables

The output variables contain data that can be used in subsequent activities. The output consists of data from the firewall configuration, as well as dynamically generated data.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipEDLName [string]</td>
<td>The External Dynamic List name for IP addresses.</td>
</tr>
<tr>
<td>urlEDLName [string]</td>
<td>The External Dynamic List name for URLs.</td>
</tr>
<tr>
<td>domainEDLName [string]</td>
<td>The External Dynamic List name for domains.</td>
</tr>
<tr>
<td>firewallVersionSysId [string]</td>
<td>The system id for the firewall version.</td>
</tr>
<tr>
<td>refreshEDLCommand [string]</td>
<td>The command to be used to refresh the EDL from the source.</td>
</tr>
<tr>
<td>ShowEDLDetailsCommand [string]</td>
<td>The command to be used to get the EDL details.</td>
</tr>
<tr>
<td>error [string]</td>
<td>The error, if any, that occurred in the activity.</td>
</tr>
<tr>
<td>endpoint [Encrypted]</td>
<td>The encrypted endpoint from the database.</td>
</tr>
</tbody>
</table>

Palo Alto Firewall: Get Log activity

The **Palo Alto Firewall: Get Log** workflow activity schedules a query on the firewall to retrieve logs and returns a JobID used to retrieve the log data.

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FirewallIpAddress [string]</td>
<td>The IP address of the firewall. This input variable is mandatory.</td>
</tr>
<tr>
<td>FirewallApiKey [string]</td>
<td>The API access key of the firewall. This input variable is mandatory.</td>
</tr>
</tbody>
</table>
Input variables (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FirewallLogType [string]</td>
<td>The type of log data to be retrieved (set to threat). This input variable is mandatory.</td>
</tr>
<tr>
<td>FirewallLogFilterQuery [string]</td>
<td>The query to be executed to search for logs on the firewall. This input variable is mandatory.</td>
</tr>
<tr>
<td>LogDirection [string]</td>
<td>Specifies whether logs are shown oldest first (backward) or newest first (forward) order.</td>
</tr>
<tr>
<td>LogNumber [string]</td>
<td>Specifies the number of logs to retrieve.</td>
</tr>
<tr>
<td>LogSkipCount [string]</td>
<td>Specifies the number of logs to skip when doing a log retrieval.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities. The output consists of data from the firewall configuration, as well as dynamically generated data.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QueuedJobID [string]</td>
<td>The Job ID returned from the firewall.</td>
</tr>
<tr>
<td>JobScheduled [string]</td>
<td>Specifies (success or failure) whether the job was sent to the firewall.</td>
</tr>
<tr>
<td>error [string]</td>
<td>Any errors returned.</td>
</tr>
</tbody>
</table>

Palo Alto Firewall: Job Data Action activity

After the Palo Alto Firewall: Get Log activity queues the search query to the firewall and the job runs, the Palo Alto Firewall: Job Data Action activity retrieves the threat log data from the firewall.

Input variables

Input variables determine the initial behavior of the activity. All input fields are mandatory.
Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FirewallIpAddress</td>
<td>The IP address of the firewall.</td>
</tr>
<tr>
<td>FirewallApiKey</td>
<td>The API access key of the firewall.</td>
</tr>
<tr>
<td>JobID</td>
<td>The ID of the queued job.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities. The output consists of data from the firewall configuration, as well as dynamically generated data.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>commandStatus</td>
<td>Specifies (success or failure) whether data was retrieved from the firewall.</td>
</tr>
<tr>
<td>JobData</td>
<td>The data collected from the firewall.</td>
</tr>
<tr>
<td>error</td>
<td>Any errors returned.</td>
</tr>
</tbody>
</table>

Write content to record as attachment activity

This activity writes the content passed in from an input and creates a designated attachment to a given record.

The Write content to record as attachment activity can be used with any workflow to write content and attach it to a record.

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tablename</td>
<td>The table name for the record. This input field is mandatory.</td>
</tr>
<tr>
<td>sysid</td>
<td>The system identifier (sys_id) of a task record. This input field is mandatory.</td>
</tr>
</tbody>
</table>
Input variables (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>payload</td>
<td>The plain text content to be written as an attachment. This input field is mandatory.</td>
</tr>
<tr>
<td>filename</td>
<td>The attachment file name.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result [string]</td>
<td>Indicates whether the update was successful.</td>
</tr>
</tbody>
</table>

Palo Alto Networks - WildFire integration

Palo Alto Networks - WildFire is a cloud-based application that interacts with your system firewall.

Explore

- Security Incident Response integrations

Use

- Get WildFire Data Enrichment workflow

Set up


Develop

- ServiceNow Security Operations integration development guidelines
- Tips for writing integrations
- Developer training
- Developer documentation
- Find components installed with an application

Troubleshoot and get help

- Integration troubleshooting
- Ask or answer questions in the Security Operations community

Before you can use the Security Operations Palo Alto Networks - WildFire integration, you must download the integration from the ServiceNow Store.

**Before you begin**
Role required: admin

**Procedure**

1. **Download the integration from the ServiceNow Store.**

2. **Navigate to Security Operations > Integrations > Integration Configurations.**
   The available security integrations appear as a series of cards.

3. In the Carbon Black card, click **Configure**.
4. Enter the API key, and click **Submit**. The integration configuration card displays.

5. To return to the original list of integration configuration cards, select **No** from the **Show Configurations** drop-down list.

**Get WildFire Data Enrichment workflow**

When the **Security Operations Palo Alto Networks - Get WildFire Data Enrichment** workflow is executed, a hash file is uploaded to WildFire. The data is enriched, and reports are downloaded to the instance to aid in processing potential malware attacks.

**Before you begin**

Role required: sn_si.analyst

**About this task**

The **Security Operations Palo Alto Networks - Get WildFire Data Enrichment** workflow is executed when a security incident is created from an alert received from the Palo Alto Network Firewall application. A malware hash from the email notification received from Firewall is entered on the **IoC** tab of the security incident, and the record is updated.
Procedure

1. Navigate to Security Incident > Show Open Incidents.
2. Based on the email notification received from Firewall, locate and open the security incident that was created.
3. Click the Indicators of Compromise tab and populate the Malware hash with the hash you received in the alert.
4. Click Update.
   The workflow causes the hash file to be uploaded to WildFire where the data is enriched. Reports in the PDF and XML formats are attached to the record (security incident or IoC) in your instance to aid in processing potential malware attacks.
Note: If the enriched data includes packet capture information, PCAP information is also downloaded. PCAP data captures what actions the file was performing. For example, it can report on what servers the file was contacting. To view PCAP files, you need a packet analyzer, such as Wireshark.

Sample PDF generated by Wildfire

1 File Information

<table>
<thead>
<tr>
<th>File Type</th>
<th>PE</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Signer</td>
<td>None</td>
</tr>
<tr>
<td>SHA-256</td>
<td>ab9f64bf15b1c67b6db555d5e65b12345a6458b745b67c2</td>
</tr>
<tr>
<td>SHA-1</td>
<td>81b05b4d45bf45b6b6c107abedef65b56bc</td>
</tr>
<tr>
<td>MD5</td>
<td>26ca4a53a5f8ebdef7e6b2097231532</td>
</tr>
<tr>
<td>File Size</td>
<td>55296bytes</td>
</tr>
<tr>
<td>First Seen Timestamp</td>
<td>2016-05-04 12:56:00 UTC</td>
</tr>
<tr>
<td>Verdict</td>
<td>Malware</td>
</tr>
<tr>
<td>Anomalous Coverage</td>
<td>ViraTotal Information</td>
</tr>
</tbody>
</table>

2 Static Analysis

2.1. Suspicious File Properties

This sample was found to contain any high-risk content during a pre-screening analysis of the sample.

Contains an invalid checksum
The PE file checksum is required for drivers, boot-time DLLs, and other DLLs loaded into secure system processes. Malware often ignores this value or sets it to zero.

Contains sections with size discrepancies
Sections with a large discrepancy between raw and virtual sizes may indicate a packed or obfuscated PE file.

WildFire: get PCAP activity

The WildFire: Get PCAP workflow activity gets the packet capture (PCAP) information generated during the analysis of a specified file hash on WildFire. The result of this activity is attached to a specific record as identified by the TableName and RecordId.

Input variables

Input variables determine the initial behavior of the activity.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FileSHA256Hash [string]</td>
<td>The hash of the file received from the Palo Alto Network Firewall application.</td>
</tr>
<tr>
<td>TableName [string]</td>
<td>The affected table.</td>
</tr>
<tr>
<td>RecordId [string]</td>
<td>The security incident or IoC being updated.</td>
</tr>
</tbody>
</table>

### Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>commandStatus [Boolean]</td>
<td>True if a result is obtained and attached successfully.</td>
</tr>
<tr>
<td>errorMessage</td>
<td>The error, if any, that occurred in the activity.</td>
</tr>
</tbody>
</table>

### WildFire: get PDF report activity

The WildFire: Get PDF Report workflow activity gets the report generated during the analysis of a specified file hash on WildFire in PDF format. The result of this activity is attached to a specific record as identified by the TableName and RecordId.

### Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TableName [string]</td>
<td>The affected table.</td>
</tr>
<tr>
<td>FileSHA256Hash [string]</td>
<td>The hash of the file received from the Palo Alto Network Firewall application.</td>
</tr>
<tr>
<td>RecordId [string]</td>
<td>The security incident or IoC being updated.</td>
</tr>
</tbody>
</table>
Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>commandStatus</td>
<td>True if a result is obtained and attached successfully.</td>
</tr>
<tr>
<td>errorMessage</td>
<td>The error, if any, that occurred in the activity.</td>
</tr>
</tbody>
</table>

WildFire: get XML report activity

The WildFire: Get XML Report workflow activity gets the report generated during the analysis of a specified file hash on WildFire in XML format. The result of this activity is attached to a specific record as identified by the TableName and RecordId.

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TableName [string]</td>
<td>The affected table.</td>
</tr>
<tr>
<td>FileSHA256Hash [string]</td>
<td>The hash of the file received from the Palo Alto Network Firewall application.</td>
</tr>
<tr>
<td>RecordId [string]</td>
<td>The security incident or IoC being updated.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>commandStatus</td>
<td>True if a result is obtained and attached successfully.</td>
</tr>
<tr>
<td>errorMessage</td>
<td>The error, if any, that occurred in the activity.</td>
</tr>
</tbody>
</table>
Write content to record as attachment activity

This activity writes the content passed in from an input and creates a designated attachment to a given record.

The **Write content to record as attachment** activity can be used with any workflow to write content and attach it to a record.

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tablename</td>
<td>The table name for the record. This input field is mandatory.</td>
</tr>
<tr>
<td>sysid</td>
<td>The system identifier (sys_id) of a task record. This input field is mandatory.</td>
</tr>
<tr>
<td>payload</td>
<td>The plain text content to be written as an attachment. This input field is mandatory.</td>
</tr>
<tr>
<td>filename</td>
<td>The attachment file name.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Indicates whether the update was successful.</td>
</tr>
</tbody>
</table>

Palo Alto Networks Next-Generation Firewall integration

Once installed and configured, the security incident analyst uses this integration to block malicious IP addresses, URLs, and domains using External Dynamic List (EDL) capabilities with the ServiceNow Security Incident Response (SIR) products. The security incident analyst creates entries for an EDL from observables determined to be malicious on ServiceNow SIR security incidents.

An EDL is a text file that is hosted on an external web server. For this integration, this web server is your Now Platform instance, which permits the Palo Alto Networks Next-Generation Firewall to import objects that are included in the list, IP addresses, URLs, and domains, and to enforce policy.
To enforce policy on the EDL entries, the list is referenced in a policy rule or profile. As the EDL entries are modified, the firewall dynamically imports the list at the configured interval and enforces policy without a configuration change or a commit on the firewall. For this integration, Now Platform has created a table containing EDL entries that are retrieved by authorized Palo Alto Networks Next-Generation Firewalls at the configured retrieval intervals.

The integration includes the following features:

- Flexibility to create multiple EDLs that apply to different firewall deny or allow policies.
- Detailed reporting on the types of sites being blocked (phishing, malware, and allow listed sites).
- Tagging of Now Platform security incidents with EDL entries by the observable type (URL, domain, IP address).
- Configuring EDL expiration periods to maintain EDL list size by automatically expiring or removing older entries.
- Searching, deleting, or migrating EDL entries between EDL lists.
- Linking EDL entries to observable records and security incidents that include threat intelligence results and details about why an entry is blocked.

The integration requires that the (com.snc.security_incident) and (com.snc.secops.orchestration) plugins from the Security Incident Response product are activated.

This integration only supports Palo Alto Networks (PAN-OS 8.x). Earlier versions are not supported.

This integration is compatible with the Kingston, London, Madrid, and New York releases of the Now Platform®.

**Note:** The following topics are numbered. For a smooth installation, configuration, and verification of expected results, follow the topics in the order they are presented.

**Create a certificate profile for the Palo Alto Networks Next-Generation Firewall**

The integration requires a certificate profile to validate and authenticate the secure connection between the Now Platform® server and the Palo Alto Networks Next-Generation Firewall server.

**Before you begin**

Role required: Palo Alto Networks Next-Generation Firewall Administrator
About this task

A Palo Alto Networks Next-Generation Firewall authenticates to a Now Platform® instance, retrieves EDL entries from the database table, and incorporates the entries into corresponding firewall policy rules. This retrieval requires the API user account role in the Now Platform® instance, which is used by the PAN firewall admin to access the Now Platform® API.

The Palo Alto Networks Next-Generation Firewall administrator creates a certificate profile in Palo Alto Networks. This certificate validates and authenticates the secure connection between the Now Platform® server and Palo Alto Networks firewall server.

Now Platform® uses Entrust as a Certificate Authority, and the required certificate profile is created using the entrust_ev_ca.cer certificate. This certificate is available for downloading on the EntrustData card™ website. To ensure that you are getting the most current versions, download these certificates directly from the Entrust website.

Procedure

1. Navigate to Root Certificates Download.

2. On the Entrust website, scroll to the Entrust Root Certificate Authority certificate as shown in the following figure.

3. Click Download. The name of the downloaded file is entrust_ev_ca.cer.

4. Refer to Palo Alto Networks documentation for how to configure the certificate profile once you have downloaded it. The requirements can be found on the Palo Alto Networks website.
Set up and install Palo Alto Networks Next-Generation Firewall

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation.

**Before you begin**
Role required: (admin)

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Verify that you have the required Now Platform and Security Incident Response roles assigned. | The following roles are required:  
• The System Administrator (admin) installs the app and assigns the Security Incident Administrator (sn_si.admin) role.  
• The Security Incident Administrator (sn_si.admin) oversees the configuration, and creates, activates, and removes EDLs. This role also assigns the sn_si.analyst role.  
• The (admin) assigns the Now Platform® API account role (sn_sec_panfw.api_account_access) which is used exclusively for entering credentials required for authentication on Palo Alto Networks so the firewalls can retrieve EDLs from the Now Platform®.  
• (sn_si.analyst), or Security Operations Center (SOC) Analyst, creates EDL entries and works with security incidents. |
<p>| Verify that you are using Palo Alto Networks Next-Generation Firewall version-OS 9.x, and 10.x. | This integration only supports Palo Alto Networks Next-Generation Firewall-OS 9.0 and later. |
| Set up any EDL profiles, security policy rules, and certificate profiles in Palo | Refer to Palo Alto Networks general documentation and |</p>
<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alto Networks as recommended in Palo Alto Networks documentation.</td>
<td>requirements at the: Paloalto Networks Documentation website.</td>
</tr>
<tr>
<td>Verify that you have downloaded and configured the Entrust™ Root Certificate Authority certificate.</td>
<td>The integration requires this certificate to validate and authenticate the secure connection between the Now Platform server and the Palo Alto Networks Next-Generation Firewall server. For more information on setting up the certificate, see &quot;Configure a Certificate Profile&quot; in the PAN-OS 10.0 Administrator’s Guide. For the download, see Create a certificate profile for the Palo Alto Networks Next-Generation Firewall and Root Certificates Download.</td>
</tr>
<tr>
<td>Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration.</td>
<td>Madrid and later release requirements For the Madrid release and later family releases, the Security Incident Response Dependency plugin (com.snc.si_dep) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications required by the integration. Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation.</td>
</tr>
</tbody>
</table>
| | 1. Security Incident Response  
2. Security Integration Framework |
<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Security Support Common</td>
<td>For more information on setting up your Now Platform instance for the integration, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.</td>
</tr>
<tr>
<td>4. Security Support Orchestration</td>
<td></td>
</tr>
</tbody>
</table>

If your organization has Now Platform® change management and approval processes for email deletion, verify that email send/receive capability is enabled.

To verify that email send/receive capability is enabled in your Now Platform® instance, navigate to Email properties > Administration > Email Properties. In Outbound Email Configuration, verify Email sending and Email receiving are selected.

**Procedure**

If you have not installed the application for the integration, see Install a Security Operations integration and follow the steps to install it.

**Create the API account role for Palo Alto Networks Next-Generation Firewall**

An API account role is required in your Now Platform® instance for this integration. The Username and Password associated with this account are created in the Now Platform® and entered in Palo Alto Networks so the Palo Alto Networks Next-Generation Firewall authenticates with the Now Platform® when retrieving EDL entries.

**About this task**

The Now Platform® admin creates an API account role (sn_sec_panfw.api_account_access). This account is used exclusively for entering credentials required for authentication on Palo Alto Networks so the firewalls can retrieve EDLs from the Now Platform®. This account is a separate, unique API user account in the Now Platform® instance, and assigned to the Palo Alto Networks Next-Generation Firewall administrator. Role required: (admin)
Procedure

1. Navigate to **Organization > Users**.
2. Click the **Users** module.

   ![ServiceNow Users Module](image1.png)

3. On the Users list that is displayed, click **New**.

   ![New User Form](image2.png)

A new user form is displayed.

4. Fill in the form.

   ![Filled User Form](image3.png)

   **Note:** The values for User ID title, and email address shown in the following table and figure are example values.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>Unique User ID for the role in your Now Platform® instance. This user ID is entered in the <strong>Username</strong> field in the <strong>Client Authentication</strong> section of the External Dynamic Lists dialog on the Palo Alto Networks site. An example is API account SN.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>First name</td>
<td>Person you are assigning.</td>
</tr>
<tr>
<td>Last name</td>
<td>Person you are assigning.</td>
</tr>
<tr>
<td>Title</td>
<td>Job title, for example, FW admin.</td>
</tr>
<tr>
<td>Password</td>
<td>Unique password created for this role. This password is entered in the Password field in the Client Authentication section of the External Dynamic Lists dialog on the Palo Alto Networks site.</td>
</tr>
<tr>
<td>Email</td>
<td>Unique email address.</td>
</tr>
</tbody>
</table>

5. Click Submit. Once submitted, you can assign the role.

6. On the Users list in the User ID column, click the name of the user ID you entered, API account SN, for example.

7. On the open record in the Roles section, click Edit.
8. On the **Edit Members** form that is displayed, enter

```
sn_sec_panfw.api_account_access
```

in the **Collection** field. Below the **Collection** field, the role is displayed in the column.

9. In the **Collection** column, select then move **sn_sec_panfw.api_account_access** to the **Roles List**.

10. Click **Save**.
11. Navigate to Users, and in the User column on the list, click the ID name that you created for the role (API account SN).

The user record is displayed. This record verifies that the user account has been assigned. The State is active, and the role is not inherited.

**Supported External Dynamic Lists for Palo Alto Networks Next-Generation Firewall**

The ServiceNow Palo Alto Networks Next-Generation Firewall integration supports External Dynamic Lists (EDLs) that accept IP, URL, and domain observables.

**Supported EDLs and observables**

An External Dynamic List is a text file that is hosted on an external web server, which for this integration is the Now Platform instance. The Palo Alto Networks Next-Generation Firewall can then import objects — IP addresses, URLs, domains — included in the list and enforce policy. To enforce policy on the EDL entries, the list is referenced in a policy rule or profile.

This integration supports three types of EDLs:

- **IP** (This includes a single IP Address, as well as CIDR blocks (ranges) of addresses).
- **URL**
- **Domain**

The following table lists descriptions of the observables supported by this integration and example formats for each type.
### Supported observables and example formats

<table>
<thead>
<tr>
<th>Observable</th>
<th>Example formats</th>
<th>Description</th>
</tr>
</thead>
</table>
| IP Address | 95.153.103.54 (IPv4)  
       (IPv6): 2001:00b8:130f:fe03:0000:9c0:080f:130b | Represents a single, distinct interface address. The integration supports IPv4, IPv6, and CIDR formats. Support for IP address observables includes CIDR (Classless Inter-Domain Routing) ranges, for example, 95.153.100.0/22. Note: An error message is displayed when you try to attach a single IP address to an EDL that you have already blocked as a part of a CIDR range. For example, the single address 95.153.103.54 is part of the CIDR range represented by 95.153.100.0/22 (95.153.100.0-95.153.103.255). |
| URL        | www.example.com  
       www.example.com/article.html  
       example.com  
       *.example.com | Wildcards are supported. The Now Platform reformats URL entries to comply with Palo Alto Networks EDL format requirements. |
| Domain     | www.example.com  
       example.com  
       mail.example.com | Wildcards are not supported. |
For more information about formatting guidelines and EDLs, see "Formatting Guidelines for an External Dynamic List" in the PAN-OS 10.0 Administrator's Guide on the Palo Alto Networks website.

Create an EDL for Palo Alto Networks Next-Generation Firewall

Create an External Dynamic List (EDL) in your Now Platform instance. Once approved and activated, you can create entries for EDLs from observables determined to be malicious on Now Platform Security Incident Response (SIR) incidents and request approval to block them.

Before you begin
Role required: sn_si.admin

About this task
Create the EDL on your Now Platform instance so that the firewall can import objects — IP addresses, URLs, domains — included in the list and enforce policy. To enforce policy on the EDL entries, the list is referenced in a policy rule or profile.

The figures in the following section are shown with Tabbed forms cleared in System Settings. For more information about selecting and clearing tabbed forms, see the section titled Display tabbed forms in Configuring the form layout on the ServiceNow Product Documentation website.

Procedure
1. After the application installation is complete, navigate to Integrations > Integration Configurations.
2. Locate the Palo Alto Networks Next-Generation Firewall tile and click Configure.
3. Click Create new EDL List.

4. On the form, fill in the fields.

### Palo Alto Networks Firewall External Dynamic List form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Palo Alto Networks Firewall Dynamic List name. Include the observable type (URL, IP, domain) in this field so the security analyst can easily recognize the intention of the EDL by its name. The name should also clearly indicate what firewall policy these EDL objects are mapped to. Some examples of EDL names are, Outbound Malware IP, or Outbound Phishing URL.</td>
</tr>
<tr>
<td>Active</td>
<td>This check box is cleared by default to indicate that the EDL is inactive. When inactive, the EDL is unable to receive additional entries. When the check box is selected, the EDL is activated and available for EDL entries.</td>
</tr>
<tr>
<td>Display tag</td>
<td>Check box is selected by default to automatically tag the observable</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>and the associated security incident record if the observable is blocked on an EDL. When selected, the Tag type and EDL tag for observables fields are available on the form.</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> A tag name is created by default from the value you enter in the Name field with an EDL- prefix, for example, EDL-Malware OutBound IP. You can change the tag name and color. See: <em>(Optional)</em> Edit the security tag name for Palo Alto Networks Next-Generation Firewall. The tag name is displayed in the EDL tag for observables field once the EDL is saved.</td>
<td></td>
</tr>
<tr>
<td>When the check box is cleared, no tag is created, and the Tag type and EDL tag for observables fields are not available on the form.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Observable type</th>
<th>Select an observable type this EDL accepts from the choice list: IP (including CIDR), URL, or domain.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag type</td>
<td>Tags that are available from the choice list. A Block list is a list of observables that you want the Palo Alto Networks Next-Generation Firewall to block. An Allow list is a list of observables you want the Palo Alto Networks Next-Generation Firewall to allow. By default, the Block list tag color is black, and the Allow list tag color is gray. You can change the color. See: <em>(Optional)</em> Edit the security tag name for Palo Alto Networks Next-Generation Firewall.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Create change request** | This check box is selected by default to automatically create a change request and change tasks in your Now Platform instance, which are attached to the EDL record.  

The change request is used to configure the EDL list retrieval URL in the Palo Alto Networks Next-Generation Firewall server.  

This option is recommended if your firewall administrator is also using the Now Platform for firewall policy or rule changes. If you create a request, once it is closed, the EDL list is automatically activated.  

Clear the check box to manually activate the EDL after receiving notice via email from the firewall administrator that the configuration on Palo Alto Networks is completed.  

When the check box for Create change request is cleared, the Change request field is unavailable. |
| **EDL tag for observables** | This field is displayed only if the Display tag check box is selected.  

Field is automatically populated after the EDL is saved with a default value from the Name field.  

For more information on changing the default tag name and color, see *(Optional) Edit the security tag name for Palo Alto Networks Next-Generation Firewall* |
<p>| <strong>Change request</strong>     | When the Create change request check box is selected, the change request number is displayed on the |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Description of the Palo Alto Networks Firewall Dynamic List. The name generally contains the types of sites and observables you would expect to be on this EDL, and you can use this field for more details.</td>
</tr>
<tr>
<td>Expiration period (days)</td>
<td>Expiration period of the EDL. 0 (the default) indicates that the EDL entry never expires. If you change this value, this entry is active for the number of days you enter. You can enter a minimum value of 1, and there is no maximum value. For example, if you enter 30 days at 2:01 PM on May 1, the EDL will expire at 2:01 PM on May 31. All entries in this EDL then inherit this value by default unless you override the value on individual entry basis.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.
6. If the Palo Alto Networks Firewall External Dynamic Lists list is not displayed, navigate to **Palo Alto Networks NGFW Integration > Firewall EDL Configuration** and click **Firewall EDL Configuration**.

The new EDL is displayed. The EDL status is still inactive (`false`), which means the EDL is not available to accept entries. If Create change request was configured, a message is displayed indicating a change request and tasks have been created in your Now Platform instance.

7. In the **Name** column, click an item to open the record. The EDL record is displayed. This example shows a Malware Outbound IP EDL. The following fields, options, and links are displayed on the new record after submission and described in the following table.
### Retrieval URL and change request links on EDL record

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email FW retrieval URL</td>
<td>Emails a notice that the EDL link is available for configuration to the Palo Alto Networks firewall administrator.</td>
</tr>
<tr>
<td>EDL retrieval URL</td>
<td>This URL is placed in the <strong>Source</strong> field in the External Dynamic Lists authentication dialog box on the <strong>Create List</strong> tab on the Palo Alto Networks website. The URL link the Palo Alto Networks firewall administrator uses for configuration in the Palo Alto Networks firewall is automatically generated and displayed.</td>
</tr>
<tr>
<td>Now Platform change request</td>
<td>A link to the change request record is displayed in the Change Requests section when configured, and the request number is displayed in the Change request field.</td>
</tr>
<tr>
<td>Update</td>
<td>Modify data and update the editable fields.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete the record.</td>
</tr>
</tbody>
</table>

8. Create and add more EDLs as required. The EDLs are displayed on the Palo Alto Networks External Dynamic Lists list.

**What to do next**
Activate an EDL manually, or with a Now Platform change request.
Activate an EDL for Palo Alto Networks Next-Generation Firewall

After the External Dynamic List (EDL) has been created in your Now Platform® and the URL is available, the Palo Alto Networks firewall administrator configures the EDL in the Palo Alto Networks Next-Generation Firewall. The retrieval URL is used by the Palo Alto Networks firewall administrator to configure the EDL in the Palo Alto Networks Next-Generation Firewall server. Before it can accept EDL entries, the EDL must be configured in Palo Alto Networks and activated in the Now Platform®.

About this task
After the EDL is configured, as the security incident administrator, you can activate the EDL manually, or, the EDL is automatically activated upon completion of a Now Platform® Change Request. The EDL must be approved and moved from the inactive state to the active state before it can accept EDL entries.

Role required: sn_si.admin

Procedure
1. Navigate to Palo Alto Networks NGFW Integration > Firewall EDL Configuration and select the Firewall EDL Configuration module.
2. In the Palo Alto Networks Firewall Dynamic Lists list that is displayed, select your new EDL in the Name column.
3. On the record that is displayed, note the Email FW retrieval URL buttons, the active EDL Retrieval URL link, and, if configured, the Now Platform® change request in the Change Requests section. Also note that the Active check box is cleared.
Note: With Tabbed forms cleared in your system settings, the EDL Retrieval URL appears in EDL Retrieval Info section as shown in the previous figure.

The following figure shows the EDL Retrieval Info displayed as a tab with Tabbed forms selected in your system settings. Click the EDL Retrieval Info tab to display the retrieval URL. The link to the change request (CH0030015) is also displayed.
4. To complete the configuration and move the EDL from inactive to active, you must choose one of the following options to notify the firewall administrator that the retrieval URL is available.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Click Email FW retrieval URL.</strong></td>
<td>Email EDL Retrieval URL directly to the firewall administrator. This option permits the firewall administrator to finish the configuration on the Palo Alto Networks platform. Choose this option if the firewall administrator is not using the Now Platform®.</td>
</tr>
<tr>
<td>Note:</td>
<td>The security incident administrator manually activates the EDL in the Now Platform® after receiving notice that the Palo Alto Networks Next-Generation Firewall configuration is completed. See: Activate an EDL manually for Palo Alto Networks Next-Generation Firewall.</td>
</tr>
<tr>
<td><strong>Complete the Now Platform® change request and assign the configuration tasks to the firewall administrator.</strong></td>
<td>This option is available only if the firewall administrator for Palo Alto Networks is also using the Now Platform®, and the Now Platform® change management and approval processes are configured.</td>
</tr>
<tr>
<td>Note:</td>
<td>Users with the sn_si.admin role can approve the Now Platform® change request. Once the configuration tasks are completed and the change request has been closed, the EDL is activated automatically. See: Activate an EDL for Palo Alto Networks Next-Generation Firewall with a change request.</td>
</tr>
</tbody>
</table>
After you notify the firewall administrator that the retrieval URL is available and you confirm the EDL has been configured in Palo Alto Networks, as the security incident administrator, your next step is to activate the EDL. You either activate the EDL manually, or, if configured, use the Now Platform change request form to activate the EDL.

Related information
- Configure an EDL in Palo Alto Networks Next-Generation Firewall
- Activate an EDL manually for Palo Alto Networks Next-Generation Firewall

Activate an EDL manually for Palo Alto Networks Next-Generation Firewall

If the Palo Alto Networks firewall administrator is not using the Now Platform, and you are directly notified that the Palo Alto Networks Next-Generation Firewall is configured, you can activate the External Dynamic List (EDL) manually.

Before you begin
In Palo Alto Networks, assign an EDL object, policy, and the source URL to the EDL you created. For more information about configuring the EDL to the Palo Alto Networks Next-Generation Firewall in Palo Alto Networks, see Configure an EDL in Palo Alto Networks Next-Generation Firewall.

Role required: sn_si.admin

About this task
As the Now Platform security incident administrator, you are notified by the Palo Alto Networks firewall administrator when the EDL configuration is complete in the Palo Alto Networks Next-Generation Firewall.

Procedure
1. Navigate to Palo Alto Networks NGFW Integration > Firewall EDL Configuration.

2. Select the Firewall EDL Configuration module.
3. In the Palo Alto Networks Firewall External Dynamic Lists list, click an item in the **Name** column to open it.

4. On the record that opens, select the **Active** check box.

5. Click **Update**. In the **Active** column of the Palo Alto Networks Firewall External Dynamic Lists list, true is displayed for the state of the EDL.

**Results**
The EDL is activated and ready to receive EDL entries

**What to do next**
Submit EDL entries from a security incident or from the blocklist.
Configure an EDL in Palo Alto Networks Next-Generation Firewall

The Palo Alto Networks firewall administrator configures an EDL to the Palo Alto Networks Next-Generation Firewall once notified the Retrieval URL is available from the Now Platform. Before the EDL can accept EDL entries, it must be configured in Palo Alto Networks, and activated in the Now Platform®.

Before you begin
Role required: Palo Alto Networks firewall administrator

About this task
The Palo Alto Networks Next-Generation Firewall administrator creates an EDL object, and assigns the source (Retrieval) URL and policy to the EDL. These tasks are performed in Palo Alto Networks before the EDL is activated in the Now Platform.

The images in the following section are used by permission and are PRIVILEGED and PROPRIETARY.

Procedure
1. If you have not configured the EDL to the firewall, navigate to External Dynamic Lists > Objects in Palo Alto Networks.
2. In the **Name** column, select the ServiceNow EDL you want to configure from the list, for example, **ServiceNow EDL for URL**.

3. In the External Dynamic Lists dialog box, enter the Username and Password to authenticate with the Now Platform®. These credentials are the Username and Password you created for the API account role (sn_sec_panfw.api_account_access) in your ServiceNow instance.
4. In the Source field, enter the URL that was generated on the EDL list in your ServiceNow instance.
5. Select a Certificate Profile from the choice list, SN2, for example.
6. Click OK.

Activate an EDL for Palo Alto Networks Next-Generation Firewall with a change request

If configured, the ServiceNow change request form is used to activate the External Dynamic List (EDL). This option is recommended if your firewall administrator is also using the Now Platform for firewall policy or rule changes. The EDL is activated automatically and ready to receive EDL entries upon closure of the Now Platform change request.

Before you begin

Note: The figures in the following section are shown with Tabbed forms selected in System Settings. For more information about selecting and clearing tabbed forms, see the section titled Display tabbed forms in Configuring the form layout on the ServiceNow Product Documentation website.

Role required: sn_si.admin for approving the change request and change tasks
Palo Alto Networks firewall administrator for completing configuration tasks in Palo Alto Networks

About this task

If configured, monitor your Now Platform change request and assign any tasks that are required to configure the Palo Alto Networks Next-Generation Firewall. After these tasks are completed, close the Now Platform change request to activate the EDL automatically.

Procedure

1. Navigate to Palo Alto Networks NGFW Integration > Firewall EDL Configuration.

2. Select the EDL module and click an EDL in the Name column.
3. In the open EDL record, click the change request number in the Change Requests related list.

The change request record is displayed. The Description field lists the retrieval URL used to configure the Palo Alto Networks EDL. Details about mapping the EDL to the appropriate Palo Alto Networks Next-Generation Firewall policy are also included. In the Short description field, a comment indicates that there is a request to add a new EDL.
4. In the upper-right corner of the record, click **Request Approval**. The State changes to Assess, and a message is displayed that the change request is waiting for approval.

5. To complete the change request and activate the EDL, follow the steps to assign the tasks and close the change request.
a. If not displayed, open the change request and select the **Change Tasks** tab.

b. Click the task associated with creating the EDL object to open it.

c. On the record that is displayed, assign the task to the Palo Alto Networks firewall administrator, and click **Update**.

The firewall administrator is notified and creates the EDL object in the Palo Alto Networks Next-Generation Firewall.

To create the EDL object, the Now Platform retrieval URL is copied in Palo Alto Networks at **External Dynamic Lists > Create Lists > Source**.
After you have verified that the EDL object has been created in Palo Alto Networks, in the Now Platform, navigate to the change request associated with creating the EDL object and click **Close task**.

On the task record for this example, CTASK0010037 was closed for this task.

Navigate to the Change Tasks tab and click the task for assigning a firewall policy to the EDL Object.
The status for CTASK0010037 is **Closed**.

**f. Open the record and assign the next task.**

After the task has been assigned, in Palo Alto Networks, the firewall administrator navigates to the **Policies** tab to assign the policy.

**g. In the Name column, locate and click the security policy rule you want to add the EDL to, for example, **ServiceNow ip edl list**.**

**h. In the Security Policy Rule dialog box, select the Destination tab to add an EDL in the Destination Address field. To view all the available EDLs, click the Add icon.**
i. Click **OK**.

j. After you have verified that the EDL object has been assigned to a security policy, in the Now Platform, navigate to the change request, open the task associated with assigning the EDL object, and click **Close task**. After both tasks are closed, the change request is ready for approval.

k. On the change request record, click the **Approvers** related list, and select an item in the **State** column to open the request used for creating the EDL.

l. On the open approval request form, click **Approve**. The change request state moves to Scheduled.
m. Click Implement.

n. Click the Closure Information related tab and enter notes to close the request.

An entry in this field is required to close the change request.

After the change request is closed, the EDL is activated automatically. If you have not verified that the EDL is activated, navigate to Palo Alto Networks NGFW Integration > Firewall EDL Configuration.

In the Active column in the list, note that the status for the EDL is (true).
In the Name column, click the EDL name, and in the open record, note that the **Active** check box is also selected.

The EDL is now ready to accept EDL entries.

**What to do next**
Submit EDL entries from a security incident or from the blocklist.

**Submit EDL entries from a security incident record for Palo Alto Networks Next-Generation Firewall**

Observables attached to a security incident record are submitted for approval as External Dynamic List (EDL) entries to EDLs. An approval process for EDL entries is part of the preconfigured workflow. The firewall imports EDL entries — IP addresses, URLs, domains — that are included in EDL lists and enforces policy.

**Before you begin**
Role required for submitting EDL entries: sn_si.analyst
Role required for approving EDL entries: Approval is assigned to sn_si.admin by default, but this authority can be assigned as required by your organization.
About this task
Users with the sn_si.analyst role submit EDL entries by requesting a block on observables attached to a security incident record. Once submitted, an EDL entry with a status of Pending is generated and sent for approval. The following example shows a block request for a URL observable.

Procedure
1. Navigate to Security Incident > Incidents > Show All Incidents, and click a security incident record to open it.
2. Click the Show IoC related link.
3. In the Observables related list, select the observables you want to block and from the Actions on selected rows list, select Block Request.
4. In the dialog box that is displayed, click the search icon (🔍).
5. From the list that is displayed, select the EDL you want to attach this entry to.
Note: For this example, the entry observable type (URL) should match the EDL observable type (URL).

6. In the Block Request dialog box with the EDL name displayed in the Implementation field, click Block.

7. Navigate to Palo Alto Networks NGFW Integration > Firewall EDL Entries and click Firewall EDL Entries.
8. In the Palo Alto Networks Firewall External Dynamic List Entries list, click your observable in the Entry value column to open the record.

For this example, the record for mail.dgtnetworks.com is displayed.

The status is Pending, the Active check box is cleared, and the work notes show that there is a request to add the observable. This EDL Entry request is ready for approval.

The Entry value and Observable fields show different formats for the URL observable.
The icon next to the **Observable** field is a link to the Now Platform® Observable table.

The value in the **Observable** field (http://mail.dgtnetworks.com) links to the Observable table, and it matches the format that was brought over from the Security Incident Response incident-triggering event.

The Now Platform® may automatically modify EDL entries so that they are compatible with the Palo Alto Networks EDL URL format.

In this example, the observable was created with the http:// protocol (http://mail.dgtnetworks.com), and this format is displayed in the Observable field. The http:// protocol is stripped off automatically from the observable by the Now Platform® so it is compatible with Palo Alto Networks and can be retrieved. As a result, mail.dgtnetworks.com is displayed in the Entry value field.

**What to do next**
Approve EDL entries.

**Related reference**
EDL entry exceptions for Palo Alto Networks Next-Generation Firewall
Submit EDL entries from the blocklist for Palo Alto Networks Next-Generation Firewall

For observables determined to be malicious, and not associated with a specific Now Platform security incident, you submit External Dynamic List (EDL) entries from the blocklist.

Before you begin
Role required: sn_si.analyst

About this task
When you want to block an observable that you have determined is malicious, or allow an observable you have determined is not malicious, and the observable is not associated with a specific Now Platform security incident record, you submit EDL entries directly from the blocklist. Examples of these types of EDL entries might be URLs or domains for specific sites.

Procedure
1. Navigate to Palo Alto Networks NGFW Integration > Firewall EDL Entries.

2. Click the Firewall EDL Entries module.

3. In the Palo Alto Networks Firewall External Dynamic List Entries list, click New.

4. In the new record that is displayed, in the Entry value field, enter a value for your observable.

   The two possible outcomes of this entry:

   The remaining fields on the form are completed automatically.
   
   A matching observable is found, and a message is displayed that a matching observable exists. Select the EDL you want to attach this entry to and click Submit. Select the EDL you want to attach this entry to prior to setting the Expiration period.

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
A message is displayed that instructs you to complete the form.

A matching observable has not been found, and you must complete the form. After you complete it, select the EDL you want to attach the observable to and click **Submit**. An observable record is created.

The following figure shows an example of an existing domain observable and how the fields are completed automatically.

5. Click the search icon to select the EDL you want to attach the entry to.

6. Click **Submit**.

   If you have email approval configured in your workflow, an approval email request is sent.

7. If a message is displayed that requests you to fill in the rest of the information manually, fill in the fields.
### Field Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observable type</td>
<td>Observable type that is supported from the dialog.</td>
</tr>
<tr>
<td>EDL name</td>
<td>EDL you want to attach the entry to.</td>
</tr>
<tr>
<td>Enable override (default is selected)</td>
<td>Note: Select the EDL you want to attach the entry to prior to setting the Expiration period.</td>
</tr>
<tr>
<td>Lookup result or source</td>
<td>Lookup result or source. When configured, permits you to enter a <strong>Lookup result</strong> and the source used to find the results. These fields are typically populated when a security incident record is created. In this case, there is no lookup result or source, and you fill in these fields manually.</td>
</tr>
<tr>
<td>Source</td>
<td>Source that performs a threat lookup on the EDL entry, for example, ThreatCrowd, etc.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Expiration period</strong></td>
<td>The expiration period inherited from the EDL by default. You can override this value, but only during the creation of the entry. 0 indicates that the EDL entry never expires. If you change this value, this entry is active for the number of days you enter. You can enter a minimum value of 1, and there is no maximum value. For example, if you enter 30 days at 2:01 PM on May 1, the EDL entry will expire at 2:01 PM on May 31.</td>
</tr>
</tbody>
</table>

8. Click **Submit**.

If you have changed the default expiration period of the EDL entry, a warning confirmation dialog box is displayed indicating that the period differs from the selected EDL.

<table>
<thead>
<tr>
<th>Confirmation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expiration period entry differs from default value configured for this EDL list. Please confirm that you would like to submit this value?</td>
</tr>
<tr>
<td>No</td>
</tr>
</tbody>
</table>

9. Choose one option to configure the expiration period.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Yes</strong></td>
<td>Confirms your expiration override, saves the record, and returns you to the <strong>Palo Alto Networks Firewall External Dynamic List Entries</strong> list. If you have email approval configured in your workflow, an approval email request is sent.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>No</td>
<td>Cancels the override. At this point, you can change the value for the Expiration period. After changing the value, click Submit to return to the Palo Alto Networks Firewall External Dynamic List Entries list.</td>
</tr>
</tbody>
</table>

10. If not displayed, navigate to the Palo Alto Networks Firewall External Dynamic List Entries list and note that the status for the entry is Pending.

The entry is now ready for approval.

What to do next
Approve EDL entries.

Related reference
EDL entry exceptions for Palo Alto Networks Next-Generation Firewall

Approve EDL entries for Palo Alto Networks Next-Generation Firewall
An approval process for External Dynamic List (EDL) entries is part of the preconfigured workflow. You approve EDL entries before the entries are activated on EDLs. One you approve the EDL entry, the firewall retrieves the entry, and your observable is blocked from that point forward.

Before you begin
Role required: Approval for EDL entries is assigned to sn_si.admin by default, but this authority can be assigned as required by your organization. In the following example, the Now Platform admin has approval authority.
About this task
When the approval process is enabled, an EDL entry is not activated or deactivated on the EDL until it is approved.

Procedure

1. Navigate to Palo Alto Networks NGFW Integration > Firewall EDL Entries and open the EDL record.
2. On the EDL record, scroll to the Approval Requests section.

   Note: If you have Tabbed forms selected in System Settings, the section appears as a tab on the record.

   3. In Approval requests, click an item in the State column to open it. The approval record is displayed.
4. Choose one option for approving the EDL entry.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approve</td>
<td>On the entry record, the <strong>Status</strong> field changes to <strong>Added</strong>, and the <strong>Active</strong> check box is selected. The <strong>Deactivate</strong> button is displayed and active. Work notes show that the request for the EDL entry has been approved.</td>
</tr>
<tr>
<td>Reject</td>
<td>On the entry record, the <strong>Status</strong> field changes to <strong>Rejected</strong>, and the <strong>Active</strong> check box is cleared indicating the entry is not blocked on the firewall. Work notes show that the request for the EDL entry has been rejected.</td>
</tr>
</tbody>
</table>

After you have approved the EDL entry and it is activated, the Palo Alto Networks Next-Generation Firewall retrieves the EDL entry after the next retrieval interval. After the entry is retrieved, the observable is blocked from that point forward. In the following figure, note that the **Active** check box is selected, the status is **Added**, and the work notes indicate that the request has been approved.
After the EDL entry is approved and activated, the security incident record is marked with a security tag. The tag is displayed at the top of the record.

The security tag is also displayed on the observable record.

EDL entry exceptions for Palo Alto Networks Next-Generation Firewall

There are restrictions for adding External Dynamic List (EDL) entries to EDLs. If duplicate, compatibility, or CIDR (Classless Inter-Domain Routing) conflicts exist when you try to add EDL entries to EDLs, error messages are displayed that help you resolve these errors.

Compatibility exception

Each EDL only accepts entries that are compatible with its observable type. If you create a Domain EDL and you try to attach an IP address observable to it, an incompatible error message is displayed. For example, a domain EDL can only accept domain observables, as illustrated in the following figure.
Compatibility error

192.168.24.25 is incompatible with EDL Malware Blocked Domains. Please submit to a different EDL if you would still like to add the entry.

Invalid Insert

Duplication exception

An observable cannot be activated on multiple EDLs of the same observable type. If a URL observable is already activated on a URL EDL, and you try to activate the same observable on a Phishing URL EDL, a duplication error message is displayed.

Duplication error

mail.dgtnetworks.com already exists and active on the EDL

Invalid insert
CIDR (Classless Inter-Domain Routing) exception

If you attempt to attach a single IP address to an EDL, and this IP address is part of a CIDR observable already on an EDL, a CIDR conflict error is displayed. This error indicates that the single IP address is already included on the EDL as part of the CIDR observable. For example, 192.168.24.25 is part of the CIDR block 192.168.0.0/22.

CIDR conflict

192.168.24.25 already exists and active on the EDL

192.168.24.25

Observable type
IP address (V4)

EDL name
Malware Outbound IP

(Optional) Edit the security tag name for Palo Alto Networks Next-Generation Firewall

If the Display tag check box is selected when you create the External Dynamic List (EDL) record, you can edit the tag names and colors of the security tags. Security tags help you track observables that are already blocked.

Before you begin
Role required: sn_si.admin
About this task
Security tags help you quickly identify which security incidents have observables on a block list. Tags also help you identify whether an observable is already blocked, or, if it has been removed from an EDL. By default, the color of the security tag is black for block list entries and gray for allow list entries. You can change the names and colors of the tags to help you recognize certain tags more easily.

Procedure
1. Navigate to Palo Alto Networks NGFW Integration > Firewall EDL Configuration.

2. Click an item in the Name column to open it
   The EDL record is displayed. By default, the security tag name is the same value you entered in the Name field of the EDL when you created it. By default, the name also includes an EDL prefix, for example, EDL – Malware Malicious URLs.

3. Click the information icon (i) next to EDL tag for observables then Open record.
4. In the **Name** field, modify the security tag name and click **Update**. The updated EDL record is displayed with the modified tag name. In the following example, **Outbound** has been added to the tag name. Keep the **EDL** prefix in your new tag name to help you identify the tag is associated with the Palo Alto Networks Next-Generation Firewall integration.

The security tags are displayed for each observable type (IP, URL, Domain) on the Security Incident record and the Observable record each time that observable is added to an EDL.
If an observable has already been added to an EDL, and a security tag is displayed on a security incident for this observable, the EDL security tag also is displayed automatically on any subsequent security incident records that are created. This duplication tells you that the observable is already on a block list. You do not need to add this observable and re-block it.

When an observable is no longer blocked, a security tag is not displayed on the security incident record or the observable record. In this instance, no security tag indicates that the expiration date of the observable may have passed, or the observable has been deactivated from an EDL.

Uninstall Palo Alto Networks Next-Generation Firewall

If you want to uninstall Palo Alto Networks Next-Generation Firewall from your Now Platform instance and remove all remnants from the integration, refer to the ServiceNow documentation site for instructions on uninstalling applications.

Before you begin
Role required: System Administrator (admin)
See Uninstall applications on the ServiceNow Product Documentation website.

PhishTank integration

PhishTank is a community-based phishing verification system into which users submit suspected threats, and other users in the system vote to determine whether the phishing threats are legitimate. When integrated with the Now Platform Security Operations product, the threat intelligence results provide analysts with additional insight into phishing-related security incidents or investigations.

The PhishTank integration performs lookups on potential phishing site URLs.
The workflow checks for new observables as they arrive in security incidents. If the observables are of a type recognized by the API integration, the observables are evaluated. Observables determined to be malicious are tagged.

This integration is compatible with the Kingston, London, Madrid, and New York releases of the Now Platform®.

**Install and configure PhishTank**

Before you run the integration on your instance, complete the installation and configuration steps so the PhishTank application properly integrates with Now Platform Security Operations.

**Before you begin**

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

<table>
<thead>
<tr>
<th>Setup tasks</th>
<th>Description</th>
</tr>
</thead>
</table>
| Verify that you have assigned the required Now Platform roles for your instance. | The following roles are required for installation, configuration, and verification of expected results:  
  - The System Administrator (admin) installs the app and assigns the Security Incident Administrator (sn_si.admin) role.  
  - The Security Incident Administrator (sn_si.admin) oversees the configuration and verifies the expected results. This role also has access to the Security Operations module. |
| Obtain an API key.               | Visit the PhishTank website for information on API keys and to create an account: PhishTank website.                                                                                                        |
| Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration. | Madrid and later release requirements  
For the Madrid release and later family releases, the Security Incident Response Dependency plugin (com.snc.si_dep) is required. This plugin automatically installs all the dependencies that are required. |
<table>
<thead>
<tr>
<th>Setup tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications required by the integration. Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation.</td>
</tr>
<tr>
<td></td>
<td>1. Security Incident Response</td>
</tr>
<tr>
<td></td>
<td>2. Security Integration Framework</td>
</tr>
<tr>
<td></td>
<td>3. Security Support Common</td>
</tr>
<tr>
<td></td>
<td>4. Security Support Orchestration</td>
</tr>
</tbody>
</table>

For more information on setting up your Now Platform instance for the integration, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.

Role required: admin

**Procedure**

1. If you have not installed the application for the integration, see Install a Security Operations integration and follow the steps to install it.

2. After the installation completes, navigate to Integrations > Integrations Configurations and locate the PhishTank tile.

3. Click Configure.
4. In the **PhishTank Configuration** dialog box, enter the Name of the configuration, the Username (developer account created in PhishTank), and the API key you obtained from the PhishTank website and click **Submit**.

5. Verify successful configuration.
   Configuration is successfully completed unless an error message is displayed.

   **Trouble?**
   If an error message is displayed during the configuration, the PhishTank API key may be invalid.

   **Verify expected results for PhishTank**
   Observables are generated automatically by a security incident and scanned by the application. Lookup results are displayed on the Threat Lookup Results tab at the bottom of the security incident record.
Before you begin
Role required: sn_si.analyst

Procedure

1. Open the security incident form you are working with and verify that the lookup has run successfully.

![Automation activity](image)

After the application is configured, the workflow launches automatically upon incident creation. The execution and completion status of the lookup is then displayed in the work notes in the security incident record.

2. Review the work notes for more information and how to proceed if you cannot verify that the lookup ran successfully.

3. Navigate to the bottom of the security incident and click the Show All Related Lists related link.

Note: The figures in the following steps are shown with the Tabbed forms setting active in the System Settings. If tabbed forms are not displayed, in the upper-right corner of the banner frame, click the Settings gear icon. In the System Settings dialog box that is displayed, click Forms and verify that Tabbed forms and With the Form are selected.

The Threat Lookup Results tab at the bottom of the security incident record displays the lookup results.
The **Finding** column displays **Unknown** for records not determined to be malicious. For results matching malicious, **Malicious** is displayed in the **Finding** column.

4. In the **Observable** column, click an observable to open a record and display more information.

On the observable record, for lookups matching malicious, **Malicious** is displayed the **Finding** field. The observable is tagged with the Threat Intelligence source that found it to be malicious, in this case, the PhishTank application.

5. To view raw data, navigate back to the security incident and click the blue information icon next to an observable.

6. In the window that is displayed, click **Open Record**.
The link created by the API and the **Finding** field displayed with the results.

**Trouble?**
If you do not see results under the **Threat Lookup Results** tab, verify that the observable is a type that is supported for lookup by the integration.

**(Optional) Manually attach an observable for PhishTank**
You can manually attach observables to a security incident. You manually attach observables when you want to perform threat lookups on observables that are not attached to a security incident on the initial event trigger. Also, you might perform this task when you want more information about a related observable.

**Before you begin**
Role required: sn_si.analyst

**Procedure**
1. Navigate to your open security incident.
2. On the open security incident record, click the **Show IoC** link in Related Links to display the **Observables** tab.
3. Click **New**. The Observable form is displayed.

4. In the **Value** field, enter a URL.

5. Click the search icon and from the **Observable Type Categories** dialog box, click **URL** in the list to populate the field.
6. Click **Submit**.
   The workflow launches and checks for the new observable. The execution and completion status is displayed in the work notes section on the Security Incident record.

7. Navigate to your security incident and review the work notes.

8. Click the **Show All Related Lists** related link at the bottom of the security incident.

9. Click the **Threat Lookup Results** tab to view the results.

10. In the **Observable** column, click the blue information icon next to a given observable for more information and raw data.

11. In the dialog box that is displayed, click **Open Record**.
Trouble?
Review the work notes for more information and how to proceed if you cannot verify that the lookup ran successfully.

Reverse Whois integration
Reverse Whois is a service that performs searches on domain names registered by individuals or organizations.

Perform domain lookups using search terms in observables that you attach to a security incident. The Reverse Whois API searches domain records based on search terms you enter, and it returns all records that correspond with those terms.

Analysts sometimes use this integration along with the Whois integration for security incident research. The Whois integration provides additional enrichment information based on the domain lookups from the Reverse Whois integration.

This integration is compatible with the Kingston, London, Madrid, and New York releases of the Now Platform®.

Install and configure Reverse Whois
Before you run the integration on your instance, complete the installation and configuration steps so the Reverse Whois application properly integrates with the Security Operations product.

Before you begin
Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have assigned the required ServiceNow roles.</td>
<td>The following roles are required for installation, configuration, and verification of expected results:</td>
</tr>
<tr>
<td></td>
<td>• The System Administrator (admin) installs the app and assigns the Security Incident Administrator (sn_si.admin) role.</td>
</tr>
<tr>
<td></td>
<td>• The Security Incident Administrator (sn_si.admin) oversees the configuration. The security incident administrator also assigns the Security Incident Analyst (sn_si.analyst) role.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain an API key.</td>
<td>Visit the WhoisXML API website for information on API keys and to create an account: <a href="http://www.whoisxmlapi.com">WhoisXML API website</a>. The configuration requires that you enter the API keys.</td>
</tr>
</tbody>
</table>
| Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration. | Madrid and later release requirements For the Madrid release and later family releases, the Security Incident Response Dependency plugin (com.snc.si_dep) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications required by the integration. Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation.  
1. Security Incident Response  
2. Security Integration Framework  
3. Security Support Common  
4. Security Support Orchestration  
For more information on setting up your Now Platform instance for the integration, see [Get entitlement](http://www.servicenow.com). |
<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>for a Security Operations product or application and Activate a ServiceNow Store application.</td>
</tr>
</tbody>
</table>

Role required: admin

**Procedure**

1. If you have already installed and configured the Reverse Whois application, follow these steps:
   a. Delete the existing configuration.
   b. Install and create a new configuration using the API key that you have obtained.

2. If you have not installed the application for the integration, see Install a Security Operations integration and follow the steps to install it.

3. After the installation completes, navigate to Integrations > Integrations Configurations and locate the Reverse Whois API tile.

4. Click Configure.

5. In the Reverse Whois API Configuration dialog box, enter the API key you obtained from the Whois XML API website.

6. Choose one option in the following table to filter domain lookups for your search terms.
Your search includes all domains, active and expired, that were registered after the Since date for the search terms you enter.
This is the recommended setting.

Your search includes all active domains for the search terms you enter.

<table>
<thead>
<tr>
<th>Description</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your search includes all domains, active and expired, that were registered after the Since date for the search terms you enter.</td>
<td><strong>Since date</strong>: Date entered in <em>yyyy-mm-dd</em> format. For example, <em>1991-06-01</em> for June 1, 1991.</td>
</tr>
<tr>
<td>This is the recommended setting.</td>
<td><strong>Since date</strong>: Field cleared.</td>
</tr>
</tbody>
</table>

These configuration settings remain saved until you change them and apply to all Reverse Whois API searches.

7. Click **Submit**.  
Configuration is successfully completed unless an error message is displayed.

**Trouble?**
If an error message is displayed, the API key may be invalid.

**Error message**

_One or more configuration parameters are incorrect and integration failed to initiate. Please make changes and submit again. More..._

**(Optional) Install and configure Whois**

Install the Whois plugin to provide additional enrichment information on your domain lookups from the Reverse Whois API. This lookup provides additional enrichment data on the domain, such as the registration date, name of registrar, and country of origin.
Before you begin

1. If you have not requested entitlement for the application, see Get entitlement for a Security Operations product or application for the Whois application from the ServiceNow Store.

2. Obtain credentials for the Whois API key from the product website: WHOIS API website.

Role required: admin

Procedure

1. If you have not installed the application, see Install a Security Operations integration and follow the steps to install it.

2. After the installation completes, navigate to Integrations > Integrations Configurations and locate the Whois API tile.

3. Click Configure.

4. In the Whois API Configuration dialog box, enter the API key you obtained from the product website.
5. Click **Submit**.
   Configuration is successfully completed unless an error message is displayed. You can now run enrichment lookups on the domains returned from the Reverse Whois integration.

**Trouble?**
If an error message is displayed, the API key may be invalid.

Initiate the lookup for the
Initiate domain lookups using search terms in observables that you manually attach to a security incident record.

**Before you begin**
Role required: sn_si.analyst

**Procedure**
1. If not open, navigate to **Security Incident > Incidents > Show All Incidents** and open the security incident you are working with.
2. At the bottom of the record, click the **Show IoC** related link to display the Observables tab.

**Note:** The figures in the following steps are shown with the Tabbed forms setting active in the System Settings. If you do not see tabs on the security incident, in the upper-right corner of the banner frame, click the **Settings** gear icon. In the System Settings dialog box that is displayed, click **Forms** and verify that Tabbed forms and With the Form are selected.
3. On the Observables tab, click **New**.

4. Fill in the fields.

**Required fields on the new record**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>Unique search term for a domain.</td>
</tr>
<tr>
<td>Observable type</td>
<td>This field is automatically cleared.</td>
</tr>
<tr>
<td>Finding</td>
<td>This field is automatically set to <strong>Unknown</strong>.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

You are returned to the security incident record and the workflow initiates the lookup.

**What to do next**

Verify the lookup results on the security incident. See [Verify expected results for Reverse Whois](#).
Verify expected results for Reverse Whois

Enrichment results are displayed on the ReverseWhois Domains tab at the bottom of the security incident record. Locate the lookup results to verify that the lookup ran successfully.

Before you begin
Role required: sn_si.analyst

Procedure

1. If not already open, navigate to Security Incidents > Incidents > Show All Incidents and locate the security incident you are working with.

After the application is configured and you have attached an observable, the workflow launches automatically. The work notes on the security incident record display the execution and completion status of the lookup.

2. If you cannot verify that the lookup ran successfully, review the work notes for more information on how to proceed.

3. Navigate to the bottom of the security incident and click the Show All Related Lists related link.

Note: For the filtered lookup results shown in the following figure, the configuration settings in the Reverse Whois API configuration tile were saved with 1991-06-01 entered in the Since date field.
Enrichment results are displayed on the ReverseWhois Domains tab. The active domains for this observable are displayed in the Domain column.

4. Click the blue information icon next to an item then click Open record in the dialog box that is displayed.

The record is displayed with enrichment details, including the raw data.

5. Navigate back to the security incident, and with the ReverseWhois Domains tab selected, click an observable in the Observable column to open a record.
The child observables are displayed on the **Child Observables** tab on the Observable record. The child observables are generated only if the Reverse Whois application has returned domains.

**Trouble?**
If the lookup does not successfully complete, verify that the search terms you entered are supported by the integration. Review the work notes for more information.

**What to do next**
For more enrichment data on the domain lookup results, you can run the Whois integration to perform enrichment lookups on the child observables returned by the Reverse Whois integration. This enrichment data on the child observables includes information on registration date, name of registrar, and country of origin.

**(Optional) Run enrichment lookup and verify expected results for Whois**
Run the Whois integration to perform enrichment lookups on the domains returned from the Reverse Whois integration.

**Before you begin**
Verify that you have installed and configured the Reverse Whois and Whois plugins. Perform these steps only after you have run the domain lookup with the Reverse Whois plugin successfully.

Role required: sn_si.analyst
About this task
Results are displayed on the Observable Enrichment Results tab on the Observable record.

Procedure

1. Navigate to Security Incidents > Incidents > Show All Incidents and locate the security incident you are working with that has run the domain lookup successfully.
2. Open the record and click the Show All Related Lists related link.
3. Select the Reverse Whois Domains tab at the bottom of the record.

In the Domains column, the list of returned domains is displayed.

4. In the Observable column, click an observable.
   On the Child Observables tab, the child observables are displayed. The child observables are generated only if the initial scan of the observable by the Reverse Whois application returned returned domains.
5. Select the child observables you want to run the observable enrichment on, and, in the Action on selected rows choice list, select Run Observable Enrichment.

6. Move the Whois integration from Available to Selected and click Submit.

The Run Observable Enrichment dialog box is displayed.
Results are displayed on the **Observable Enrichment Results** tab of the observable record.

7. Click the blue information icon then click **Open Record** in the dialog box that is displayed.
More information and raw data related to the original domain lookup is displayed, such as the registration date, name of registrar, and country of origin.

Trouble?
If you cannot locate child observables or enrichment results, verify that the Reverse Whois integration ran successfully and returned domains. Also, refer to the work notes on the record for more information.

Related information
- Install and configure Reverse Whois
- Verify expected results for Reverse Whois

RISKIQ and WHOISIQ integration
With the integration of RISKIQ and WHOISIQ APIs with the Now Platform® Security Operations product, security analysts are provided with additional enrichment data and insight into the validity of websites.

The RISKIQ SSL Certificates API performs lookups on SSL Certificates, which include details on the issuing certificate authority, organizations who request certificates, the entity certificates are issued to, and the domain. SSL certificate lookups are performed automatically when security incidents are created.

The RISKIQ WHOISIQ API performs lookups on other observable types, such as domain, email, nameserver, organization, address, and phone number. URL and domain observables are enriched automatically when security incidents are created.

The integration requires the Security Incident Response and Threat Intelligence products.

This integration is compatible with the Kingston, London, Madrid, and New York releases of the Now Platform®.
Supported observables for RISKIQ and RISKIQ WHOISIQ

The RISKIQ API supports automatic SSL certificate lookups on IP address, file hash, Certificate Serial Number, domain, and URL observables. URL and domain observables are enriched automatically with the WHOISIQ API. For observable enrichment on other types of observables with the WHOISIQ API, create observables and run lookups manually from the Observables table.

Supported observables

The following table lists the type of APIs used in this integration, and the observables each API supports. The table also indicates whether a lookup occurs automatically when security incidents are created, or if the lookup is run manually from the Observables table.

<table>
<thead>
<tr>
<th>API</th>
<th>Supported observables</th>
<th>Lookup (automated or manual)</th>
</tr>
</thead>
</table>
| RISKIQ SSL certificate API | • IP address  
  • File hash (certificate thumb print). See the following figure for an example of a file hash.  
  • Certificate Serial Number, or Serial Number. This string is a unique ID for the entity. See the following figure for an example of a certificate serial number.  
  • Domain (www.site.com, or site.com) | Automated lookup when incidents are created.  
  Results are displayed on the SSL Certificates tab of the security incident record. |
Supported observables and lookup (continued)

<table>
<thead>
<tr>
<th>API</th>
<th>Supported observables</th>
<th>Lookup (automated or manual)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RISKIQ WHOISIQ API</td>
<td>• Domain</td>
<td>Automated lookup when incidents are created. Results are displayed on the <strong>Observable Enrichment Results</strong> tab on the security incident record.</td>
</tr>
<tr>
<td></td>
<td>• URL</td>
<td></td>
</tr>
<tr>
<td>Note: automatic scans are run for the URL format using the https:// protocol, for example, https:// example.com/ index.html</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RISKIQ WHOISIQ API</td>
<td>• Email address</td>
<td>Manual lookup is run from the Observables table. Results are displayed on the <strong>Observable Enrichment Results</strong> tab on the Observable record.</td>
</tr>
<tr>
<td></td>
<td>• Organization name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Phone number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mailing address</td>
<td></td>
</tr>
</tbody>
</table>

**Example of a file hash and certificate serial number**

This figure shows an example of the file hash and certificate serial number observables used for the SSL certificate lookups for this integration. The file hash refers to a SHA-1 fingerprint. This value is displayed in your Now Platform instance without the colon separators. For example, 646D4B7A0C59A66656E94DDADD6C798027EFC10F.

The certificate serial number observable refers to the unique ID or serial number for the entity. This value is also displayed without the colon separators. For example, 00EA0F74B56D44BBBE0000000050DE1DFD.
Install and configure RISKIQ and WHOISIQ

Before you run the integration on your instance, complete the installation and configuration steps so the RISKIQ and WHOISIQ applications properly integrate with Now Platform Security Operations.

Before you begin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have assigned the required roles.</td>
<td>The following roles are required for installation, configuration, and verification of expected results:</td>
</tr>
<tr>
<td>Setup task</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Obtain an API key and secret (password).</td>
<td>Visit the website for information on the API key and how to create an account: <a href="#">RISKIQ website</a>. The configuration requires that you enter the API key.</td>
</tr>
<tr>
<td>Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration.</td>
<td>Madrid and later release requirements for the Madrid release and later family releases, the Security Incident Response Dependency plugin (com.snc.si_dep) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications required by the integration. Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation.</td>
</tr>
<tr>
<td>Setup task</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1. Security Incident Response</td>
<td></td>
</tr>
<tr>
<td>2. Security Integration Framework</td>
<td></td>
</tr>
<tr>
<td>3. Security Support Common</td>
<td></td>
</tr>
<tr>
<td>4. Security Support Orchestration</td>
<td></td>
</tr>
</tbody>
</table>

For more information on setting up your Now Platform instance for the integration, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.

**Procedure**

1. If you have not installed the application for the integration, see Install a Security Operations integration and follow the steps to install it.

2. Once the installation completes, navigate to **Security Operations > Integrations > Integrations Configurations** and locate the API tile.

3. Click **Configure**.

4. In the API Configuration dialog box that is displayed, enter the API key and secret (password) you obtained from the website. The **Maximum results** default setting is **1000**. This value is the maximum returned results on a lookup for a given observable. The maximum attribute for this value is **10,000**. You can enter a value up to **10,000**. The setting remains saved until you change it.
5. Click **Submit**.

6. Verify successful configuration.
   When configuration is successfully completed, the Security Integrations page with the integration tiles is displayed.

**Trouble?**
If an error message is displayed, the username or secret (password) may be invalid. Verify that your username and password are correct, and that the API key is valid.

One or more configuration parameters are incorrect and integration failed to initiate. Please make changes and submit again. More ...

**Verify expected results for RISKIQ SSL certificate lookups**
When a security incident generates observables for URLs, domains, IP addresses, certificate file hashes (SHA-1 fingerprint), and certificate serial numbers, security incident analysts use the SSL certificate lookup results to verify sites have certificates that have been issued by a trusted public Certificate Authority (CA).

**Before you begin**
Role required: sn_si.analyst

**About this task**
For supported observables, the Now Platform scans for the most recent occurrence of URLs, domains, IP addresses, certificate file hashes (SHA-1...
fingerprint), and certificate serial numbers. These are possible outcomes from the scan:

**An exact match is found**

A valid issuer of an SSL certificate is listed on the Security Incident record.

**No certificate results are found**

No results are listed on the Security Incident record.

**An exact match is found for a self-signed, or internally generated certificate**

Results for an internally generated SSL certificate are displayed on the Security Incident record.

**An exact match is not found for a primary SSL certificate**

A lookup value returns multiple entries and a primary certificate cannot be identified. A summary message is displayed on the Security Incident record.

**Procedure**

1. To view the observables and verify lookup results, open the security incident record you are working with and locate the work notes.

**Example**

To illustrate examples for the possible lookup results for this integration, suppose that a security incident was generated with the following observables:

- community.servicenow.com
- invalidsubdomain.servicenow.com
- mail.dgnetworks.com
- servicenow.com

**Observables and location of lookup results**

<table>
<thead>
<tr>
<th>Observable (example)</th>
<th>Scan results</th>
<th>Description and location</th>
</tr>
</thead>
<tbody>
<tr>
<td>community.servicenow.com</td>
<td>Found certificate with a SHA1 hash.</td>
<td>An exact match is found, and a valid issuer of an SSL certificate is listed. Results for the exact match are displayed on the <a href="#">SSL Certificates</a> tab on the security incident record.</td>
</tr>
<tr>
<td>Observable (example)</td>
<td>Scan results</td>
<td>Description and location</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>invalidsubdomain.servicenow.com</td>
<td>No certificate found.</td>
<td>A summary that indicates no certificate results were found is displayed on the Observable Enrichment Results tab on the security incident record.</td>
</tr>
<tr>
<td>mail.dgnetworks.com</td>
<td>Found certificate with SHA1 hash.</td>
<td>An exact match is listed for a self-signed, or internally generated certificate. Results are displayed on the SSL Certificates tab on the security incident record.</td>
</tr>
<tr>
<td>servicenow.com</td>
<td>Search returned 138 certificates, and a single primary certificate could not be identified.</td>
<td>An exact match is not found for a primary SSL certificate, because a lookup value returns multiple certificates. A summary that indicates no primary certificate was found is displayed on the Observable Enrichment Results tab on the security incident record.</td>
</tr>
</tbody>
</table>

After the application is configured, the workflow launches automatically. The lookup status and the observables are displayed in the work notes.

2. Verify that the lookup ran successfully.

```
<table>
<thead>
<tr>
<th>System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workflow Security Operations Integration - Enrich Observable execution completed.</td>
</tr>
<tr>
<td>Finished running Enrich observable capability</td>
</tr>
<tr>
<td>Automation activity + 2018-05-01 10:49:36</td>
</tr>
</tbody>
</table>
```

```
<table>
<thead>
<tr>
<th>System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workflow Security Operations Integration - Enrich Observable execution started.</td>
</tr>
<tr>
<td>Data inputs for this action: mail.dgnetworks.com, community.servicenow.com, invalidsubdomain.servicenow.com, servicenow.com</td>
</tr>
<tr>
<td>Automation activity + 2018-05-01 10:49:16</td>
</tr>
</tbody>
</table>
```
Trouble?
If you cannot view expected results, verify that the observable is supported by the SSL certificate lookup for the integration.

Related reference
Supported observables for RISKIQ and RISKIQ WHOISIQ

RISKIQ SSL certificate lookups that return an exact match
RISKIQ SSL certificate lookup results for an exact match are displayed on the SSL Certificates tab on the security incident record. An exact match provides a valid certificate authority name, which helps a security incident analyst determine the validity of a website.

Example: Exact match for a valid SSL certificate
The following example shows a valid issuer of an SSL certificate from an exact match in the lookup results. Follow the steps to view the results and raw data.

Note: The figures in the following examples are shown with the Tabbed forms setting active in the System Settings. If your screen does not match the view shown below, follow the steps to set tabbed forms.

1. In the upper-right corner of the banner frame, click the Settings icon.
2. In the System Settings dialog box that is displayed, click Forms and verify that Tabbed forms and With the Form are selected.

1. In the security incident record, click the SSL Certificates tab.

![SSL Certificates tab](image)

Information about the certificate issuer's name, the issuer's organization, and who the certificate is issued to (Organization) is displayed along with other data.
Two items are displayed in the **Issuer Name** column. The first item (Entrust Certification Authority – L1K) provides a valid certificate authority name (Entrust) in the **Issuer Organization** column. Another recognizable entity (ServiceNow) is displayed in the **Issued to (Organization)** column.

No information in the **Issuer Organization** and **Issued to** columns is displayed for the second item (dgt.sbs).

2. Click the first item in the **Issuer name** column (Entrust Certification Authority – L1K) to open the entry record. Alternatively, click the information icon next to the item followed by **Open record**.

3. Select the **Raw Data** tab.

The SSL Certificate Entry record includes the observable in the **Raw Data** tab under the **Entity name** column, as well as other data.

Note in the **Category** column, the **Subject**, and **Issuer** correspond to recognizable entities in the **Entity name** column. The issuer of this certificate is most likely valid and from a trusted public certificate authority. Also note,
the **Subject**, and **Issuer** are different entities. These separate entities indicate that the certificate is not an internally signed certificate from an unknown certificate authority.

**Example: Exact match for a self-signed SSL Certificate**

The following example shows results for a self-signed SSL certificate from the lookup. Follow the steps to view the results and raw data.

1. Navigate back to the security incident record. In the **Issuer Name** column, click the other item (**dgtsbs**).

2. On the open record, select the **Raw Data** tab.
The **Category** column indicates the **Issuer** (mail.dgtnetworks.com and dgtsbs.DGTNetworks.local) are not trusted public certificate authorities. Also note the **Issuer** and **Subject** are the same entity (dgtsbs.DGTNetworks.local), and each contains the name of the observable (dgtsbs). This certificate is possibly a self-signed certificate. Self-signed certificates may warrant further investigation, as these certificates are not issued by a known certificate authority.

**RISKIQ SSL certificate lookups that return multiple certificates or no certificates**

A security incident analyst can use multiple SSL certificate results to determine whether a site is part of a common, recognizable entity. No SSL certificate results may indicate sites with obscure or suspicious names have no trusted certificates. Lookup results for observables that do not return SSL certificates, or that return multiple SSL certificates, are displayed on the **Observable Enrichment Results** tab on the security incident record.

**Example: No SSL certificate results or multiple SSL certificate results**

Follow the steps to view the results for observables that do not return SSL certificates, or that return multiple certificates.
1. In the security incident record, click the **Observable Enrichment Results** tab.

![Observable Enrichment Results tab](image)

The observable enrichment results for the RISKIQ and WHOISIQ lookup are displayed.

In the **Observable** column, **servicenow.com** corresponds to the *Search returned 138 certificates* message in the **Summary** column. Similarly, **invalidsubdomain.servicenow.com** corresponds to *No certificates were found* in the **Summary** column. These summaries indicate that multiple SSL certificates were found, and that no exact matches for SSL certificates were found, respectively.

2. In the **Observable** column, click **servicenow.com**.

![Multiple SSL certificates](image)

The summary message that is displayed on the record indicates that multiple results for SSL Certificates were returned for **servicenow.com**, and a primary SSL Certificate could not be matched. This message is often returned on lookups that include common domain names, such as **servicenow.com**.
If you require more information on a common domain, you can perform the search directly with the RISKIQ API.

3. Navigate back to the **Observable Enrichment Results** tab, and in the **Observable** column, click **invalidsubdomain.servicenow.com**.

   ![No SSL Certificates]

   No SSL certificates were found.

**Verify expected results for WHOISIQ URL lookups**

When a security incident generates observables for URLs or domains, the WHOISIQ API performs the observable enrichment automatically upon security incident creation. The lookup results are displayed on the **Observable Enrichment Results** and **SSL Certificates** tabs on the security incident record.

**Before you begin**

*Note:* The figures in the following steps are shown with the **Tabbed forms** setting active in the System Settings.

**Role required:** sn_si.analyst

**About this task**

Observable enrichment results are displayed on the **Observable Enrichment Results** tab at the bottom of the security incident record. For supported observables, an SSL certificate search is also run and the results are displayed on the **SSL Certificates tab**.
Procedure

1. Open the security incident record you are working with and verify that the lookup has run successfully in the work notes.

Once the application is configured, the workflow launches automatically upon incident creation. The execution and completion status of the lookup is displayed in the work notes in the Security Incident record.

2. If you cannot verify that the lookup ran successfully, review the work notes for more information on how to proceed.

3. On the open security incident, click the **Show All Related Lists** related link.

4. Click the **Observable Enrichment Results** tab to select it.

5. In the **Summary** column, click the first item, **Domain: uber.com Registrar: Markmonitor**.

The record that is displayed contains information about the domain.

6. Navigate back to the **Observable Enrichment Results** tab, and, in the **Summary** column, click the second item, **Found certificate with SHA1 hash**.
This record indicates that an SSL Certificate was found with a file hash.

7. Navigate back to the security incident record and click the **SSL Certificates** tab.

The SSL Certificate results for the file hash are also displayed here.

**Trouble?**
If you cannot view expected results, review the work notes. Also, verify the observable is supported for the lookup by the integration.

**Related reference**

- Supported observables for RISKIQ and RISKIQ WHOISIQ

**Create an observable for manual WHOISIQ lookups**

Security incident analysts use information from observable enrichment with the WHOISIQ API to learn more about the email addresses, names, and phone numbers of organizations.

**Before you begin**
Role required: `sn_si.analyst`
Procedure

1. Navigate to **IoC Repository > Observables**.

   **Enter Observables in navigation filter**

   Under the navigation panel, the Observables module is displayed.

2. Click the **Observables** module to display the Observables list.

3. Click **New** to create a new observable.

4. On Observable form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>Email address, organization name, phone number, or mailing address. For example, <a href="mailto:test1@gmail.com">test1@gmail.com</a></td>
</tr>
<tr>
<td>Observable type</td>
<td>The field is automatically cleared.</td>
</tr>
<tr>
<td>Finding</td>
<td>The field is automatically set to <strong>Unknown</strong>.</td>
</tr>
</tbody>
</table>
Create a new observable

5. Click Submit.
You are returned to the Observables list. In the Value column, your new observable is displayed.

Note: If you cannot locate your observable on the part of the list that is displayed, use the search functionality to find it.

6. Edit the Observable type field to change the type from Unknown to Email address to match your observable.

a. In the Observable type column, single-click to the right of the Unknown text to select it.

The selected field is outlined in blue.

b. With the field outlined in blue, double-click anywhere inside the highlighted field to open the editor.

c. In the field that is displayed, enter the observable type (Email address) and click the green check mark to save the value.
Edit the Observable type field

In the **Observable type** column on the list, **Email Address** is displayed for your new observable.

Updated Observable type field

What to do next
If you have created and edited an observable for lookup, run the observable enrichment lookup from the Observable record with the WHOISIQ API.

Verify expected results for manual WHOISIQ lookups
Run a manual lookup on an observable when it does not automatically generate a security incident. For observable enrichment lookups using the WHOISIQ API for email addresses, organization names, phone numbers, or mailing addresses, initiate the lookup manually from the Observables table.

Before you begin
Create an observable for a manual lookup using the WHOISIQ API. For more information on how to create and edit an observable, see [Create an observable for manual WHOISIQ lookups](#).

Role required: sn_si.analyst

Procedure
1. Navigate to **IoC Repository > Observables** and locate the observable in the list you are working with.
2. Click your observable in the **Value** column to open the record.
3. Click the **Run Observable Enrichment** related link to run the lookup.

4. In the **Run Observable Enrichment** window, move **RiskIQ Whois** to the Selected list.

5. Click **Submit**.
Lookup results are displayed on the **Observable Enrichment Results** tab on the observable record.

![Observable Enrichment Results](image)

**Trouble?**
If no results are returned for the observable, a message is displayed in the **Summary** column. If you do not see results, verify the observable is supported by the API.

**Related reference**
- Supported observables for RISKIQ and RISKIQ WHOISIQ

**Secureworks CTP Ticket Ingestion Integration**
The Secureworks Counter Threat Platform ticket ingestion integration enables you to automatically fetch Secureworks CTP tickets, convert them into security incidents and perform automated response actions.

The key features of this integration include:

- Automatic ingestion of selected tickets (including attachments) based on a pre-defined schedule.
- Mapping of ticket and event fields to Security Incident Response fields.
- Preview of security incidents mapped to the ticket fields.
- Filtering and aggregation of tickets.
- On demand retrieval of events associated with a ticket.
• Periodic tracking of key updates to tickets.
• Automating ticket updates and closures based on SIR incident status
• Master ticket update.
• Synchronization of Secureworks worklogs with Security Incident Response worknotes.

**Setup your NOW Platform instance for the Secureworks CTP ticket ingestion integration**

The following section lists the setup tasks that you are required to complete in your Now Platform instance prior to installing the application from the ServiceNow Store.

**About this task**

Refer to the following table and verify that you have completed all the listed tasks before you download and install the application to ensure a smooth installation and configuration.

Role required: sn_si.admin

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have assigned the required Now Platform and Security Incident Responseroles.</td>
<td>The following roles are required for the installation, setup, and use of the integration in your Now Platform instance.</td>
</tr>
</tbody>
</table>

• A user with the Now Platform administrator role (admin) installs the application from the ServiceNow Store and assigns the SIR administrator (sn_si.admin) role.

• A user with the sn_si.admin role oversees the following tasks in the Now Platform:
  ◦ Names, creates, and edits profiles.
  ◦ Selects and maps Secureworks CTP ticket fields to the security incident fields.
  ◦ Previews security incident details for accuracy prior to finalizing the configuration.
  ◦ Schedules on-going ticket ingestion.
  ◦ Enables ticket updates when a SIR SIR incident is created and closed. |
<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
</table>
| ◦ Assigns the security incident analyst (sn_si.analyst) role.  
◦ Users with the sn_si.analyst work with security incidents. | For more information about roles and assigning roles to users, see Roles section on the Servicenow Product Documentation website. |
| Verify that you are using the following versions:  
• Secureworks Ticket API 4.0  
• Secureworks Event API 1.0  
• Secureworks Enrichment API 1.0 | If you have access to the Secureworks CTP portal, you have access to the API that is required for this integration. There is no other special setup required for the API. |
| Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration. | Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation.  
1. Security Incident Response  
2. Event and Alert Ingestion for Security Operations (Required for SIEM integrations):  
   This application requires:  
   • com.glide.hub.integration.runtime => ServiceNow IntegrationHub Runtime  
   • com.glide.hub.action_step.rest => ServiceNow IntegrationHub Action Step - REST  
   | Note: The Integration Hub components are installed along with the Event and Alert Ingestion plugin. If these are not installed, contact Customer Support for assistance.  
For more information about installing the Security Operations core applications, see Get
<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>entitlement for a Security Operations product or application and Activate a ServiceNow Store application.</td>
</tr>
</tbody>
</table>

**Install and configure the ServiceNow application for the Secureworks CTP ticket ingestion integration**

Before you run the integration on your Now Platform instance, complete these installation and configuration steps so the application properly integrates with the Security Incident Response and Security Operations products on your Now Platform instance.

**Before you begin**

Role required: sn_si.admin

**Procedure**

1. **If you have not installed the Secureworks CTP ticket application from the ServiceNow Store for the integration, see Install a Security Operations integration and follow the steps to install it.**

2. **After you have successfully installed the application, navigate to Integrations > Integrations Configurations and locate the Secureworks CTP Ticket Ingestion Integration tile.**

3. To configure the application, click **New**.

4. Alternatively, if a **Configure** button is displayed on a tile, click it to edit an existing configuration.

5. In the dialog that is displayed, fill in the fields.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Secureworks CTP instance used for the integration. You can enter only alphanumeric values and hyphens (-) in this field.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the user account.</td>
</tr>
</tbody>
</table>
| Username      | Enter the username for the Secureworks CTP API account. Note that the username is case sensitive. To find the username, follow these steps:  
  • Login to the Secureworks CTP portal.  
  • Navigate to Account > Account Management > API Credentials. The username is displayed on the API Credential page. |
| API Password  | Enter the Secureworks CTP API Password. To find the API Password, follow these steps:  
  • Login to the Secureworks CTP portal.  
  • Navigate to Account > Account Management > API Credentials. The API Password is displayed on the API Credential page. For more information on how to obtain the username and API password, follow the steps in the Generating a Persistent API Key section in the Secureworks Ticketing API Guide. |

6. Click **Submit**.  
After it is successfully validated and submitted, each configuration is saved on the Security Integrations page as a tile. If your saved configuration tiles are not displayed on the Security Integrations page, on the top right corner of the page, from the Show Configurations choice list, click **Yes**.
Create a profile for Secureworks CTP ticket ingestion integration

As a user with the sn_si.admin role, create a profile in your Now Platform instance and determine which tickets need to be ingested and which tickets will be used to create security incidents. Before security incidents are created from ingested tickets, the field values from tickets are displayed on a layout of a Now Platform security incident so that you can preview how the actual security incident will be displayed.

The integration allows you to ingest tickets based on the profiles that you configure in the Security Operations environment of your instance. All tickets are initially ingested for a configured ticket type in a profile. Ingested tickets can then be further filtered to specify which tickets create security incidents.

For example, you may prefer filters that create security incidents only for tickets that are identified as high-risk. Before a profile is activated, and it creates security incidents from ingested tickets, individual field values on the tickets are mapped to corresponding fields on a layout of security incident for a preview.

Identify the source of the profile

Specify the name and source of the profile.

Before you begin

Role required: sn_si.admin

Procedure

1. To create a profile for a ticket in your Now Platform instance, navigate to Secureworks Ticket Ingestion Integration > Secureworks Profiles.
2. Click New.
3. Fill in the fields.

An example of a completed form follows the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the profile. If names are not unique, an error will be displayed and duplicate profile names are not saved. Profile names in your Now Platform instance must be unique.</td>
</tr>
<tr>
<td>Source</td>
<td>Select the source from where you want to ingest the data.</td>
</tr>
<tr>
<td>Order</td>
<td>Default is 100.</td>
</tr>
</tbody>
</table>
If you have created multiple profiles, this value provides a run time execution priority when two or more profiles share the same triggering conditions. The lower the order value, higher the priority.

Active

This option is cleared by default. If this option is disabled, the profile is not active.

Note: You should complete all sections in the profile before making it active.

The following figure is an example of a completed form.

What to do next
The next step is to map the ticket fields.

Mapping of ticket fields for the SecureWorks CTP integration
Map the ticket and event fields to the fields in the security incident form.
For the mapping step, you must first ingest sample tickets and then ensure that all the relevant ticket fields are mapped to the appropriate place on the Security Incident Response form and then visualize the security incident in the preview section.
Mapping of the sample ticket fields involves the following:
• Fetching and populating of the sample data: See Ingesting the sample Secureworks tickets

• Mapping the ticket fields to the security incident: See Mapping Secureworks ticket fields to security incident response fields

**Ingesting the sample Secureworks tickets**

Select the sample tickets that are to be ingested.

**Before you begin**

Role required: sn_si.admin

**Procedure**

1. If the mapping form is not displayed, click **Mapping** on the progress bar.

2. You can either pull the five most recent sample tickets or provide the unique ticket IDs for the specific tickets that you want to use for your mapping experience. From the **Ingestion Preference** choice list, select one of the following:
   - Retrieve most recent tickets: The 5 most recent tickets are retrieved.
   - Select tickets based on ticket ID: Specify the ticket ID for the ticket to be retrieved. You can specify a maximum of 5 ticket ids separated by commas.

3. Click **Fetch Sample Data** to pull the latest sample ticket data from the Secureworks CTP server. The pull for sample tickets may take a few moments. A message indicating that the transaction is working is displayed at the top of the screen.

   The retrieved tickets are displayed as individual tabs. Click on a tab to view the ticket data. For each ticket, you can see the ticket fields and their values, and details of the contributing event that triggered the ticket.

   **Note:** You will see details of contributing events only if they have occurred in the last 7 days. Events older than 7 days are not displayed.

**What to do next**

After you have fetched the sample data, the next step is map the ticket fields to the security incident.

**Mapping Secureworks ticket fields to security incident response fields**

Map individual ticket or event fields to fields on a Now Platform SIR security incident.
Ticket field mapping

As a user with the sn_si.admin role, use the fields from the Sample Tickets section on the left and map them to the security incident fields in the SIR Incident Field Mapping column. Edit the mapping configuration by dragging ticket or event fields from the left side and dropping them on the SIR Incident Field Mapping section on the right. The mapping on the right associates the incoming ticket field with an outgoing security incident field.

1. To map a field value from the left side of the form to a field on the security incident on the right side of the form, click-hold a blue field name on the left side of the form.

2. You can manually enter the field name in the Input Expression column or drag and drop the field name. For example, description, and drop it on a field in the Input Expression column next to a field name in the Security Incident column.

   The field value is displayed in the Input Expression column. In the following image, categoryClass is mapped to the Category field on the security incident.

   ![Image of field mapping](image)

   **Note:** If you enter the event field name manually in the Input Expression section, you must add a prefix as `${Event:eventfield}` before the name of the field being mapped.

To help you ensure that no ticket or event fields are overlooked or duplicated in the mapping process, fields are color-coded. Color-coding of the ticket fields helps you keep track of the ticket values that you have already mapped as they become greyed out while all remaining unmapped fields appear in blue. This helps you better visualize which field values have been added to the security incident and if any remaining important ticket information remains unmapped.
Light blue fields on the left indicate that a ticket field is not yet selected and mapped on the security incident. You may prefer to associate an incoming ticket or event field with more than one field on a security incident. A gray field indicates that a field has been selected and mapped to a field on the security incident. This color-coding helps you track the mapping.

3. To add fields to the default fields displayed on the security incident on the right side of the form, follow these steps:

   a. On the right of the form in the SIR Incident Field Mapping section, at the bottom of the grid, click the plus (+) icon. A new field is displayed.

   b. In the Security Incident column, expand the choice list that is displayed, and select a field.

In the expanded choice list for the new field, some fields are shaded. In the following figure, Category has a gray background, because it has been mapped in the security incident. Similar to the color-coding for the ticket fields on the left side of the form, this color-coding for the security incident fields on the right helps you track the already mapped SIR incident fields.
Note: As multiple observables can be displayed on the same security incident, the Observable field can be mapped multiple times with different values. Similarly, the Configuration Item and Work notes fields support multiple values. If you try to map two values to a field that cannot support multiple values, when you preview the incident, an error message is displayed that there is no value for the field. Similarly, if a field on a security incident has a choice list from which you can choose multiple options, and you try to map an option to that field that is not displayed on the choice list, the field is not populated on the security incident.

c. Alternatively, type a value in the Search field for the new row.

d. From the left side of the form, select the ticket field and drag-and-drop it to an appropriate security incident field on the right.

4. Remove fields by using the - icon next to the field name in the SIR Incident Field Mapping section.

5. Continue mapping by adding or removing field values to the mapping.

Format Field Translation

In certain cases, ticket fields may not translate directly to the fields on the SIR security incident. For these values, you can use a script editor to format field values on the security incident during the mapping step. Use the script editor if you want to format values that are similar, but not identical. For example, with the script editor, a category value of Malware Alert and Virus Infection may have different field values for the source category but both values can be translated to a common Malicious Code Activity in the Category field on the SIR security incident using the Format Field Translation functionality.

To use the script editor, click the {} icon next to the Category field. The script editor is displayed
Incident generation conditions

Once the mapping section is complete, you can set filter conditions so that you can specify which tickets should create security incidents versus which tickets should be filtered out, for example, low priority tickets. You can use the same field values in the Incident Generation Conditions builder to define additional criteria that an incoming ticket must satisfy to create a security incident. To set incident generation conditions, follow these steps.

1. Scroll to the **Incident Generation Conditions** section on the form and select the **Filter based on conditions** check box to enable the option.

   The Filter conditions builder is displayed. Use these filters to create security incidents that match the specific conditions described by the fields.

   The options in the choice lists for the first field in the Filter conditions builder match the fields that are displayed on the **Sample Ticket Ingestion** section for the ingested tickets. These fields are dynamic and change depending on the tickets that you ingest. Criteria that you enter are case-sensitive, and they must match exactly the values of the Secureworks CTP ticket. If you are not
sure about the values to enter in the filter fields, you may prefer to return to your Secureworks CTP console and review your tickets for the keywords.

**Note:** The worklogs, devices, attachments, watchers, availableactions, and closeCodes ticket fields can have multiple values (as the values are stored in arrays). As the filter condition can retrieve only strings, you must use the contains filter condition for these fields to ensure that the data is filtered correctly.

2. Using the choice lists and fields of the conditions builder, set filters for the first row.

3. To add more conditions, to the right of the fields, click **AND** or **OR**.
   - If **AND** is selected, all conditions must be matched.
   - If **OR** is selected, either condition can be matched.

4. (Optional) In the second row, set a second filter condition.

   This type of incident generation condition filtering helps you narrow down the tickets, and limit the number of unnecessary security incidents that you create without modifying the underlying rule or filters. If additional filtering criteria are set, only tickets that match all criteria are mapped to security incidents.

---

**Ticket aggregation criteria to handle similar tickets and prevent duplicate incidents**

Define additional ticket aggregation criteria that aggregates an incoming ticket to an existing SIR security incident instead of creating similar, potentially duplicate incidents. Using field matching value criteria for each profile, this additional aggregation capability can reduce the number of active, overlapping security incidents by placing all related ticket data on a single security incident. To set the criteria, follow these steps below:

1. Scroll to the **Ticket Aggregation Criteria** section on the form and select the **Aggregation Conditions** check box to enable this option.

   The Incident Field Matching Values columns are displayed. These field names are the fields on the security incident that include any custom fields that are configured on the SIR security incident.

2. From the Available list, select the field values that you want to match on existing security incidents in your NOW Platform and move them to the Selected list.

   All the field values that you select must be matched to append this incoming ticket to an existing security incident. This includes fields, such as Observables and Configuration Items, that may have multiple ticket field values mapped to them. All values must match. If only a subset of the values are matched, the
ticket aggregation conditions will not be met and a new security incident will be created. See screen shot below for multi-value field mapping.

If a new ticket matches all the values that are selected in the aggregation field conditions in the mapping step, the new ticket is automatically added to the most recently opened security incident with the same field values. As a user with the sn_si.analyst role working with security incidents, you can view all the added aggregated tickets on a related list on a security incident. This list details associated time stamps and aggregated field values. This information helps you understand why these tickets are being aggregated to existing security incidents. If this tab is not displayed in a security incident, scroll to the left side of the record under Related Links and click the Show All Related Lists link.

**Note:** The Secureworks Aggregated Tickets related list is not available with the base system. You must configure the Related List layout and explicitly include it with the other related lists.

3. (Optional) To log a work note for a new ticket that is recently added on the security incident, select the check box to enable this option. The work note logs that a new ticket has been added along with a link to the ticket details and any other details that may have been added to the work note field in your mapping section.

You have successfully mapped values from a Secureworks CTP ticket to fields on a security incident. Also, you have configured additional conditions to limit the creation of security incidents with incident generation filtering criteria. You
also appended tickets to existing security incidents when ticket field values match the configured aggregation criteria.

4. Click Continue to continue with the profile configuration. The next step is to preview the fields you mapped on a SIR security incident.

Preview the mapped values in the security incident

After you complete the mapping step, preview the values that you mapped in a SIR security incident. This preview step permits you to verify that you have mapped all the ticket fields that you want displayed on the security incident.

About this task

Preview a security incident and edit the mapping again as required to fix fields with errors or to populate any missing data. If the preview is not successfully completed, you cannot proceed to the scheduling step. Previews of SIR security incidents are not saved as actual incidents in the Security Incident Response product.

Role required: sn_si.admin

Procedure

1. If the security incident preview is not displayed, click Preview in the progress bar.

2. The tickets are displayed as tabs. Click on a tab to preview the security incident. This view is a read-only view, and a record of this security incident is not saved.

3. Review the field mapping of the ticket values on the security incident.
4. To resolve this error, click **Mapping** in the progress bar.

5. Edit the mapping to fix incorrect values or populate any missing data.

6. Preview the mapping again and continue to fix any errors that are described in error messages.

**What to do next**

If no error messages are displayed, and you are satisfied with the field mapping on the security incident, the next step is to define the schedule.

**Define schedule for the Secureworks CTP Ticket ingestion**

Verify the default settings for ticket retrieval or modify the scheduling as needed. This step permits you to filter your ticket retrieval based on a date range and a polling interval.

**About this task**

You also choose how often you will poll for future tickets that match the ticket profile configuration. As a user with the sn_si.admin role, you configure these polling intervals on a per-profile basis. When scheduling, you may prefer to balance system load against incident urgency. A one-minute default value is set for any profile, but you may prefer to modify this setting based on the urgency of the incident and the anticipated load on your system.
Procedure

1. If the Scheduling page on the progress bar is not displayed, select **Scheduling**.

2. Choose one to schedule how and when tickets are pulled from the Secureworks CTP portal.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Ongoing ticket ingestion selected</td>
<td>Based on the default setting, the Now Platform instance pulls from the Secureworks CTP portal for new tickets every five minutes. Security incidents are created if tickets are found and incident generation filtering criteria are matched. To balance ticket ingestion against server load, and to pull the most current data, five minutes is the setting you may prefer. However, this value can be modified as needed.</td>
</tr>
</tbody>
</table>
| • Ongoing ticket ingestion selected • Set initial ticket ingestion time | Initial ingestion time
If you want to schedule the initial ingestion at a specific time, follow these steps:
  • Select the Ongoing ticket ingestion and Set initial ticket ingestion time fields.
  • Specify the time in the Input initial ticket ingestion time field.

The initial ingestion will take place at the time specified here. Subsequent ingestions will be based on the schedule defined in the Polling increment (minutes) field.

As an example for scheduling, if you have a daily ticket job that runs once a day at 4 AM local time, you can set up the corresponding ticket profile in your Now Platform instance to run at 4:05 AM local time to capture the ticket right away and create a security incident.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enter 04 05 00 in the Initial ticket ingestion field. In the Polling increment (minutes) field, enter 1440 (24 hours) to schedule the next ticket ingestion for 24 hours from the initial ticket ingestion. Both the initial ticket ingestion time and next ticket ingestion time are displayed in the fields.</td>
</tr>
</tbody>
</table>

To configure the settings in this example, follow these steps:

- Select the **Ongoing ticket ingestion** option.
- In the Polling Increment (minutes) field, enter 1440 (24 hours).
- Select the **Set initial ticket ingestion time** option.
- In the Input initial ticket ingestion time field, enter 04 05 00. The time of the next ticket ingestion is displayed in the Next ticket ingestion time (estimated) field.

3. Click **Continue** to navigate to the Additional Options page.
Automate ticket updates and closure based on SIR incident status

The Secureworks CTP ticket ingestion integration has a bi-directional interface that allows for both tickets to create security incidents, as well as an ability to update the tickets once the security incident is created and/or closed with relevant incident details such as security incident number, assignment group, security incident URL, and so on.

Before you begin
Role required: sn_si.admin

Procedure
1. If the Additional Options page on the progress bar is not displayed, select Additional Options.
2. Follow the instructions below to complete the configuration for updating tickets when the security incident is created:

<table>
<thead>
<tr>
<th>Option or Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update SIR worknotes with Secureworks worklogs</td>
<td>Select this option to enable the Secureworks worklogs and SIR worknotes synchronization feature. This allows you to track updates made to the ticket in Secureworks CTP after the security incident is created.</td>
</tr>
<tr>
<td>Update Secureworks tickets upon SIR Incident Creation</td>
<td>Select this option to update the Secureworks CTP ticket and add additional comments when a security incident is created from the ticket. This can occur for both the initial trigger-</td>
</tr>
</tbody>
</table>

Note:

- If the Secureworks worklogs field has been mapped to the SIR Worknotes field, the Secureworks worklogs are retrieved till the security incident is created.
- If the synchronization feature is enabled, only worklogs created or updated after a security incident has been created are retrieved.
### Option or Field | Description
---|---
Initial comments posted back to Secureworks ticket | When a security incident is created, the ticket is automatically updated in Secureworks CTP with comments. You can modify the default text and use the `${field name}` format to add or modify any fields available in the security incident form.
Close Secureworks tickets upon SIR Incident Closure | Select this option if you want to use the automated ticket closure option. This can occur for both the initial triggering tickets that create the security incident, as well as aggregated tickets. When a security incident is closed, the corresponding ticket is automatically closed in Secureworks CTP along with the same close code as the security incident and the default closure comments specified in the profile.
Note: You cannot use this option to update the Master Ticket status.
Closure comments posted back to Secureworks ticket | The default closure comments are displayed here. You can edit the default text and use the `${field name}` format to add or modify any fields available in the security incident form.

3. Click **Finish** to complete the configuration and move the profile to the **Waiting** state.  
A confirmation dialog is displayed. You have successfully set up the profile. Activate this profile to pull tickets from the Secureworks CTP portal based on your scheduling.
Optional: Copy a Secureworks CTP profile

Copy an existing profile and its associated settings instead of creating new profiles. If you are creating multiple profiles, and you want to reuse the settings of an existing profile, you may prefer to copy profiles to save time.

Before you begin
Role required: sn_si.admin

About this task
As a user with the sn_si.admin role, if you copy a profile, the profile name is initially modified to avoid duplicate profiles. In addition, the copied profile is disabled (false) so it is not activated accidentally prior to completing the configuration. Copy profiles and use existing maps for security incidents that you have already previewed and verified.

Procedure
1. Navigate to Secureworks Ticket Ingestion Integration > Secureworks Profile.
2. In the Secureworks Profiles list that is displayed, select a profile that you want to copy, and, from the Actions on selected rows choice list, click Copy.
   The profile is copied and displayed on the list. The copy has all the settings of the original profile including the mapping and scheduling configuration. The name of the profile contains copy. Although the original profile is enabled (true), the copy is disabled at this point (false). You may prefer to edit values of the copied profile and rename it so the configuration settings apply to the new profile as required.
   You have successfully copied the settings from an existing profile to a new profile. Note that the Active column status is set to false as the profile needs to be activated.

What to do next
You are prompted to activate (enable) the new profile after you complete the configuration steps.

Security Incident Response form changes after ticket ingestion
After a Secureworks CTP ticket has been ingested, a security incident is created and the corresponding updates are made to the security incident record.

Worknotes
A worknote is posted with details of the ticket that triggered the security incident.
Click on the ticket link to navigate to the internal Secureworks Ticket to Task record. The **Click here** hyperlink takes you to the Secureworks CTP dashboard where you can view the ticket details.

If you had selected the **Log work note for new ticket** option in the Ticket Aggregation Criteria as described in the Create Profile: Mapping page, a worknote is posted when the ticket is aggregated.

**Aggregated tickets**

Click **Related Lists > Secureworks Aggregated Tickets** to view the ticket aggregated to the security incident. Click the ticket hyperlink to view the ticket in the Secureworks CTP dashboard.

Create security incident: Select a ticket from the list, click the **Actions** menu and click **Create security incident**. This option creates a new security incident for the ticket and this ticket is de-aggregated from the parent security incident.

Delete ticket record: Select a ticket from the list, click the **Actions** menu and click **Delete**. This option deletes the ticket record.
Secureworks Ticket updates

This shows the standard ticket fields and tracks changes to the tickets during every polling interval. This is helpful as you can view any ticket updates directly without navigating to the Secureworks CTP dashboard. Any changes to the values are displayed in the Previous Value and Current Value fields.

<table>
<thead>
<tr>
<th>Ticket ID</th>
<th>Previous Value</th>
<th>Current Value</th>
<th>Ticket Last Updated Time</th>
<th>Last Pulled Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>345461243</td>
<td>v4</td>
<td>v5</td>
<td>2020-08-25 17:19:46</td>
<td>2020-08-25 19:02:05</td>
</tr>
<tr>
<td>345461243</td>
<td>ESC - Health Events</td>
<td>Health</td>
<td>2020-08-25 17:19:46</td>
<td>2020-08-25 19:02:05</td>
</tr>
<tr>
<td>345461243</td>
<td>/api/ticket/v4/tickets/143601238/content</td>
<td>/api/ticket/v4/tickets/143601238/content</td>
<td>2020-08-25 17:19:46</td>
<td>2020-08-25 19:02:05</td>
</tr>
<tr>
<td>345461243</td>
<td>categorizationClass</td>
<td>Health</td>
<td>2020-08-25 17:19:46</td>
<td>2020-08-25 19:02:05</td>
</tr>
</tbody>
</table>

Secureworks Recent Events

Click the Fetch Recent Secureworks Events option under the Related Links to view the most recent Secureworks events.

By default, a maximum number of 50 events will be displayed. You can modify this default setting in the Secureworks Integration Settings.
View the Secureworks tickets and the corresponding security incidents

The imported Secureworks CTP tickets are initially stored in the Ticket Import table. View all the Secureworks CTP tickets that have been imported before any filter conditions are applied.

Before you begin
Role required: sn_si.admin

Procedure
1. Navigate to Secureworks Ticket Ingestion Integration > Secure Ticket Import.
2. You can view all the Secureworks CTP tickets that have been imported before they are aggregated or any filter conditions are applied.
3. Click on a Ticket ID to see the raw ticket data.
4. Navigate to Secureworks Ticket Ingestion > Secureworks Ticket to Task. The Secureworks CTP tickets with their corresponding security incidents are displayed.

Secureworks CTP Master Ticket Closure Notice

Before you close a security incident created by a Secureworks CTP master ticket, you must verify that all child tickets associated with the master ticket are closed.

Before you begin
Role required: sn_si.admin

Procedure
1. Navigate to Secureworks Ticket Ingestion > Secureworks Ticket to Task. The Secureworks CTP tickets with their corresponding security incidents are displayed.
2. Click on the security incident with the `isGlobalParent` field set to `true`.

3. Change the security incident State to Closed, specify the close codes and click Save.
   The following dialog box is displayed.

   ![MASTER TICKET CLOSURE](image)

   This security incident is associated with a Secureworks Master Ticket. A Master Ticket may have one or more child tickets associated with it. Before the Master Ticket can be closed, you must first verify if all the child tickets associated with this Master Ticket are closed.

4. Add a note requesting closure of the Master Ticket in Secureworks and click Submit Request. The Master Ticket is now reassigned to the Secureworks SOC team.

5. Once the request has been submitted, you can close the security incident.

6. Navigate to Application > Module.

**Secureworks CTP integration configuration settings**

Use this option to modify the Secureworks CTP ticket ingestion integration default system properties.

To modify the system properties, log in as a user with the `sn_si.admin` role and navigate to Secureworks Ticket Ingestion Integration > Secureworks Integration Settings.
The default configuration settings are displayed. You can modify these settings if required.

<table>
<thead>
<tr>
<th>System Properties - Secureworks CTP Ticket Ingestion Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secureworks API base URL.</td>
</tr>
<tr>
<td><a href="https://api.secureworks.com">https://api.secureworks.com</a></td>
</tr>
<tr>
<td>Secureworks ticket API version. Integration is certified with ticket API version V4.</td>
</tr>
<tr>
<td>v4</td>
</tr>
<tr>
<td>SecureWorks Sample Ticket Ingestion Flow Timeout (in Seconds)</td>
</tr>
<tr>
<td>120</td>
</tr>
<tr>
<td>Timeout for Secureworks flows that run at the time of scheduled ingestion (in seconds).</td>
</tr>
<tr>
<td>1200</td>
</tr>
<tr>
<td>Import attachments with ticket</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>Fetch enrichment summary and append the information to security incident</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>Timeout for ‘Fetch Attachments Subflow’ (in seconds).</td>
</tr>
<tr>
<td>600</td>
</tr>
<tr>
<td>Number of worklogs to be ingested at the time of incident creation</td>
</tr>
<tr>
<td>25</td>
</tr>
<tr>
<td>Number of security incidents that can be created in 24 hour period.</td>
</tr>
<tr>
<td>1000</td>
</tr>
</tbody>
</table>

Any modified integration settings will be applied during the next polling interval as defined in the profile.

**Security Incident Response integration with Zscaler**

You can use the Security Incident Response integration with Zscaler to easily connect your Zscaler Internet Access (ZIA) logs with the Now Platform, view dashboards, create custom alerts, and improve investigation.

**Request apps on the Store**

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release
notes information for all released apps, see the ServiceNow Store version history release notes.

**Overview**

Zscaler is a secure internet and web gateway product delivered from the cloud. It provides key data points and valuable insights into your enterprise security environment. The Security Incident Response integration with Zscaler easily connects Zscaler Internet Access with your Now Platform instance. Using Zscaler on the Now Platform provides you more insights into your organization’s internet usage, and enhances its security operation capabilities.

**Key features**

This integration includes the following key features:

- Perform a reputation lookup of observables against the global threat library maintained by Zscaler.
- Maintain observables in a block list or allow list on Zscaler.
- Fetch and review sandbox reports from Zscaler for an MD5 hash.
- Create a security incident from Patient 0 alerts that are generated in Zscaler when a user downloads an unknown malicious file.
- Create multiple URL Category lists that act as deny list or allow list as defined in Zscaler.
- Tag Now Platform security incidents to identify the URL Category the observables are added to.
- Configure expiration periods to maintain URL Category list entries size by automatically expiring or removing older entries.
- Enable approval workflow for adding and removing observables from the URL Category lists.
- Link URL Category entries to observable records and security incidents that include threat intelligence results and details about why an entry is blocked.

**Learn about this integration**

<table>
<thead>
<tr>
<th>Document identifier</th>
<th>Document title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zscaler product documentation website</td>
<td>ZScaler Product Documentation website</td>
</tr>
<tr>
<td>ServiceNow product documentation website</td>
<td>ServiceNow Product Documentation website</td>
</tr>
</tbody>
</table>
Get started with Security Incident Response integration with Zscaler

You can activate and set up Zscaler to interface with your Now Platform instance and Security Incident Response product.

Before you begin

Before you can use the Security Incident Response integration with Zscaler, you must download it from the ServiceNow Store.

Review the following setup checklist and verify that you have completed all the tasks for a smooth integration.

Checklist

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign and verify the required Now Platform and Security Incident Response roles.</td>
<td>These roles are required for configuration and verification of the expected results:</td>
</tr>
<tr>
<td>• The admin role installs the integration from the ServiceNow Store and assigns the sn_si.admin role.</td>
<td></td>
</tr>
<tr>
<td>• The sn_si.admin role performs the following tasks:</td>
<td></td>
</tr>
<tr>
<td>◦ Configures the integration.</td>
<td></td>
</tr>
<tr>
<td>◦ Create, activate, and remove URL Category lists.</td>
<td></td>
</tr>
<tr>
<td>◦ Assigns the sn_si.analyst role.</td>
<td></td>
</tr>
<tr>
<td>• The sn_si.analyst role creates entries and works with security incidents.</td>
<td></td>
</tr>
</tbody>
</table>
| Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you configure this integration. | The ServiceNow IntegrationHub Enterprise Pack Installer [com.glide.hub.integrations.enterprise] plugin is required.  
The Security Incident Response plugin (com.snc.security_incident) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and |
<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>activate the other Security Operations applications that are required by the integration.</td>
</tr>
<tr>
<td></td>
<td>Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If these applications are not already installed, you must install and activate each application one at a time in the following order to ensure a smooth installation:</td>
</tr>
<tr>
<td>1.</td>
<td>Security Incident Response Dependency (com.snc.si_dep)</td>
</tr>
<tr>
<td>2.</td>
<td>Security Integration Framework</td>
</tr>
<tr>
<td>3.</td>
<td>Security Support Common</td>
</tr>
<tr>
<td>4.</td>
<td>Security Support Orchestration</td>
</tr>
<tr>
<td>5.</td>
<td>Threat Intelligence Support Common</td>
</tr>
<tr>
<td>6.</td>
<td>Trusted Security Circles</td>
</tr>
<tr>
<td>7.</td>
<td>Security Operations Setup Assistant</td>
</tr>
<tr>
<td>8.</td>
<td>Security Incident Response</td>
</tr>
</tbody>
</table>

Verify the Zscaler versions.

- This integration is supported on Zscaler Internet Access version 1.0 or later.
- This integration is tested with the following Zscaler versions:
  - Zscaler Client Connector for Windows - 3.0
  - Zscaler Client Connector for macOS - 3.0
  - Zscaler Client Connector for Linux - Beta
  - Zscaler Cloud Connector - 6.1
Checklist (continued)

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Verify that you have the required Zscaler permissions and have configured access to the Zscaler Internet Access APIs. | - Verify that you have the admin credentials for Zscaler Internet Access.  
- You must have a valid cloud service API subscription and Zscaler Support must provide your key.  
- API authentication is based on a combination of the API key and Zscaler Internet Access admin credentials (user name and password). |

⚠️ **Note:** For more information on managing the Zscaler Internet Access API keys, view the Zscaler documentation.

Configure access to Zscaler Internet Access APIs

Validate and authenticate the secure connection between the Now Platform instance and the Zscaler server. Retrieve the Zscaler base URL and add an API key to complete the authentication.

**Before you begin**

After Zscaler enables your API subscription for your organization's cloud service, the API key is initially provisioned, enabled, and displayed in the Zscaler Internet Access API key management page along with the base URL. Your organization can only have one API key or token. You must delete the existing key or token before you can add a new one.

The base URL for the API is `${Cloud_Name}/api/v1`. Check the Zscaler cloud name provisioned for your organization and use it to replace `{Cloud_Name}` in the base URI. The following are examples of the base URL:

- example.zscalerbeta.net
- example.zcalerone.net
- example.zcalertwo.net
- example.zscaler.net
- example.zscloud.net
Role required: Zscaler Internet Access admin

⚠️ Note: For more information on Zscaler Internet Access administration portal, view the Zscaler documentation.

Procedure
1. Log in as an admin to the Zscaler Internet Access administration portal.
2. Navigate to Administration > API Key Management.
3. Click Add API Key.
   If you do not see the Add API key option, then delete the existing key. The new API key is immediately valid and displayed in the tab.

Results
Retrieve the base URL and the API key to configure access to Zscaler from the Now Platform instance.

Install and configure Security Incident Response integration with Zscaler
Install and configure the Security Incident Response integration with Zscaler from the ServiceNow Store on your Now Platform instance.

Before you begin
Role required: sn_si.admin

Procedure
1. Download the Security Incident Response integration with Zscaler from the ServiceNow Store and install it.
4. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Zscaler Configuration form</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>Zscaler server name. For example, ZSserver.</td>
</tr>
<tr>
<td>Active</td>
<td>Indicator that the profile is active.</td>
</tr>
<tr>
<td>Order</td>
<td>Flow priority. The value for this field indicates the order that flows are</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Zscaler API URL</td>
<td>The base URL hosting the Zscaler API. For example, <a href="https://example.zscalerbeta.net">https://example.zscalerbeta.net</a></td>
</tr>
<tr>
<td>User Name</td>
<td>Enter the user name for the Zscaler Internet Access admin account.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the Zscaler Internet Access admin account.</td>
</tr>
<tr>
<td>API Key</td>
<td>The API key you obtained from the Zscaler Internet Access administration portal.</td>
</tr>
</tbody>
</table>

5. Click **Validate and Update**.
   After the configuration is validated, it is saved and you return to the Zscaler Configurations page.
Add Zscaler Internet Access URL category lists

Zscaler organizes URLs into a hierarchy of categories for granular filtering and policy creation. Add the URL categories available in Zscaler to the Now Platform instance to specify an action for each URL.

Before you begin
Role required: sn_si.admin

About this task
The Security Incident Response integration with Zscaler provides a default allow list and deny list URL category lists. The URL category you add specifies an action for each URL.

The URL categories that you add in the Now Platform instance should already be present in your Zscaler environment. You cannot use this integration to create URL categories on Zscaler.

⚠️ Note: For more information on URL Category Lists in Zscaler, view the Zscaler documentation on URL Categories.

Procedure
1. Navigate to ZScaler Integration > ZScaler URL Category Lists.
2. Click New.
3. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Zscaler URL Category Lists form</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>Source</td>
<td>Name of the server. You can only view previously configured Zscaler servers from the list.</td>
</tr>
<tr>
<td>Active</td>
<td>Indicator that the URL Category List is active.</td>
</tr>
<tr>
<td>URL Category</td>
<td>The URL Category field is enabled after you select the Source. You can view the list of URL Categories created in Zscaler. Select the appropriate URL Category.</td>
</tr>
<tr>
<td>Expiration Period (days)</td>
<td>The expiration period of the URL Category List. 0 (by default) indicates</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Display Tag</td>
<td>The security tag that appears on the SIR security incident. When you enable the Display Tag option, Zscaler Tag for observables field is available on the form.</td>
</tr>
<tr>
<td>Create Change Request</td>
<td>Creates a change request and change tasks in your Now Platform instance for the records that are attached to the URL Category List. When you enable the Create Change Request option, the Change Request field is available on the form.</td>
</tr>
<tr>
<td>Require Approval</td>
<td>List of approver groups. After you submit a request, an approval is required from the group to complete the request. When you enable the Require Approval option, the Approvers field is available on the form.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the Zscaler URL Category List. You can use this field for adding more details regarding the URL category record.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

The following illustration shows how to add the URL category list.
A successful submission triggers an email notification to the approval group.
Submit observables from a security incident record for URL category list

Observables attached to a security incident record are submitted to a configured URL Category List using the allow or block request action.

Before you begin
Role required: sn_si.analyst

About this task
Submit observable entries using the Allow or Block request action from the Associated Observables related list. The list of URL Categories configured previously is available for selection to submit the observable. Once you submit the request, an approval request is sent.
Procedure

1. Navigate to Security Incident > Incidents > Show All Incidents.
The following illustration shows, selecting the security incident, selecting the observable, and adding the allow list.
2. Select the security incident that you want to associate with Zscaler allow or block request.

3. Click **Show All Related Lists** and the **Associated Observables** tab. If you do not find any observables, then click **New** to create an observable.

4. Select the observable and then from the Actions menu, click **Allow/Block Request**.

5. In the Allow/Block Request dialog, select an implementation to perform the allow or block request on the selected observable.

6. Click **Submit**.

7. After you initiate the submission, you can view the Work notes to see the status of your submission and the security tags. Click the links for further information on the status of the submission or to analyze the details on the flow-designer.

8. To view the observable, navigate to **Zscaler Integration > Zscaler URL Category List Entries**.
9. In the Zscaler URL Category List Entries page, click and open the observable to view the record. View the record and see the status and activity of the record.

**Approve observables to URL category lists**

Once an observable is added to a URL Category List, any member of an approval group can approve the request for addition to the list.

**Before you begin**
Role required: sn_si.analyst

**Procedure**
1. Navigate to Zscaler Integration > Zscaler Approvals.
2. Select the record you must approve.
3. Click Approve to approve the record.
   - The approvers group receives an email notification for the approval request.
   - Once the approvers click the Approve/Reject link in the email, the status changes.

**Manually submit the security incident to the Zscaler URL category list**

Submit entries directly for observables that are not associated with a specific Now Platform security incident record.

**Before you begin**
Role required: sn_si.admin

**Procedure**
1. Navigate to Zscaler Integration > Zscaler URL Category List Entries.
2. Click New.
3. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Zscaler URL Category Lists Entries form</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Entry Value</td>
<td>The observable name.</td>
</tr>
<tr>
<td></td>
<td>If a matching observable is found, then the rest of the form is automatically filled.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Observable</td>
<td>The value (for example, IP address or hash) associated with the observable.</td>
</tr>
<tr>
<td>Observable Type</td>
<td>Select the observable classification, such as an IP address or file hash.</td>
</tr>
<tr>
<td>URL Category List</td>
<td>Select the appropriate URL Category.</td>
</tr>
<tr>
<td>Source</td>
<td>Name of the server. You can only view previously configured Zscaler servers from the list.</td>
</tr>
<tr>
<td>Incident count</td>
<td>The number of incidents that this observable appears in. This value is automatically updated when the observable is added to another incident manually or through a work flow.</td>
</tr>
<tr>
<td>Active</td>
<td>Indicator that the URL Category List is active.</td>
</tr>
<tr>
<td>Status</td>
<td>Identifies the status if the observable is approved or rejected.</td>
</tr>
<tr>
<td>Expiration Period (days)</td>
<td>The expiration period of the URL Category List. 0 (by default) indicates that the URL Category List entry never expires. If you change this value, any observable added to this URL category is active for the number of days you enter. You can enter a minimum value of 1. For example, if you set the expiration period to 30 days, entries are removed from the category list after 30 days.</td>
</tr>
</tbody>
</table>
### Run threat lookup using Zscaler global threat library

Threat Lookup in the Security Incident Response integration with Zscaler performs a lookup on observables against Zscaler’s global threat library. Zscaler supports lookup against observables type IPs, URLs, and domain.

**Before you begin**

Role required: sn_si.admin

**About this task**

You can perform threat intelligence lookups on one or more observables to determine whether they are associated with known security threats. When an observable is associated with a security incident for the first time, all the active threat lookup implementations in the Now Platform perform an auto-threat lookup. You can view the results against the Threat Look Up Results related list.

In the Security Incident Response integration with Zscaler, by default, the configuration with the least order is picked to perform the threat look-up against Zscaler’s global threat library. You can also perform the threat look-up manually.

**Procedure**

1. Navigate to Security Incident > Incidents > Show All Incidents.
2. Select the security incident that you want to run the threat lookup on.
3. Click Show All Related Lists and the Associated Observables tab.
4. Select the observable and then from the Actions menu, click Run Threat Lookup.

---

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
The following illustration shows, selecting a security incident, selecting the observable, running threat lookup, and viewing the results in the work notes.

After you initiate the threat lookup, you can view the Work notes to see the status of your submission.

Submit to Zscaler Sandbox analysis

Use the Zscaler sandbox service to analyzes files in a virtual environment to detect malicious behavior. The Security Incident Response integration with Zscaler supports fetching of sandbox report for the observable type MD5 hash.

Before you begin
Role required: sn_si.admin

About this task
When you create a Zscaler configuration, a Zscaler sandbox submission configuration is created by default in the Zscaler Sandbox Configuration module. The name and source fields are auto-filled, and the configuration is enabled by default. You can only edit the display tag and the active options. Zscaler supports only fetching of the sandbox report for the MD5 hash type observables. The MD5 hash should have a report already present on the Zscaler sandbox for the integration to fetch the report. This means that the analysis for the file associated with the MD5 hash should have already been complete on the Zscaler sandbox and the corresponding report should be available on the Zscaler sandbox. If the MD5 hash that you send does not have a report on Zscaler, you get an error message.
Procedure

1. Navigate to Security Incident > Incidents > Show All Incidents.
2. Select the security incident that you want to run the sandbox analysis.
3. Click Show All Related Lists and the Associated Observables tab.
4. Select an MD5 hash type observable and then from the Actions menu, select Submit to Sandbox.
   Create an MD5 hash type observable if you do not find an existing MD5 hash type observable.
5. In the File Submission dialog, select the Zscaler - Sandbox Submission - Server option in the Submission configuration and click Submit to sandbox.
   After you initiate the sandbox submission, you can view the Work notes to see the status of your submission. A tag is also appended to the security incident.
6. In the Work notes, click the link in the Sandbox Submission Result post.
   Alternatively, you can view the results from the Show All Related Lists and Sandbox Submission Results.
Setup up email for Patient 0 alerts

When a user download a malicious file, you can configure Zscaler to identify the unknown file and perform a sandbox analysis. A patient 0 event occurs when the unknown file is scanned and found to be malicious. You can set up the Now Platform to receive email alerts at regular intervals for the Zscaler Patient 0 events.

Before you begin
Role required: sn_si.admin, Zscaler Internet Access admin

Procedure
1. Navigate to System Mailboxes > Administration > Email Properties.
2. In the Inbound Email Configuration section, select the option for Email receiving enabled.
3. Click Save.
4. Navigate to System Mailboxes > Administration > Email Accounts.
5. Select the **ServiceNow SMTP** email account.

6. Note the **User name**. The user name identified here is the Now Platform email address that you use to configure in Zscaler for Patient 0 alerts.
7. Login to the Zscaler Internet Access administration portal.

   **Note:** For more information on Zscaler Internet Access administration portal, view the Zscaler documentation.

8. Navigate to **Administration > Alerts > Publish Alerts**.

9. Click **Add Alert Subscription**.

10. On the form, fill in the fields.

    **Add Alert Subscription form**

    | Field         | Description                                      |
    |---------------|--------------------------------------------------|
    | Email         | The Now Platform SMTP account email address.     |
    | Description   | You can use this field for adding more details regarding the Patient 0 Alerts. |

11. Click **Save** and activate your changes.
Shodan integration

Shodan is a search engine that analyzes service banner information from connected devices all around the globe. Service banners include information about a computer system, such as host name, device type, operating system, geographic location, and connected ISP. When integrated with the Now Platform Security Operations product, this service banner information provides analysts with additional enrichment data and insight for security incidents or investigations.

The integration requires the Security Incident Response and Threat Intelligence plugins.

The Shodan integration performs enrichment on the following observables:

- IP addresses
- URLs
- File hashes

The application checks for new observables every five minutes. If the observables are of a type recognized by the Shodan integration, the observables are enriched.

This integration is compatible with the Kingston, London, Madrid, and New York releases of the Now Platform®.

Install and configure Shodan

Before you run the integration on your instance, complete the installation and configuration steps so the Shodan application properly integrates with Now Platform Security Operations.

Before you begin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

<table>
<thead>
<tr>
<th>Setup tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have assigned the required Now Platform roles for your instance.</td>
<td>The following roles are required for installation, configuration, and verification of expected results:</td>
</tr>
<tr>
<td></td>
<td>• The System Administrator (admin) installs the app and assigns the Security Incident Administrator (sn_si.admin) role.</td>
</tr>
<tr>
<td>Setup tasks</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>• The Security Incident Administrator (sn_si.admin) oversees the configuration and verifies the expected results. This role also has access to the Security Operations module.</td>
<td></td>
</tr>
<tr>
<td>Obtain the Shodan API key.</td>
<td>Create an account and obtain the API key from the Shodan website: Shodan website.</td>
</tr>
<tr>
<td>Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration.</td>
<td>For the Madrid release and later family releases, the Security Incident Response Dependency plugin (com.snc.si_dep) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications required by the integration. Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation. 1. Security Incident Response 2. Security Integration Framework 3. Security Support Common 4. Security Support Orchestration For more information on setting up your Now Platform instance for the integration, see Get entitlement for a Security Operations product</td>
</tr>
</tbody>
</table>
Role required: admin

**Procedure**

1. If you have not installed the application for the integration, see Install a Security Operations integration and follow the steps to install it.

2. After the installation completes, navigate to Integrations > Integrations Configurations and locate the Shodan tile.

3. Click **Configure**.

4. In the Shodan Configuration dialog box, enter the API key you obtained from the Shodan website and click **Submit**.

5. Verify successful configuration.
Configuration is successfully completed unless an error message is displayed.

Trouble?
If an error message is displayed during the configuration, the Shodan API key may be invalid.

Verify expected results for Shodan
Observables are generated automatically by a security incident and scanned by the application. Enrichment results are displayed on the Observable Enrichment Results and Network Banners tabs.

Before you begin
Role required: sn_si.analyst.

Procedure
1. Open the security incident you are working with and verify that the lookup has run successfully.

Once the application is configured, the workflow launches automatically upon incident creation. The execution and completion status of the lookup is displayed in the work notes in the security incident.

2. Review the work notes for more information and how to proceed if you cannot verify that the lookup ran successfully.

3. Navigate to the bottom of the security incident and click the Show All Related Lists link in Related Links.

Note: The figures in the following steps are shown with the Tabbed forms setting active in the System Settings. If tabbed forms are not displayed, in the upper-right corner of the banner frame, click the Settings gear icon. In the System Settings dialog box that is displayed, click Forms and verify that Tabbed forms and With the Form are selected.
Results are displayed in the **Observable Enrichment Results** and **Network Banners** tabs at the bottom of the security incident.

4. With the **Network Banners** tab selected, click the blue information icon next to an observable.

5. In the dialog box that is displayed, click **Open Record** to view raw data and more details.

**Trouble?**
If you do not see results under the **Observable Enrichment Results** and **Network Banners** tabs, verify that the observable is a type that is supported for lookup by the integration.

**Optional** Manually attach an observable for Shodan

You can manually attach observables to a security incident. You manually attach observables when you want to perform threat lookups on observables that are not attached to a security incident on the initial event trigger. Also, you might perform this task when you want more information about a related observable.
Before you begin
Role required: sn_si.analyst

Procedure
1. Navigate to Security Incident > Incidents > Show All Incidents and open a security incident to which you want to attach the observable.
2. At the bottom of the record, click the Show IoC link in Related Links.
3. On the Observables tab, click New. The Observable form is displayed.
4. In the Value field, enter an observable (IP address, file hash, or URL).
5. Click the search icon and from the Observable Type Categories dialog box, click the desired observable type in the list to populate the field.
6. Click Submit.
   The workflow launches and checks for the new observable. The execution and completion status is displayed in the work notes section on the security incident record.

7. Navigate to your security incident and review the work notes.

8. At the bottom of the record, click the Show All Related Lists related link.

9. Click the Observable Enrichment Results or Network Banners tabs for results, and click the blue information icon next to an observable for more information on a specific item.
10. In the dialog that is displayed, click **Open Record** to view raw data and more details.

11. Optional: Click the blue settings icon near the search icon to personalize column output and order.

12. In the **Personalize List Columns**, select available settings, move them to the **Selected** column, and click **OK**.

---

**Trouble?**
Review the **Work notes** for more information and how to proceed if you cannot verify that the lookup ran successfully.

---

**ServiceNow Security Operations add-on for Splunk overview**

The ServiceNow Security Operations add-on for Splunk allows a Splunk software administrator to collect data from ServiceNow and create incidents and events in ServiceNow. It is installed from **Splunkbase**.

**Splunk integration setup**

Setup procedures for the ServiceNow Security Operations add-on for Splunk include downloading the add-on file in Splunk, installing the add-on, and setting up the ServiceNow instance where security incidents and events are created.

**Required role**

Before performing Splunk integration setup procedures, be sure to define an integration user with the `sn_si.integration_user` and `sn_si.analyst` roles on your ServiceNow instance. Additionally, in order to perform imports, you need the `import_transformer` role to obtain read and write permission to the security tables. The `sn_si.integration_user` role should be defined with the `import_transformer` portion of the role.
Download the ServiceNow Security Operations application
The first step in setting up the ServiceNow-to-Splunk integration is to download the ServiceNow Security Operations application from Splunkbase.

Procedure
1. Open Splunkbase.
3. Download the application.

Install the ServiceNow Security Operations add-on for Splunk
Install the ServiceNow Security Operations add-on for Splunk to link Splunk to ServiceNow.

Procedure
1. Open Splunk.
2. Click either the Apps gear icon, or the Manage Apps shortcut menu item.
3. Click Install app from file.
4. Click Choose File, select sn_sec_ops.spl, and click Upload.
5. If prompted, restart Splunk.
   The ServiceNow Security Operations add-on for Splunk is installed and ready to be set up.

Set up or change the instance where incidents or events are created
To set up or change the ServiceNow instance where new security incidents and security events are created, use the Setup action in the application list.

Procedure
1. Open Splunk.
2. Click either the Apps gear icon, or the Manage Apps shortcut menu item.
3. In the list of applications, click the Set up action for the ServiceNow Security Operations Integration.
4. Provide the ServiceNow URL, user name, and password. The user name and password are for the integration user created in ServiceNow.
5. Click Save.
Manual search commands

Manual search commands are entered from any Search window. You can create a security incident or event. After the command, there are pairs of field names and values used to create the desired record.

Security event

The security event command, `snsecevent`, creates an event in ServiceNow with the Security classification.

These events can be reviewed on their own, or alert rules within ServiceNow or manual actions can turn an event or collection of events into a security incident.

If the event becomes a security incident and each parameter is sent into the event, this data is used to populate the security incident as follows:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Required</th>
<th>Use</th>
<th>Use in Security Incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>node</td>
<td>Yes</td>
<td>The node represents the server or configuration item for the event. Ideally, this node maps to an existing CI within ServiceNow.</td>
<td>Affected CI, Short description</td>
</tr>
<tr>
<td>type</td>
<td>Yes</td>
<td>The category of event.</td>
<td>Short description</td>
</tr>
<tr>
<td>resource</td>
<td>Yes</td>
<td>The configuration item.</td>
<td>Short description</td>
</tr>
<tr>
<td>source</td>
<td>No</td>
<td>The origination of this data. By default, the Splunk server generates the data.</td>
<td>Activity log</td>
</tr>
<tr>
<td>external_url</td>
<td>No</td>
<td>The drilldown URL to use in External URL accessed via the Drilldown button on the</td>
<td></td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Required</td>
<td>Use</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>----------</td>
<td>----------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>ServiceNow to get back to the Splunk data regarding this event. By default, this URL contains the result link for any alert, or a link to the default Splunk search page.</td>
<td>N/A</td>
<td>Use in Security Incident</td>
<td></td>
</tr>
<tr>
<td>time_of_event</td>
<td>No</td>
<td>The time that the event was logged in Splunk.</td>
<td></td>
</tr>
<tr>
<td>All other values (category, subcategory in the example)</td>
<td>No</td>
<td>Any field that is not part of the information field in the event. If a security incident is created, it is used.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the field exists, and is not populated, the security incident uses that value. For example, the category passed through the Event becomes the category of the new security incident. If a field with this name does not exist, the value is placed in the activity log.</td>
<td></td>
</tr>
</tbody>
</table>

**Security incident**

The Security Incident command, `snsecincident`, creates a Security Incident in your ServiceNow instance.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>short_description</td>
<td>Yes</td>
<td>A short, one line description of the incident.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Required</td>
<td>Use</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>category</td>
<td>No</td>
<td>The category of the security incident. If this category does not exist, it is created.</td>
</tr>
<tr>
<td>subcategory</td>
<td>No</td>
<td>The subcategory. If this subcategory does not exist, it is created.</td>
</tr>
<tr>
<td>cmdb_ci</td>
<td>No</td>
<td>The configuration item for the security incident. Ideally, this item maps to an existing CI within ServiceNow.</td>
</tr>
<tr>
<td>description</td>
<td>No</td>
<td>The longer, detailed description of the incident.</td>
</tr>
</tbody>
</table>

There are many possible useful columns – anything in the Security Incident transform map can be used. If new columns are added to the security incident, they too are used, as long as they are in the transform map. Some useful columns: location, priority, assignment_group, assigned_to, affected_user, attack_vector, and watch_list.

**Splunk event actions**

When reviewing Splunk logs, you can rapidly create security events and security incidents from any item in the log using the Event Actions.

Clicking either of these actions creates a manual search command populated with the data in the log entry, and run it to generate the new record.

These actions are easily configured to add fields in your normalized data. Within Splunk, using **Settings > Fields > Workflow Actions**, you can select and edit either of these actions using the manual search fields.

You can choose where the action is shown, for what fields, and modify the search string that contains a search command to create your record.

**Single-record Splunk alerts**

Within any alert, you can specify security events or security incidents to be created when the alert is fired.

Open or create your alert, and when editing actions, select the type of record you want, and fill in the alert dialog box.
Multiple-record, custom field Splunk alerts

Multi-record alerts (defined using the Create Multiple ServiceNow Security Incidents and Create Multiple ServiceNow Security Events trigger actions) can automatically create records with any set of fields supported.

These act differently from the other alert actions in that default values are provided. However, most of the data comes from the search result for that alert.

**Note:** In previous versions of the add-on and this documentation, scripted alerts were supported. That feature has been deprecated and replaced by these instructions.

Create a multi-record, custom field Splunk alert

To create a multiple record Splunk alert with custom fields, you must build a search that is designed to match the ServiceNow columns you want to populate.

**Procedure**

1. Navigate to Search.
2. In the Search box, create a search that generates your record data. See the examples for recommended search criteria.
3. Click Save As and select Alert.
4. Set the name, permissions, and schedule, as needed.
5. Click Add Actions.
6. Make one of the following selections.
   - To create one event per result from your search, select Create Multiple ServiceNow Security Events.
   - To create one incident per result from your search, select Create Multiple ServiceNow Security Incidents.
7. Set any defaults, as needed.
   
   If the field in the search result is blank or not present, the defaults are used. If there is a value in the result, the defaults are overwritten.

**Multi-record, custom field Splunk alert examples**

When you are creating multiple record Splunk alerts with custom fields, you need to define search criteria for generating alert data. Examples of search criteria for security incidents and security events are shown.
Security incident search
For a security incident, this criteria builds a search to fill in columns in the security incident table.

```
host=Development source="/CodeArchive/password/password_decrypt.cpp" |
eval contact_type="Monitoring" |
eval cmdb_ci=host |
eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```

Security event search
For a security event, this is the same search, but it populates Event fields instead. If this event is turned into a security incident, and any fields that do not exist in the event are populated, they are transferred to the security incident. Otherwise, they remain in the additional information field of the event and alert.

```
host=Development source="/CodeArchive/password/password_decrypt.cpp" |
eval type="Monitoring" |
eval node=host |
eval source=source

eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```

⚠️ Note: The search criteria you use will add as many records as are found in the search. It may add 5 or 10,000,000,000 records. So this is NOT a recommended method for the bulk transfer of data. The intent of this method is to add one record per REST call into the ServiceNow instance.

Splunk error reporting
Whenever a connectivity issue with your ServiceNow instance occurs, an error is logged in Splunk with information describing the problem.

Error messages are stored in a new index named servicenow with sourcetype servicenow.

To search for error logs, ensure you are specifying the servicenow index in your search. Alternatively, refer to the current Splunk documentation on how to add the new servicenow index to the default search indexes.
Splunk Enterprise Event Ingestion integration for Security Operations by ServiceNow

The Splunk Enterprise event and alert data integration with the Security Incident Response (SIR) product allows security incident analysts to collect and process security logs and related event data. Data is collected in real-time, and it is used by analysts to identify and report on potential cyber threats. The security events that are collected can be processed into triggered alerts that are ingested automatically with this integration. Also, individual security events can be manually forwarded on-demand from the Splunk Enterprise search and reporting interface into the Security Incident Response product of the Now Platform to create security incidents.

Overview

This integration provides a security operations center (SOC) analyst with visibility to events and related alert data. This data can be integrated into Now Platform Security Incident Response (SIR) security incidents for further investigation and remediation. Profiles for Splunk ongoing ingested alerts and forwarded events are created in your Now Platform instance. These profiles customize how different Splunk alert and event fields are displayed on SIR security incidents. A default mapping of alert fields is provided that can be edited and augmented to meet customer-specific needs.

Key features

This integration includes the following key features:

- Create multiple alert ingestion profiles to create SIR security incidents for specific types of threats such as phishing and malware.
- Create multiple event profiles for on-demand event forwarding from your Splunk console to create SIR security incidents.
- Drag-and-drop mapping of Splunk alert and event field values to associated SIR security incident fields.
- A preview of the SIR security incident layout based on sample alerts or events to validate profile configuration.
- Ingest historical alerts as well as ongoing, future alerts on configurable intervals.
- Aggregate events or alerts to existing SIR security incidents based on matching field values to avoid duplicate security incidents.
**Supported Now Platform versions**

This integration supports the Kingston, London, Madrid, and New York Now Platform releases.

Madrid release and later family releases

For the Madrid release and later family releases, the com.snc.si_dep plugin is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before installing and activating the other Security Operations applications.

The following Security Operations applications must be installed and activated from the ServiceNow Store. Install and then activate one application at a time in the order listed below to ensure a smooth installation:

1. Security Integration Framework
2. Security Support Common
3. Security Support Orchestration
4. Security Incident Response

For more information about installing the Security Operations core applications, see [Get entitlement for a Security Operations product or application](#) and [Activate a ServiceNow Store application](#).

**ServiceNow Addons**

The ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise is required only if you prefer to forward events manually from your Splunk Enterprise console into your Now Platform instance. This ServiceNow addon is available in splunkbase.

This ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise application in splunkbase is not required for the automated alert ingestion that is supported by the integration.

**Splunk Supported versions**

This integration supports version 6.0 or later of Splunk Enterprise. The integration also supports the Splunk Enterprise Cloud service.

**MID Server**

This integration requires an installed and configured MID Server in your Now Platform® instance to connect to the Splunk service if the Splunk server is deployed within your corporate network. If you are using the Splunk
Cloud service, a MID Server is not required. See the ServiceNow Product Documentation website for more information about MID Servers.

**References**

<table>
<thead>
<tr>
<th>Reference</th>
<th>Document Identifier</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Splunk product website</td>
<td>Splunk product website.</td>
</tr>
<tr>
<td>2</td>
<td>ServiceNow Product documentation website</td>
<td>ServiceNow Product Documentation website</td>
</tr>
</tbody>
</table>

**Integration architecture and systems connection**

For more information about the architecture of the integration including key terms and external systems connection details, see Integration architecture and external systems connection for the Splunk Enterprise Event Ingestion integration.

**Checklist**

For a printable checklist of these topics, see Checklist for the Splunk Enterprise Security Notable Event Ingestion integration. You can use this list to monitor your progress as you work through the tasks of the integration.

The images used in the following topics were generated for the Kingston release of the Now Platform. For information about the London user interface, see Managing security threats using the Security Analyst Workspace on the ServiceNow Product Documentation website.

The following topics are numbered. Follow the topics listed below in the order that they are presented for a smooth installation and configuration of the application.

**Set up your Now Platform® instance for the Splunk Enterprise Event Ingestion integration**

The following section lists the setup tasks that you are required to complete in your Now Platform® instance prior to installing the application from the ServiceNow Store.

**About this task**

Refer to the following table and verify that you have completed all the listed tasks before you download and install the application to ensure a smooth installation and configuration.

Role required: admin
<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have assigned the required Now Platform® and Security Incident Response (SIR) roles.</td>
<td>The following roles are required for the installation, setup, and use of the integration in your Now Platform® instance.</td>
</tr>
<tr>
<td>• A user with the Now Platform® administrator role (admin) installs the application from the ServiceNow Store and assigns the security incident administrator (sn_si.admin) role.</td>
<td></td>
</tr>
<tr>
<td>• If you want to forward events manually from Splunk Enterprise for this integration, a user with the Now Platform® admin role assigns a user with the (sn_sec_splunk_v2.api_account_access) role in the Now Platform®. This role permits a user with the Splunk Enterprise administrator role to access the API in the Now Platform® that is required for manual event forwarding for this integration. The (sn_sec_splunk_v2.api_account_access) role is not required for the integration if you are ingesting alerts automatically from Splunk Enterprise into your Now Platform® instance.</td>
<td></td>
</tr>
</tbody>
</table>
| • A user with the sn_si.admin role oversees the following tasks in the Now Platform®: | }
<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
</table>
| ◦ Previews security incident details for accuracy prior to finalizing the configuration.  
◦ Schedules on-going alert ingestion.  
◦ Assigns the security incident analyst (sn_si.analyst) role.  
◦ Users with the sn_si.analyst work with security incidents. | For more information about roles and assigning roles to users, see Roles on the Servicenow Product Documentation website. |
| Verify that you are using version 6.0 or later of the Splunk API. Earlier versions are not supported. | If you have access to the Splunk Enterprise console, you have access to the API that is required for this integration. There is no other special setup required for the API. |
| Verify that you have installed and configured a MID Server. | Configured MID Server  
A MID Server in your Now Platform® instance is required to connect to the Splunk service if the Splunk server is deployed within your corporate network. See the ServiceNow Product Documentation website for information about MID Servers.  
If you are using the Splunk Cloud service, a MID Server is not required. |
| Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration. | Madrid and later release requirements  
For the Madrid release and later family releases, the Security Incident Response Dependency plugin (com.snc.si_dep) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and |
### Setup task

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>activate this plugin before you install and activate the other Security Operations applications required by the integration. Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation. 1. Security Incident Response 2. Security Integration Framework 3. Security Support Common 4. Security Support Orchestration For more information about installing the Security Operations core applications, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.</td>
</tr>
</tbody>
</table>

### What to do next

You have successfully set up your Now Platform® instance for the integration. The next step is to install the Splunk Enterprise Event Ingestion application from the ServiceNow Store for the integration. For more information, see Install and configure the ServiceNow application for the Splunk Enterprise Event Ingestion integration.

If you have not saved searches in your Splunk Enterprise console for ingestion, or if you are performing the initial setup for this integration in your Splunk Enterprise console and the Security Operations product of your Now Platform® instance simultaneously, see (Optional) Save searches in your Splunk Enterprise console for the Splunk Enterprise Event Ingestion integration for more information.

If you want to export events manually and on-demand from your Splunk Enterprise console for the integration, see (Optional) Set up your Splunk environment for manual event ingestion for the Splunk Enterprise event ingestion integration for more information.
Install and configure the ServiceNow application for the Splunk Enterprise Event Ingestion integration

Before you run the integration on your Now Platform® instance, complete these installation and configuration steps so the application properly integrates with the Security Incident Response and Security Operations products on your Now Platform® instance.

**Before you begin**
Role required: admin

**Procedure**

1. If you have not installed the Splunk Enterprise Event Ingestion application from the ServiceNow Store for the integration, see [Install a Security Operations integration](#) and follow the steps to install it.

2. After you have successfully installed the application, navigate to Integrations > Integrations Configurations and locate the Splunk Event Ingestions tile.

3. To configure the application, click **New**.

4. Alternatively, if a **Configure** button is displayed on a tile, click it to edit an existing configuration.

5. In the Event Ingestions Configuration dialog that is displayed, fill in the fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Splunk Enterprise console or Splunk Cloud instance used for the integration.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Splunk API Base URL</td>
<td>URL for your Splunk Enterprise console or Splunk Cloud instance.</td>
</tr>
<tr>
<td>API Account User Name</td>
<td>User name that you created for your individual user account on the Splunk Enterprise console.</td>
</tr>
<tr>
<td>API Password</td>
<td>Password that you created for your individual user account on the Splunk Enterprise console.</td>
</tr>
<tr>
<td>MID Server</td>
<td>Specific MID Server that is set up in your environment. Only MID Servers that are active and validated are available from this choice list.</td>
</tr>
</tbody>
</table>

**On Premises Deployment**

Default is disabled.

If you are using the cloud-based version of Splunk Enterprise, verify that the check box is cleared.

If this option is enabled, the MID Server choice list is displayed. If you are using an on-premises version of Splunk Enterprise, follow these steps to select a MID Server.

a. Select the check box.
   A choice list is displayed. Default is **Any**.

b. Select **Any** only if this MID server is configured for the Splunk Enterprise Event Ingestion integration.

c. From the choice list, select the Now Platform® MID server that you configured in your instance for this specific integration.
The following figure is an example of a completed form for a configuration of an on-premises version of Splunk Enterprise with a MID Server.

Each Splunk Enterprise alert that you ingest from your Splunk Enterprise console requires a unique event profile in your Now Platform® instance. However, the source that you configure on the Event Ingestions Configuration form can be reused for multiple Now Platform® profiles as long as each profile ingests unique Splunk triggered alerts.

6. Click **Submit**.

After validation is successfully completed, the Security Integrations page is displayed with each of your configurations. On each valid configuration tile, **Configure** and **Delete** buttons are displayed as shown in the following figure.
After it is successfully validated and submitted, each Event Ingestions Splunk server configuration is saved on the Security Integrations page as a tile. If your saved configuration tiles are not displayed on the Security Integrations page, on the top right corner of the page, from the Show Configurations choice list, click Yes.

Trouble?
If an error message is displayed after you click Submit, enter your information again and click Submit.

What to do next
You have successfully installed and configured the application. The next step is to create an event profile.
Create and name an event profile for the Splunk Enterprise Event Ingestion integration

As a user with the sn_si.admin role, you create an event profile in your Now Platform instance and determine which Splunk alerts create security incidents. Before Now Platform Security Incident Response (SIR) security incidents are created from ingested alerts, the field values from alerts are displayed on a layout of a Now Platform security incident so that you can preview how the actual security incident will be displayed.

About this task
From an integration perspective using available APIs, Splunk events are forwarded individually and manually as discreet events, or they are combined into triggered alerts that are automatically ingested into the Security Operations environment of your Now Platform instance. The integration workflows ingest different types of alerts such as unauthorized access attempts and malware, for example. These alerts are ingested based on the profiles that you configure in the Security Operations environment of your instance. All alerts are initially ingested for a configured alert type in a profile. Ingested alerts can then be further filtered to specify which alerts create security incidents. For example, you may prefer filters that create security incidents only for alerts that are identified as high-risk. Before a profile is activated, and it creates security incidents from ingested alerts, individual field values on the filtered alerts are mapped to corresponding fields on a layout of security incident for a preview.

Alert names for event profiles in your Now Platform instance must be unique and can only be mapped to one active event profile at any given time. These are the triggered alert names that you configured in your Splunk service as part of the setup for the integration. For more information about configuring alerts in your Splunk Enterprise environment, see (Optional) Save searches in your Splunk Enterprise console for the Splunk Enterprise Event Ingestion integration.

The Now Platform ingests specific alerts using the workflows of the integration. All alerts that meet the selection criteria in your Splunk enterprise console are initially ingested into your Now Platform instance.

A profile in your Now Platform is an encapsulation of a Splunk alert in your Splunk enterprise console. There is a one-to-one relationship between alerts that are ingested with a profile and connections to your Splunk enterprise console: one alert for one connection. There is a single https connection to a search head in your Splunk Enterprise console. Multiple alerts can come from a single search head. If you connect to multiple search heads in your Splunk Enterprise console, you must create multiple profiles in your Now Platform instance to ingest these alerts.

Role required: sn_si.admin

© 2021 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Steps to create profiles for scheduled alert ingestion

Procedure
1. To create an event profile for an alert, in your Now Platform instance, navigate to Splunk Integration > Splunk Event Profile.
2. If the Splunk Event Profile form is not displayed, click Name in the Progress bar.
3. Click New.
4. Fill in the fields.
   An example of a completed form follows the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the profile. If names are not unique, duplicate profile names are not saved. Profile names in your Now Platform instance must be unique.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box is cleared by default. If this option is disabled, the profile is not active. If this check box is selected and the option is enabled, this profile is not active until you complete all the profile configuration steps and click Finish.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the profile type from the choice list.</td>
</tr>
<tr>
<td></td>
<td>• Scheduled Alert Ingestion - This type of profile supports triggered alerts that are ingested on a schedule that you configure. Fill in the fields and click Continue to proceed to the Alert Selection step of the profile.</td>
</tr>
<tr>
<td></td>
<td>• Manual Event Forwarding - This type of profile supports individual events that are forwarded manually from your Splunk Enterprise con-</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sole on demand. See the following steps to fill out the form for these types of profiles.</td>
<td></td>
</tr>
<tr>
<td>Source Type</td>
<td>Splunk server or search end that you configured to ingest alerts. If you have multiple Splunk servers configured, select the appropriate server for the alert types that you are planning to ingest for the profile. You are required to enter a value.</td>
</tr>
<tr>
<td>Order</td>
<td>Default is 100. Leave this setting at the default. If you have created multiple profiles, this value provides a run time execution priority when two or more profiles share the same triggering conditions. The workflow in the profile with the lowest number has the highest priority.</td>
</tr>
<tr>
<td>(Optional) Description</td>
<td>Text to help you distinguish this profile from other profiles.</td>
</tr>
</tbody>
</table>

The following figure is an example of a completed form for a scheduled alert.
5. For a profile with a scheduled alert, choose one option to continue with the profile configuration.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continue</td>
<td>Save the profile and progress to the Alert Selection step.</td>
</tr>
<tr>
<td>Update</td>
<td>Save updates to this profile and return to the Splunk Event Profiles list.</td>
</tr>
<tr>
<td>Save</td>
<td>Save this profile and remain on the page.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete this profile record and return to the Splunk Event Profiles list.</td>
</tr>
</tbody>
</table>

Steps to create profiles for manual event forwarding

6. To create a profile that supports manual event forwarding, follow these steps.

For events that you forward on-demand from your Splunk enterprise console, you can base the individual field mapping on any existing profile. Alternatively, you can create a new mapping grid for exported attachment data. Events that you forward manually are not scheduled in the event profile.

a. If not already selected, in the choice list for the Type field, select **Manual Event Forwarding**.

b. In the Mapping Option field that is displayed, from the choice list, choose one mapping option to continue.

Refer to the following figures and tables for more information about the available mapping options in the Mapping Options choice list.
Create new field mapping option

Two different profiles are supported. Ongoing alert ingestion profiles will query the Splunk source on a periodic basis to ingest new alerts and map the alert field values as specified in the profile field mapping. Manual event forwarding will allow for forwarding individual events on an on-demand basis and map events based on expected field values specified in the profile field mapping. If you are creating a manual field mapping you can use any existing profile as the basis to create the individual field mapping or create a new mapping from scratch using the output of an imported Splunk event.

<table>
<thead>
<tr>
<th>Type</th>
<th>Manual Event Forwarding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mapping Option</td>
<td>Create new field mapping</td>
</tr>
<tr>
<td>Default profile</td>
<td>✓ Source Type</td>
</tr>
<tr>
<td>Order</td>
<td>100</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
</tbody>
</table>

Create New field mapping option

<table>
<thead>
<tr>
<th>Option or field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create new field mapping option</td>
<td>New field mapping for your event. If you do not have an existing field mapping that is similar to the profile that you are creating, select this option to create a new map.</td>
</tr>
<tr>
<td>Default profile</td>
<td>Default event forwarding profile for all Splunk events. Default is cleared (disabled). When this option is enabled, this profile becomes the default profile for manual event forwarding. This profile is the only profile that is active and used for every Splunk event field mapping to a SIR security incident. One profile fits all forwarded events. The Source field is unavailable if the default profile option is enabled.</td>
</tr>
<tr>
<td>Source type</td>
<td>Splunk server. This field is unavailable if the default profile option is enabled.</td>
</tr>
<tr>
<td>Option or field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>If available, the Source Type option permits unique event field mapping to security incident fields based on the Splunk source type. If you want to manage firewall log events differently than endpoint detection events, and they have different Splunk source types, you can create different event profiles based on source types to accomplish this requirement.</td>
<td></td>
</tr>
<tr>
<td>Order</td>
<td>Default is 100. Leave this setting at the default. If you have created a large number of profiles, this value provides a run time execution priority when two or more profiles share triggering conditions. The workflow in the profile with the lowest number has the highest priority.</td>
</tr>
<tr>
<td>(Optional) Description</td>
<td>Text to help you distinguish this profile from other profiles.</td>
</tr>
</tbody>
</table>

For a profile with a new field mapping, verify that you have entered a value in the Source type field and click **Continue** to proceed to the mapping step of the configuration.

For a profile with an existing field mapping, refer to the following figure and table for more information.
Select existing profile for field mapping option

Two different profiles are supported. Ongoing alert ingestion profiles will query the Splunk source on a periodic basis to ingest new alerts and map the alert field values as specified in the profile field mapping. Manual event forwarding will allow for forwarding individual events in an on-demand basis and map events based on expected field values specified in the profile field mapping. If you are creating a manual field mapping you can use any existing profile as the basis to create the individual field mapping or create a new mapping from scratch using the output of an imported Splunk event.

<table>
<thead>
<tr>
<th>Option or field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Select existing profile for field mapping | An existing field mapping for your event. The Copy from profile field is displayed. Follow these steps to copy an existing field mapping for this profile. 

i. To the left of the Copy from profile field that is displayed, click the search icon.

ii. In the Splunk Event Profiles list that is displayed, click the profile name that has the map that you want to copy.

The profile name is displayed in the Copy from profile field. |
<p>| Default profile | Default event forwarding profile for all Splunk events. Default is cleared (disabled). When this option is enabled, this profile becomes the default profile for manual event forwarding. This |</p>
<table>
<thead>
<tr>
<th>Option or field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile</td>
<td>profile is the only profile that is active. It is used for every Splunk event field mapping to a SIR security incident. One profile fits all forwarded events. The Source field is unavailable if the default profile option is enabled.</td>
</tr>
</tbody>
</table>
| Source type    | Splunk server.  
This field is unavailable if the default profile option is selected.  
If available, the Source Type option permits unique event field mapping to security incident fields based on the Splunk source type.  
If you want to manage firewall log events differently than endpoint detection events, and they have different Splunk source types, you can create different event profiles based on source types to accomplish this requirement. |
| Order          | Default is 100. Leave this setting at the default.  
If you have created multiple profiles, this value provides a run time execution priority when two or more profiles share triggering conditions. The workflow in the profile with the lowest number has the highest priority. |
| (Optional) Description | Text to help you distinguish this profile from other profiles. |

At the bottom of the form for selecting an existing mapping for your profile, click **Finish** to complete the profile configuration.
What to do next
You have successfully completed the steps to create profiles for both scheduled alerts and manual event forwarding. For profiles for manual event forwarding, you have completed the profile configuration. The next step is to load attachment data in the mapping step. For profiles for scheduled alerts, the next step is to select alerts for automatic ingestion.

Select scheduled alerts for the Splunk Enterprise Event Ingestion integration
After you have created a profile for a scheduled alert, select a Splunk alert for this profile that you want to map to a Now Platform Security Incident Response ((()) security incident.

About this task
As a user with the security sn_si.admin role, view the available alerts in your Now Platform instance so you know which field values are available for mapping. Select an alert to verify that you receive the expected results on the basic form layout before you map the values to fields on SIR security incidents. You can only select one alert from the list in this form.

Role required: sn_si.admin

Procedure
1. If the Alert Selection page is not displayed, select it on the progress bar to display it.

2. By default, the core Search & Reporting App is selected. If the alert to be ingested is part of a different Splunk app, select Splunk App Selection and choose your Splunk app from the Selected App list.

3. From the Alert List, choose an alert and move it to from the Available column to the Selected column. You can also choose multiple alerts. If the alerts are selected as part of a single profile, then the alerts will have common field mappings and profile settings.

The list of alerts on this form matches the list of alerts in your Splunk console. Up to 500 alerts are displayed on this form. If there are more than 500 alerts listed in your Splunk console on the Alerts page, only the first 500 alerts are displayed on this form in your Now Platform instance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the Alert List search field, enter text.</td>
<td>The column below the search field is filtered with available options based on the text that you enter. Select an</td>
</tr>
</tbody>
</table>
### Option | Description
--- | ---
In the Alert List, double-click an Alert. | The **Selected** column is populated with your selection.
In the Alert List, single-click an alarm rule. | The alarm is selected. With the arrow keys, move the selected alert from **Available** to **Selected**.

#### Option

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Continue, or alternatively, click Mapping in the progress bar</strong></td>
<td>The Mapping form is displayed. <strong>Mapping</strong> is selected on the progress bar. The next step is to map alert fields to a SIR security incident.</td>
</tr>
<tr>
<td><strong>Update</strong></td>
<td>Your data is saved and the Splunk Event Profiles list is displayed.</td>
</tr>
<tr>
<td><strong>Previous</strong></td>
<td>The <strong>Name</strong> step is displayed.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete this event profile and the Splunk Event Profiles list is displayed.</td>
</tr>
</tbody>
</table>

You have successfully selected an alert for a scheduled alert profile. The next step is map alert values to fields on a security incident.

**Mapping alerts and events for the Splunk Enterprise Event Ingestion integration**

After you identify the sources for scheduled alert ingestion or manual event forwarding, the next step is to map individual event fields to the fields on a Now Platform Security Incident Response (SIR) security incident.

**Overview**

For the mapping step, as a user with the sn_si.admin role, you ingest sample alerts from your Splunk Enterprise console, or you export event data for a Splunk Enterprise event.

The following figures are examples of the default mapping grids that are provided for each type of event profile. This default mapping can be edited. This modification allows you to customize the fields that populate the security incident. With the mapping step, you can visualize how adding or removing event fields impacts the SIR security incident field values.

Select the **Alert Name**, and after you click to **Fetch Sample Data**, the Splunk alert field values are populated on the left side of the form when sample alerts are ingested by the profile. These are the Splunk alert fields that you map to the SIR security incident fields.
After you click to load attachment data for forwarded events, the Splunk event fields are populated on the left side of the form. These are the Splunk data fields that are mapped to the SIR security incident fields.
You may prefer to review a few sample alerts on your Splunk console to ingest for the field mapping configuration step. This step is labeled Mapping on the progress bar. If this page is not displayed, click Mapping on the progress bar.

Mapping alerts and exporting events on-demand from your Splunk enterprise console includes the following concepts and tasks:

- Fetch Sample data for automatically ingested alert profiles. After data is fetched (pulled) from a fired alert on the Splunk Enterprise console, available alert fields and their corresponding values are displayed in a default mapping layout on the left side of the mapping form. Tabs are displayed for you to view the values for an alert ID that you pulled. Verify that all the critical fields from the Alert Sample Ingestion section on the left of the form are mapped to the grid on the right of the form.

- If required, load event sample data for any manually forwarded event profiles. Sample data for these events is exported in a .xml file from the Splunk Enterprise console and loaded into your Now Platform® instance. The imported data is displayed in the Alert Sample Ingestion section on the left of the form.

- Edit the mapping configuration by dragging alerts from the left side and dropping them on the mapping grid on the right. The mapping grid on the right associates the incoming alert field with an outgoing security incident field.

- Customize the mapping grid by adding or removing fields. Track overlooked or duplicated fields with the color coding that is provided.

- Set filter conditions so that you can specify which alerts are ingested into the SIR application, and which alerts are filtered out.

- Define additional incident field criteria that aggregates an incoming alert to an existing SIR security incident to prevent duplicate incidents. This additional filtering can reduce the number of active, overlapping security incidents by placing all related security event data on a single security incident.

- In certain cases, event field values in the Splunk Enterprise console may not translate directly to the fields on the SIR security incident. For these values, you can use a script editor to format field values on the security incident during the mapping step. Use the script editor if you want to format values that are similar, but not identical. For example, with the script editor, the Malware Alert and Virus Infection field values in the Splunk console both translate to Malicious Code Activity in the Category field on the SIR security incident.

Scheduled alert profiles

After creating a scheduled alert profile, the process flow for the configuration is shown in the following figure.
Process flow for scheduled alert profiles

![Flowchart for scheduled alert profiles]

Manual Event forwarding profiles

After creating a profile for an event, the process flow for the configuration is shown in the following figure.

Process flow for event profiles

![Flowchart for event profiles]

The next step is to ingest triggered alerts or export data and map values to the SIR security incident fields.

Map alerts for the Splunk Enterprise Event Ingestion integration

During the event field-mapping step, you map individual event fields from triggered alerts or imported event data to fields on a Now Platform Security Incident Response (SIR) security incident. The preconfigured mapping grid of the default security incident fields can be edited. The color-coding of the event fields helps you monitor the field values that you have already mapped. This step helps you visualize how your edits impact the fields on the security incident.

About this task

As a user with the sn_si.admin role, map up to five alerts from the Alert Sample Ingestion column on the left of the form to the security incident fields in the SIR Incident Field Mapping column on the right.
Create custom maps by adding or removing the fields on the mapping grid on the right side of the form. Customizing the fields permits you to map Splunk fields that are not displayed on the default-mapping grid on the SIR security incident.

Role required: sn_si.admin

Procedure

1. If the mapping form is not displayed, click Mapping on the progress bar.

2. For a profile with a scheduled alert, below Alarm Sample Ingestion, select the alert in the Alert Name and click Fetch Sample Data to pull the latest instance of a fired alert from the Splunk Enterprise console.

The alerts are displayed as tabs. You can ingest up to five of the most recent alerts.

The pull for sample events may take a few moments. A message indicating that the transaction is working is displayed at the top of the screen.

Note: An additional mapping field, Splunk Alert Name, is added by the integration to allow for tracing an event to the source alert rule in Splunk. This may be helpful in scenarios where multiple Splunk alerts are combined into a single profile.

When a single field contains multiple values, those values are parsed and mapped to individual field entries on the SIR incident field mapping section. For example, the source IP addresses, asset names, or URLs may have multiple observable field entries or multiple CIs, those are parsed and mapped to individual field entries on the SIR incident field mapping section.

In the following figure, the field-name value pairs for the ingested alert, or the imported sample event, are displayed on the left side of this form after the pull is completed. These values are the values that you map to the security incident fields on the SIR Incident Field Mapping side of the form.
3. For scheduled alert profiles, proceed to step five to map the values.

**Steps for manual event forwarding**

4. Alternatively, for a profile for an event type that you want to export from your Splunk Enterprise console, follow these steps to upload attachment data in your Now Platform® instance.

   a. If not already logged in, log in to your Splunk Enterprise console.

   b. Navigate to the Search tab and enter a name for a search that has the event data that you want to export.

      For example, malware is a search term used for all malware events that you can forward with the workflow of this integration.

   c. Expand the event, and in the Field column, select the fields that you want to import.

      These fields are the field-value pairs that are exported and displayed on the Mapping page in your Now Platform® instance.

   d. In your Splunk Enterprise console, in the upper right of the Search page, click the Export icon.

   e. In the list for the Format field in the dialog that is displayed, click XML Format.
f. Optional: Enter a new filename.

g. Click Export.
The file is downloaded to your Now Platform® instance.

h. If the Mapping page is not already displayed in your Now Platform® instance, click Mapping in the progress bar.

i. In the Alert Sample Ingestion column, click Load Attachment Data.

![Image of the mapping form]

j. In the dialog that is displayed, click Choose files and navigate to the .xml file that you exported and click Open.
The value pairs for the fields that you exported for the event are displayed on the left side of the mapping form.

In the following figure, the data pairs for an ingested scheduled alert are displayed on the left side of this form. Value pairs for imported events are also displayed on this side of the form. These values are the field values that you map to the security incident fields on theSir Incident Field Mapping side of the form.

5. To map a field value from the left side of the form to a field on the security incident on the right side of the form, click-hold a blue field name on the left side of the form.
6. Drag the field name, for example, `category`, and drop it on a field in the `Input Expression` column next to a field name in the `Security Incident` column.

The field value is displayed in the `Input Expression` column. In the following image, `category` is mapped to the `category` field on the security incident. However, you can match any value from the left side to a field on the right. Verify that the value is mapped correctly on the security incident during the preview step.

To help you ensure that no events are overlooked or duplicated in the mapping process, fields are color-coded. Light blue fields on the left indicate that a field is not yet selected and mapped on the security incident. You may prefer to associate an incoming alert field with more than one field on a security incident.

A gray field indicates that a field has been selected and mapped to a field on the security incident. This color-coding helps you track the mapping, because in certain cases, alert event fields may only be assigned once. For instance, you can only assign values to fields such as `Short Description` once. However, you can assign list fields such as `Work Note` multiple times by adding additional rows to the mapping grid.
7. To add fields to the default mapping of the security incident on the right side of the form, follow these steps.

a. On the right of the form in the SIR Incident Field Mapping section, at the bottom of the grid, click the plus icon.

```
<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>${destination}$</td>
<td>Priority</td>
</tr>
<tr>
<td>${destination_ip}$</td>
<td>Configuration item</td>
</tr>
<tr>
<td>${dest_ip}$</td>
<td>Configuration item</td>
</tr>
<tr>
<td>${host}$</td>
<td>Observable</td>
</tr>
</tbody>
</table>
```

A new field is displayed.

b. In the Security Incident column, expand the list that is displayed, and select a field.

In the expanded list for the new field, some fields are shaded. In the following figure, Category has a gray background, because it has been mapped in the security incident. Similar to the color-coding for alert fields on the left side of the form, this color-coding for the security incident fields on the right helps you track the mapping.

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Note: So that multiple observables can be displayed on the same security incident, the Observable field can be mapped multiple times with different values. Similarly, the Configuration Item and Work notes fields support multiple values. If you try to map two values to a field that cannot support multiple values, when you preview the incident, an error message is displayed that there is no value for the field. Similarly, if a field on a security incident has a list from which you can choose multiple options, and you try to map an option to that field that is not displayed on the list, the field is not populated on the security incident.

c. Alternatively, type a value in the Search field for the new row.

d. From the left side of the form, left-click to select the Alert ID that you want in the Input Expression field. With the drag feature, map it next to your new field.

8. Continue mapping by adding or removing fields and adding values to the map.
The following figure is an example of an edited mapping grid. In the bottom field on the right, the Work notes field is added, and it has more than one value. The values are separated by spaces and punctuation marks: 

Category: ${category} | destination IP:78.146.73.180
In the preview, these values are displayed in the Work notes on the security incident. Because the value is for a field that you added to the grid, and there are multiple values mapped to the Work notes field, the values are displayed as entered. In this example, the spaces and punctuation marks that you entered in the field are displayed on the Related Items section as a work note on the preview of the security incident.

The following image is an example of how the values in the preceding image are displayed on the security incident.

**Incident generation filtering conditions**

9. **Optional:** After you have completed the preceding field-level mapping steps, you can use the same field values in the Filter conditions builder to define additional criteria that an incoming alert must satisfy to create a SIR security incident. To set filtering conditions, follow these steps.

   a. Scroll to the Incident Generation Conditions section on the form and select the **Filter based on conditions** check box to enable the option.

   (Optional) The Filter conditions builder is displayed. Use these filters to create security incidents that match the specific conditions described by the fields.

   The options in the lists for the first field in the Filter conditions builder match the fields that are displayed on the Alert Sample Ingestion section for the alert you ingested. These fields are dynamic and change depending on the Splunk alert that you ingest, or the event that you manually forward. Criteria that you enter are case-sensitive, and they must match exactly the values of the Splunk Enterprise alert or event. If you are not sure about the values to enter in the filter fields, you may prefer to return to your Splunk Enterprise console and review your alerts and events for the keywords.
b. Using the lists and fields of the conditions builder, set filters for the first row.

c. To add more conditions, to the right of the fields, click **AND** or **OR**.
   If **AND** is selected, all conditions must be matched. If **OR** is selected, either condition can be matched.

d. **Optional:** In the second row, set a second filter condition.
   (Optional) The following image is an example with two conditions that must be matched before security incidents are created.

(Optional) You have set the triggering conditions so that security incidents are created only when both of the filtering conditions that you entered are matched.

This type of filtering helps you isolate security events, and it limits the number of security incidents that you create. If additional filtering criteria are set, only alerts that are required are ingested without having to change the Splunk query or the triggered alert configuration.

**Aggregation Alerts to Prevent Duplicate Incidents**

10. **Optional:** To avoid potentially creating duplicate security incidents, define additional incident field criteria so incoming alerts are aggregated to an open security incident. To set this criteria, follow these steps.
a. Scroll to the **Alert Aggregation Criteria** section on the form and select the Aggregate conditions check box to enable this option.

(Optional) The Incident Field Matching Values columns are displayed. These field names are the fields on the security incident that include any custom fields that are configured on the SIR security incident.

![Alert Aggregation Criteria](image)

b. From the Available list, select the field values that you want to match on existing security incidents in your Now Platform and move them to the Selected list.

(Optional) All the field values that you select must be matched to append this incoming alert to an existing security incident. If you prefer to review field values on security incidents to use for this criteria, navigate to **Incidents > Show all incidents**.

If a new alert matches all the values that are selected in the aggregation field conditions in the mapping step, the alert is automatically added to the most recently opened security incident with the same field values. As a user with the sn_sia.analyst role working with security incidents, you can view all the added aggregate alerts on a related list on a security incident. All of the aggregated alerts on a security incident are displayed on the **Splunk Event to Tasks** related list. This list details associated timestamps and aggregated field values. This information helps you understand why alerts are added to existing security incidents. If this tab is not displayed, scroll to the left side of the record under **Related Links** and click the **Show All Related Lists** link.
c. **Optional:** To log a work note for a new alert that is recently added on the security incident, select the check box to enable this option. The work note logs that a new alert has been added along with a link to the alert details.

You have successfully mapped values from a Splunk alert or event to fields on a SIR security incident. Also, you have configured additional conditions to limit the creation of security incidents with filtering criteria. You also appended alerts or events to existing SIR security incidents.

11. **Optional:** Open the script editor and continue editing.

(Optional) For more information about the script editor, see (Optional) Use the script editor to format alert values for the Splunk Enterprise Event Ingestion integration.

12. Choose one to continue with the profile configuration.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continue</td>
<td>The Mapping form is displayed. <strong>Preview</strong> is selected on the progress bar. The next step is to preview the fields you mapped on a SIR security incident.</td>
</tr>
<tr>
<td>Update</td>
<td>Your data is saved and the Splunk Event Profiles list is displayed.</td>
</tr>
<tr>
<td>Previous</td>
<td>The Alert Selection form is displayed.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete this event profile and the Splunk Event Profiles list is displayed.</td>
</tr>
</tbody>
</table>
What to do next
The next step is to preview the values that you mapped on the security incident.

Preview the security incident for the Splunk Enterprise Event Ingestion integration

After you complete the mapping step, preview the values that you mapped in a Now Platform® Security Incident Response (SIR) security incident. This preview step permits you to verify that you have mapped all the alert fields that you want displayed on the security incident.

About this task
As a user with the sn_si.admin role, preview a security incident and edit the mapping again as required to fix fields with errors or to populate any missing data. If the preview is not successfully completed, you cannot proceed to the scheduling step. Previews of SIR security incidents are not saved as actual incidents in the SIR product.

Role required: sn_si.admin

Procedure
1. If the security incident preview is not displayed, click Preview in the progress bar.
2. Select the Alert Name and then select an item from the Sample Alert IDs list.

The security incident is displayed. Do not change any information in the fields. This view is a read-only view, and a record of this security incident is not saved.

3. Review the field mapping of the alert values on the security incident.
The preceding image is an example of a preview with a mapping error. In this example, a field on the security incident does not exist for a value, or the field does not support the value that you mapped. An error message is displayed that indicates an input value was not found for the Configuration item field.

4. To resolve this error, click **Mapping** in the progress bar.

5. Edit the mapping to fix incorrect values or populate any missing data.

6. Preview the mapping again and continue to fix any errors that are described in error messages.

The following figure is an example of the Incident Details tab on the bottom half of a SIR security incident after all error messages are resolved. For this example, the Description and Work notes fields were mapped, and these fields are populated with the values from the value pairs pulled from the Splunk Enterprise console. The first Work notes field has no value. This field was left empty on the mapping grid during the mapping step. The additional Work Note fields that have values were added to the mapping grid during the mapping step.
7. After you have fixed any errors and verified that the fields are the way you want them, choose one option to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Continue</strong></td>
<td>The Scheduling form is displayed for profiles with scheduled alerts. <strong>Scheduling</strong> is selected on the progress bar.</td>
</tr>
<tr>
<td><strong>Finish</strong></td>
<td>For profiles with configured for manual event forwarding, click <strong>Finish</strong>. There is no scheduling step for profiles with event data that are exported on-demand directly from the Splunk Enterprise console.</td>
</tr>
<tr>
<td><strong>Update</strong></td>
<td>Your data is saved, and you are returned to the Splunk Event Profiles list.</td>
</tr>
<tr>
<td><strong>Previous</strong></td>
<td>The Mapping step on the progress bar is displayed.</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Delete this event profile and the Splunk Event Profiles list is displayed.</td>
</tr>
</tbody>
</table>
What to do next
If no error messages are displayed, and you are satisfied with the field mapping on the security incident, the next step is to Schedule and retrieve alerts for the Splunk Enterprise Event Ingestion integration.

Schedule and retrieve alerts for the Splunk Enterprise Event Ingestion integration
For automated alert ingestion profiles, this step is final step of the event profile configuration. During this step, you can verify the default settings for alert retrieval or modify the scheduling as needed. This step permits you to filter your alert retrieval based on a date range.

About this task
After you have completed all the steps in the progress bar for the profile configuration as shown in the following figure, you have completed the configuration for profiles for manual event forwarding. There is no scheduling available for events forwarded manually from your Splunk Enterprise console. For profiles for automated alert ingestion, you choose whether you want to ingest any historical alerts during the Scheduling step. You also choose how often you will poll for future alerts that match the alert profile configuration.

For automated alert ingestion profiles, before the profile is activated, you verify and modify the scheduling and alert retrieval. This step is the final step of the event profile configuration process for scheduled alert profiles.

As a user with the sn_si.admin role, you configure these polling intervals on a per-profile basis. The performance of the Splunk event ingestion integration is impacted by the different polling intervals. When scheduling, you may prefer to balance system load against incident urgency. A five-minute default value is set for any profile, but you may prefer to modify this setting based on the urgency of the incident and the anticipated load on your system.

In the Splunk Enterprise console, you set an alert to trigger that is based on increments or on a specific time. Use this setting to help you configure the scheduling in your Now Platform instance so the time increments in your Splunk Enterprise console synchronize with the scheduling that you set up in your Now Platform instance.

Procedure
1. If the Scheduling page on the progress bar is not displayed, select Scheduling.
2. Choose one to schedule how and when alerts are pulled from the Splunk Enterprise console.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• On-going Alert field selected</td>
<td>Based on the default setting, the Now Platform instance pulls from the Splunk Enterprise server for new alerts every five minutes. Security incidents are created if triggered alerts are found and filtering criteria are matched. To balance alert ingestion against server load, and to pull the most current data, five minutes is the setting you may prefer. However, this value can be modified as needed.</td>
</tr>
<tr>
<td>• One-Time Retrieval field cleared</td>
<td>One-time retrieval</td>
</tr>
<tr>
<td></td>
<td>Use this configuration if you want a one-time pull to ingest alerts based on historic events.</td>
</tr>
<tr>
<td></td>
<td>When configured, a profile is used once to retrieve triggered alerts including alerts from historical events that are based on a date range. To the right of the Since date field, click the calendar icon. In the calendar that is displayed, select the date that you want to start pulling alerts. Starting with the Since date value, triggered alerts are retrieved up through the current date.</td>
</tr>
<tr>
<td></td>
<td>After the alerts are pulled, this setting will not retrieve triggered alerts for this profile going forward from the current date. This setting populates the security incident with all the alerts that are found for the range you enter.</td>
</tr>
</tbody>
</table>
As an example for scheduling, if you have a daily Splunk alert that runs once a day at 4 AM local time, you can set up the corresponding alert profile in your Now Platform instance to run at 4:05 AM local time to capture the alert right away and create a security incident. Enter 04 05 00 in the Initial alert ingestion field. In the Increment (Minutes) field, enter 1440 (24 hours) to schedule the next alert ingestion for 24 hours from the initial alert ingestion. Both the initial alert ingestion time and next alert ingestion time are displayed in the fields.

3. To configure the settings for this example, follow these steps.

   a. With the Scheduling page displayed, select the **Ongoing alert** check box to enable this option.

   b. In the **Increment (minutes)** field, enter 1440 (24 hours).

   c. Click the **Select Initial alert ingestion** check box to enable editing for the Initial alert ingestion and Next alert ingestion fields.

   d. In the Initial alert ingestion field, enter 04 05 00. In the **The Next alert ingestion (estimated)** field, the time of the next alert ingestion is displayed.

4. Click **Finish** to complete the configuration.
A confirmation dialog is displayed. You have successfully completed the setup and configuration for the integration. This profile is activated, and it pulls alerts from the Splunk Enterprise console based on your scheduling. There is a limit of 1,000 security incidents that can be created in a 24-hour period. Up to 100 events are per fired alert. Subsequent events will be ignored after the limits are reached.

**Integration architecture and external systems connection for the Splunk Enterprise Event Ingestion integration**

The following topic outlines the integration architecture developed to support the ingestion of triggered alerts from the Splunk Enterprise console. This information clarifies, at a high level, the conceptual operation of the integration. It also explains why there are setup steps that are required prior to installing the application from the ServiceNow Store.

**Key terms used for this integration**

The following key terms are used during the installation and configuration. For more information about these terms, see the ServiceNow Product Documentation website and the Splunk website and resources on Splunk Resources page.

**Now Platform**

An enterprise ServiceNow product. The Now Platform is the base upon which individual components such as Security Incident Response (SIR), IT Service Management (ITSM), and other products are built.

**ServiceNow Splunkbase Addon**

A ServiceNow application that is installed on your Splunk Enterprise console that supports the manual event forwarding option of the integration. Manual event forwarding is an optional feature of the integration. This ServiceNow Splunkbase addon is not required for the automated alert ingestion that is provided by the integration.

**Security Incident Response (SIR)**

A Now Platform application that tracks the progress of security incidents from discovery and initial analysis, through containment, eradication, and recovery, and into the final post incident review and closure.

**Splunk Enterprise**

An automated security incident event management (SIEM) product or cloud service that collects data used for incident analysis and
management. This service is on a host that is sometimes also referred to as a Splunk console in this guide.

**Splunk alert**

A search that you configure and save in Splunk to scan for specific data based in the parameters you set up in the Splunk Enterprise service. When you pull alerts from Splunk, you also pull all the events associated with that alert.

**Splunk triggered alert**

A configured search in the Splunk Enterprise console that returns results and flags these results as triggered alerts. The triggered alerts are ingested from the Splunk console into your Now Platform instance for this integration. Triggered alerts have one or more Splunk events.

**Splunk event**

One or more data elements that result in the triggered alerts of the Splunk service. From your Now Platform instance, you can look up which Splunk events triggered Now Platform security incidents.

**MID Server**

This application facilitates communication and movement of data between the Now Platform and external applications, data sources, and services. This application is typically required for integration with on-premises technologies, and, for this Splunk Enterprise Event Ingestion integration, the MID Server facilitates communication between the Now Platform and the on-premises instance of Splunk Enterprise. A MID Server is not required if you are integrating your Now Platform instance with a Splunk Cloud instance.

**Security incident admin (sn_si.admin)**

The user with this role oversees the configuration of the integration with the SIR product in your Now Platform instance.

**Security incident analyst (sn_si.analyst)**

The user with this role interacts with and analyzes security incidents in the ServiceNow Security Incident Response product.

**External systems connection**

An event profile is a container that you create, name, and configure for a singular connection and call to the Splunk service to pull the most current triggered alerts that match specific criteria. After triggered alerts that match your profile have been pulled from Splunk, you select which of these alerts
you want displayed as a Now Platform Security Incident Response SIR security incident. A default view of the Splunk Enterprise alert fields is available, and you edit this mapping of alert fields to the fields on a SIR security incident to meet your needs. You preview your mapping to verify that you have all the required alert field values populated on the SIR security incident. To complete the configuration of the alert profile, you schedule the retrieval of alerts and then activate the profile. After you activate the profile in the Now Platform, you are ready to ingest historical and on-going Splunk alerts automatically.

As a user with the sn_si.admin role, if you determine that a new triggered alert is similar to alerts previously ingested, you can aggregate new triggered alerts to existing SIR security incidents. You set criteria to specify matching target field values in the Splunk Enterprise alert profile that define when an existing security incident is updated and when a new security incident is created. If the aggregation feature is enabled in your event profile, when the import set is transformed, your Now Platform instance checks for an existing record in the target table that has the same value in the target and source fields. If an existing record with a matching value in the target table is found, that record is updated. If no matching record is found, a new record is created in the target table. If enabled, the aggregation option updates existing security incidents with new triggered alerts, and you avoid creating multiple security incidents. For more information about updating records using aggregation options, see Updating records using coalesce on the Servicenow product documentation website.

This application uses the Splunk API service to retrieve information from the Splunk service. An outbound HTTPS connection from the MID server to this environment is necessary for the integration to work properly.

After it is connected to the Splunk service, the integration supports the pulling and ingestion of triggered alerts and events that trigger security incidents.

The basic data flow is illustrated in the following figures. In each figure, your Now Platform is pulling (ingesting) data. Splunk is not pushing data for scheduled alerts.
Connection to on premises Splunk enterprise service with single MID server

Connection to a Splunk enterprise cloud instance
Copy an existing profile and its associated settings instead of creating new profiles. If you are creating multiple profiles, and you want to reuse the settings of an existing profile, you may prefer to copy alarm profiles to save time.

Before you begin

About this task
As a user with the sn_si.admin role, if you copy a profile, the profile name is initially modified to avoid duplicate profiles. In addition, the copied profile is disabled (`false`) so it is not activated accidentally prior to completing the configuration. Copy profiles and use existing maps for security incidents that you have already previewed and verified.

Role required: sn_si.admin

Procedure
1. Navigate to Splunk Integration > Splunk Event Profile.
2. In the Splunk Event Profiles list that is displayed, select a profile that you want to copy, and, from the Actions on selected rows choice list, click Copy.
The profile is copied and displayed on the list. The copy has all the settings of the original profile including the mapping and scheduling configuration. The name of the profile contains copy. Although the original profile is enabled (true), the copy is disabled at this point (false). You may prefer to edit values of the copied profile and rename it so the configuration settings apply to the new profile as required.

You have successfully copied the settings from an existing profile to a new profile.

**What to do next**

You are prompted to activate (enable) the new profile after you complete the configuration steps.

(Optional) Set up your Splunk environment for manual event ingestion for the Splunk Enterprise event ingestion integration

If you want to export events manually and on-demand from your Splunk Enterprise console for this integration, install and set up the ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise application in your Splunk enterprise console or Splunk Cloud instance.

**Before you begin**

Verify that you have installed the application for this integration from the ServiceNow Store prior to installing the addon plugin from splunkbase that is
required for manual event ingestion. If you have not installed the application
for the integration from the ServiceNow Store, see Install and configure the
ServiceNow application for the Splunk Enterprise Event Ingestion integration and
follow the instructions to install it.

Role required: Now Platform administrator (admin)

About this task
If you want to export events manually and on-demand from your Splunk
Enterprise console for the integration, as a user with the Splunk Enterprise
administrator role, download, install, and set up the ServiceNow Security
Operations Event Ingestion Addon for Splunk Enterprise from splunkbase in your
Splunk Enterprise console. This ServiceNow extension addon is required so that
security incidents can be created from manually exported events in your Now
Platform instance. This ServiceNow Security Operations Event Ingestion Addon
for Splunk Enterprise application is available on splunkbase.

For manual event forwarding, you can identify up to two different Now Platform
endpoints (instances) in your Splunk Enterprise console. You forward the events
to the endpoint or endpoints manually to create security incidents. For example,
you can specify both a staging (development) instance and a production
instance. By specifying separate instances and naming primary and secondary
workflows for each instance, you can choose where you want to forward
different events.

Role required: Splunk Enterprise administrator

Procedure
1. If you have not already installed the ServiceNow Security Operations Event
   Ingestion Addon for Splunk Enterprise, follow these steps to install and
   configure it.

   a. Navigate to splunkbase.

      Ingestion Addon for Splunk Enterprise.

      Note: Verify that you have selected ServiceNow Security Operations
      Event Ingestion Addon for Splunk Enterprise. There are additional
      ServiceNow addons that are displayed in this list. These addons are for
different ServiceNow-Splunk integrations, and they are not required for
this integration.

   c. Download the application.
d. Open your Splunk Enterprise account.

e. On the Apps page, click the gear icon or the Manage Apps shortcut on the menu drop-down list.

f. On the upper left of the Apps page that is displayed, click Install app from file.

g. Click Choose File, select ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise, and click Upload.

h. If prompted, restart Splunk Enterprise.

   The ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise is installed in your Splunk Enterprise enterprise console. The next step to set up the Addon.

2. To set up the Addon, follow these steps.

   a. In Splunk Enterprise, click the Apps gear icon or Manage Apps on the menu drop-down list.

   b. On the list of applications that is displayed, in the Actions column, click Set up for ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise.

   c. Fill out the form.
The following figure is an example of a completed form in your Splunk Enterprise console.

<table>
<thead>
<tr>
<th>Field on Specify ServiceNow Primary Instance section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workflow action label</td>
<td>Name of the Now Platform workflow for your production (primary) instance. This name is the name of a Now Platform instance that your users who are monitoring Splunk events identify as a primary instance, for example, Servicenow Event Ingestion (Production). Default for this field is Servicenow Event Ingestion (Production).</td>
</tr>
<tr>
<td>Field on Specify ServiceNow Primary Instance section</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>In your Splunk Enterprise console, this workflow name is displayed for the production (Primary) instance in the expanded Event Actions drop-down list of a search. This name is the name of your production instance. You can edit the name.</td>
<td></td>
</tr>
<tr>
<td>The URL for the Now Platform instance you entered in the preceding Workflow action label field.</td>
<td>URL</td>
</tr>
<tr>
<td>Copy the URL in your browser and paste it in this field in the form.</td>
<td></td>
</tr>
<tr>
<td>Base API path. For more information, refer to the figure that follows the table.</td>
<td>Endpoint</td>
</tr>
<tr>
<td>If you do not have a value for the endpoint of your Now Platform production instance, follow these steps.</td>
<td></td>
</tr>
<tr>
<td>a. Log in to your Now Platform production instance as a user with the system administrator (admin) role.</td>
<td></td>
</tr>
<tr>
<td>b. Enter Scripted REST APIs in the navigation panel.</td>
<td></td>
</tr>
<tr>
<td>c. After the navigation panel is refreshed, select the Scripted REST APIs module that is displayed.</td>
<td></td>
</tr>
<tr>
<td>d. If Event Ingestion is not listed in the Name column of the Scripted REST APIs list that is displayed, in the search field at the top, enter Event Ingestion.</td>
<td></td>
</tr>
<tr>
<td>e. In the Base API path column on the refreshed page, copy this value and paste it in the Endpoint field</td>
<td></td>
</tr>
<tr>
<td>Field on Specify ServiceNow Primary Instance section</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Username</td>
<td>User name for your Now Platform instance. This name is the user name for the Now Platform instance in which you assigned a user with the (sn_sec_splunk_v2.api_account_access) role for manual event forwarding. For more information about assigning this role, see Set up your Now Platform instance for the Splunk Enterprise Event Ingestion integration.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for your Now Platform instance. This password is the password for the Now Platform instance in which you assigned a user with the (sn_sec_splunk_v2.api_account_access) role for manual event forwarding.</td>
</tr>
<tr>
<td>(Optional) Fields on Specify ServiceNow Secondary Instance section</td>
<td>Description</td>
</tr>
<tr>
<td>Workflow action label</td>
<td>Name of the Now Platform workflow for your secondary (staging) instance. This name is the name of a Now Platform instance that your users who are monitoring Splunk events identify as a secondary instance, for example, Servicenow Event Ingestion (Staging). In your Splunk Enterprise console, this workflow name is displayed for the staging (Secondary) instance in the expanded Event Actions drop-down list of a search. This Now Platform in-</td>
</tr>
<tr>
<td>Field on Specify ServiceNow Primary Instance section</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>URL</td>
<td>The URL for the Now Platform instance you entered in the preceding Workflow action label field for the secondary Now Platform instance. Copy the URL in your browser and paste it in this field in the form.</td>
</tr>
<tr>
<td>Endpoint</td>
<td>Base API path. This value for the Base API path for your secondary instance is the same value as the Base API path for your primary instance. See the preceding figure of the form for more information.</td>
</tr>
<tr>
<td>Username</td>
<td>Username for your Now Platform staging instance. The user must have the (sn_sec_splunk_v2.api_account_access) role.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for your Now Platform staging instance. The user must have the (sn_sec_splunk_v2.api_account_access) role.</td>
</tr>
</tbody>
</table>

The following figure is an example of the Scripted REST APIs list in your Now Platform. The list displays the location of the endpoint value of a Now Platform instance that you enter in the form as part of the set up for the ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise extension in your Splunk Enterprise console.

![Scripted REST APIs list in the Now Platform](image)
3. In the setup form in your Splunk Enterprise console, click **Save** to save your edits.

   After a few moments, at the top left of the form in your Splunk Enterprise console, a message is displayed that the record is successfully updated.

   After you save the form, the names (Workflow action labels) for your Now Platform instance(s) that you created in the form are available from the Event Actions choice list on a selected event of a search in your Splunk Enterprise console.

**What to do next**

If you have not already save searches in your Splunk Enterprise console, the next step is to save searches as alerts in your Splunk Enterprise console.

**(Optional) Save searches in your Splunk Enterprise console for the Splunk Enterprise Event Ingestion integration**

The following steps for saving searches in your Splunk Enterprise console are provided for a user with the Splunk Enterprise administrator role. If you already have existing saved searches and triggered alerts in your Splunk Enterprise console, you are not required to modify these searches for this integration.

**Before you begin**

The integration of the Now Platform® Security Operations product with the Splunk event notification service pulls event and alert information from Splunk.

Prior to ingesting alerts into your Security Operations environment, configure searches in your Splunk Enterprise console so that you automatically pull the relevant security events in Splunk Enterprise that you want to save as alerts.

If you do not have saved searches and triggered alerts established for notification when important security events occur in your Splunk Enterprise console, follow these steps to save searches.

Role required: Splunk Enterprise administrator

**Procedure**

1. Log in to your Splunk Enterprise account.
2. Click the **Search** tab.
3. In the New Search field that is displayed, enter a value for the alert, for example, *Malware*.
4. To view the events related to your search, to the right of the New Search field, click the search icon or press enter.
   The search results with events are displayed.
5. To save the search as an alert, in the upper right of the page, expand the Save As choice list and select **Alert**.

6. In the form that is displayed, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title</strong></td>
<td>Descriptive name for the alert, for example, <em>Malware Events</em>. After you save this search as an alert, events from a fired alert in the Splunk service are automatically processed into triggered alerts using this search data. This triggered alert title is used in the event profile that you create in your Now Platform instance to identify which events are ingested into your instance for Now Platform® Security Incident Response SIR security incident creation.</td>
</tr>
<tr>
<td><em>(Optional) Description</em></td>
<td>Text to help you distinguish this alert from other alerts.</td>
</tr>
<tr>
<td><strong>Alert type</strong></td>
<td>In the fields that are displayed, select <strong>Scheduled</strong> to search for this alert on a schedule, or <strong>Real-time</strong> to search continuously for this alert.</td>
</tr>
<tr>
<td><strong>Trigger results</strong></td>
<td>You may prefer to set one of the following filter conditions:</td>
</tr>
<tr>
<td></td>
<td>• Number of Results is greater than or less than</td>
</tr>
<tr>
<td></td>
<td>• One-time (once) for each result</td>
</tr>
<tr>
<td><strong>Trigger actions</strong></td>
<td>Add actions to trigger this alert. Expand the Add choice list and click <strong>Add to Triggered Alerts</strong> so that it is displayed on the form. You may prefer this setting for the alerts that you ingest into your Now Platform instance.</td>
</tr>
</tbody>
</table>

7. Click **Save**.
   Your alert is saved, and it is displayed under the Alerts tab on the Search page.
The Splunk service pulls in the events by matching the criteria that you configured in the alert. It caches the events, and you then request these events from your profiles that you set up in your Now Platform instance. Because the ingestion pull of events occurs from a cache in the Splunk service, this ingestion from your Now Platform does not impact performance on your Splunk platform.

**Results**
You have successfully completed the required setup for the integration in your Splunk Enterprise console. If you have not already installed the application for the integration from the ServiceNow Store, the next step is to install the application for the integration and configure it.

(Optional) Use the script editor to format alert values for the Splunk Enterprise Event Ingestion integration
In addition to the directly mapped fields from the pulled alert values, and the alert values you enter manually, use the script editor to format field values on the security incident during the mapping step. The script editor changes the values of a Splunk alert so that values that are supported by the Now Platform® Security Incident Response (SIR) security incident are mapped to the Category, Configuration item (CI), and Observable fields.

**About this task**
In certain cases, Splunk Enterprise alert values are mapped to the Category, Configuration item (CI), and Observable fields on the SIR incident and are not supported. As a user with the sn_si.admin role, you may prefer to edit the mapped values. If you want to translate the value of a Splunk Enterprise alert to a value that is supported by these fields on the SIR security incident, use the script editor.

Role required: sn_si.admin
Procedure

1. With the mapping form displayed, click the link to open the script editor.

2. From the choice list, select a destination field for the value that you want to edit.

3. Alternatively, in the SIR Incident Field Mapping section, click the bracket icon 
   \[
   \{}
   \]
   next to a field to open the script editor for that field.

   In certain instances, a script include may be appropriate for the Configuration item field. For an alert, for example, a value for the Configuration item may not be matched.

   As shown in the following figure, if a match for a host name cannot be found in the Now Platform® CMBD for the Configuration item field, you can edit the rule so that if an IP address is found, it populates the Configuration item field. If there is no value for the alarm, the field on the security incident is set to null.

   The editor opens with the field displayed in Destination Field. The following image shows the editor with the Configuration item field as the Destination Field.
4. Enter any changes to the script, and click **Update** to save your changes. The Splunk Field Translations table is displayed.

5. Close the table to return to the Mapping form.

**Checklist for the Splunk Enterprise Event Ingestion integration**

Use this checklist to guide you through all the tasks of the integration. The following checklist includes setup and installation tasks and examples of use cases that include expected results for the integration.

**About this task**

Role required: admin

Track your progress with the setup, installation, and configuration of the integration with the following table. Complete all the tasks for a step before moving on to the next step. Each row of the table lists tasks and identifies the roles that are required to perform the tasks. Numbered topics of the installation and configuration guide are also referenced.

Roles required: Roles are listed for each step in the following table.

**Procedure**

Follow the steps in the table in the order that they are presented.

<table>
<thead>
<tr>
<th>Checklist</th>
<th>As a user with the Now Platform admin role, set up your Now Platform instance.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Assign users with the sn_si.admin and sn_si.analyst roles as required.</td>
</tr>
<tr>
<td></td>
<td>• Install and configure a MID Server if the Splunk server is deployed within your corporate network.</td>
</tr>
<tr>
<td></td>
<td>• Verify that the ServiceNow Security Incident Response plugins are activated for your release of the Now Platform.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) If you want to forward events manually from your Splunk Enterprise console into your Now Platform instance, verify that you have assigned the (sn_sec_splunk_v2.api_account_access) role to a user with the Splunk Enterprise enterprise administrator permission.</td>
</tr>
</tbody>
</table>

For more information, see **Set up your Now Platform instance for the Splunk Enterprise Event Ingestion integration**.
|   | As a user with the Now Platform admin role, install and configure the Splunk Enterprise Event Ingestion application from the ServiceNow Store.  
**a.** Download and install the application on your Now Platform instance.  
**b.** Configure the application and connect to your Splunk Enterprise console.  
For more information, see Install and configure the ServiceNow application for the Splunk Enterprise Event Ingestion integration.  
|   | (Optional) If you intend to export events manually from your Splunk Enterprise console to your Now Platform instance, perform the following tasks:  
• As a Splunk Enterprise administrator, install, set up, and enable the ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise from splunkbase in your Splunk Enterprise console.  
• As a Splunk Enterprise administrator, if not already configured, save searches as alerts in your Splunk Enterprise console.  
For more information, see (Optional) Set up your Splunk environment for manual event ingestion for the Splunk Enterprise event ingestion integration and (Optional) Save searches in your Splunk Enterprise console for the Splunk Enterprise Event Ingestion integration.  
|   | As a user with the Now Platform sn_si.admin role, create and name an event profile.  
Select the profile type from the choice list. Options are a scheduled alert profile that you use to ingest sample data, or, an event profile that you use to export attachment data manually from your Splunk Enterprise console.  
• For a scheduled alert, select an available alert.  
• For profile for manually exported data, create a new map or copy an existing map.  

© 2021 ServiceNow, Inc. All rights reserved.  
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
For more information, see Create and name an event profile for the Splunk Enterprise Event Ingestion integration.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>As a user with the Now Platform sn_si.admin role, map values ingested or attachment data that is exported from Splunk Enterprise to Now Platform security incidents.</td>
</tr>
<tr>
<td>□</td>
<td>a. Fetch sample data for a scheduled alert.</td>
</tr>
<tr>
<td>□</td>
<td>b. (Optional) Export attachment data manually from Splunk Enterprise for an event.</td>
</tr>
<tr>
<td>□</td>
<td>c. Edit the default mapping configuration.</td>
</tr>
<tr>
<td>□</td>
<td>d. Optionally add filtering criteria, append an alert to an existing security incident, and use the script editor.</td>
</tr>
</tbody>
</table>

For more information, see Mapping alerts and events for the Splunk Enterprise Event Ingestion integration and Map alerts for the Splunk Enterprise Event Ingestion integration.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>As a user with the Now Platform sn_si.admin role, preview the data from Splunk Enterprise that is displayed on a Now Platform security incident.</td>
</tr>
<tr>
<td>□</td>
<td>• Fix any errors or add any missing data so that no error messages are displayed.</td>
</tr>
</tbody>
</table>

For more information, see Preview the security incident for the Splunk Enterprise Event Ingestion integration.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>As a user with the Now Platform sn_si.admin role, schedule alert retrieval for a profile with a scheduled alert.</td>
</tr>
<tr>
<td>□</td>
<td>For more information, see Schedule and retrieve alerts for the Splunk Enterprise Event Ingestion integration.</td>
</tr>
</tbody>
</table>

You have successfully completed the set up steps and verified expected results for the integration.

**Splunk Enterprise Security event ingestion integration for Security Operations by ServiceNow**

The Splunk Enterprise Security notable event ingestion integration with the Security Incident Response (SIR) product allows security incident analysts to collect and process notable event data (referred to as notables). Data is ingested continually based on a configured polling schedule and it is used by analysts to identify and respond to potential cyber threats. Security events that
are collected can be correlated into notable events in Splunk Enterprise Security and then ingested automatically with this integration. Also, individual notable events can be manually forwarded on-demand from the Splunk Enterprise Security Incident Review console and reporting interface into the Security Incident Response product of the Now Platform to create security incidents.

**Overview**

This integration provides a security operations center (SOC) analyst with visibility to notable events and related contributing event data. This data can be integrated into Now Platform Security Incident Response (SIR) security incidents for further investigation and remediation. Profiles are created in your Now Platform instance to handle different notable event types that are created via correlation searches in Splunk Enterprise Security. These profiles customize how different Splunk event fields are displayed on SIR security incidents.

**Key features**

This integration includes the following key features:

- Create multiple notable event ingestion profiles to create SIR security incidents for specific types of threats such as phishing and malware and unauthorized access attempts.
- Create multiple event profiles for on-demand event forwarding from your Splunk ES incident review console to create SIR security incidents.
- Drag-and-drop mapping of Splunk notable event field values to associated SIR security incident fields.
- A preview of the SIR security incident layout based on sample notable events to validate event mapping details.
- Ingest historical notable events as well as ongoing, new, and updated notable events on configurable intervals.
- Filter out notable events that do not meet SIR incident generation criteria, for example, low priority events, events that have yet to achieve a specific status, and so on.
- Aggregate events or alerts to existing SIR security incidents based on matching field values to avoid duplicate security incidents.
- Update notable events based on SIR incident creation and/or closure conditionals via a bi-directional interface to keep Splunk ES notable event updates in sync with the ServiceNow SIR incident status.

**Supported Now Platform versions**

This integration supports the Madrid and New York Now Platform releases.
The com.snc.si_dep plugin is required for this integration. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before installing and activating the other Security Operations applications.

The following Security Operations applications must be installed and activated from the ServiceNow Store. Install and then activate one application at a time in the order listed below to ensure a smooth installation:

1. Security Integration Framework
2. Security Support Common
3. Security Incident Response

For more information about installing the Security Operations core applications, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.

ServiceNow Addons

The ServiceNow Security Operations Event Ingestion Addon for Splunk ES is required only if you prefer to forward events manually from your Splunk Enterprise Security Incident Review console into your Now Platform instance. This ServiceNow addon is available in splunkbase.

This ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise application in splunkbase is not required for the automated alert ingestion that is supported by the integration.

Splunk Supported versions

This integration has been tested with Splunk Enterprise version 8.0.1 and with Splunk Enterprise Security application version 6.2.1. The integration also supports the Splunk Enterprise Security Cloud service.

MID Server

This integration requires an installed and configured MID Server in your Now Platform® instance to connect to the Splunk service when the Splunk server is deployed within your corporate network. If you are using the Splunk Cloud service, a MID Server is not required. See the ServiceNow Product Documentation website for more information about MID Servers.
References

<table>
<thead>
<tr>
<th>Reference</th>
<th>Document Identifier</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Splunk product website</td>
<td>Splunk Enterprise Security product website.</td>
</tr>
<tr>
<td>2</td>
<td>ServiceNow Product documentation website</td>
<td>ServiceNow Product Documentation website</td>
</tr>
</tbody>
</table>

Checklist

For a printable checklist of these topics, see Checklist for the Splunk Enterprise Security Notable Event Ingestion integration. You can use this list to monitor your progress as you work through the tasks of the integration.

Key terms used in this integration

This section describes some of the key terms used in this integration.

The following key terms are used during the installation and configuration. For more information about these terms, see the ServiceNow Product Documentation website and the Splunk website and resources on Splunk Resources page.

**Now Platform**

An enterprise ServiceNow product. The Now Platform is the base upon which individual components such as Security Incident Response (SIR), IT Service Management (ITSM), and other products are built.

**ServiceNow Splunkbase Addon**

A ServiceNow application that is installed on your Splunk Enterprise Security console that supports the manual event forwarding option of the integration. Manual event forwarding is an optional feature of the integration. This ServiceNow Splunkbase add-on is not required for the automated notable event ingestion that is provided by the integration which pulls events from Splunk.

**Security Incident Response (SIR)**

A Now Platform application that tracks the progress of security incidents from discovery and initial analysis, through containment, eradication, and recovery, and into the final post incident review and closure.

**Splunk Enterprise Security**

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Splunk Enterprise Security helps teams gain organization-wide visibility and security intelligence for continuous monitoring, incident response, SOC operations, and providing executives a window into business risk. Splunk Enterprise Security is a premium security solution requiring a paid license. This service is on a host or a Splunk cloud offering that is referred to as a Splunk console in this guide.

**Splunk Enterprise Security notable event**

When a correlation search identifies an event or a pattern of events, it creates a notable event. Correlation searches filter the security data and correlate across events to identify a particular type of incident (or pattern of events) and then create notable events.

**Splunk event**

One or more data elements that result in the notable events of the Splunk service. From your Now Platform instance, you can look up which Splunk events triggered Now Platform security incidents.

**MID Server**

This application facilitates communication and movement of data between the Now Platform and external applications, data sources, and services. This application is typically required for integration with on-premises technologies, and, for this Splunk Enterprise Security event ingestion integration, the MID Server facilitates communication between the Now Platform and the on-premises instance of Splunk Enterprise Security. A MID Server is not required if you are integrating your Now Platform instance with a Splunk Cloud instance.

**Security incident admin (sn_si.admin)**

The user with this role oversees the configuration of the integration with the SIR product in your Now Platform instance.

**Security incident analyst (sn_si.analyst)**

The user with this role interacts with and analyzes security incidents in the ServiceNow Security Incident Response product.

**Set up your Now Platform® instance for the Splunk Enterprise Security integration**

The following section lists the setup tasks that you are required to complete in your Now Platform® instance prior to installing the application from the ServiceNow Store.
About this task
Refer to the following table and verify that you have completed all the listed tasks before you download and install the application to ensure a smooth installation and configuration.
Role required: admin

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have assigned the required Now Platform® and Security Incident Response (SIR) roles.</td>
<td>The following roles are required for the installation, setup, and use of the integration in your Now Platform® instance.</td>
</tr>
<tr>
<td></td>
<td>• A user with the Now Platform® administrator role (admin) installs the application from the ServiceNow Store and assigns the security incident administrator (sn_si.admin) role.</td>
</tr>
<tr>
<td></td>
<td>• If you want to forward notable events manually from Splunk Enterprise Security for this integration, a user with the Now Platform® admin role assigns a user with the (sn_sec_splunkenes.api_account_access) role in the Now Platform®. This role permits a user with the Splunk Enterprise Security administrator role to access the API in the Now Platform® that is required for manual event forwarding for this integration.</td>
</tr>
<tr>
<td></td>
<td>The (sn_sec_splunkenes.api_account_access) role is not required for the integration if you are ingesting notable events automatically from Splunk Enterprise Security into your Now Platform® instance.</td>
</tr>
<tr>
<td></td>
<td>• A user with the sn_si.admin role oversees the following tasks in the Now Platform®:</td>
</tr>
<tr>
<td></td>
<td>◦ Names, creates, and edits event profiles.</td>
</tr>
<tr>
<td></td>
<td>◦ Selects and maps values from Splunk Enterprise Security to Now Platform® security incidents.</td>
</tr>
</tbody>
</table>
|                                                                            | ◦ Previews security incident details for accuracy prior to finalizing the configuration.                                                                                                                                                                                                                                                                                                                                                                                                 
<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>◦ Schedules on-going notable event ingestion.</td>
</tr>
<tr>
<td></td>
<td>◦ Enables notable event updates when a SIR incident is created and closed.</td>
</tr>
<tr>
<td></td>
<td>◦ Assigns the security incident analyst (sn_si.analyst) role.</td>
</tr>
<tr>
<td></td>
<td>◦ Users with the sn_si.analyst work with security incidents.</td>
</tr>
</tbody>
</table>

For more information about roles and assigning roles to users, see Roles on the ServiceNow Product Documentation website.

<table>
<thead>
<tr>
<th>Assign the Splunk user role.</th>
<th>Assign a Security Analyst (ess_analyst) user role in Splunk ES to perform all integration-related activities on the Splunk server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you are using version 7.2.6 or later of the Splunk API. Earlier versions are not supported.</td>
<td>If you have access to the Splunk Enterprise Security console, you have access to the API that is required for this integration. There is no other special setup required for the API.</td>
</tr>
<tr>
<td>Verify that you have installed and configured a MID Server.</td>
<td>Configured MID Server</td>
</tr>
<tr>
<td>Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration.</td>
<td>Madrid and later release requirements</td>
</tr>
</tbody>
</table>

For the Madrid release and later family releases, the Security Incident Response Dependency plugin (com.snc.si_dep) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install the application for the integration.
and activate the other Security Operations applications required by the integration.

Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation.

1. Security Incident Response
2. Security Integration Framework
3. Security Support Common

For more information about installing the Security Operations core applications, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.

### What to do next

You have successfully set up your Now Platform® instance for the integration. The next step is to install the Splunk Enterprise Security Notable Event Ingestion application from the ServiceNow Store for the integration. For more information, see Install and configure the ServiceNow application for the Splunk Enterprise Security Notable Event Ingestion integration.

If you want to export notable events manually and on-demand from your Splunk Enterprise Security console for the integration, see (Optional) Set up your Splunk environment for manual event ingestion for the Splunk Enterprise Security Notable Event Ingestion integration for more information.

### Install and configure the ServiceNow application for the Splunk Enterprise Security Notable Event Ingestion integration

Before you run the integration on your Now Platform® instance, complete these installation and configuration steps so the application properly integrates with the Security Incident Response and Security Operations products on your Now Platform® instance.

### Before you begin

Role required: admin
Procedure

1. If you have not installed the Splunk Enterprise Security Event Ingestion application from the ServiceNow Store for the integration, see Install a Security Operations integration and follow the steps to install it.

2. After you have successfully installed the application, navigate to Integrations > Integrations Configurations and locate the Splunk Event Ingestions tile.

3. To configure the application, click New.

4. Alternatively, if a Configure button is displayed on a tile, click it to edit an existing configuration.

5. In the Event Ingestions Configuration dialog that is displayed, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Splunk Enterprise Security console or Splunk Cloud instance used for the integration.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Spaces</strong></td>
<td>Spaces are supported for names, but parentheses are not supported. For example, enter SplunkES2.</td>
</tr>
<tr>
<td><strong>Splunk API Base URL</strong></td>
<td>URL for your Splunk Enterprise Security console or Splunk Cloud instance. The URL should include the API port, for example: <a href="https://mysplunkserver.com:8089">https://mysplunkserver.com:8089</a></td>
</tr>
<tr>
<td><strong>API Account User Name</strong></td>
<td>User name that you created for your API user account on the Splunk Enterprise Security console.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Assign the user with the Security Analyst (ess_analyst) user permissions on the Splunk server.</td>
</tr>
<tr>
<td><strong>API Password</strong></td>
<td>Password that you created for your API user account on the Splunk Enterprise Security console.</td>
</tr>
<tr>
<td><strong>MID Server</strong></td>
<td>Specific MID Server that is set up in your environment and will be used by this integration to pull notable events into ServiceNow. Only MID Servers that are active and validated are available from this list.</td>
</tr>
<tr>
<td><strong>On Premises Deployment</strong></td>
<td>Default is disabled.</td>
</tr>
<tr>
<td></td>
<td>If you are using the cloud-based version of Splunk Enterprise Security, verify that the check box is cleared.</td>
</tr>
<tr>
<td></td>
<td>If this option is enabled, the MID Server list is displayed. If you are using an on-premises version of Splunk Enterprise Security, follow these steps to select a MID Server.</td>
</tr>
<tr>
<td></td>
<td><strong>a.</strong> Select the check box.</td>
</tr>
<tr>
<td></td>
<td>A list is displayed. Default is <strong>Any</strong>.</td>
</tr>
</tbody>
</table>
b. Select **Any** only if all MID servers are configured to be used for the Splunk Enterprise Security Event Ingestion integration.

c. From the list, you can alternatively select a specific Now Platform® MID server that you configured in your instance for this specific integration.

The following figure is an example of a completed form for a configuration of an on-premises version of Splunk Enterprise Security with a MID Server.

![Splunk Enterprise Security - Event Ingestion Configuration](image)

Complete the fields below to configure the Splunk Enterprise Security integration within ServiceNow. This integration requires a configured MID server for on site Splunk deployments:

- **Name**: SplunkES2
- **Splunk API Base URL**: https://splunkes.secops-eng.com:3089
- **API Account Username**: now.integration
- **API Account Password**: ********
- **On Premises Deployment**: ✔
- **MID Server**: splunkes

Each Splunk Enterprise Security notable event type that you ingest from your Splunk Enterprise Security incident review console requires a unique event profile in your Now Platform® instance. However, the source that you configure on the Event Ingestions Configuration form can be reused for multiple Now Platform® profiles as long as each profile ingests unique notable event types.
6. Click **Submit**.
   After validation is successfully completed, the Security Integrations page is displayed with each of your configurations. On each valid configuration tile, **Update** and **Delete** buttons are displayed as shown in the following figure.

![Splunk Enterprise Security - Event Ingestion - SplunkES2](image)

After it is successfully validated and submitted, each Event Ingestions Splunk server configuration is saved on the Security Integrations page as a tile. If your saved configuration tiles are not displayed on the Security Integrations page, on the top-right corner of the page, from the Show Configurations list, click **Yes**.

**What to do next**
You have successfully installed and configured the application. The next step is to create an event profile.

**Authentication errors**
This section describes some common authentication errors and how they can be resolved.
Certificate validation issue

If an error occurs during authentication, you may see the following screen:

If you have verified that your API account credentials and the Splunk Base URL information are correct, this error may be due to an issue with the Splunk certificate for the port 8089 communication. ServiceNow® instance requires a valid certificate with a common name that matches the server host name to establish secure connections. For more information, see .Certificates. . If you see this error, you can verify that the issue is due to a certificate problem by viewing the system logs.

An error condition similar to the following will likely appear:

To proceed with the authentication, you must replace the Splunk default certificate that is provided for API access on port 8089. For detailed instructions on how to replace the SSL certificate, see KB0778285.
The following image shows the default Splunk certificate with a common name or host name mismatch error:

![Default Splunk Certificate Error](image1.png)

The following image shows a valid certificate with matching host name:

![Valid Certificate with Matching Host Name](image2.png)
Create and name an event profile for the Splunk Enterprise Security event ingestion integration

As a user with the sn_si.admin role, you create an event profile in your Now Platform instance and determine which Splunk notable events create security incidents. Before Now Platform Security Incident Response (SIR) security incidents are created from ingested notable events, the field values from alerts are displayed on a layout of a Now Platform security incident so that you can preview how the actual security incident will be created.

About this task
From an integration perspective using available APIs, Splunk ES notable events are forwarded individually and manually as discrete notable events, or they are automatically ingested into the Security Operations environment of your Now Platform instance depending on the profile type defined. The integration workflows ingest different types of notable events such as unauthorized access attempts and malware, for example. These notable events are ingested based on the profiles that you configure in the Security Operations environment of your instance. All notables are initially ingested for a configured correlation search type in a profile. Ingested notables can then be further filtered to specify which notables create security incidents. For example, you may prefer filters that create security incidents only for notable events that are identified as high-risk. Before a profile is activated, and it creates security incidents from ingested notable events, individual field values on the notable events are mapped to corresponding fields on a layout of security incident for a preview.

Names for the event profiles in your Now Platform instance must be unique and can only be mapped to one active event profile at any given time.

The Now Platform ingests specific notables using the workflows of the integration. All notable events that meet the selection criteria in your Splunk ES console are initially ingested into your Now Platform instance.

A profile in your Now Platform is an encapsulation of a notable event in your Splunk ES console. There is a one-to-one relationship between notable events that are ingested with a profile and connections to your Splunk ES console: one notable event type for one connection. There is a single https connection to a search head in your Splunk ES console. Multiple notable event types can come from a single search head. If you connect to multiple search heads in your Splunk ES console, you must create multiple sources and an individual profile to ingest all notables across multiple Splunk servers or search heads.

To create profiles for scheduled notable events, see Set up a profile for scheduled notable event ingestion.
To create profiles for manual event forwarding, see Set up a profile for manual event forwarding.

**Set up a profile for scheduled notable event ingestion**

Depending on the profile defined, Splunk ES notable events are automatically ingested into the Security Operations environment of your Now Platform instance.

The following table shows the list of tasks you need to follow to set up a profile for scheduled ingestion of notable events:

<table>
<thead>
<tr>
<th>Task</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create an event profile</td>
<td>See Create profiles for scheduled notable event ingestion</td>
</tr>
<tr>
<td>Select notable events based on correlation search name</td>
<td>See Select notable events based on correlation rule name for the profile for Splunk ES Event Ingestion integration</td>
</tr>
<tr>
<td>Map notable event fields</td>
<td>See Mapping notable event fields for the Splunk Enterprise Security integration</td>
</tr>
<tr>
<td>Create custom mappings</td>
<td>See Create mappings for Splunk ES notable event incident review and contributing event details (scheduled ingestion)</td>
</tr>
<tr>
<td>Preview the security incident</td>
<td>See Preview the security incident for the Splunk Enterprise Security Event Ingestion integration</td>
</tr>
<tr>
<td>Schedule and retrieve new and updated notable events</td>
<td>See Schedule and retrieve new and updated notable events for the Splunk Enterprise Security Event Ingestion integration</td>
</tr>
<tr>
<td>Automate notable event updates and closure based on SIR incident status</td>
<td>See Automate notable event updates and closure based on SIR incident status</td>
</tr>
</tbody>
</table>

**Create profiles for scheduled notable event ingestion**

You can set up a profile so that notable events are automatically ingested.
Before you begin
Role required: sn_si.admin

Procedure
1. To create an event profile for a notable event or correlation rule type in your Now Platform instance, navigate to Splunk Integration > Splunk Event Profile.
2. If the Splunk Event Profile form is not displayed, click Name in the Progress bar.
3. Click New.
4. Fill in the fields.

An example of a completed form follows the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the profile. If names are not unique, an error will be displayed and duplicate profile names are not saved. Profile names in your Now Platform instance must be unique.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box is cleared by default. If this option is disabled, the profile is not active. You should complete all sections in the profile before making it active.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the profile type from the choice list.</td>
</tr>
<tr>
<td></td>
<td>• Scheduled Event Ingestion: This type of profile supports notable events that are ingested on a configured schedule. Fill in the fields.</td>
</tr>
<tr>
<td></td>
<td>• Manual Event Forwarding: This type of profile supports notable events that are forwarded manually from your Splunk Enterprise Security Incident Review console on demand. See the following steps to fill out the form for these types of profiles.</td>
</tr>
<tr>
<td>Source</td>
<td>Splunk server or search end that you configured to ingest notable events.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>If you have multiple Splunk servers configured, select the appropriate server for the notable event types that will be ingested for the profile. You are required to enter a value.</td>
<td></td>
</tr>
<tr>
<td>Order</td>
<td>Default is 100.</td>
</tr>
<tr>
<td>If you have created multiple profiles, this value provides a run time execution priority when two or more profiles share the same triggering conditions. The workflow in the profile with the lowest number has the highest priority.</td>
<td></td>
</tr>
<tr>
<td>(Optional) Description</td>
<td>Additional text to help you distinguish this profile from other profiles.</td>
</tr>
</tbody>
</table>

The following figure is an example of a completed form for a scheduled notable event type.

![Completed form example](image)

5. For a profile with a scheduled notable event, choose one option to continue with the profile configuration.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continue</td>
<td>Save the profile and progress to the Event Selection step.</td>
</tr>
<tr>
<td>Update</td>
<td>Save updates to this profile and return to the Splunk Event Profiles list.</td>
</tr>
<tr>
<td>Save</td>
<td>Save this profile and remain on the page.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete this profile record and return to the Splunk Event Profiles list.</td>
</tr>
</tbody>
</table>

**What to do next**
The next step is to select notable events for automatic ingestion.

**Select notable events based on correlation rule name for the profile for Splunk ES Event Ingestion integration**

After you have created a profile for a scheduled notable event type ingestion, select a Splunk Enterprise Security correlation rule name for this profile for which you want to map corresponding notable events to a Now Platform Security Incident Response (SI) security incident.

**About this task**
View the available correlation rules in your Now Platform instance so you know the notable event types for which you want to ingest and create security incidents. Select a correlation rule. You can only select one notable event from the list in this form.

Role required: sn_si.admin

**Procedure**

1. If the Notable Event Selection page is not displayed, select it on the progress bar to display it.

2. From the Correlation Rule List, choose one of the following options to select a single correlation rule and move it to from the Available column to the Selected column.

The list of correlation rules on this form matches the list of correlation rules in your Splunk ES Incident Review console. Up to 500 correlation rules are displayed on this form. If there are more than 500 correlation rules listed in your Splunk ES, only the first 500 notable events are displayed on this form in your Now Platform instance.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the Correlation Rule List search field, enter text.</td>
<td>The column below the search field is filtered with available options based on the text that you enter. Select an correlation rule, and with the arrow keys, move the selected alarm from Available to Selected.</td>
</tr>
<tr>
<td>In the Correlation Rule List, double-click a Correlation Rule.</td>
<td>The Selected column is populated with your selection.</td>
</tr>
<tr>
<td>In the Correlation Rule List, single-click a Correlation Rule.</td>
<td>The correlation rule is selected. With the arrow keys, move the selected correlation rule from Available to Selected.</td>
</tr>
</tbody>
</table>

3. Choose one option to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continue, or alternatively, click Mapping in the progress bar</td>
<td>The Mapping form is displayed. <strong>Mapping</strong> is selected on the progress bar. The next step is to map notable event fields to a SIR security incident.</td>
</tr>
</tbody>
</table>
### Mapping notable event fields for the Splunk Enterprise Security integration

After you identify the specific correlation rule and notable event type for the profile, the next step is to map individual notable event fields to the fields on a Now Platform Security Incident Response (SIR) security incident.

### Overview

For the mapping step, you can ingest sample notable events for the selected correlation rule or export notable event data for manually forwarded notable events. The event mapping process is identical regardless of the profile type you are creating.

The following figures are examples of the default mapping configurations that are provided for each type of event profile. You can customize the fields that populate the security incident. During this mapping phase, you can ensure all relevant notable event field data is mapped to the appropriate place on the SIR incident form and then visualize the SIR incident in the preview section.

Use **Alert Name** to choose your alert if you have configured multiple alerts for ingestion.

After you click to fetch data, the Splunk notable event field names and corresponding values are populated on the left side of the form. These are the Splunk notable event fields that are available to map to the SIR security incident fields.
You may prefer to review a few sample notable events on your Splunk console to ingest for the field mapping configuration step. This step is labeled Mapping on the progress bar. If this page is not displayed, click Mapping on the progress bar. You can ingest up to five sample notable events from Splunk Enterprise Security to assist with the notable event field mapping process. There are options to either ingest the five most recent notable events for the correlation rule selected or ingest up to five specific notable events based on the notable event IDs.

Below is a summary of the steps required to map notable events:

- **Scheduled Notable Event Sample Data Ingestion:** For sample data that is used for automatically ingested notable event profiles, available notable event fields and their corresponding values are displayed in a default mapping layout on the left side of the mapping form once the sample data is retrieved. Tabs are displayed for you to view the values for a specific notable event ID that you pulled. Verify that all the critical fields from the notable event sample ingestion section on the left of the form are mapped to ServiceNow security incident fields on the right of the form.

- **Field Mapping:** Edit the mapping configuration by dragging notable event fields from the left side and dropping them on the ServiceNow SIR incident mapping section on the right. The mapping on the right associates the incoming notable event field with an outgoing security incident field.

- **Mapping Experience:** Customize the mapping grid by adding or removing fields using the + icon at the bottom of the SIR incident field mapping section.
Track overlooked or duplicated fields with the color coding that is provided (mapped fields are greyed out, blue fields are unmapped).

- Incident Generation Conditions: Once the mapping section is complete, you can set filter conditions so that you can specify which notable events should create security incidents versus which notable events should be filtered out, for example, low priority notable events. This is done in the Incident Generation Conditions section located below the Notable Event Mapping section.

- Event Aggregation Criteria: Define additional Event Aggregation criteria that aggregates an incoming notable event to an existing SIR security incident instead of creating similar, potentially duplicate incidents. Using field matching value criteria for each profile, this additional aggregation capability can reduce the number of active, overlapping security incidents by placing all related security notable event data on a single security incident.

- Format Field Translation: In certain cases, event field values in the Splunk Enterprise notable events may not translate directly to the fields on the SIR security incident. For these values, you can use a script editor to format field values on the security incident during the mapping step. Use the script editor if you want to format values that are similar, but not identical. For example, with the script editor, a category value of *Malware Alert* and *Virus Infection* may have different field values for the source category but both values can be translated to a common *Malicious Code Activity* in the Category field on the SIR security incident using the Format Field Translation functionality.

The next step is to ingest notable events and map values to the SIR security incident fields.

**Create mappings for Splunk ES notable event incident review and contributing event details (scheduled ingestion)**

During the notable event field-mapping step, you map individual event fields from notable events to fields on a Now Platform Security Incident Response (SIR) security incident. The mapping grid can be customized for the notable event type selected in the correlation rule selection. Color-coding of the event fields helps you keep track of the event values that you have already mapped as they become grayed out while all remaining unmapped fields appear in blue. This helps you better visualize which field values have been added to the security incident and if any remaining important event information remains unmapped.
About this task
As a user with the sn_si.admin role, map up to five notable events from the Notable Event Sample Ingestion column on the left of the form to the security incident fields in the SIR Incident Field Mapping column on the right.

Create custom mappings by adding or removing the fields on the mapping grid on the right side of the form. Default fields that are typically important field to populate on the security incident response form are displayed. However, these fields can be removed and any additional fields can be displayed using the + and - buttons. Create custom maps by adding or removing the fields on the mapping grid on the right side of the form. Customizing the fields permits you to map Splunk fields that are not displayed on the default-mapping grid on the SIR security incident.

Role required: sn_si.admin

Procedure
1. If the mapping form is not displayed, click Mapping on the progress bar.

2. For a profile with a scheduled ingestion, below Notable Event Sample Ingestion, click Fetch Sample Data to pull the latest sample notable events from the Splunk Enterprise console for the correlation rule selected. Note that you can either pull the most recent sample notable events or provide the unique notable event IDs for the specific notable events that you want to use for your notable event mapping experience.

The notable event fields and values results are displayed as individual tabs. You can ingest up to five notable events.

The pull for sample notable events may take a few moments. A message indicating that the transaction is working is displayed at the top of the screen.

In the following figure, the field-name value pairs for the ingested notable event, or the imported sample events, are displayed on the left side of this form after the ingestion pull is completed. These values are the values that you map to the security incident fields on the SIR Incident Field Mapping side of the form.
3. To map a field value from the left side of the form to a field on the security incident on the right side of the form, click-hold a blue field name on the left side of the form.

4. Drag the field name, for example, `src_category`, and drop it on a field in the `Input Expression` column next to a field name in the `Security Incident` column.
The field value is displayed in the Input Expression column. In the following image, `src_category` is mapped to the `category` field on the security incident. However, you can match any value from the left side to a field on the right. Verify that the value is mapped correctly on the security incident during the preview step.

To help you ensure that no event fields are overlooked or duplicated in the mapping process, fields are color-coded. Light blue fields on the left indicate that a notable event field is not yet selected and mapped on the security incident. You may prefer to associate an incoming notable field with more than one field on a security incident.

A gray field indicates that a field has been selected and mapped to a field on the security incident. This color-coding helps you track the mapping.
To add fields to the default fields displayed on the security incident on the right side of the form, follow these steps.

**a.** On the right of the form in the SIR Incident Field Mapping section, at the bottom of the grid, click the plus icon. A new field is displayed.

**b.** In the Security Incident column, expand the list that is displayed, and select a field.

In the expanded list for the new field, some fields are shaded. In the following figure, Category has a gray background, because it has been mapped in the security incident. Similar to the color-coding for the notable events fields on the left side of the form, this color-coding for the security incident fields on the right helps you track the already mapped SIR incident fields.
Note: So that multiple observables can be displayed on the same security incident, the Observable field can be mapped multiple times with different values. Similarly, the Configuration Item and Work notes fields support multiple values. If you try to map two values to a field that cannot support multiple values, when you preview the incident, an error message is displayed that there is no value for the field. Similarly, if a field on a security incident has a list from which you can choose multiple options, and you try to map an option to that field that is not displayed on the list, the field is not populated on the security incident.

c. Alternatively, type a value in the Search field for the new row.

d. From the left side of the form, left-click to select the Event ID that you want in the Input Expression field. With the drag feature, map it next to your new field.

6. Continue mapping by adding or removing field values to the mapping. The following figure is an example of an edited mapping. In the bottom field on the right, the Work notes field is added, and it has more than one value. Note that for long text string field, you can expand the mapping field to see
the full string and resize as needed by pulling the lower right corner of the field as indicated in screenshot below with the added Work notes field:

In the preview, these values are displayed in the Work notes on the security incident. Because the value is for a field that you added to the mapping section, and there are multiple values mapped to the Work notes field, the values are displayed as entered. In this example, the spaces and punctuation marks that you entered in the field are displayed on the Related Items section as a work note on the preview of the security incident.

The following image is an example of how the values in the preceding image are displayed on the security incident.

<table>
<thead>
<tr>
<th>Related Items</th>
<th>Field Name</th>
<th>Field Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work Note</td>
<td>Category: Malware Activity</td>
<td>destination IP: 78.45.123.180</td>
</tr>
<tr>
<td>Work Note</td>
<td>Source: MalwareDemoData Top 100 events with 15 host machines</td>
<td></td>
</tr>
</tbody>
</table>

**7. Optional:** Open the script editor and continue editing.

(Optional) For more information about the script editor, see (Optional) Use the script editor to format alert values for the Splunk Enterprise Event Ingestion integration.

Including hyperlinks for notable event incident review and contributing events
In addition to mapping fields, the `sn_si.admin` can map a string value that allows the security analyst working on an incident to hyperlink back to both the notable event incident review in the Splunk Enterprise Security console, as well as the underlying contributing events that are part of the drill down search.

The following string values contain the Splunk Enterprise Security server name and appropriate variables that can be used for hyper linking these details:


  where `splunkes2.secops-eng.com:8000` is the Splunk server source and `info_min_time` and `event_id` are event field values extracted from the notable events.


  where `splunkes2.secops-eng.com:8000` is the Splunk server source and `drilldown_search` is an event field value extracted from the notable events.

The following image shows the Notable Event Incident Review URL mapped to the work note field and the Notable Event Contributing Events (drill-down Search) Hyperlink mapped to a custom field called Notable Event Incident URL:
The following image is the SIR Incident Preview with the Notable Event Incident Review Hyperlink and Contributing Events URL:
(Optional) **Incident generation filtering conditions**

**8. Optional:** After you have completed the preceding field-mapping steps, you can use the same field values in the Incident Generation Conditions builder to define additional criteria that an incoming notable event must satisfy to create a SIR security incident. To set incident generation conditions, follow these steps.
a. Scroll to the **Incident Generation Conditions** section on the form and select the **Filter based on conditions** check box to enable the option.

(Optional) The Filter conditions builder is displayed. Use these filters to create security incidents that match the specific conditions described by the fields. The options in the lists for the first field in the Filter conditions builder match the fields that are displayed on the **Notable Event Sample Ingestion** section for the events you ingested. These fields are dynamic and change depending on the Splunk notable events that you ingest, or the event that you select for the manually forwarded notable event samples. Criteria that you enter are case-sensitive, and they must match exactly the values of the Splunk Enterprise Security notable event. If you are not sure about the values to enter in the filter fields, you may prefer to return to your Splunk Enterprise Security console and review your notable events for the keywords.

b. Using the lists and fields of the conditions builder, set filters for the first row.

c. To add more conditions, to the right of the fields, click **AND** or **OR**.

If **AND** is selected, all conditions must be matched. If **OR** is selected, either condition can be matched.

d. **Optional:** In the second row, set a second filter condition.

(Optional) The following image is an example with two conditions that must be matched before security incidents are created.
You have set the incident generation conditions so that security
incidents are created only when both of the filtering conditions that you
entered are matched.

This type of incident generation condition filtering helps you narrow down
the security events, and limit the number of unnecessary security incidents
that you create without modifying the underlying correlation search or
filters in Splunk. If additional filtering criteria are set, only notable events that
match all criteria are mapped to incidents.

Note: If any of the event field names have special characters such
as quotes ("), hyphens (-), underscores (_), or ampersands (@), these
characters may need to be replaced for mapping translation purposes
and possibly create a duplicate event name. The mapping can be
done appropriately but a numerical suffix is appended to differentiate
fields with duplicate event names. For example, if the first event field
is `alerts.alert` and the second event field is `alerts@alerts`, these
fields cannot be uniquely identified as the remaining standard text
characters are the same. In this case, a suffix is added to the second
event field and the field is renamed to `alerts@alert(1)`.

Event Aggregation Criteria to Handle Similar Notables and Prevent Duplicate
Incidents

9. Optional: To avoid creating duplicate security incidents, define additional
event aggregation criteria so that incoming notable events are aggregated
to an open security incident. To set the criteria, follow these steps below:

   a. Scroll to the Event Aggregation Criteria section on the form and select the
      Aggregate Conditions check box to enable this option.

      (Optional) The Incident fields with matching values are displayed. These field
      names are the fields on the security incident that include any custom fields
      that are configured on the SIR security incident.
b. From the multi-select input field, select the field values that you want to match on existing security incidents in your Now Platform. Use the Add New Criteria to select multiple field matching conditions. All the field values that you select in the multi-selection input field are matched for aggregation criteria using the AND condition. Click Add New Criteria to select multiple field matching conditions where aggregation occurs if any one of the multi-selected field conditions that are defined are met using the OR condition.

If a new notable event matches all the values that are selected in the aggregation field conditions in the mapping step, the new notable event is automatically added to the most recently opened security incident with the same field values. As a user with the sn_si.analyst role working with security incidents, you can view all the added aggregate notable events on a related list on a security incident. All of the aggregated notable events on a security incident are displayed on the Splunk Event to Tasks related list. This list details associated timestamps and aggregated field values. This information helps you understand why these notable events are being aggregated to existing security incidents. If this tab is not displayed, scroll to the left side of the record under Related Links and click the Show All Related Lists link.
c. Optional: To log a work note for a new notable event that is recently added on the security incident, select the check box to enable this option. The work note logs that a new notable has been added along with a link to the alert details and any other details that may have been added to the work note field in your mapping section.

You have successfully mapped values from a Splunk notable event to fields on a SIR security incident. Also, you have configured additional conditions to limit the creation of security incidents with incident generation filtering criteria. You also appended notable events to existing SIR security incidents when event field values match the configured aggregation criteria.

10. Choose one to continue with the profile configuration.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continue</td>
<td>The Mapping form is displayed.</td>
</tr>
<tr>
<td></td>
<td><strong>Preview</strong> is selected on the progress bar. The next step is to preview the fields you mapped on a SIR security incident.</td>
</tr>
<tr>
<td>Update</td>
<td>Your data is saved and the Splunk Event Profiles list is displayed.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>Previous</td>
<td>The Notable Event Selection form is displayed.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete this event profile and the Splunk Event Profiles list is displayed.</td>
</tr>
</tbody>
</table>

**What to do next**
The next step is to preview the values that you mapped on the security incident.

**Preview the security incident for the Splunk Enterprise Security Event Ingestion integration**

After you complete the mapping step, preview the values that you mapped in a Now Platform® Security Incident Response (SIR) security incident. This preview step permits you to verify that you have mapped all the notable fields that you want displayed on the security incident.

**About this task**
As a user with the sn_si.admin role, preview a security incident and edit the mapping again as required to fix fields with errors or to populate any missing data. If the preview is not successfully completed, you cannot proceed to the scheduling step. Previews of SIR security incidents are not saved as actual incidents in the SIR product.

Role required: sn_si.admin

**Procedure**
1. If the security incident preview is not displayed, click **Preview** in the progress bar.
2. From the Sample Notable Event IDs choice list, select an item.
The security incident is displayed. Do not change any information in the fields. This view is a read-only view, and a record of this security incident is not saved.

3. Review the field mapping of the notable event values on the security incident.

The preceding image is an example of a preview with a mapping error. In this example, a field value from the notable event does not have an acceptable value for the reference field on the SIR incident form. An error message is displayed that indicates an input value was not found for the Configuration item field in the ServiceNow® customer management database (CMDB). As a result, this mapped field value will not appear on the SIR security incident form without further modification.

4. To resolve this error, click Mapping in the progress bar.

5. Edit the mapping to fix incorrect values or populate any missing data.

6. Preview the mapping again and continue to fix any errors that are described in error messages.

The following figure is an example of the Incident Details tab on the bottom half of a SIR security incident after all error messages are resolved. For this example, the Description and Work notes fields were mapped, and these fields are populated with the values from the value pairs pulled from the Splunk Enterprise Security notable event samples. The first Work notes field has no value. This field was left blank on the mapping grid during the mapping
7. After you have fixed any errors and verified that the fields are the way you want them, choose one option to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Continue</strong></td>
<td>The Scheduling form is displayed for profiles with scheduled notable events.</td>
</tr>
<tr>
<td></td>
<td><strong>Scheduling</strong> is selected on the progress bar.</td>
</tr>
<tr>
<td><strong>Finish</strong></td>
<td>For profiles with configured for manual event forwarding, click <strong>Finish</strong>. There is no scheduling step for profiles with event data that are exported on-demand directly from the Splunk Enterprise Security console.</td>
</tr>
<tr>
<td><strong>Update</strong></td>
<td>Your data is saved, and you are returned to the Splunk Event Profiles list.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>Previous</td>
<td>The Mapping step on the progress bar is displayed.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete this event profile and the Splunk Event Profiles list is displayed.</td>
</tr>
</tbody>
</table>

**What to do next**

If no error messages are displayed, and you are satisfied with the field mapping on the security incident, the next step is to Schedule and retrieve alerts for the Splunk Enterprise Event Ingestion integration.

**Schedule and retrieve new and updated notable events for the Splunk Enterprise Security Event Ingestion integration**

For automated notable event ingestion profiles, this step is a required step in the event profile configuration. During this step, you can verify the default settings for notable event retrieval or modify the scheduling as needed. This step also permits you to retrieve historical notable events using a date range.

**About this task**

For profiles for automated notable event ingestion, you choose whether you want to ingest any historical notable events during the Scheduling step. You also choose how often you will poll for future new notable events and updated notable events that match the alert profile configuration.

For automated notable event ingestion profiles, before the profile is activated, you verify and modify the scheduling and alert retrieval. This is a required step for all event profile configuration process for scheduled alert profiles.

As a user with the sn_si.admin role, you configure these polling intervals on a per-profile basis. The performance of the Splunk event ingestion integration may be impacted by the different polling intervals. When scheduling, you may prefer to balance reducing polling overhead on the Splunk Enterprise Security server against a desire to be notified as soon as possible when a notable event is created or updated. A five-minute default value is set for any profile, but you may prefer to modify this setting to as low as one minute if required.

**Pulling new and updated notable events**

When the polling schedule is set, the scheduled job pulls both new and updated notable events that were pulled previously but did not meet the incident filtering criteria. This provides you with the flexibility to create incidents based on criteria that may not be present when a notable event is first created but becomes available after an update occurs, for example, during the investigation phase. Once an incident is created for a specific notable event, its subsequent updates
are ignored since it is expected that the notable is now being treated as an active ServiceNow® security incident. However, all other notables that have been previously ingested but failed to meet the incident generation criteria, will continue to be pulled and checked against the incident generation criteria until they become part of an active incident.

**Procedure**

1. If the Scheduling page on the progress bar is not displayed, select **Scheduling**.

2. Choose one to schedule how and when notable events are pulled from the Splunk Enterprise Security console.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>On-going Event Ingestion field selected</strong></td>
<td>On-going Event</td>
</tr>
<tr>
<td><strong>One-Time Retrieval field cleared</strong></td>
<td>One-Time Retrieval</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Current date</td>
<td>Note that you can pull as far back as seven days from the current date. This functionality is not intended to retrieve significant amounts of historical events from Splunk Enterprise Security for archival reasons but rather a minimal amount of in-flight events that are being actively worked at the time of profile activation. After the notable events are pulled, this setting will not retrieve more notable events for this profile going forward from the current date. This setting populates the security incident with all the notable events that are found for the range you enter.</td>
</tr>
</tbody>
</table>

As an example for scheduling an initial notable event ingestion time, if you have a daily Splunk security check that runs once a day at 4 AM local time, you can set up the corresponding notable event profile in your Now Platform instance to run at 4:05 AM local time to capture the security failure event right away and create a security incident. Enter 04 05 00 in the Initial.
event ingestion field. In the Increment (Minutes) field, enter 1440 (24 hours) to schedule the next event ingestion for 24 hours from the initial event ingestion. Both the initial event ingestion time and next event ingestion time are displayed in the fields.

3. To configure the settings for this example, follow these steps.

   a. With the Scheduling page displayed, select the **Ongoing event ingestion** check box to enable this option.

   b. In the Increment (minutes) field, enter 1440 (24 hours).

   c. Click the **Select Initial event ingestion** check box to enable editing for the Initial event ingestion and Next event ingestion fields.

   d. In the Initial event ingestion field, enter 04 05 00.

      In the The Next event ingestion (estimated) field, the time of the next event ingestion is displayed.

4. Click one of the following to continue with the profile configuration.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Continue</strong></td>
<td>The Additional Options form is displayed. <strong>Additional Options</strong> is selected on the progress bar. The next step is to update the notable events when the SIR incident is created and/or closed.</td>
</tr>
<tr>
<td><strong>Update</strong></td>
<td>Your data is saved and the Splunk Event Security Profiles list is displayed.</td>
</tr>
<tr>
<td><strong>Previous</strong></td>
<td>The Scheduling form is displayed.</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Delete this event profile and the Splunk Enterprise Security Event Profiles list is displayed.</td>
</tr>
</tbody>
</table>

**Automate notable event updates and closure based on SIR incident status**

The Splunk Enterprise Security integration has a bi-directional interface that allows for both notable events to create security incidents, as well as an ability to update the notable events once the security incident is created and/or closed with relevant incident details such as SIR incident number, assignment group, SIR incident URL, and so on. This section is the final portion of the profile.
configuration set-up that provides optional capabilities to update the Splunk Enterprise Security notable events.

Before you begin
Role required: sn_si.admin

Procedure
1. If the Additional Options page on the progress bar is not displayed, select Additional Options.
2. Follow the instructions below to complete the configuration for updating notable events based on security incident updates:

<table>
<thead>
<tr>
<th>Option or Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Update Notable Events upon SIR Incident Creation</strong></td>
<td>Select this option if you want to update the notable event status and add additional comments when a security incident is created from the notable event. This can occur for both the initial triggering notable events that create the security incident, as well as aggregated events.</td>
</tr>
<tr>
<td><strong>Initial Notable Event Status Update</strong></td>
<td>You must select a status option from the menu that displays all available status values retrieved from the Splunk Enterprise Security server. This may include a custom created status, such as ServiceNow-Assigned as shown in the screen shot below. Select the status value to be set for all notable events when a security incident is created for an ingested notable event. This includes notables that create new incidents and notables that are ingested and aggregated to an existing open incident.</td>
</tr>
<tr>
<td><strong>Initial Comments posted back to Notable Event</strong></td>
<td>In addition to updating the notable status value, you can also post comments to the notable event incident review history. As indicated in the instructions, you may edit the default text displayed in the comments sec-</td>
</tr>
<tr>
<td>Option or Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Close out Notable Events upon SIR Incident Closure</td>
<td>Select this option if you want to update the notable event status and add additional comments when a security incident is closed from the notable event. This will occur for both the initial triggering notable events that create the security incident, as well as aggregated events.</td>
</tr>
<tr>
<td>Closure Notable Event Status Update</td>
<td>You must select a status option from the list menu that displays all available status values that are retrieved from the Splunk Enterprise Security server. This may include a custom created status, such as ServiceNow-Assigned as shown in the screen shot below. Select the status value to be set for all notable events when a security incident is created for an ingested notable event. This includes notables that create new incidents as well as notables that are ingested and aggregated to an existing open incident.</td>
</tr>
<tr>
<td>Closure Comments Posted back to Notable Event</td>
<td>In addition to updating the notable status value, you can also post closure comments to the notable event incident review history. As indicated in the instructions, you may edit the default text displayed in the comments section including adding or modifying the substitution variables using format <code>${field name}</code> for any field on the Security Incident Response incident form.</td>
</tr>
</tbody>
</table>

3. Click **Finish** to complete the configuration.
A confirmation dialog is displayed. You have successfully completed the setup and configuration for the integration. Activate this profile to pull notable events from the Splunk Enterprise Security console based on your scheduling. There is a limit of 1,000 security incidents that can be created in a 24-hour period. Up to 100 notable events are per fired alert. Subsequent notable events will be ignored after the limits are reached.

The following image shows the Additional Options tab with default values populated:

With the Additional Options configuration enabled, the notable event incident review shows the status change and an update to the history comments:
Set up a profile for manual event forwarding

Depending on the profile defined, Splunk ES notable events are forwarded manually as discrete notable events into the Security Operations environment of your Now Platform instance.

To set up a profile for manual forwarding of notable events:

<table>
<thead>
<tr>
<th>Task</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create an event profile</td>
<td>See Create profiles for manually forwarded events</td>
</tr>
<tr>
<td>Map notable event fields</td>
<td>See Mapping notable event fields for the Splunk Enterprise Security integration</td>
</tr>
<tr>
<td>Create custom mappings</td>
<td>See Create mappings for Splunk ES notable event incident review and contributing event details (manual forwarding)</td>
</tr>
<tr>
<td>Preview the security incident</td>
<td>See Preview the security incident for the Splunk Enterprise Security Event Ingestion integration</td>
</tr>
<tr>
<td>Set up your Splunk environment for manual ingestion</td>
<td>See (Optional) Set up your Splunk environment for manual event ingestion for the Splunk Enterprise Security Notable Event Ingestion integration</td>
</tr>
<tr>
<td>Automate notable event updates and closure based on SIR incident status</td>
<td>See Automate notable event updates and closure based on SIR incident status</td>
</tr>
</tbody>
</table>

Create profiles for manually forwarded events

You can set up a profile for manual forwarded events.

Before you begin
Role required: sn_si.admin

Procedure
To create a profile that supports manual event forwarding, follow these steps.
For events that you forward on-demand from your Splunk Enterprise Security console, you can base the individual field mapping on any existing profile. Alternatively, you can create a new mapping grid for exported attachment data. Events that you forward manually are not scheduled in the event profile.

**a.** If not already selected, in the choice list for the Type field, select **Manual Event Forwarding**.

**b.** In the Mapping Option field that is displayed, from the choice list, choose one mapping option to continue. Refer to the following figures and tables for more information about the available mapping options in the Mapping Options choice list.

### Create New field mapping option

<table>
<thead>
<tr>
<th>Option or field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create new field mapping option</td>
<td>New field mapping for your event. If you do not have an existing field mapping that is similar to the profile that you are creating, select this option to create a new map.</td>
</tr>
<tr>
<td>Default profile</td>
<td>Default event forwarding profile for all Splunk events. Default is cleared (disabled).</td>
</tr>
<tr>
<td>Option or field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Option or field</td>
<td>When this option is enabled, this profile becomes the default profile for manual event forwarding. This profile is used when there is no match on source from the manually forwarded event. It becomes the default profile for all events with unknown sources. The Source field is unavailable if the default profile option is enabled.</td>
</tr>
<tr>
<td>Source (Notable Event field)</td>
<td>This is a field that typically defines the correlation rule that triggered the notable, for example, Brute Force Attacks. This field is unavailable if the default profile option is enabled. If available, this field permits unique event field mapping to security incident fields based on the splunk correlation rule that is typically different for different event types. If you want to manage different correlation rules separately, you can create different profile event profiles based on correlation rule to accomplish this requirement.</td>
</tr>
<tr>
<td>Automate Notable Event Updates</td>
<td>Select this check box if you want to update the notable event status and add additional comments when a SIR incident is created from the notable event and / or when the SIR incident is closed. This will occur for both the initial triggering notable events that creates the SIR incident, as well as aggregated events.</td>
</tr>
<tr>
<td>Source (Splunk Server)</td>
<td>The Splunk server that you configured as the source for notable events. If you have multiple Splunk servers configured, select the appropriate</td>
</tr>
<tr>
<td>Option or field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>server for the notable event types that will be updated for the profile. You are required to enter a value.</td>
<td></td>
</tr>
<tr>
<td>Order</td>
<td>Default is 100. Leave this setting at the default. If you have created a large number of profiles, this value provides a run time execution priority when two or more profiles share triggering conditions. The workflow in the profile with the lowest number has the highest priority.</td>
</tr>
<tr>
<td>(Optional) Description</td>
<td>Text to help you distinguish this profile from other profiles.</td>
</tr>
</tbody>
</table>

For a profile with a new field mapping, verify that you have entered a value in the Source type field and click **Continue** to proceed to the mapping step of the configuration.

For a profile with an existing field mapping, refer to the following figure and table for more information.
### Select existing profile for field mapping option

<table>
<thead>
<tr>
<th>Option or field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Select existing profile for field mapping | Reuse an existing field mapping for your new notable event profile. The Copy from profile field is displayed. Follow these steps to copy an existing field mapping for this profile.  
  
   ı. To the left of the Copy from profile field that is displayed, click the search icon.  
  ıı. In the Splunk ES Event Profiles list that is displayed, click the profile name that has the map that you want to copy.  
   
   The profile name is displayed in the Copy from profile field. |
| Default profile              | Default event forwarding profile for all Splunk notable events with unmatched source. Default is cleared (disabled).  
   
   When this option is enabled, this profile becomes the default profile for manual event forwarding.  
   
   The Source field is unavailable if the default profile option is enabled. |
| Source (Notable Event field) | This is a field that typically defines the correlation rule that triggered the notable, for example, Brute Force Attacks.  
   
   This field is unavailable if the default profile option is enabled.  
   
   If available, this field permits unique event field mapping to security incident fields based on the splunk correlation rule that is typically different for different event types. |
<table>
<thead>
<tr>
<th>Option or field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If you want to manage different correlation rules separately, you can create different profile event profiles based on correlation rule to accomplish this requirement.</td>
</tr>
<tr>
<td>Automate Notable Events</td>
<td>Select this check box if you want to update the notable event status and add additional comments when a security incident is created from the notable event or when the security incident is closed. This occurs for both the initial triggering notable events that creates the security incident, as well as aggregated events.</td>
</tr>
<tr>
<td>Source (Splunk Server)</td>
<td>Splunk server or search end that you configured as the source for notable events. If you have multiple Splunk servers configured, select the appropriate server for the notable event types that will be updated for the profile. You are required to enter a value.</td>
</tr>
<tr>
<td>Order</td>
<td>Default is 100. Leave this setting at the default. If you have created multiple profiles, this value provides a run time execution priority when two or more profiles share triggering conditions. The workflow in the profile with the lowest number has the highest priority.</td>
</tr>
<tr>
<td>(Optional) Description</td>
<td>Text to help you distinguish this profile from other profiles.</td>
</tr>
</tbody>
</table>

At the bottom of the form for selecting an existing mapping for your profile, click **Finish** to complete the profile configuration.
Create mappings for Splunk ES notable event incident review and contributing event details (manual forwarding)

During the notable event field mapping step, you map individual event fields from notable events to fields on a Now Platform Security Incident Response (SIR) security incident.

About this task
As a user with the sn_si.admin role, map up to five notable events from the Notable Event Sample Ingestion column on the left of the form to the security incident fields in the SIR Incident Field Mapping column on the right.

Create custom mappings by adding or removing the fields on the mapping grid on the right side of the form. Default fields that are typically important field to populate on the SIR incident form are displayed. However, these fields can be removed and any additional fields can be displayed using the + and - buttons. Create custom maps by adding or removing the fields on the mapping grid on the right side of the form. Customizing the fields permits you to map Splunk fields that are not displayed on the default mapping grid on the SIR security incident.

Role required: sn_si.admin

Procedure
1. If the mapping form is not displayed, click Mapping on the progress bar.
2. Follow these steps to upload attachment data in your Now Platform® instance.

a. If not already logged in, log in to your Splunk Enterprise console.

b. Navigate to the Search tab and enter a name for a search that has the notable event data that you want to export. An example search format to retrieve notable events for the Brute Force Access Behavior correlation rule would be the following: `notable`|search source="Access - Brute Force Access Behavior Detected - Rule".

c. Expand the notable event, and in the Field column, select the fields that you want to import.

These fields are the field-value pairs that are exported and displayed on the Mapping page in your Now Platform® instance.
d. In your Splunk Enterprise console, in the upper right of the Search page, click the Export icon.

e. In the choice list for the Format field in the dialog that is displayed, click XML Format.

f. Optional: Enter a new filename.

g. Click Export.
The exported Splunk notable event XML file must now be uploaded to your Now Platform® instance.

h. If the Mapping page is not already displayed in your Now Platform® instance, click **Mapping** in the progress bar.

i. In the Notable Event Sample Ingestion column, click **Load Attachment Data**.
j. Load Attachment Data button highlighted. In the dialog that is displayed, click **Choose files** and navigate to the .xml file that you exported and click **Open**.

After you click to load attachment data for manually forwarded events, the Splunk ES notable event fields are populated on the left side of the form. These values are the field values that you map to the security incident fields on the Sir Incident Field Mapping side of the form. The value pairs for the fields that you exported for the event are displayed on the left side of the mapping form.

3. Follow steps 5 to 10 in the **Create mappings for Splunk ES notable event incident review and contributing event details (scheduled ingestion)** section.

(Optional) **Set up your Splunk environment for manual event ingestion for the Splunk Enterprise Security Notable Event Ingestion integration**

If you want to export events manually and on-demand from your Splunk Enterprise Security console for this integration, install and set up the ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security application in your Splunk enterprise console or Splunk Cloud instance.

**Before you begin**

Verify that you have installed the application for this integration from the ServiceNow Store prior to installing the addon plugin from splunkbase that is required for manual event ingestion. If you have not installed the application
for the integration from the ServiceNow Store, see Install and configure the ServiceNow application for the Splunk Enterprise Security Notable Event Ingestion integration and follow the instructions to install it.

Role required: Splunk administrator

About this task
If you want to export events manually and on-demand from your Splunk Enterprise console for the integration, as a user with the Splunk Enterprise administrator role, download, install, and set up the ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security from splunkbase in your Splunk Enterprise Security console. This ServiceNow extension addon is required so that security incidents can be created from manually exported events in your Now Platform instance. This ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security application is available on splunkbase.

For manual event forwarding, you can identify up to two different Now Platform endpoints (instances) in your Splunk Enterprise Security console. You forward the events to the endpoint or endpoints manually to create security incidents. For example, you can specify both a staging (development) instance and a production instance. By specifying separate instances and naming primary and secondary workflows for each instance, you can choose where you want to forward different events.

Role required: Splunk Enterprise Security administrator

Procedure
1. If you have not already installed the ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security, follow these steps to install and configure it.

   a. Navigate to splunkbase.


   Note: Verify that you have selected ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security. There are additional ServiceNow addons that are displayed in this list. These addons are for different ServiceNow-Splunk integrations, and they are not required for this integration.

   c. Download the application.
d. Open your Splunk Enterprise Security account.

e. On the Apps page, click the gear icon or the Manage Apps shortcut on the menu drop-down list.

f. On the upper left of the Apps page that is displayed, click Install app from file.


h. If prompted, restart Splunk Enterprise.

The ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security is installed in your Splunk Enterprise Security console. The next step to set up the Addon.

2. To set up the Addon, follow these steps.

a. In Splunk Enterprise Security, click the Apps gear icon or Manage Apps on the menu drop-down list.

b. On the list of applications that is displayed, in the Actions column, click Set up for ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security.

c. Fill out the form.

The following figure is an example of a completed form in your Splunk Enterprise Security console.
Specify ServiceNow Primary Instance

Configure the settings below for event forwarding to your primary ServiceNow instance

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workflow action label</td>
<td>Name of the Now Platform workflow for your production (primary) instance. This name is the name of a Now Platform instance that your users who are monitoring Splunk events identify as a primary instance, for example, Servicenow Event Ingestion (Production). Default for this field is Servicenow Event Ingestion (Production). In your Splunk Enterprise Security console, this workflow name is displayed for the production (Primary) instance.</td>
</tr>
<tr>
<td>URL</td>
<td></td>
</tr>
<tr>
<td>Endpoint</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
<tr>
<td>Optional proxy settings</td>
<td></td>
</tr>
<tr>
<td>Proxy URL</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
</tbody>
</table>

Specify ServiceNow Secondary Instance

Configure the settings below for event forwarding to your secondary ServiceNow instance

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workflow action label</td>
<td>Name of the Now Platform workflow for your production (primary) instance. This name is the name of a Now Platform instance that your users who are monitoring Splunk events identify as a primary instance, for example, Servicenow Event Ingestion (Production). Default for this field is Servicenow Event Ingestion (Production). In your Splunk Enterprise Security console, this workflow name is displayed for the production (Primary) instance.</td>
</tr>
<tr>
<td>URL</td>
<td></td>
</tr>
<tr>
<td>Endpoint</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Field on Specify ServiceNow Primary Instance section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL</strong></td>
<td>The URL for the Now Platform instance you entered in the preceding Workflow action label field. Copy the URL in your browser and paste it in this field in the form.</td>
</tr>
<tr>
<td><strong>Endpoint</strong></td>
<td>Base API path. For more information, refer to the figure that follows the table. If you do not have a value for the endpoint of your Now Platform production instance, follow these steps.</td>
</tr>
<tr>
<td></td>
<td>a. Log in to your Now Platform production instance as a user with the system administrator (admin) role.</td>
</tr>
<tr>
<td></td>
<td>b. Enter <strong>Scripted REST APIs</strong> in the navigation panel.</td>
</tr>
<tr>
<td></td>
<td>c. After the navigation panel is refreshed, select the <strong>Scripted REST APIs</strong> module that is displayed.</td>
</tr>
<tr>
<td></td>
<td>d. If <strong>Event Ingestion</strong> is not listed in the <strong>Name</strong> column of the <strong>Scripted REST APIs</strong> list that is displayed, in the search field at the top, enter <strong>Event Ingestion</strong>.</td>
</tr>
<tr>
<td></td>
<td>e. In the <strong>Base API path</strong> column on the refreshed page, copy this value and paste it in the Endpoint field on the form. An example base api path is, <code>/api/sn_secSplunk_v2/event_ingestion</code>.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>User name for your Now Platform instance. This name is the user name for...</td>
</tr>
<tr>
<td>Field on Specify ServiceNow Primary Instance section</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Password</td>
<td>Password for your Now Platform instance. This password is the password for the Now Platform instance in which you assigned a user with the (sn_sec_splunk_v2.api_account_access) role for manual event forwarding.</td>
</tr>
</tbody>
</table>

(Optional) Fields on Specify ServiceNow Secondary Instance section

<table>
<thead>
<tr>
<th>Workflow action label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the Now Platform workflow for your secondary (staging) instance. This name is the name of a Now Platform instance that your users who are monitoring Splunk events identify as a secondary instance, for example, Servicenow Event Ingestion (Staging).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The URL for the Now Platform instance you entered in the preceding Workflow action label field for the secondary Now Platform instance.</td>
<td></td>
</tr>
<tr>
<td>Field on Specify ServiceNow Primary Instance section</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Copy the URL in your browser and paste it in this field in the form.</td>
<td></td>
</tr>
<tr>
<td>Base API path. This value for the Base API path for your secondary instance is the same value as the Base API path for your primary instance. See the preceding figure of the form for more information.</td>
<td></td>
</tr>
<tr>
<td>Username for your Now Platform staging instance. The user must have the (sn_sec_splunk_v2.api_account_access) role.</td>
<td></td>
</tr>
<tr>
<td>Password for your Now Platform staging instance. The user must have the (sn_sec_splunkes.api_account_access) role.</td>
<td></td>
</tr>
</tbody>
</table>

The following figure is an example of the Scripted REST APIs list in your Now Platform. The list displays the location of the endpoint value of a Now Platform instance that you enter in the form as part of the set up for the ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security extension in your Splunk Enterprise Security console.
3. In the setup form in your Splunk Enterprise Security console, click **Save** to save your edits.

After a few moments, at the top left of the form in your Splunk Enterprise Security console, a message is displayed that the record is successfully updated.

After you save the form, the names (Workflow action labels) for your Now Platform instance(s) that you created in the form are available from the Event Actions choice list on a selected event of a search in your Splunk Enterprise Security console.

**What to do next**

If you have not already save searches in your Splunk Enterprise Security console, the next step is to save searches as alerts in your Splunk Enterprise Security console.

(Optional) **Copy an event profile for the Splunk Enterprise Security Event Ingestion integration**

Copy an existing profile and its associated settings instead of creating new profiles. If you are creating multiple profiles, and you want to reuse the settings of an existing profile, you may prefer to copy alarm profiles to save time.
Before you begin

About this task
As a user with the sn_si.admin role, if you copy a profile, the profile name is initially modified to avoid duplicate profiles. In addition, the copied profile is disabled (false) so it is not activated accidentally prior to completing the configuration. Copy profiles and use existing maps for security incidents that you have already previewed and verified.

Role required: sn_si.admin

Procedure
1. Navigate to Splunk Integration > Splunk Event Profile.
2. In the Splunk Event Profiles list that is displayed, select a profile that you want to copy, and, from the Actions on selected rows choice list, click Copy.

The profile is copied and displayed on the list. The copy has all the settings of the original profile including the mapping and scheduling configuration. The name of the profile contains copy. Although the original profile is enabled (true), the copy is disabled at this point (false). You may prefer to edit values of the copied profile and rename it so the configuration settings apply to the new profile as required.
You have successfully copied the settings from an existing profile to a new profile.

What to do next
You are prompted to activate (enable) the new profile after you complete the configuration steps.

(Optional) Use the script editor to format alert values for the Splunk Enterprise Security Event Ingestion integration
In addition to the directly mapped fields from the ingested notable event values, and the values you enter manually, use the script editor to format field values on the security incident during the mapping step. The script editor changes the values of a Splunk notable event field so that values that are supported by the Now Platform® Security Incident Response (SIR) security incident are mapped to the Category, Configuration item (CI), and Observable fields.

About this task
In certain cases, Splunk Enterprise Security notable event values are mapped to the Category, Configuration item (CI), and Observable fields on the SIR incident are not supported. As a user with the sn_si.admin role, you may prefer to edit the mapped values. If you want to translate the value of a Splunk Enterprise Security notable event to a value that is supported by these fields on the SIR security incident, use the script editor.

Role required: sn_si.admin

Procedure
1. With the mapping form displayed, click the link to open the script editor.
2. From the choice list, select a destination field for the value that you want to edit.

3. Alternatively, in the SIR Incident Field Mapping section, click the bracket icon [{} ] next to a field to open the script editor for that field.

   In certain instances, a script include may be appropriate for the Configuration item field. For an notable event, for example, a value for the Configuration item may not be matched.

   As shown in the following figure, if a match for a host name cannot be found in the Now Platform® CMDB for the Configuration item field, you can edit the rule so that if an IP address is found, it populates the Configuration item field. If there is no value for the alarm, the field on the security incident is set to null.

   The editor opens with the field displayed in Destination Field. The following image shows the editor with the Configuration item field as the Destination Field.
4. Enter any changes to then script, and click Update to save your changes. The Splunk Field Translations table is displayed.

5. Close the table to return to the Mapping form.

Checklist for the Splunk Enterprise Security Notable Event Ingestion integration

Use this checklist to guide you through all the tasks of the integration. The following checklist includes setup and installation tasks and examples of use cases that include expected results for the integration.

About this task
Role required: sn_si.admin
Track your progress with the setup, installation, and configuration of the integration with the following table. Complete all the tasks for a step before moving on to the next step. Each row of the table lists tasks and identifies the roles that are required to perform the tasks. Numbered topics of the installation and configuration guide are also referenced.

Roles required: Roles are listed for each step in the following table.

Procedure
Follow the steps in the table in the order that they are presented.

| Checklist | As a user with the Now Platform admin role, set up your Now Platform instance. |
- Assign users with the sn_si.admin and sn_si.analyst roles as required.
- Install and configure a MID Server if the Splunk server is deployed within your corporate network.
- Verify that the ServiceNow Security Incident Response plugins are activated for your release of the Now Platform.
- (Optional) If you want to forward events manually from your Splunk Enterprise Security console into your Now Platform instance, verify that you have assigned the (sn_secSplunkes.api_account_access) role to a user with the Splunk Enterprise Security administrator permission.

For more information, see Set up your Now Platform instance for the Splunk Enterprise Security integration.

<table>
<thead>
<tr>
<th>As a user with the Now Platform admin role, install and configure the Splunk Enterprise Security application from the ServiceNow Store.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>a.</strong> Download and install the application on your Now Platform instance.</td>
</tr>
<tr>
<td><strong>b.</strong> Configure the application and connect to your Splunk Enterprise Security console.</td>
</tr>
</tbody>
</table>

For more information, see Install and configure the ServiceNow application for the Splunk Enterprise Security Notable Event Ingestion integration.

<table>
<thead>
<tr>
<th>(Optional) If you intend to export events manually from your Splunk Enterprise Security console to your Now Platform instance, perform the following tasks:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• As a Splunk Enterprise Security administrator, install, set up, and enable the ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security from splunkbase in your Splunk Enterprise Security console.</td>
</tr>
<tr>
<td>• As a Splunk Enterprise Security administrator, if not already configured, save searches as notable events in your Splunk Enterprise Security console.</td>
</tr>
</tbody>
</table>

For more information, see (Optional) Set up your Splunk environment for manual event ingestion for the Splunk Enterprise Security Notable Event Ingestion integration.
|   | As a user with the Now Platform sn_si.admin role, create and name an event profile.  
Select the profile type from the choice list. Options are a scheduled alert profile that you use to ingest sample data, or, an event profile that you use to export attachment data manually from your Splunk Enterprise Security console.  
• For a scheduled alert, select an available alert.  
• For profile for manually exported data, create a new map or copy an existing map.  
For more information, see Create and name an event profile for the Splunk Enterprise Security event ingestion integration.  |
|   | As a user with the Now Platform sn_si.admin role, map values ingested or attachment data that is exported from Splunk Enterprise Security to Now Platform security incidents.  
   | a. Fetch sample data for a scheduled alert.  
   | b. (Optional) Export attachment data manually from Splunk Enterprise Security for an event.  
   | c. Edit the default mapping configuration.  
   | d. Optionally add filtering criteria, append an alert to an existing security incident, and use the script editor.  
For more information, see Mapping notable event fields for the Splunk Enterprise Security integration and Create mappings for Splunk ES notable event incident review and contributing event details (scheduled ingestion).  |
|   | As a user with the Now Platform sn_si.admin role, preview the data from Splunk Enterprise that is displayed on a Now Platform security incident.  
   | • Fix any errors or add any missing data so that no error messages are displayed.  
For more information, see Preview the security incident for the Splunk Enterprise Security Event Ingestion integration.  |
|   | As a user with the Now Platform sn_si.admin role, schedule alert retrieval for a profile with a scheduled alert.  |
For more information, see Schedule and retrieve new and updated notable events for the Splunk Enterprise Security Event Ingestion integration.

You have successfully completed the set up steps and verified expected results for the integration.

### Splunk - Incident Enrichment integration

The Splunk - Incident Enrichment integration searches your logs and adds relevant sighting information to your security incidents.

<table>
<thead>
<tr>
<th>Explore</th>
<th>Set up</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Security Incident Response integrations</td>
<td>• Get started with the Splunk Search integration for Security Operations</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use</th>
<th>Develop</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Run a Sightings Search</td>
<td>• ServiceNow Security Operations integration development guidelines</td>
</tr>
<tr>
<td>• Security Operations Integration - Sightings Search workflow</td>
<td>• Tips for writing integrations</td>
</tr>
<tr>
<td>• Security Operations Integration - Splunk Sightings Search workflow</td>
<td>• Developer training</td>
</tr>
<tr>
<td>• View Sightings Search Details</td>
<td>• Developer documentation</td>
</tr>
<tr>
<td>• View Sightings Search Results</td>
<td>• Find components installed with an application</td>
</tr>
</tbody>
</table>

### Troubleshoot and get help

| • Integration troubleshooting |
| • Ask or answer questions in the Security Operations community |
| • Search the Known Error Portal for known error articles |
| • Contact Customer Service and Support |

### Get started with the Splunk Search integration for Security Operations

Splunk software searches, monitors, and analyzes machine-generated big data and integrates easily with Security Operations. Before you can use the Splunk - Incident Enrichment integration, you must download it from the ServiceNow Store and add the appropriate API Base URL and login credentials.
Before you begin
Role required: sn_si_admin

Procedure
1. Download the integration from the ServiceNow Store.
2. When the installation is complete, access Splunk and obtain the API Key and API ID under your profile.
4. In the Splunk - Incident Enrichment card, click New.

5. Fill in the fields, as needed.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of this configuration.</td>
</tr>
<tr>
<td>Splunk API Base URL</td>
<td>The base URL you acquired from the Splunk site.</td>
</tr>
<tr>
<td>Link URL</td>
<td>[Optional] The Link URL that links to the Splunk web interface, when available.</td>
</tr>
<tr>
<td>Username</td>
<td>Your Splunk username.</td>
</tr>
<tr>
<td>Password</td>
<td>Your Splunk password.</td>
</tr>
<tr>
<td>Max Rows</td>
<td>The maximum number of rows you want to search.</td>
</tr>
<tr>
<td>Earliest Result (days)</td>
<td>The earliest results you want to see in number of days.</td>
</tr>
<tr>
<td>Include raw data samples</td>
<td>Select this to include samples of raw data in your sightings search results.</td>
</tr>
<tr>
<td>in search results</td>
<td>The amount of data returned depends on your setting in the <strong>number of rows of raw data</strong> property in Security Incident Response properties.</td>
</tr>
<tr>
<td>MID Server</td>
<td>Select <strong>Any</strong> to use any active MID Server, or select a specific</td>
</tr>
<tr>
<td></td>
<td>MID Server name.</td>
</tr>
</tbody>
</table>

**Note:** Configuring this integration activates workflows. To manage the workflows, navigate to the **Workflow Editor**.

6. Click **Submit**.
   The integration configuration card displays.

7. When viewing the new configuration card, you can click **Configure** or **Delete** to change or delete the configuration, respectively.

8. To return to the original list of integration configuration cards, select **No** from the **Show Configurations** drop-down list.

**Tanium Endpoint Platform integration**

The Tanium Endpoint Platform uses a workflow and workflow activities to return running processes for affected CIs.

<table>
<thead>
<tr>
<th>Explore</th>
<th>Set up</th>
</tr>
</thead>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Use</th>
<th>Develop</th>
</tr>
</thead>
</table>
| • Tanium - Get Running Processes workflow  
• Tanium - Get File Details workflow | • ServiceNow Security Operations integration development guidelines  
• Tips for writing integrations  
• Developer training  
• Developer documentation  
• Find components installed with an application |

<table>
<thead>
<tr>
<th>Troubleshoot and get help</th>
</tr>
</thead>
</table>
| • Integration troubleshooting  
• Ask or answer questions in the Security Operations community  
• Search the Known Error Portal for known error articles  
• Contact Customer Service and Support |

**Tanium Endpoint Platform integration setup**

Before you can use the Tanium integration, activate the plugin and configure the integration. If necessary, you must also update your X.509 SSL certification.

Whenever a CI is added to an open security incident in Security Incident Response, the **Tanium - Get running processes** workflow is triggered when the record is saved. Tanium is asked a Get Processes question, and Tanium returns the running processes for the affected CI in a table. For more information on the workflow and associated workflow activities, see **Tanium - Get Running Processes workflow**.

**Activate and configure the Security Operations Tanium integration**

The Integration Configuration feature allows you to quickly activate and set up third-party security integrations, including Tanium integration. Before you can
use the Tanium Endpoint Platform integration, you must download it from the ServiceNow Store.

**Before you begin**
Role required: sn_si_admin

**Procedure**

1. Download the integration from the ServiceNow Store.

2. When the installation is complete, navigate to **Security Operations > Integration Configuration**. The available security integrations appear as a series of cards.

3. In the Tanium card, click **Configure**.

4. Fill in the fields on the Tanium Configuration form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tanium Server URL</td>
<td>The URL for accessing the Tanium server SOAP endpoint. Typically, the URL takes a format similar to <a href="https://tanium.server.local/soap">https://tanium.server.local/soap</a>. An IP address can also be used. For example, <a href="https://12.13.14.15/soap">https://12.13.14.15/soap</a>.</td>
</tr>
<tr>
<td>Tanium Username and Password</td>
<td>The username and password for the Tanium integration administrator (for Tanium version 6.1 and above).</td>
</tr>
<tr>
<td>Tanium Session (pre 6.1)</td>
<td>The Tanium Session SOAP key (for Tanium versions prior to 6.1). For Tanium 6.1 and later installations, this field is typically left empty.</td>
</tr>
<tr>
<td>Running Processes Sensor</td>
<td>The name of the Running Processes sensor to use. For example, <strong>Running Processes</strong>.</td>
</tr>
<tr>
<td>IP Address Sensor</td>
<td>The name of the IP address sensor to use for limiting a query to a set of specific client machines. For example, <strong>IP Address</strong>.</td>
</tr>
<tr>
<td>Index File Sensor</td>
<td>The name of the sensor used to get file details. This field defaults to <strong>Index Query File Details</strong>.</td>
</tr>
<tr>
<td>Max Index File</td>
<td>The limit on the number of files returned per machine in a Get File Details query. This field defaults to 10.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Entries per IP</td>
<td></td>
</tr>
<tr>
<td>Use MID Server</td>
<td>If the Tanium server is behind a MID Server, authentication credentials must be included in the body of SOAP messages. The credentials, along with the rest of the SOAP message body, are stored as plain text in the External Communication Channel (ECC Queue).</td>
</tr>
</tbody>
</table>

5. Click **Submit** to store the integration configuration.

**Configure for MID Server access**

If the Tanium server is behind a MID Server, perform these additional configuration steps to proxy requests through the MID Server. All SOAP messages sent through a MID Server are performed asynchronously.

**Before you begin**

There must be a running MID Server associated with your instance.

On the **Tanium Configuration form**, you must select the **Use MID Server** check box.

Role required: admin

**Procedure**

1. Navigate to **System Web Services > Outbound > Soap Message**.
2. Locate and click **Tanium Server**.
3. Click the **SOAP Message Functions** tab.
4. For each of the following three functions, set the **MID server** field with the appropriate MID Server used to communicate with the Tanium server.
   - Get running processes - AddObject
   - GetResultData
   - GetResultInfo
5. Click **Update**.

**Update your X.509 certificate**

If you require an SSL connection for the integration, there are circumstances when the certificate provided by the third-party vendor is either not yet trusted in ServiceNow or has expired. This task is optional.
Before you begin
Role required: admin

Procedure
1. Acquire the SSL certificate from the third-party vendor. For example, you can import an X.509 Certificate (PEM) from an SSL endpoint in the Firefox browser, as follows.
   a. Enter the endpoint URL into the browser address bar. For example: https://<3rdparty>/
   b. Click the lock icon in the address line.
   c. Click More Information and click the Security tab.
   d. Click View Certificate and click the Detail tab.
   e. Click Export to save the PEM into your local file system.
   f. Open the saved file in any text editor tool and copy the content to the clipboard. It must begin with -----BEGIN CERTIFICATE----- and end with -----END CERTIFICATE-----.
2. Navigate to System Definition > Certificates.
3. Click New and create a new record for the integration.
4. In PEM Certificate, paste in the certificate you downloaded and copied into the clipboard earlier.
5. Click Save.
   The other fields in the record are generated automatically.

Tanium - Get File Details workflow
This workflow queries the Tanium server for the existence of files with a specific hash value or file name. The activities collect the results and store them as enrichment data on a security incident.
Note: This workflow illustrates how you can query the Tanium server for the existence of files with a specific hash value or file name, collect the data, and store it as enrichment data on a security incident. In its current implementation, the workflow does not return the enriched data for use by the system. It is provided to exemplify the process you can use to increase the effectiveness of your security incident investigation.

Activities specific to this integration are described here. For more information on other activities, see Common integration workflow activities.

Tanium: Build Get Sensor ID Request activity

This activity takes a sensor name, and builds a request to perform a lookup on the Tanium server. It returns a sensor ID used by subsequent activities.

Input variables

Input variables determine the initial behavior of the activity.
Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sensor_name [string]</td>
<td>A string that identifies the sensor name.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpoint [string]</td>
<td>The encrypted endpoint from the database.</td>
</tr>
<tr>
<td>request_body [Encrypted]</td>
<td>The SOAP request body.</td>
</tr>
<tr>
<td>http_timeout [Integer]</td>
<td>The HTTP timeout value, in seconds.</td>
</tr>
<tr>
<td>use_mid [Boolean]</td>
<td>A boolean flag indicating whether to use the MID Server.</td>
</tr>
</tbody>
</table>

Tanium: Execute Request activity

This workflow activity executes an HTTP request. The inputs define the endpoint and the expected request body. The request body itself is the encrypted SOAP envelope.

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>request_body [Encrypted]</td>
<td>The SOAP request body. This input field is mandatory.</td>
</tr>
<tr>
<td>use_mid [Boolean]</td>
<td>A boolean flag indicating whether to use the MID Server.</td>
</tr>
<tr>
<td>endpoint [string]</td>
<td>The encrypted endpoint from the database.</td>
</tr>
<tr>
<td>http_timeout [integer]</td>
<td>The HTTP timeout value, in seconds.</td>
</tr>
</tbody>
</table>
Output variables
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_code</td>
<td>Standard HTTP status codes.</td>
</tr>
<tr>
<td>header</td>
<td>The SOAP header.</td>
</tr>
<tr>
<td>body</td>
<td>The SOAP body.</td>
</tr>
<tr>
<td>error</td>
<td>Any errors provided by the server.</td>
</tr>
</tbody>
</table>

Tanium: Execute Request activity
This workflow activity executes an HTTP request. The inputs define the endpoint and the expected request body. The request body itself is the encrypted SOAP envelope.

Input variables
Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>request_body</td>
<td>The SOAP request body. This input field is mandatory.</td>
</tr>
<tr>
<td>use_mid</td>
<td>A boolean flag indicating whether to use the MID Server.</td>
</tr>
<tr>
<td>endpoint</td>
<td>The encrypted endpoint from the database. This input field is mandatory.</td>
</tr>
<tr>
<td>http_timeout</td>
<td>The HTTP timeout value, in seconds.</td>
</tr>
</tbody>
</table>
Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_code</td>
<td>Standard HTTP status codes.</td>
</tr>
<tr>
<td>header</td>
<td>The SOAP header.</td>
</tr>
<tr>
<td>body</td>
<td>The SOAP body.</td>
</tr>
<tr>
<td>error</td>
<td>Any errors provided by the server.</td>
</tr>
</tbody>
</table>

Tanium: Get Sensor ID From Response activity

This activity processes the SOAP response body provided as input, and outputs the corresponding sensor ID.

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>response_body</td>
<td>the SOAP response body coming back from Tanium.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sensor_id</td>
<td>The string sensor ID associated with the requested sensor.</td>
</tr>
</tbody>
</table>

Tanium: Execute Request activity

This workflow activity executes an HTTP request. The inputs define the endpoint and the expected request body. The request body itself is the encrypted SOAP envelope.

Input variables

Input variables determine the initial behavior of the activity.
Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>request_body</td>
<td>The SOAP request body. This input field is mandatory.</td>
</tr>
<tr>
<td>use_mid</td>
<td>A boolean flag indicating whether to use the MID Server.</td>
</tr>
<tr>
<td>endpoint</td>
<td>The encrypted endpoint from the database. This input field is mandatory.</td>
</tr>
<tr>
<td>http_timeout</td>
<td>The HTTP timeout value, in seconds.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_code</td>
<td>Standard HTTP status codes.</td>
</tr>
<tr>
<td>header</td>
<td>The SOAP header.</td>
</tr>
<tr>
<td>body</td>
<td>The SOAP body.</td>
</tr>
<tr>
<td>error</td>
<td>Any errors provided by the server.</td>
</tr>
</tbody>
</table>

Tanium: Get Question ID from Response activity

This workflow activity processes the response body to obtain the Question ID.

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>response_body</td>
<td>The SOAP response body.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.
Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>question_id [integer]</td>
<td>The Question ID returned from the Tanium server.</td>
</tr>
</tbody>
</table>

Tanium: Build Check if Done Request activity

This workflow activity builds a request of the Tanium server to check if data collection for the question is complete. It returns the encrypted request and other components necessary to execute the request.

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>question_id [integer]</td>
<td>The Question ID returned from the Tanium server.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpoint [string]</td>
<td>The encrypted endpoint from the database.</td>
</tr>
<tr>
<td>request_body [Encrypted]</td>
<td>The SOAP request body.</td>
</tr>
<tr>
<td>http_timeout [Integer]</td>
<td>The HTTP timeout value, in seconds.</td>
</tr>
<tr>
<td>use_mid [Boolean]</td>
<td>A boolean flag indicating whether to use the MID Server.</td>
</tr>
</tbody>
</table>

Tanium: Execute Request activity

This workflow activity executes an HTTP request. The inputs define the endpoint and the expected request body. The request body itself is the encrypted SOAP envelope.

Input variables

Input variables determine the initial behavior of the activity.
### Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>request_body [Encrypted]</td>
<td>The SOAP request body. This input field is mandatory.</td>
</tr>
<tr>
<td>use_mid [Boolean]</td>
<td>A boolean flag indicating whether to use the MID Server.</td>
</tr>
<tr>
<td>endpoint [string]</td>
<td>The encrypted endpoint from the database. This input field is mandatory.</td>
</tr>
<tr>
<td>http_timeout [integer]</td>
<td>The HTTP timeout value, in seconds.</td>
</tr>
</tbody>
</table>

### Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_code [integer]</td>
<td>Standard HTTP status codes.</td>
</tr>
<tr>
<td>header [string]</td>
<td>The SOAP header.</td>
</tr>
<tr>
<td>body [string]</td>
<td>The SOAP body.</td>
</tr>
<tr>
<td>error [string]</td>
<td>Any errors provided by the server.</td>
</tr>
</tbody>
</table>

### Tanium: Determine if done from Response activity

This workflow activity determines if a request has completed based on the response body.

### Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>response_body [string]</td>
<td>The SOAP request body returned from Tanium.</td>
</tr>
</tbody>
</table>
### Tanium: Build Get Result Data Request activity

This workflow builds a request to collect all the data returned from Tanium in answer to a question. It takes a Question ID as input and provides the output to execute the request, including an encrypted SOAP envelope payload.

#### Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>question_id</td>
<td>The question ID of the question posed to Tanium.</td>
</tr>
</tbody>
</table>

#### Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpoint</td>
<td>The encrypted endpoint from the database.</td>
</tr>
<tr>
<td>request_body</td>
<td>The SOAP request body.</td>
</tr>
<tr>
<td>http_timeout</td>
<td>The HTTP timeout value, in seconds.</td>
</tr>
<tr>
<td>use_mid</td>
<td>A boolean flag indicating whether to use the MID Server.</td>
</tr>
</tbody>
</table>

### Tanium: Execute Request activity

This workflow activity executes an HTTP request. The inputs define the endpoint and the expected request body. The request body itself is the encrypted SOAP envelope.

#### Input variables

Input variables determine the initial behavior of the activity.
Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>request_body</td>
<td>The SOAP request body. This input field is mandatory.</td>
</tr>
<tr>
<td>[Encrypted]</td>
<td></td>
</tr>
<tr>
<td>use_mid [Boolean]</td>
<td>A boolean flag indicating whether to use the MID Server.</td>
</tr>
<tr>
<td>endpoint [string]</td>
<td>The encrypted endpoint from the database. This input field is mandatory.</td>
</tr>
<tr>
<td>http_timeout</td>
<td>The HTTP timeout value, in seconds.</td>
</tr>
<tr>
<td>[integer]</td>
<td></td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_code [integer]</td>
<td>Standard HTTP status codes.</td>
</tr>
<tr>
<td>header [string]</td>
<td>The SOAP header.</td>
</tr>
<tr>
<td>body [string]</td>
<td>The SOAP body.</td>
</tr>
<tr>
<td>error [string]</td>
<td>Any errors provided by the server.</td>
</tr>
</tbody>
</table>

Tanium: Get Result Data from Response activity

The Tanium: Get Result Data from Response workflow activity processes the response body from the result data and outputs an array of JSON objects representing the results from Tanium.

The Tanium: Get Result Data from Response activity can be used with any workflow to retrieve result data to use in the workflow.

Results

Possible results for this activity are:
Results

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Retrieved result data.</td>
</tr>
<tr>
<td>Failure</td>
<td>No data retrieved. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>response_body</td>
<td>Encrypted SOAP response contents</td>
</tr>
<tr>
<td>implementation_id</td>
<td>Implementation identifier.</td>
</tr>
<tr>
<td>affected_ci</td>
<td>Configuration item affected.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Output variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variable</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>result_data</td>
</tr>
<tr>
<td>output</td>
</tr>
</tbody>
</table>

Tanium - Get Running Processes workflow

This workflow creates an audit trail, and the Tanium: Get-Processes Question activity takes the IPV4 address of the CI as input and runs a query on the Tanium server. The output is a list of all the running processes on the affected CI.
Security Operations Tanium Integration - Get Running Processes workflow

When the **Configuration item** field in a security incident is modified, this workflow is launched.

**How the workflow works**

Given a string question ID (normally the result of an AddObject command), the **Tanium: Check if Done** activity queries the Tanium server to check if data collection is complete. This activity uses the `sn_sec_tanium.TaniumEndpointUtil` script include and relies on the **GetResultInfo** Tanium server SOAP message.

When the **Tanium: Check if Done** activity returns true, the **Tanium: Get Result Data from Response** activity collects all the data returned from the Tanium server in answer to the Get-Processes question. The output consists of an array of objects, each containing key-value pairs composed of the column and values returned from the server. If no data is received from the server, the output is an empty array.

Activities specific to this integration are described here. For more information on other activities, see **Common integration workflow activities**.

**Get IP from CI activity**

This workflow activity determines the IPV4 address associated with a configuration item (CI).

The **Get IP from CI** activity can be used with any workflow to retrieve the IPv4 address of a CI.

**Input variables**

Input variables determine the initial behavior of the activity.
Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ci_sys_id</td>
<td>Configuration item system identifier</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_addr</td>
<td>IPv4 address. If the IP address cannot be determined, this value is empty.</td>
</tr>
</tbody>
</table>

Exit Conditions

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>An IPv4 address was returned.</td>
</tr>
<tr>
<td>Failure</td>
<td>An IPv4 address could not be determined.</td>
</tr>
</tbody>
</table>

Tanium: Build Get-Processes Request activity

This workflow activity takes the IPv4 address of a CI added to a security incident and builds a request to the Tanium server for all the running processes for that CI. The output is the details necessary for executing the request, with the payload encrypted.

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ci_ip_address</td>
<td>The IPv4 address of the CI that was added to a security incident. This input field is mandatory.</td>
</tr>
</tbody>
</table>
Output variables
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpoint [string]</td>
<td>The encrypted endpoint from the database.</td>
</tr>
<tr>
<td>request_body [Encrypted]</td>
<td>The SOAP request body.</td>
</tr>
<tr>
<td>http_timeout [Integer]</td>
<td>The HTTP timeout value, in seconds.</td>
</tr>
<tr>
<td>use_mid [Boolean]</td>
<td>A boolean flag indicating whether to use the MID Server.</td>
</tr>
</tbody>
</table>

Tanium: Build Check if Done Request activity
This workflow activity builds a request of the Tanium server to check if data collection for the question is complete. It returns the encrypted request and other components necessary to execute the request.

Input variables
Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>question_id [integer]</td>
<td>The Question ID returned from the Tanium server.</td>
</tr>
</tbody>
</table>

Output variables
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpoint [string]</td>
<td>The encrypted endpoint from the database.</td>
</tr>
<tr>
<td>request_body [Encrypted]</td>
<td>The SOAP request body.</td>
</tr>
<tr>
<td>http_timeout [Integer]</td>
<td>The HTTP timeout value, in seconds.</td>
</tr>
</tbody>
</table>
Output variables (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>use_mid [Boolean]</td>
<td>A boolean flag indicating whether to use the MID Server.</td>
</tr>
</tbody>
</table>

**Tanium: Build Get Result Data Request activity**

This workflow builds a request to collect all the data returned from Tanium in answer to a question. It takes a Question ID as input and provides the output to execute the request, including an encrypted SOAP envelope payload.

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>question_id [string]</td>
<td>The question ID of the question posed to Tanium.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpoint [string]</td>
<td>The encrypted endpoint from the database.</td>
</tr>
<tr>
<td>request_body [Encrypted]</td>
<td>The SOAP request body.</td>
</tr>
<tr>
<td>http_timeout [Integer]</td>
<td>The HTTP timeout value, in seconds.</td>
</tr>
<tr>
<td>use_mid [Boolean]</td>
<td>A boolean flag indicating whether to use the MID Server.</td>
</tr>
</tbody>
</table>

**Tanium: Determine if done from Response activity**

This workflow activity determines if a request has completed based on the response body.

**Input variables**

Input variables determine the initial behavior of the activity.
### Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>response_body [string]</td>
<td>The SOAP request body returned from Tanium.</td>
</tr>
</tbody>
</table>

### Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>done [Boolean]</td>
<td>Returns true if the request processing is done.</td>
</tr>
</tbody>
</table>

### Tanium: Execute Request activity

This workflow activity executes an HTTP request. The inputs define the endpoint and the expected request body. The request body itself is the encrypted SOAP envelope.

### Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>request_body [Encrypted]</td>
<td>The SOAP request body. This input field is mandatory.</td>
</tr>
<tr>
<td>use_mid [Boolean]</td>
<td>A boolean flag indicating whether to use the MID Server.</td>
</tr>
<tr>
<td>endpoint [string]</td>
<td>The encrypted endpoint from the database. This input field is mandatory.</td>
</tr>
<tr>
<td>http_timeout [integer]</td>
<td>The HTTP timeout value, in seconds.</td>
</tr>
</tbody>
</table>

### Output variables

The output variables contain data that can be used in subsequent activities.
Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_code [integer]</td>
<td>Standard HTTP status codes.</td>
</tr>
<tr>
<td>header [string]</td>
<td>The SOAP header.</td>
</tr>
<tr>
<td>body [string]</td>
<td>The SOAP body.</td>
</tr>
<tr>
<td>error [string]</td>
<td>Any errors provided by the server.</td>
</tr>
</tbody>
</table>

**Tanium: Get Question ID from Response activity**

This workflow activity processes the response body to obtain the Question ID.

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>question_id [integer]</td>
<td>The Question ID returned from the Tanium server.</td>
</tr>
</tbody>
</table>

**Tanium: Get Result Data from Response activity**

The **Tanium: Get Result Data from Response** workflow activity processes the response body from the result data and outputs an array of JSON objects representing the results from Tanium.

The **Tanium: Get Result Data from Response** activity can be used with any workflow to retrieve result data to use in the workflow.

**Results**

Possible results for this activity are:
Results

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Retrieved result data.</td>
</tr>
<tr>
<td>Failure</td>
<td>No data retrieved. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>response_body</td>
<td>Encrypted SOAP response contents</td>
</tr>
<tr>
<td>implementation_id</td>
<td>Implementation identifier.</td>
</tr>
<tr>
<td>affected_ci</td>
<td>Configuration item affected.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result_data</td>
<td>Array Element type of API variables. Each array contains key-value pairs composed of the column and values returned from the server. If no data is received from the server, the output is an empty array.</td>
</tr>
<tr>
<td>output</td>
<td>Formatted return data on running processes used by the abstract workflow.</td>
</tr>
</tbody>
</table>

Tanium integration v2

When the Tanium integration v2 Endpoint Security product is integrated with the Now Platform Security Incident Response (SIR) product, security operation center (SOC) analysts are provided with an Endpoint Detection and Response (EDR) strategy for identifying cyber threats and protecting their company's endpoints (assets) from compromise. Analysts use the configuration item (CI) enrichment results from queries to conduct searches across their networks to help them determine if their assets have been compromised. They quarantine assets with the host isolation capability for further investigation and remediation.
Overview

This initial version of the Tanium integration supports expanded use cases for Tanium capabilities. A more limited Tanium integration is currently available in the ServiceNow Store that supports queries for running process details. For more feature options and product capabilities, you may prefer the Tanium integration v2 version of the Tanium integration.

As a user with the sn_si.analyst role, you launch queries about your assets to the Tanium console in your environment. These queries are based on security event information found in Now Platform Security Incident Response (SIR) security incidents. Using profiles that you create and configure in your Now Platform instance that contain the Tanium capabilities, you request queries that scan your assets and gather CI enrichment data. The data is then pulled from the Tanium console into your Now Platform instance, and it is displayed in the fields of a SIR security incident. Based on the enrichment data results, you launch follow-up actions to isolate host machines from your networks or initiate sightings searches across your network for malicious file hashes. Tanium capability profiles typically define automatic search behaviors on your assets, but you can initiate sightings searches and isolate host machines on your network manually from SIR security incidents.

The following Tanium capabilities are available for this integration.

- Get network statistics
- Get running processes
- Get system details
- Isolate host
- Remove host isolation
- Get Running services
- Get logged on users
- Sighting search

Key features

This integration includes the following key features:

- Supports automated triggering of Tanium queries and actions that are based on incident conditions.
- Supports launching of Tanium capabilities manually from Now Platform Security Incident Response (SIR) security incidents that perform on-demand actions.
• Flexibility to create multiple profiles for triggering different types of Tanium and Now Platform Security Operations capabilities. These profiles automatically gather threat event information that is based on the conditions of a specific incident type such as malware.

• Validate your profile configuration with a preview of the Tanium results on SIR security incidents.

• Isolate compromised systems from the network, and, after remediation, return the systems to the network.

• Launch enterprise-wide searches for malicious hashes, and create child incidents or response tasks to track follow-up remediation.

• If tagging is enabled, security tags identify which Tanium capabilities are initially launched by a workflow and when the queries or actions are successfully completed.

• A full audit trail of Tanium queries and actions is logged in the work notes on SIR security incidents.

• Supports multiple Tanium consoles so that you can apply different policies to user groups and regions.

Supported versions of the App App

Now Platform Plugins
Madrid and later release requirements
For the Madrid release and later family releases, the com.snc.si_dep plugin is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before installing and activating the other Security Operations applications.

The following Security Operations applications must be installed and activated from the ServiceNow Store. Install and then activate one application at a time in the order listed below to ensure a smooth installation:

1. Security Integration Framework
2. Security Support Common
3. Security Support Orchestration
4. Security Incident Response
For more information on setting up your Now Platform instance for the integration, see Install the application and configure the Tanium integration v2

**MID Server**

This integration requires an installed and configured MID Server in your Now Platform instance to connect to the Tanium server (console). For more information, see MID Server on the ServiceNow Product Documentation website.

**Tanium version support and product requirements**

This integration has been tested with Tanium console versions 7.2x and 7.3x. It is recommended that the most up-to-date version of the Tanium client and sensor packages are deployed.

Verify that the following Tanium sensors are active:

- Process Details
- Service Process Details
- Network Details
- Initial Content - Hardware
- Initial Content - OS
- Quarantine
- Incident Response
- Index Query File Exists
- Index Query File Details

Verify these solutions are installed by checking the Tanium Content section on the Tanium Solutions page. An Imported Version is listed for any installed solution.

To confirm a sensor is active, use these query strings for the following sensors:

- Initial Content - Hardware: use "CPU Details"
- Initial Content - OS: use "Operating System Build Number"
- Quarantine: use "Is Quarantined"
- Incident Response: use "Running Processes with Hash"
- Initial Content - Tanium Index: use "Get Computer Name and Index Status from all machines"
For a checklist to track your progress with setup, installation, and verification of expected results for the integration, see Checklist for the Tanium integration v2.

The images used in the following topics were generated for the Kingston release of the Now Platform. For information about the London user interface, see Managing security threats using the Security Analyst Workspace on the ServiceNow Product Documentation website.

The following topics are numbered. For a smooth installation and configuration, and to help you verify expected results, follow the topics in the order they are presented.

**Setup your Now Platform instance for the Tanium integration v2**

The following section lists the setup tasks that you are required to complete in your Now Platform® instance prior to installing the Tanium integration v2 application.

**About this task**

The following table is a list of setup requirements for the application.
Role required: Now Platform administrator (admin)

**Procedure**

1. Verify that you have completed the following tasks before you install the application for the integration.

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Verify that you have assigned the required Now Platform® and (SIR) roles. | The following roles are required:  
  - A user with the system administrator (admin) role installs the application for the integration and assigns the security incident administrator (sn_si.admin) role. |
<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
</table>
| • A user with the security incident administrator (sn_si.admin) role configures the integration, and creates, activates, and removes profiles. A user with this role also assigns the security incident analyst (sn_si.analyst) role.  
• A user with the security incident analyst (sn_si.analyst) role works with security incidents. A user with this role also launches profiles manually from security incidents. If the approval option is enabled for profiles with the Tanium capabilities, a user with this role submits requests for actions such as isolate host and sightings searches to an approval group. | |
| Verify that you are using the versions of Tanium supported for the integration. | This integration has been tested with Tanium console versions 7.2.x and 7.3.x. It is recommended that the most up-to-date version of the Tanium client and sensor packages are deployed.  
For more information about verifying the installation and confirming that sensors are active, see Tanium Version Support and Product Requirements in Tanium integration v2. |
<p>| Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration. | For the Madrid release and later family releases, the com.snc.si_dep plugin is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before installing and activating the other Security Operations applications. |</p>
<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following Security Operations applications must be installed and</td>
<td>The following Security Operations applications must be installed and activated from the ServiceNow Store. Install and then activate one application at a time in the order listed below to ensure a smooth installation:</td>
</tr>
</tbody>
</table>
| activated from the ServiceNow Store. Install and then activate one        | **a. Security Integration Framework**  
| application at a time in the order listed below to ensure a smooth        | **b. Security Support Common**  
| installation:                                                             | **c. Security Support Orchestration**  
|                                                                          | **d. Security Incident Response**  
|                                                                          | For more information on setting up your Now Platform instance for the integration, see [Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application](https://www.servicenow.com/applications/security/operations/product-entitlement.html). |
| Verify that you have installed and configured a MID Server.               | An installed and configured MID Server is required. See the [ServiceNow Product Documentation website](https://www.servicenow.com/productdocumentation/) for more information about MID Servers. |
Approval requests submitted by a user with the sn_si.analyst role to isolate host machines, return hosts to the network, and initiate sightings searches are assigned to a user with the sn_si.admin role by default. As security incident administrator, you can reassign this approval authority during the configuration step for a profile. Before you can assign authority to an approval group, an approval group must be available on the Groups list in your instance.

2. If you want to enable the approval option for profiles during profile configuration, and you do not have an approval group identified, follow these steps to create one.

   a. Navigate to User Administration > Groups.

   b. In the Groups list that is displayed, click New.

   c. Fill in the form.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the group that is displayed when an approval request is submitted, for example, <em>Tanium approvers security ops</em>.</td>
</tr>
<tr>
<td>Group email</td>
<td>(Optional) Group email distribution list or the email address of the point of contact, such as the group manager.</td>
</tr>
<tr>
<td>Manager</td>
<td>(Optional) Name of group manager. Click the search icon to view the list.</td>
</tr>
<tr>
<td>Parent</td>
<td>(Optional) Other group of which this group is a member, if this group has a parent.</td>
</tr>
<tr>
<td>Type</td>
<td>(Optional) Define categories of groups.</td>
</tr>
<tr>
<td>Vendors</td>
<td>(Optional) Assign the vendor_manager role to users who are involved with your organization's vendor management process.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Additional information about the group.</td>
</tr>
</tbody>
</table>

d. **Click Submit.** The new group is displayed in the Groups list.
You have successfully created an approval group. If the **Require approval** option is enabled during configuration step for this profile, this group is available to process requests. In the preceding example, each user in the *Tanium approvers security ops* group has approval authority. Add users to your new group as required who can approve the requests submitted by the security analyst. A user inherits roles from all groups to which the user belongs. You can also assign roles directly to a user. For more information about assigning approval roles to groups and users, see Roles on the ServiceNow Product Documentation website.

To monitor and process requests submitted by users with the *sn_si.analyst* role, each member of the approval group navigates to **My Approvals** in the Now Platform.

**What to do next**
The next step is to install and configure the Tanium integration v2 application from the ServiceNow Store.

**Install the application and configure the Tanium integration v2**
Before you launch the workflows for the integration, install and configure the Tanium integration v2 application from the ServiceNow Store.

**About this task**
Role required: admin

**Procedure**
1. If you have not installed the application for the integration, [Install a Security Operations integration](#) and follow the steps to install it.

2. After you have successfully installed the application, follow these steps to configure it.
a. Navigate to **Integrations > Integration Configurations**, select the Integration Configurations module to display the available integrations, and locate the Tanium integration v2 tile.

![ServiceNow Integrations](image)

b. On the tile, click **Configure**.

c. In the Tanium integration v2 Configuration dialog that is displayed, click **Create new configuration**.

![Tanium Integration Configuration](image)

d. Fill in the form.
Note: You cannot associate a capability with multiple profiles.

When configuring Tanium sources (servers), you cannot reuse a Tanium capability in multiple profiles that share the same Tanium server. Profiles can have the same Tanium capability as long as each profile uses its own Tanium server. For example, as shown in the following figure, you can have the isolate host capability in multiple profiles as long as each profile is mapped to its own Tanium server.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tanium server</strong></td>
<td>Name for the Tanium server, for example, Tanium Server 1. Because you can</td>
</tr>
<tr>
<td></td>
<td>configure and run queries from multiple Tanium servers, this name helps you</td>
</tr>
<tr>
<td></td>
<td>identify a specific server when configuring your profiles.</td>
</tr>
<tr>
<td><strong>API account username</strong></td>
<td>Unique account username for access to the Tanium server, for example,</td>
</tr>
<tr>
<td></td>
<td>administrator.</td>
</tr>
<tr>
<td><strong>Tanium SOAP API URL</strong></td>
<td>Base URL hosting the Tanium SOAP API. Enter the URL with the https://</td>
</tr>
<tr>
<td></td>
<td>protocol, for example, <a href="https://SecopsEnvlbTanium-552012794.us-east-2.elb.amazonaws.com/soap">https://SecopsEnvlbTanium-552012794.us-east-2.elb.amazonaws.com/soap</a>.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>API account password</strong></td>
<td>Unique password for the API account for access to the Tanium server.</td>
</tr>
<tr>
<td><strong>Mid server</strong></td>
<td>Enter the name of the MID server you configured during the setup. Only MID servers that are active and validated are available from this choice list.</td>
</tr>
</tbody>
</table>

The following figure is an example of a completed form.

![Completed form example](image)

**e. Click Submit.**

The new configuration is displayed in the Tanium Configuration list.

![Configuration list](image)

**Trouble?**

If you cannot connect to the server, or your credentials are incorrect, a validation error message is displayed. Verify that your credentials are correct and try again.
What to do next
After you have configured a Tanium server, you are ready to create a new Tanium Capability Profile.

Create a new capability profile for the Tanium integration v2
As a user with the sn_si.admin role, create profiles to determine which Tanium capabilities are run when a new Now Platform® Security Incident Response (SIR) security incident is created. You also configure settings that determine when and under what conditions a profile runs. Profiles run automatically upon incident creation, or you launch them manually from a security incident.

About this task
As a first step to gather the CI enrichment data as security incident administrator, as a user with the sn_si.admin role, configure Tanium servers and create and name profiles in your Now Platform® instance. These profiles are containers for the Tanium capabilities that scan the endpoints (assets) of your environment for system details. Profiles also contain capabilities that perform actions such as isolating host machines and performing sighting searches from the Tanium console. In profiles, you select which Tanium capabilities are run for CI enrichment requests to the Tanium console, and under what conditions these capabilities are run. A profile can be a container for individual tasks, such as gathering network statistics, or, it can contain multiple queries and actions. Assign each Tanium capability to one profile if you want each profile to run independently. If you want a single profile with capabilities that share triggering conditions, you can select multiple Tanium capabilities that are mapped to a single profile.

The following Tanium capabilities are available for a profile:

- Get network statistics
- Get running processes
- Get system details
- Isolate host
- Remove host isolation
- Get Running service
- Logged on users
- Sighting search

A profile includes the following key properties:
• When and under what conditions the profile runs automatically upon incident creation.

• If tagging is enabled, security tags are displayed on security incidents with the profile name.

• Alternate configuration item (CI) fields check for search criteria if there is no Configuration item (CI) data populated on the associated security incident. As a user with the sn_si.admin role, select an alternate field to populate on the security incident when CIs cannot be mapped by the default mapping configuration. You may prefer to enable this option during the configuration step for the profile. For more information, see Alternate Configuration item (CI) trigger field selection for a profile for the Tanium integration v2.

⚠️ **Note:** If multiple profiles use the same source (Tanium server), and they have capabilities that overlap, a query may produce duplicate results. To avoid this conflict, a capability can only appear in one profile that uses the same source.

When configuring Tanium servers, you cannot reuse a capability across multiple profiles that share the same Tanium server. However, you can have a capability in more than one profile as long as each profile has its own Tanium source. For example, within a single Tanium server, **Tanium Server 1**, you can only have a capability such as isolate host mapped to a single profile within that server. You can have this isolate host capability in multiple profiles as long as each profile is mapped to a Tanium server other than **Tanium Server 1**.

Role required: sn_si.admin
Procedure

1. To create a new profile, navigate to **Tanium Integration > Tanium Capabilities**.

The following example is a profile for enrichment queries, but the concepts described in this example apply to all profiles for the integration.

2. With the Tanium Capabilities list displayed, click **New**, and, in the form that is displayed, fill in the fields.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the capability profile. This name helps you identify the profile type and its intention. Examples are running process or Quarantine system.</td>
</tr>
<tr>
<td>Description</td>
<td>Text for additional information about the profile, which may include and further describe the activities of the profile. An example is, Collect system details for enrichment.</td>
</tr>
<tr>
<td>Source</td>
<td>Name of the Tanium server. Only configured servers are available, for example, Tanium Server 1.</td>
</tr>
<tr>
<td>Tanium Capabilities</td>
<td>Capabilities of the Tanium profile. Select the capabilities you want for this profile from the Available column and move them to the Selected column. For this profile, in the following figure, all the capabilities that are commonly used for system enrichment queries are selected for the profile.</td>
</tr>
<tr>
<td>Order</td>
<td>Workflow priority. Default is 100. The value of this field indicates the order that workflows are executed when two or more profiles share the same triggering conditions. If two profiles share the same conditions, the workflow of the profile with the higher execution priority runs first. To set the order or operation, enter a value. For example, 100, 200, 300, 400. The profile with the lowest the number assigned has the highest execution priority. The profile with the highest number has the lowest execution priority.</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
Active | The check box is cleared. The profile is disabled by default.

When disabled, the profile will not run, and it is not available to invoke from a list.

When enabled, the profile is active and runs when the conditions you configure are met.

The following figure is an example of a form for a completed profile used to gather system enrichment data. The capabilities include Get network statistics, Get running processes, Get running service, Logged on user, and System details.

3. Choose one to continue with the configuration.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continue</td>
<td>Save this profile and proceed to the configuration step.</td>
</tr>
<tr>
<td>Update</td>
<td>Update the configuration page with new changes and return to the Tanium Capability Profiles list.</td>
</tr>
</tbody>
</table>
Option | Description
--- | ---
Save | Save this profile and remain on this page.

4. Click **Continue** or **Configuration** on the progress bar to proceed to the next step of the configuration.

If an invalid insert error message is displayed as shown in the following figure, the capabilities you have assigned to this profile already exist in another profile. You cannot reuse the capability across multiple profiles for a single configured Tanium server. In the following image, the message indicates that a profile already exists with one or more of the enrichment capabilities selected for the new profile on Tanium Server 1. You can verify this by navigating to **Tanium Integration > Tanium Capability Profiles** and selecting an item in Name column to view the capabilities of the profile. This error message prevents you from creating duplicate profiles on the same server inadvertently.

5. Review the capabilities you want for this profile and edit the Selected column by adding or removing capabilities.

6. After you are satisfied with your edits, click **Continue** to retry your entry.

After you successfully create and name a profile, the Configuration page is displayed and you are ready to set the conditions under which the profile runs. Before you configure the profile, you may prefer to review the alternate configuration item trigger field option.

### Alternate Configuration item (CI) trigger field selection for a profile for the Tanium integration v2

If the Configuration item (CI) field on the Now Platform® Security Incident Response (SIR) security incident is not populated upon incident creation, or CI search criteria is not matched during a Tanium query, you can select an alternate field on the security incident to check for your search criteria.

One of the keys to the functionality of this Tanium integration v2 and how a profile works is the Configuration Item (CI) field on SIR security incident. The value of this field is the principle value on a security incident that is used to match the IDs of your assets with the information stored in the Now Platform® database.
When a SIR security incident is created by a security event, and a profile is activated, the workflows in the profile scan your assets for a matching value for a Fully Qualified Domain Name (FQDN), a host name, or an IP address based on the value of this Configuration Item field.

In an ideal scenario, a matching value is found in the database, and data can be gathered from the Tanium console for the matching asset, pulled into your Now Platform® instance, and displayed on the related lists of a SIR security incident. The following figure shows an example of the Configuration Item field populated with a host name on a SIR security incident.

If the Configuration item (CI) field on the SIR security incident is not populated with a value, or a match cannot be found for a FQDN, a host name, or an IP address that matches the database, you can select an alternate field on the SIR incident to display any matching CI enrichment data found during the scan of your assets.

During the configuration step of the profile setup, you optionally select an alternate CI trigger field for endpoint identification to ensure that the CI enrichment data from the Tanium lookup is populated on the associated SIR security incident. You can select any field on the security incident as an alternate CI trigger field including any custom fields that you create. Selecting this alternate CI field as a backup ensures that your profiles run even if the CI
field is not populated on the associated SIR security incident upon incident creation.

As an example, a custom field, IP Address, is created and populated on a SIR security incident. If the CI field is not populated on the security incident upon incident creation, this field, IP Address, may used by Tanium as an alternate value during a search of your assets. If the alternate CI field is selected in the capability profile and IP Address is chosen as the alternate CI, Tanium uses the value for the IP Address during its search. You can select any field on the SIR incident as an alternate CI trigger field including any fields that you add to the security incident.

The process for how the alternate field is populated during a workflow is illustrated in the following figure.
Configure a profile for the Tanium integration v2

As a user with the sn_si.admin role, after you create a profile and select the Tanium capabilities you want the profile to run, you configure the settings of the profile so it is invoked only under the conditions that you define.

About this task
You configure a capability profile so it runs only under the conditions you specify and the query results are mapped to fields on a Now Platform® Security Incident Response (SIR) security incident. In the configuration step, you define which conditions on security incident trigger the Tanium capabilities selected for a profile. Click Configuration on the progress bar to return to this page and edit the profile settings at any time during the profile configuration.

Role required: sn_si.admin

Procedure
1. If the Configuration page is not displayed, click Configuration on the progress menu.
2. Fill out the form.
The image that follows the table is an example of a completed form for the profile created in the preceding section as an example for enrichment data with the running process capability.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable alternate CI trigger field</td>
<td>Alternate configuration item (CI). Default is disabled. When the check box is cleared and this option is disabled, an alternate field as a backup for the CI field for endpoint identification is not identified. The CI enrichment data from the Tanium lookup may not be displayed consistently on the associated SIR security incident. Select the check box to enable this option if you want the profile to run even if the CI field is not populated on the SIR security incident. When this option is enabled, the Alternate CI trigger field choice list is displayed. Choose an alternate field from the choice list in the profile setup that checks for your search criteria.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>For example, a value for a custom field such as <em>IP Address</em> may be populated on a SIR security incident. If you select <em>IP Address</em> as an alternate CI, the workflow uses this alternate value to check for a matching ID if no CI is present on the security incident. For more information, see <a href="#">Alternate Configuration item (CI) trigger field selection for a profile for the Tanium integration v2</a>.</td>
<td>Security tag. Default is disabled. When the check box is cleared and this option is disabled, security tags are not displayed on related SIR security incidents. When the check box is selected and the option is enabled, tag names are displayed on the form. These tags are the security tags that are displayed on the associated SIR security incident records. By default, the security tag name is the name you created for the capability profile, for example, <em>running process</em>. Tag names and colors can be edited. For more information about editing the security tag, see <a href="#">Optional) Edit the security tag name for Tanium integration v2</a>.</td>
</tr>
<tr>
<td>Display tag</td>
<td>The <em>Initiated</em> tag indicates when a workflow starts, and it specifies by name which Tanium capability is invoked by the incident. The <em>Completed</em> tag replaces the initiated tag automatically on the related security incident when the workflow is successfully completed. Tags also indicate when a host is successfully isolated from the network.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Auto trigger based on incident</td>
<td>The isolation tag is removed automatically when the host is returned to the network.</td>
</tr>
<tr>
<td></td>
<td>Filter conditions. Default is disabled.</td>
</tr>
<tr>
<td></td>
<td>When the check box is cleared and this option is disabled, the profile does not run for CI enrichment.</td>
</tr>
<tr>
<td></td>
<td>When this option is enabled, the Filter condition builder is available. You are required to set this filtering to specify the conditions under which the profile runs automatically. An common example is, Category is malicious code and Business impact is 1 - Critical.</td>
</tr>
<tr>
<td></td>
<td>These filter settings help you locate only those security incidents related to malicious code activity and critical severity during the preview and test incident step of the configuration.</td>
</tr>
<tr>
<td>Require approval</td>
<td>Request approval. Default is disabled.</td>
</tr>
<tr>
<td></td>
<td>When the check box is cleared and this option is disabled, the optional approval process for the actions selected for the profile is disabled. Verify this check box is cleared if you want to grant a user with the sn_si.analyst role permission to perform actions without requesting prior permission.</td>
</tr>
<tr>
<td></td>
<td>When the check box is selected and the approval option is enabled, a user with the sn_si.analyst role is required to submit a request to perform actions on your network. Enable this option if you want your security analyst to request permission prior to isolating a host machine, restoring it to the network, or initiating a sightings search.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>After a request is submitted, only one approval is required from the group to complete the request. Any member of the approval group has approval authority. Requests are processed in <strong>My Approvals</strong> in the Now Platform instances of the approvers. If a request is rejected, the user with the sn_si.analyst role is required to resubmit a request. The initiated tag is not replaced on the security incident after a request is rejected.</td>
</tr>
</tbody>
</table>

If you do not have an approval group set up in your Now Platform instance for processing requests for host isolation, follow the steps described in **Set-up your Now Platform instance for the Tanium integration v2**.

3. To enable the Alternate CI trigger field, tagging on the related security incident, and to set filters to define triggering conditions, follow these steps. Refer to the preceding image for more information as you read through the steps.
a. Select the **Enable Alternate CI trigger field** check box.
   In the Alternate CI trigger field choice list that is displayed, select an alternate CI field. For this example, **IP Address** is a custom field that was created on the SIR security incident.

b. To define additional filtering, select the **Auto trigger based on incident** check box.
   The filter conditions builder is displayed.

c. To set the first filtering condition, for this example, in the **Keywords** field, enter **Category** and select **Category (category)** in the list that is displayed.

d. Select **is** and **Malicious code activity** from the choice lists for the second and third fields as shown in the following figure.

e. Enter the second filtering condition for this example, **Business impact is 1-Critical**.
   If you add a second filter, only those security incidents that match both of the filtering conditions, **Category is and Malicious code activity and Business impact is 1-Critical**, trigger this profile.

   You have selected an Alternate CI trigger field (**IP Address**) and set triggering conditions for this profile. This profile is invoked automatically only when the security event matches these conditions.

4. Optional: To enable the approval process, follow these steps.
   Your organization may prefer that an analyst request approval prior to invoking actions such as isolating host machines (endpoints), returning machines to the network, or running prolonged sighting searches.

   a. Select the **Require Approval** check box.
      The Approvers field is displayed.

   b. To the right of the Approvers field, click the search icon.
The Approvers list is displayed. The list contains the groups that are available to process requests. Approvers monitor and process requests by navigating to My Approvals in their Now Platform® instances. For more information on approvals, see Approve requests for the Tanium integration v2.

5. Choose one to continue with the configuration.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Previous</td>
<td>Return to the Name step. Return to this page if you want to edit the profile name and Tanium capabilities.</td>
</tr>
<tr>
<td>Continue</td>
<td>Proceed to the Preview step. Preview lets you view security incidents that match your profile configuration.</td>
</tr>
<tr>
<td>Update</td>
<td>Update the configuration page with new changes and return to the Tanium Capability Profiles list.</td>
</tr>
<tr>
<td>Save</td>
<td>Save this profile and remain on this page.</td>
</tr>
</tbody>
</table>

What to do next
You have successfully configured a profile. The next step is to test security incidents for enrichment profiles.

Test security incidents with Tanium capabilities for the Tanium integration v2
Preview the Tanium search capability and how the Configuration item (CI) enrichment data of the capability is displayed on the Now Platform® Security Incident Response (SIR) security incident. Test the profile on a target SIR security
incident to verify that the trigger conditions and filters you set for a capability profile produce the expected results.

### About this task
As the final step in the profile configuration, you preview your Tanium search results to ensure that they match your expectations. You view the enrichment results on the related lists of a SIR security incident. You can also verify that the Tanium profiles match your triggering conditions by seeing the incidents that are created when security event conditions occur. Select from a filtered list to test SIR incidents using this preview capability. You can preview up to five incidents, and you can preview only the incidents that match the auto-trigger conditions and filters that you set during the configuration step.

After you are satisfied with the preview of the query results on the SIR security incident, you can configure the profile to be invoked automatically upon the creation of a security incident. Alternatively, you can invoke the profile manually from the related SIR security incident. After the profile is activated, the results of the queries are pulled back into the Now Platform Security Operations environment and displayed on the related lists of the SIR security incidents that match the triggering conditions.

**Note:** If you click Preview On Incident with security incidents displayed in the fields, the workflows for the preview are performed on live SIR security incidents. If your capability returns enrichment data as expected, these results change the related lists on the security incidents that match the profile conditions. Perform the test if altering the security incidents that are displayed in the preview is acceptable.

**Note:** The figures in the following section are shown with Tabbed forms selected in System Settings. For more information about selecting and clearing tabbed forms, see Configuring the form layout and the section about tabbed forms on the ServiceNow Product documentation website.

Role required: sn_si.admin

### Procedure
1. If the Preview page is not displayed, click **Preview** in the progress bar.
   The Preview page is displayed.
2. To the right of the first field, click the search icon to view a list of security incidents that match the profile criteria for the automatic triggering conditions that you set for the profile. For this example, only security incidents that match Category (category) is Malicious code activity and Business impact is 1-Critical are displayed.

3. From the list that is displayed, click a SIR incident.

The security incident number is displayed in the first field.

4. Repeat the preceding steps to select up to five security incidents for the fields on the form.
5. Click **Preview On Incidents** to display the security incidents. Tabs are displayed on the bottom of the page for the incidents that you selected. A message is displayed if the preview is loading for longer workflows.

6. To view a security incident, click a **Preview Incident** tab.

   For this example, the asset that matched the scan conditions is displayed in **IP Address** field on the security incident. This is the alternate CI field selected for the Configuration item field for this profile. In the Category and Business impact fields, the filtering conditions that you configured are displayed. If tagging is enabled, a security tag is displayed that indicates the workflow is initiated. This security tag is replaced with **Completed** tag after the workflow is completed as shown in the following figure.

7. Use the scroll bars to view the work notes.

8. In Related Links, click **Show all Related Lists**.

   If tabs are not displayed for the related lists, for more information about selecting and clearing tabbed forms, see Configuring the form layout and the section about tabbed forms on the ServiceNow Product documentation website.
The CI enrichment results of the Tanium query are displayed in the following related lists. The following table lists the general information that is displayed on the related lists that return results for the enrichment capabilities.

<table>
<thead>
<tr>
<th>Tanium Related List (Tab) name</th>
<th>Description of results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tanium Network Stats</td>
<td>Information about all processes with open ports on the endpoint including source and destination IP addresses and protocol.</td>
</tr>
<tr>
<td>Tanium Running Processes</td>
<td>Details for all active processes on the endpoint including hash information.</td>
</tr>
<tr>
<td>Tanium Running Services</td>
<td>Details for all active services on the endpoint including service type and start mode.</td>
</tr>
<tr>
<td>Tanium Logged on Users</td>
<td>Users currently logged on to the endpoint.</td>
</tr>
<tr>
<td>Tanium System Details</td>
<td>Comprehensive list of machine identification information such as Mac, FQDN, and IP address.</td>
</tr>
</tbody>
</table>

9. Click a related list (tab) and open a record on the list that is displayed to view details about the enrichment data.

10. Choose one to continue with the configuration.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click a Preview Incident tab to preview another security incident.</td>
<td>Preview another security incident.</td>
</tr>
<tr>
<td>Previous</td>
<td>Return to the Configuration step and edit the filtering conditions.</td>
</tr>
</tbody>
</table>
Create and configure a profile to Isolate host for the Tanium integration v2

After you determine that an asset is infected or otherwise compromised from the results of your enrichment queries, you may prefer to create a profile to isolate an infected endpoint using the isolate host capability. If approvals are configured, a user with the sn_si.analyst role requests approval prior to isolating the host machine.

About this task
If your enrichment query results and investigations determine that an endpoint has been infected or otherwise compromised in your environment, you can isolate the host. If, for example, you determine that a hacker is in a user's account on your network, you can quarantine the host machine from the network. An optional approval process for the host isolation action is available. If the tagging option is enabled, security incidents are tagged to indicate that the CI from the associated security incident is isolated. After it is determined that it is no longer infected or otherwise compromised, you release the host machine from quarantine and place it back online. The security tag is automatically removed from the security incident, and all workflow actions are written to work notes on the security incident to create an audit trail.

Role required: sn_si.admin
1. Navigate to **Tanium Integration > Tanium Capability Profiles**.

2. Click **New**. In the form that is displayed, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the profile to distinguish it for the isolate host capability. An example is, <strong>Quarantine endpoint</strong>.</td>
</tr>
<tr>
<td>Source</td>
<td>Name of the Tanium server for this profile, for example, <strong>Quarantine endpoint</strong>.</td>
</tr>
<tr>
<td>Tanium Capabilities</td>
<td>Move Isolate host from Available to Selected.</td>
</tr>
<tr>
<td>Order</td>
<td>Leave this field in its default setting.</td>
</tr>
<tr>
<td>Active</td>
<td>Select the check box to enable the profile.</td>
</tr>
</tbody>
</table>
3. Click **Continue**. In the Configuration form that is displayed, fill in the fields. For more general information about the fields on the configuration form, see "Configure a profile for the Tanium integration v2."

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable alternate CI trigger field</td>
<td>Alternate field for the Configuration item field. If the check box is selected and this option is enabled, choose an alternate field from the choice list. If this option is disabled, data from the Tanium query may not be displayed consistently on the associated security incident.</td>
</tr>
<tr>
<td>Display tag</td>
<td>Display security tags. If the check box is selected and this option is enabled, security tags are displayed on related SIR security incidents. For this example, tags show when the isolate host workflow is initiated and when the host is successfully isolated.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>If this option is disabled, security tags are not displayed on related SIR incidents.</td>
<td>If you prefer to invoke this profile manually from a SIR security incident, leave this check box cleared and disable this option. If the auto-trigger option is disabled, the Filter condition builder is not available. For security incidents that match this profile, you are required to submit the host isolation request manually from a SIR security incident. If you prefer that the profile runs automatically upon incident creation, select the check box to enable this option. If you set filtering conditions for this option and the approval option is disabled, host machines are isolated automatically when the triggering conditions of the profile match security incidents. If the auto-trigger option is enabled, the Filter condition builder is available. Set this filtering to specify the conditions under which the profile runs automatically.</td>
</tr>
<tr>
<td>Require approval</td>
<td>Approvals. When the check box is selected and this option is enabled, an approval step is added prior to isolating a host machine. If the Auto trigger based on incident option is enabled, but approvals are disabled, host machines are isolated automatically when the triggering conditions of the profile match security incidents.</td>
</tr>
</tbody>
</table>
If this approval option is enabled, click the search icon and select an approval group from the list to process requests.

Clear this check box to disable approvals if you want to grant a user with the sn_si.analyst role permission to isolate a host machine, or if you want the triggering conditions of the profile to isolate the host machine upon incident creation.

The following image is an example of a completed configuration form for a profile with the isolate host capability. The Alternate CI field is IP Address. Security tags are enabled. Filters are defined so that only security incidents that are related to malicious code and a critical business impact trigger the profile. The approvals option is enabled. For this example, if the incident matches the triggering conditions set for the profile, requests to isolate a host are submitted for approval automatically.
Alternatively, disable the auto triggering option and submit a request to isolate a host machine manually directly from a security incident. For more information, see Submit a request to isolate host manually from a security incident for the Tanium integration v2.

4. Choose one to continue with the configuration of the profile.

<table>
<thead>
<tr>
<th>Previous</th>
<th>Return to the Name step. Return to this page if you want to edit the profile name and capabilities.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continue</td>
<td>Proceed to the Preview step. Preview lets you view security incidents that match your profile configuration.</td>
</tr>
<tr>
<td>Save</td>
<td>Save this profile and remain on this page.</td>
</tr>
</tbody>
</table>
Update the configuration page with new changes and return to the Tanium Capability Profiles list.

**Note:** The same principles in the preceding steps apply for a profile with the Remove host isolation capability. Use a profile with Remove host isolation capability to return a host machine to the network. You may prefer to return the host machine to the network using the Isolate Host Entries list in your Now Platform. This method is described in Submit a request to isolate host manually from a security incident for the Tanium integration v2.

**What to do next**
To launch the isolate host profile manually from a security incident, see Submit a request to isolate host manually from a security incident for the Tanium integration v2. If a request is already submitted, Approve requests for the Tanium integration v2 for more information about approving requests.

**Submit a request to isolate host manually from a security incident for the Tanium integration v2**
For profiles with the host isolation capability, you may prefer to submit requests manually from related Now Platform® Security Incident Response (SIR) security incidents.

**Before you begin**
Role required: sn_si.admin

**Procedure**
1. If the security incident you are working with is not displayed, navigate to **Security Incident > Show all Incidents**.
2. In the list that is displayed, locate and click the incident in the Number column (for example, SIR0010086) to open the record. The security incident is displayed.
3. On the security incident, scroll to the Related Links section and click the **Tanium Capabilities** link.
The Tanium Profiles dialog is displayed.

4. To the right of the Tanium Profile field, click the search icon.

5. In the Tanium Capability Profiles list that is displayed, click the profile in the **Name** column that has the isolate host capability you created.

6. With the profile displayed in the **Tanium Profile** field, in the dialog, click **Submit**. In the dialog that is displayed, confirm your choice.

The security incident is displayed. If tagging and approvals are enabled, at the top of the record, the tag name for the profile with the isolate host capability is displayed, in this case, **Quarantine endpoint - initiated**.
The work notes verify that the request is pending approval.

You have successfully submitted a request manually to isolate a host machine from a SIR security incident. The request is sent to the approval group for review.

As a user in the approval group, to process the isolation request at this point for this security incident, navigate to My approvals in your instance. For more information, see Approve requests for the Tanium integration v2.

After the host isolation workflow is successfully completed and the request has been approved, work notes are posted to the security incident.
The completed security tag replaces the initiated tag.

Verify that the endpoint is isolated by checking standard network processes on your Tanium console.

After you conclude your investigation and remediation, the next step is to return the host machine to your network.

7. To remove the host from quarantine and return it to the network, follow these steps.

a. Navigate to Tanium Integration > Isolate Host Entries.

The Isolate Host Entries list is displayed. At the top of the list in the Status column, search for the asset that you isolated.

b. In the Added date column, click the item to open the record.
The Isolate Host Entries record is displayed. After a request is approved, an audit trail with all the associated actions from the SIR security incident is displayed in the work notes. The last entry in the work notes shows that a successful host isolation was completed along with the date. The Approvals for Isolated Hosts section shows that the request is approved (Approved) and no further action is required (No Longer Required) for the other member of the approval group, Abel Tuter.

c. To launch the workflow and request approval to restore the machine to the network, on the Isolate Host Entries record, click Remove Isolation. The workflow is initiated and the Isolate Host Entry record is displayed. At the top of the record, the Status field changes from Isolated to Pending Approval. A work note is posted that a request is pending approval for the machine to be restored to the network.

d. After you have been notified of the request, as an approver for host isolation, navigate to My Approvals in your instance and open the record to process the remove isolation request.
e. Click **Approve** to approve the request and return the asset to the network, or, click **Reject** to keep the request in pending approval. After you approve the request to remove the host isolation, the tag on the security incident is removed. Work notes create an audit trail for the remove isolation request.

As a user with the sn_si.analyst role, if the request to return the host to the network is rejected, you are required to submit a new request.

Alternatively, to remove a host from isolation, you can create a Tanium profile with the *Remove host isolation* capability.

8. Create a new profile with only the *Remove host isolation* capability. For more information about creating a profile, see .

9. Configure the profile with the settings you prefer.

**Note:** A single profile cannot support both the Tanium isolate host and remove host isolation capabilities. If you prefer to use a profile to remove host isolation, create two separate profiles: one profile with the isolate host capability, and the other profile with the remove host isolation capability. For more information about configuring a profile, see Create a new capability profile for the Tanium integration v2.

10. If not displayed, navigate to the SIR security incident you are working with.

11. See the preceding steps for more information about how to select the profile and invoke it directly from the SIR security incident.

12. In the dialog that is displayed, confirm your choice to launch the workflow. The SIR security incident is displayed. See the preceding steps for viewing the audit trail in work notes, locating the Isolate Host Entries record, and processing remove isolation requests in My Approvals.

You have successfully submitted a request to isolate a host machine manually from a SIR security incident. You returned the machine to the network using the Isolate Host Entries list.

**What to do next**

If the approval option is enabled in the profile, as a user with approval permission, your next step is to process requests.

**Approve requests for the Tanium integration v2**

If the approval option is enabled, a user with the sn_si.analyst role submits requests to isolate host machines or initiate sightings searches across your network. As a user with approval permission in the Now Platform®, you process these requests. If your organization requires approvals as an extra check prior to
invoking these actions, you may prefer to enable the approval option during the configuration step for a profile.

**About this task**

Users with the sn_si.analyst role submit requests to isolate host machines, return them to the network, and initiate sighting searches. The requests are by default approved by users with the sn_si.admin role. You may prefer to assign this approval authority to a group during the configuration step for a profile. Before you can reassign authority to an approval group, an approval group must be available on the Groups list.

If you have not already assigned an approval group to process requests, for more information about creating an approval group and assigning approvers, see [Setup your Now Platform instance for the Tanium integration v2](#).

The following example shows how to process a request to isolate a host. The same process applies to processing a request for a sightings search.

**Role required:** sn_si.analyst to submit a request.

**Role required to process approvals:** sn_si.admin or an assigned group

**Procedure**

If you are a user with the sn_si.admin role, or you are in an approval group assigned to process requests, follow these steps to approve or reject a request.

**a. Navigate to My Approvals in your instance.**

For this example, the user name of the approver is Mary admin.

![My Approvals](image)

The approvals list is displayed.

**b. In the State column, click a Requested item to open the approval record for the request.**
c. In the Approval record that is displayed, click **Approve** or **Reject**.

After you click **Approve** or **Reject**, the workflow may take a few moments to run. On the record at the top, a message is displayed if the transaction takes more than a few seconds.

After a few moments, in the approval record that is displayed, the **State** field changes from **Requested** to **Approved**. The State column on the Approvals list also changes from **Requested** to **Approved** as shown in the following figure.

![Approval Record](image)

After the request is approved, no additional approvals are required for this request. On the Approvals list, in the State column, for the other members of the approval group, **No Longer Required** is displayed for this request.

If the request is rejected, the host is not isolated, and the request remains pending. As a user with the sn_si.analyst role, if the request is rejected, you are required to submit a new request to isolate the endpoint.

d. Navigate to **Security Incident > Incidents > Show All Incidents** and, in the Number column, click to open the security incident you are working with.

After the request is approved, on the SIR security incident, the **Isolate Host - Completed** tag replaces the **Isolate Host - Initiated** tag.

The Work notes on the SIR security incident also indicate that the host isolation is successfully completed, and the name of the approver is listed.
**Note:** Although the security tag and Work notes on the security incident indicate that a successful isolate host workflow is completed, return to your Tanium console and verify that the host machine is isolated.

After you have completed your investigation and remediation on the asset, and you want to remove the host machine from quarantine and return it to the network, launch the Remove Isolation workflow from the Host Isolation Entries table in your Now Platform® instance. If approvals are enabled, as an approver, process this request as described in the preceding steps.

Alternatively, you may prefer to create a profile for the remove host isolation capability. For more information about creating a profile with the remove isolate host capability, see Create and configure a profile to Isolate host for the Tanium integration v2.

Create and configure a profile for a process hash sightings search with the Tanium integration v2

After an enrichment query for running processes is successfully completed, as a user with the sn_si.analyst role, you may want to use the results to launch a sightings search. Analysts use sightings searches to locate infected machines across their organizational networks and address end-to-end security incident response cases.

**Before you begin**

As a user with the sn_si.analyst role, you launch sightings searches based on enrichment data from system queries to determine which internal systems and configuration items (CIs) in your organization may be infected with the same malicious files or running processes. For example, if a phishing incident is reported that contains a file observable (file hash), you may want to determine how many users may have opened the suspicious file. Similarly, if a Now Platform® Security Incident Response SIR security incident is created for a malware incident that contains a malicious process (process hash), you may want to see how many hosts have this process. In both scenarios, after the file and process hash observables are determined to be malicious from the results of your enrichment queries, you launch a sightings search across the CIs and the internal systems of your network. The search helps you identify if there are additional sightings of these suspicious observables in your network.

The search capability is the only Tanium capability type that a sightings search profile supports. Searches can be launched only from profiles that have the sightings search capability. During the configuration, select one server, or identify multiple servers for a search to run on. Through the sightings search profile, you connect to servers for a particular search type, specifically, a process hash or a file hash. The option to connect to a single server or multiple
servers in a sightings search profile permits you to determine the scope of a particular search on various components in your organization.

When multiple servers are enabled for sightings searches, a user with the sn_si.analyst role views multiple work notes and security tags, a distinct set for each Tanium server that is configured in the sightings search profile. If the approval option is enabled, approvals are also required for each Tanium server that is configured. The following figure is a process flow for a sightings search.

Role required: sn_si.admin
Procedure

1. If you have not created a sightings search profile, follow these steps to create one.

   a. Navigate to **Tanium Integration > Sightings Search Profiles**

   b. Fill out the form.

      An example of a completed form follows the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the capability profile.</td>
</tr>
<tr>
<td>Description</td>
<td>Text for additional information about the profile.</td>
</tr>
</tbody>
</table>
| Tanium capability   | Tanium sightings search capability. Select the search capability that you want for the search. Choose one for a search.  
                        • Sightings Search - File Hash    
                        • Sightings Search - Process Hash |
| Servers             | Server(s) for the profile. Select a server, or multiple servers to use for the sightings search. Select configured servers from the Available column and move them to the Selected column. Having the flexibility to choose and employ multiple servers broadens your search capability. Each server selected for the profile runs the associated search when this profile is used. By selecting more than one server, you broaden your search. |
| Order               | Leave this field in its default setting.                                    |
| Active              | The check box is cleared by default to indicate that the profile is disabled. |
When the check box is selected and the profile is enabled (activated), the sightings search is available to invoke from a SIR security incident. If results are returned and displayed on the Running Processes related list on the security incident from an enrichment query, you launch the search directly from the security incident.

When the check box is cleared and the profile is disabled, the profile is inactive and not available to invoke from a SIR security incident. If there are no results returned from the Running Processes enrichment query, the sightings search action is not an available option on the related security incident.

c. Choose one option to continue with the configuration.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update</td>
<td>Update the configuration page with new changes and return to the Sightings Search Profiles list.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete this profile.</td>
</tr>
<tr>
<td>Continue</td>
<td>Continue to the Configuration page.</td>
</tr>
</tbody>
</table>

2. With the Configuration page displayed, fill out the form.

An example of a completed form follows the table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum wait time for sightings results (minutes)</td>
<td>Maximum time in minutes the search is gathering results. Default is five minutes.</td>
</tr>
<tr>
<td>Maximum sightings search results</td>
<td>Maximum search results returned for the wait time of the search that you selected in the preceding field. Default is 100 items.</td>
</tr>
<tr>
<td>Display tag</td>
<td>Security tag. Default is selected. If the check box is selected and tagging is enabled, a security tag for the associated SIR security incident record is automatically created. By default, the security tag name is the name you created for the profile, for example, Sightings Search - Process hash. If the check box is cleared and tagging is disabled, security tags are not displayed on the associated SIR security incident. The tag names and colors can be edited. For more information about editing the security tag, see</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>(Optional) Edit the security tag name for Tanium integration v2.</td>
<td></td>
</tr>
<tr>
<td>Requires approval</td>
<td>Approvals. Default is disabled.</td>
</tr>
<tr>
<td></td>
<td>When the check box is cleared, the optional approval process for the sightings search is disabled. Verify this check box is cleared if you want to grant a user with the sn_si.analyst role permission to perform sightings searches without requesting prior permission.</td>
</tr>
<tr>
<td></td>
<td>Select this check box to enable the approval option if you want a user with the sn_si.analyst role to request permission prior to conducting sightings searches on your network.</td>
</tr>
<tr>
<td></td>
<td>After a request is submitted, only one approval is required from the group to complete the request. Any member of the approval group has approval authority. Requests are processed in My Approvals in the Now Platform instances of the approvers.</td>
</tr>
</tbody>
</table>
3. Choose one to continue with the configuration.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Previous</td>
<td>Return to the Name page.</td>
</tr>
<tr>
<td>Update</td>
<td>Update the configuration page with new changes and return to the Sighting Search Profiles list.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete this profile.</td>
</tr>
<tr>
<td>Finish</td>
<td>Save the settings and finish the configuration. In the dialog that is displayed, confirm your choice.</td>
</tr>
</tbody>
</table>

4. To complete the configuration, click **Finish** and confirm your choice. You are now ready to invoke the sightings search from a SIR security incident.

5. Navigate to the SIR security incident you are working with.

6. If the Tanium Running Processes related list is not displayed, click the **Show all Related Lists** link.

   If no results are displayed on the Running Processes related list, with the Tanium Running Processes list selected, in the gray banner, right-click and click **Refresh** to reload the page.
7. From the list that is displayed on the Tanium Running Process list, select an item or items.

Note: To run a sightings search, you can select an item from either the Tanium Running Processes or Observables related lists on a SIR security incident.

For example, in the preceding figure, `chrome.exe` is highlighted on the Tanium Running Processes list. After the workflow is invoked, a sightings search is initiated for this item (`chrome.exe`). For this example, the workflow searches for the process hash of this item.

8. Scroll to the bottom left of the SIR security incident and expand the Action on rows choice list.

9. If Sightings Search is available in the choice list, click it to initiate the sightings search.

If you do not have a sightings search profile configured, in the expanded Actions on rows choice list, the Sightings Search action is not available.

10. In the dialog that is displayed, select the sightings search profile that you want to run the search and click Submit.
If the tagging option is enabled in the sightings search profile, a security tag is displayed on the SIR security incident that indicates the sightings search is initiated.

If the approval option is enabled, a work note is posted that a request for approval is pending. After the request is approved, the workflow for the search is launched. For more information about approving requests for searches, see Approve requests for the Tanium integration v2.

Sightings search results are displayed on the Tanium Sightings Results and Tanium Sightings Details related lists of the related SIR security incident. In the following figure, the Tanium Sightings Details list is selected.

For this search example, no prior approval was requested, and two sightings were returned as shown in the preceding figure. The work notes indicate that the search started is successfully completed.
11. To create a new child incident or a response task from the search results, from this list on the Tanium Sightings Details related list on the SIR incident, select the item that you want to create a child incident or response task for.

If you want to group search result items to a single child incident or response task, select the all items from the Tanium Sightings Details related list that you want for the incident. Any observables you select from the list are assigned to both the child incident and the related parent SIR security incident. You have the flexibility to create a single incident for multiple search results.

12. After you have selected the items you want, expand the Actions on selected rows choice list, and select either Create Child Incident or Create Response Task.

13. Click the Child Security Incident related list to view the new incident.

14. Click an item from the Sightings Search column to open a record.

15. Review the work notes.
What to do next
You have successfully created and configured a profile for a sightings search. You have located results on the related SIR security incident and launched a sightings search. You have also verified expected results from the search and created a child security incident or response task based on the search results.

Enable indexing requirements in Tanium for a file hash sightings search with the Tanium integration v2

Follow these steps to enable the Tanium file indexing functionality in the Tanium console. This indexing functionality must be enabled for sightings searches for file hashes with the Tanium integration v2.

Before you begin
Role required: Tanium console administrator

About this task
Before you can use the Sightings Search – File hash capability with this integration, you must first enable the file indexing functionality in the Tanium console. This indexing must be enabled in Tanium before the sightings search functionality of the Now Platform® is enabled in a profile and invoked from a SIR security incident.

As a Tanium console administrator, follow these steps to enable the indexing functionality in Tanium to match file hashes.

For more information about indexing in Tanium, see Indexing, prerequisites for indexing, status of indexing on the Tanium Product Documentation website.

The following Tanium sensors and solutions are required:

- Index Query File Exists
- Index Query File Details
- Tanium Index Solution.

Procedure

1. Log in to the Tanium Console.
2. On the home page, click **Tanium Solutions**.
3. Near the bottom of the list that is displayed on the Supported Solutions page, select **Tanium Index** in the Name column to select it.
4. Click **Import Solution**.
5. Navigate to **Actions > Scheduled Actions**.
6. In the Scheduled Actions list, click to select **Deploy Distribute Tanium Endpoint Index Tools**.

7. Click **More**, and from the expanded menu, click **Enable Action**.
   - This action is specific to Windows Endpoints. For Linux and Mac Endpoints, the packages are different.

8. Follow these steps to edit the enabled Action to start the deployment of tools.
   - a. If not already selected, click **Deploy Distribute Tanium Endpoint Index Tools** to select it.
   - b. Click **Edit**.
   - c. Click **Show Preview to continue** to preview the action.
   - d. Click **Save Action**.

   ![Note: During testing at ServiceNow and for this example, All Computers was selected for the Action Group field in the Targeting Criteria section, because only Windows endpoints were used. The grouping of this action should be set according to the operating system of the endpoint.]

9. Navigate to **Content > Packages**.

10. On the Packages page that is displayed, click **Distribute Tanium Endpoint Index Config** to select it.

11. Click **Edit**.
   - This action is specific to Windows Endpoints. For Linux and Mac Endpoints, the packages are different.

12. On the Edit Package page that is displayed, download `sample_config.ini` and edit the .ini file details as required.

   ![Note: This file contains Index-related settings including Max. file size to hash and hash type.]

13. After you complete your other edits, save the file as `config.ini`.

14. Click **Add** to upload the file to the Distribute Tanium Endpoint Index Config package.

15. Click **Save** to save your changes to the package.

16. With the question builder displayed, use the search criteria to list all the machines that you want to deploy the configuration to.
Names are displayed under the Name column.

17. Click **Deploy Action**.

18. With the Deploy Action screen displayed, under the Deployment Action field, select **Distribute Tanium Endpoint Index Config**.

19. Click **Show preview to continue**.
   The page that is displayed lists the machines the configuration package will be deployed to along with other deployment information.

20. On the bottom of the page, click **Deploy Action**.

21. Navigate to **Home > Actions > Scheduled Actions**.

22. On the list that is displayed, click **Deploy Start Indexing** to select it.
   This action is specific to Windows Endpoints.

23. Follow these steps to edit the enabled Action to start the Indexing.
   a. Click **Edit**.
   b. Click **Show Preview to continue** to preview the action.
   c. Click **Save Action**.

   ❄️ **Note**: During testing at ServiceNow and for this example, **All Computers** was selected for the Action Group field in the Targeting Criteria section, because only Windows endpoints were used. The grouping of this action should be set according to the operating system of the endpoint.

24. To check file indexing status, with the Tanium Question Builder displayed, in the Question field, enter **Get Computer Name and Index Status from all machines**.
   In the Index Status column, the status for each machine is displayed. Running and **Initial Index Scan Completed** status messages indicate you have successfully enabled the indexing requirements in the Tanium console required for this integration.

**Integration architecture for the Tanium integration v2**

The following topic outlines how the integration architecture works and explains why there are setup steps that you are required to complete prior to installing the application from the ServiceNow Store.
Key terms for this integration

The following key terms are used during the installation and configuration. For more information about the following terms, see the ServiceNow Product Documentation website.

Now Platform

An enterprise ServiceNow product. The Now Platform is the base upon which individual components, such as SIR, IT Service Management (ITSM), and other products are built.

Security Incident Response (SIR)

A Now Platform App application that tracks the progress of security incidents from discovery and initial analysis, through containment, eradication, and recovery, and into the final post incident review and closure.

Application (plugin)

Applications, or, Plugins, are software components that provide specific features and functionalities within your Now Platform instance.

Tanium console

Also called the Tanium server, the user interface in your environment where you manage the Tanium products and settings.

Tanium Incident Response

A Tanium solution that consists of a collection of sensors and functionality for incident response management.

Tanium Capability

An automatic activity that originates from the Tanium console that you set up to run on your endpoints (assets) in your environment.

Profile

Settings for Tanium capabilities that you configure to specify when and under what conditions sensors submit queries to, or perform actions on your assets.

MID server

An application that facilitates communication and movement of data between the Now Platform and external applications, data sources, and services.

Security incident admin (sn_si.admin)
A user with this role oversees the configuration of the integration with the SIR product in your Now Platform instance. This role also approves delete requests for emails by default and assigns the security incident analyst (sn_si.analyst) role as required. This role also has full control over all Service Management data.

**Security incident analyst (sn_si.analyst)**

A user with this role interacts with and analyzes security incidents in the SIR product. This use is sometimes also referred to as a security operations center (SOC) analyst.

**XML payloads**

The information sent via SOAP connection via XML payloads includes a plain text username and an encrypted password for the Tanium console, an FQDN or IP address as an endpoint identifier, and hashes for processes.

**System connection and data flow for queries**

The basic data flow between the Tanium console (server) and the Now Platform instance is illustrated in the following figure. A Tanium server (console) requires a MID server to connect to your Now Platform instance. Once activated, the profiles you create using the Tanium capabilities run queries on your assets to gather enrichment data or perform actions on your assets. Both queries and actions are submitted to the Tanium console via the Now Platform MID server to check if an endpoint associated with a SIR security incident has been impacted. For data enrichment, the Tanium console queries your assets and retrieves running process and service details, network statistics and active connections, logged on users, and other system details. The results of the queries are pulled back into the Now Platform and displayed on the related lists of the SIR security incident. For actions such as isolating hosts and performing sighting searches, requests are sent from your Now Platform instance, and an optional approval process is available.
As shown in the preceding and following figures, you can have one group of endpoints managed by one console, and another group of endpoints managed by another console. Data can be pulled from multiple Tanium consoles via a single MID server, however, you also have the flexibility to configure multiple MID servers to fit your organization's needs as required.
Workflows

For more general information about workflows, see Getting started with workflows on the ServiceNow Product Documentation website.

- Security Operations - Tanium - Run a query job
- Security Operations - Tanium - Create Isolate Host Entry
- Security Operations - Tanium - Get Logged On Users
- Security Operations - Tanium - Get network stats
- Security Operations - Tanium - Get network stats launcher
- Security Operations - Tanium - Get running processes
- Security Operations Tanium integration V2 - Get running processes launcher
- Security Operations - Tanium - Get running services
- Security Operations - Tanium - Get System Details
- Security Operations - Tanium - Isolate Host
- Security Operations - Tanium - Remove host isolation

**External systems connection**
The integration requires that the MID server communicates via HTTPS protocol connection to the Tanium console.

**(Optional) Edit the security tag name for Tanium integration v2**
As a user with the sn_si.admin role, you can edit the tag names and colors of the security tags for the tagging option. Security tags help you track the profiles that are invoked on Now Platform® Security Incident Response SIR security incidents.

**About this task**
Security tags help you quickly identify which security incidents have profiles. Tags also help you identify whether a host has been isolated, or, if it has been removed from isolation. By default, the name of the security tag is the name of the profile, and the color of the security tag is black. You can change the names and colors of the tags to help you recognize tags more easily.

**Role required:** sn_si.admin

**Procedure**
1. If the Tanium Capability Profiles list is not displayed, navigate to Tanium Capability Profiles.
2. In the Name column, select the profile you want to edit the tag for.

   ![Image](image.png)

   The record for the capability is displayed.
3. To edit a tag, to the right of a tag name, click the information icon, and open the tag record.
4. In the record that is displayed, edit the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the security tag.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Color</td>
<td>Security tag color. Select a color from the choice list.</td>
</tr>
<tr>
<td>Security Tag Group</td>
<td>Enter a name of the security tag group. Click the information icon to view the available groups. Default is Metatag group.</td>
</tr>
<tr>
<td>Enforce restricted access</td>
<td>Select this check box to assign read and write roles needed by users to read or write to records that have this security tag. Default is cleared.</td>
</tr>
<tr>
<td>Order</td>
<td>Specify the order the tag appears on forms or within a list. Default is 100.</td>
</tr>
<tr>
<td></td>
<td>To set the order on the list, enter a value. For example, 100, 200, 300, 400. The tag with the lowest the number is displayed first on the list. The profile with the highest number is displayed last.</td>
</tr>
<tr>
<td>Active</td>
<td>Turn the tag on or off.</td>
</tr>
<tr>
<td>Description</td>
<td>A description for the tag.</td>
</tr>
</tbody>
</table>

5. Choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update</td>
<td>Update the page with new changes.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete this tag record.</td>
</tr>
</tbody>
</table>

**Checklist for the Tanium integration v2**

Use this checklist to guide you through all the tasks of the integration. The following checklist includes setup and installation tasks and examples of use cases that include expected results for the integration.

**About this task**

Track your progress with the setup, installation, and configuration of the integration with the following table. Complete all the tasks for a step before moving on to the next step. Each row of the table lists tasks and identifies the
roles that are required to perform the tasks. Numbered topics of the installation and configuration guide are also referenced. Roles required: Roles are listed for each step.

**Procedure**

Follow the steps in the table in the order that they are presented.

<table>
<thead>
<tr>
<th>Checklist</th>
<th>As a user with the Now Platform® admin role, set up your Now Platform® instance.</th>
<th>a. Assign Now Platform® and Security Incident Response roles.</th>
<th>b. Verify ServiceNow core plugins that support the integration are installed and activated.</th>
<th>c. Install and configure a MID server in your Now Platform® instance.</th>
<th>d. Create an approval group if you want to process requests submitted from the security incident analyst for the isolate host and sighting search capabilities.</th>
<th>For more information, see Setup your Now Platform instance for the Tanium integration v2.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>As a user with the Now Platform® admin role, install the application and configure a server.</td>
<td>For more information, see Install the application and configure the Tanium integration v2.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>As a user with the Now Platform® sn_si.admin role, create an enrichment profile for Tanium capabilities.</td>
<td>For the steps required to create a profile, see Create a new capability profile for the Tanium integration v2.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>As a user with the Now Platform® sn_si.admin role, configure an enrichment profile.</td>
<td>a. Review the information about triggering conditions and settings.</td>
<td>b. Configure the triggering and filtering conditions for the profile.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
c. Test and preview security incidents.

d. Locate search results and work notes on the related lists on the related security incidents.

For information about triggering conditions and the alternate CI field, see Alternate Configuration item (CI) trigger field selection for a profile for the Tanium integration v2. For information about configuring the settings of a profile so it runs under the conditions that you want, see Configure a profile for the Tanium integration v2. For more information about testing security incidents with Tanium capabilities, see Test security incidents with Tanium capabilities for the Tanium integration v2.

As a user with the Now Platform® sn_si.admin role, create and configure a profile with the isolate host capability. As a user with the sn_si.analyst role, submit a request to isolate a host machine and review the security incident. After host isolation is approved, submit a request to restore the host to the network.

a. Review the information about triggering conditions and settings.

b. Configure the profile.

c. If approvals are enabled, as a user with the sn_si.analyst role, submit a request to isolate host from a security incident.

d. As an approver, process the isolate host request.

e. Locate work notes, security tags and details on the related security incident.

f. Remove the host isolation from the Isolate Host Entries record or with a profile that supports the remove host isolation capability.

For more information on creating and configuring a profile for the isolate host capability, see Create and configure a profile to Isolate host for the Tanium integration v2. For more information about submitting a request from a security incident to isolate a host machine or to return it to the network, see Submit a request to isolate host manually from a security incident for the Tanium integration v2. For more information about approving requests, see Approve requests for the Tanium integration v2.
As a user with the Now Platform® sn_si.admin role, create and configure a sightings search profile. As a user with the sn_si.analyst role, initiate a sightings search.

a. Create a sightings search profile.

b. Configure the profile and choose the servers you want to run the profile on.

c. Set the search time and search limits.

d. Initiate the search from the enrichment data on the Running Processes or Observable related lists on a security incident.

e. If approvals are enabled, as an approver, process the search request.

f. Locate search results on the Tanium Sightings Results and Tanium Sightings Details related lists on the related security incident.

g. Create a child incident or response task to group your search results on a single record.

For more information about sighting search profiles and search results, see Create and configure a profile for a process hash sightings search with the Tanium integration v2.

You have successfully completed the set up steps, installed and configured the application, and verified expected results for the integration.

**Threat Crowd integration**

Threat Crowd is powered by AlienVault and is part of an open Threat Intelligence community which permits global collaboration and sharing of cyber threats. Users share IP addresses or websites from which attacks have originated, or, look up specific threats to see if anyone in the intelligence community has provided information about them and determined them to be malicious. When integrated with the ServiceNow® Security Operations product, the community threat intelligence results provide analysts with additional insight for security incidents or investigations.

The integration requires the Security Incident Response and Threat Intelligence plugins.

Threat Crowd performs lookups on the following observables:

- IP addresses
- URLs
• Domains
• Email addresses
• Antivirus detections
• File hashes

The workflow checks for new observables as they arrive in security incidents. If the observables are of a type recognized by the API integration, the observables are evaluated. Observables determined to be malicious are tagged.

This integration is compatible with the Kingston, London, Madrid, and New York releases of the Now Platform®.

Install and configure Threat Crowd

Before you run the integration on your instance, complete the installation and configuration steps so the Threat Crowd application properly integrates with ServiceNow Security Operations.

Before you begin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

<table>
<thead>
<tr>
<th>Setup tasks</th>
<th>Description</th>
</tr>
</thead>
</table>
| Verify that you have assigned the required ServiceNow roles for your instance. | The following roles are required for installation, configuration, and verification of expected results:

• The System Administrator (admin) installs the app and assigns the Security Incident Administrator (sn_si.admin) role.

• The Security Incident Administrator (sn_si.admin) oversees configuration and verifies expected results. This role also has access to the Security Operations module and assigns the Security Incident Analyst (sn_si.analyst) role.

• The Security Incident Analyst (sn_si.analyst) works with Security Incident records. |
<table>
<thead>
<tr>
<th>Setup tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration.</td>
<td>For the Madrid release and later family releases, the Security Incident Response Dependency plugin (com.snc.si_dep) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications required by the integration. Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation. 1. Security Incident Response 2. Security Integration Framework 3. Security Support Common 4. Security Support Orchestration For more information on setting up your Now Platform instance for the integration, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.</td>
</tr>
</tbody>
</table>

**About this task**
Perform the following steps to update system properties and install and configure the integration.
Role required: admin

**Procedure**
1. In the navigation filter, enter `sys_properties.list`. The System Properties list is displayed.
2. Click **New**.  
A new record is displayed.

3. Fill in the fields, or select the values listed in the following table and click **Submit**.

<table>
<thead>
<tr>
<th>Field name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>glide.outbound.tls_sni.enabled</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Select true I false</td>
</tr>
<tr>
<td><strong>Value</strong></td>
<td>true</td>
</tr>
</tbody>
</table>

4. If you have not installed the application for the integration, see **Install a Security Operations integration** and follow the steps to install it.

5. Once the installation completes, navigate to **Integrations > Integrations Configurations** and locate the Threat Crowd tile.
6. Click **Configure**.

A message is displayed indicating there is no configuration required. No API key is required for the integration, because the Threat Crowd plugin is pre-configured and contains all the necessary Threat Crowd service URL information. Your integration is limited to one request every 10 seconds for a given IP address.

**Verify expected results for Threat Crowd**

Observables are generated automatically by a security incident and scanned by the application. Lookup results are displayed on the **Threat Lookup Results** tab at the bottom of the security incident record.

**Before you begin**

 Hispano: Only users with the sn_si.admin role can view and use the Security Operations module.

Role required: sn_si.analyst

**Procedure**

1. Open the security incident you are working with and verify that the lookup has run successfully.

Once the application is configured, the workflow launches automatically upon incident creation. The execution and completion status of the lookup is then displayed in the work notes in the security incident.

2. Review the work notes for more information and how to proceed if you cannot verify that the lookup ran successfully.

3. Navigate to the bottom of the security incident and click the **Show All Related Lists** related link to view results.

The figures in the following steps are shown with the **Tabbed forms** setting active in the System Settings. In the upper right of the banner frame, click the System Settings icon. In the **System Settings** dialog box that is displayed, click **Forms** and verify that the **Tabbed forms** and the **With the Form** buttons are selected.
The **Threat Lookup Results** tab displays the lookup results at the bottom of the security incident. The **Finding** column displays **Unknown** for records not determined to be malicious. For results matching malicious, **Malicious** is displayed in the **Finding** column.

### 4. In the **Observable** column, click an observable to open a record and display more information.

For lookups matching malicious, the **Finding** field displays **Malicious**, and the observable is tagged with the Threat Intelligence source that found it to be malicious, in this case, the Threat Crowd integration.

### 5. To view raw data, navigate back to the security incident and click the blue information icon next to an observable.
6. In the window that is displayed, click Open Record to view the data.

The link created by the API, the raw data, and other information are displayed. From any observables viewable in the raw data from the lookup, the Threat Crowd integration also creates child, or related observables.

7. To view a list of child observables, navigate back to the security incident.

8. Click the Show IoC related link.
   The child observables are displayed on the Child Observables tab, because the Threat Crowd integration has found an existing connection between these related observables and the observable initially submitted.

9. Click the field next to an observable in the Child column to select it, followed by the Run threat lookup related link to perform a lookup.
10. In the dialog box that is displayed, verify that the Threat Crowd integration is selected and click Submit.

11. In the work notes, verify that the lookup has run successfully, and in the Threat Lookup Results tab in the security incident, locate lookup results.

**Trouble?**
If you do not see results under the Threat Lookup Results tab, verify that the observable is a type that is supported for lookup by the integration.

**(Optional) Manually attach an observable for Threat Crowd**
You can manually attach observables to a security incident. You manually attach observables when you want to perform threat lookups on observables that are not attached to a security incident on the initial event trigger. Also, you might perform this task when you want more information about a related observable.

**Before you begin**

ℹ️ **Note:** Only users with the sn_si.admin role can view and use the Security Operations module.

Role required: sn_si.admin
Procedure

1. Navigate to your open security incident.
2. On the open security incident, click the Show IoC link in Related Links at the bottom of the record to display the Observables tab.

3. Click New.
4. In the Value field, enter an observable (domain, IP address, URL, or file hash).
5. Click the search icon and from the Observable Type Categories dialog box, and then click the desired observable type in the list to populate the field.
6. Click **Submit**. The workflow launches and checks for the new observable.

7. Navigate to your security incident and review the work notes. The execution and completion status is displayed in the work notes section on the Security Incident record.

8. Click the **Show All Related Lists** related link at the bottom of the record.

9. To view the results, click the **Threat Lookup Results** tab.
10. If you want more information and raw data, click the blue information icon next to an observable in the Observable column.

11. In the dialog box that is displayed, click Open Record to view details.

Trouble?
Review the Work notes for more information and how to proceed if you cannot verify that the lookup ran successfully.

Mobile Experience for Security Incident Response
Use your Android or iOS mobile device to manage your security operations center (SOC) tasks.

Request apps on the Store
Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Security Incident Response
If you are unfamiliar with the basic concepts of the Security Incident Response (SIR) product on your Now Platform® instance, see Security Incident Response Overview for more information about threat intelligence and how this product can help you prioritize and resolve cyber threats to your organization.

Overview
As a security operations center (SOC) manager or a user with the Now Platform security analyst role (sn_si.analyst), you can log in to a Now Platform instance directly from your mobile device. With the Security Incident Response Mobile app, you can view, edit, and assign your most current and critical SIR security
incidents and response tasks. Notifications inform you when critical security incidents assigned to you arrive.

With the Security Incident Response Mobile app, you can perform the following SIR-related tasks from your mobile device:

- View a list of critical security incidents and response tasks.
- Receive detailed notifications for security incidents and tasks that meet pre-defined notification criteria.
- View groupings of security incidents or tasks that are based on a pre-defined set of queries or filters.
- View the work notes and related lists of security incidents.
- Update security incidents and add work notes or attachments.
- Edit the fields on security incidents.
- Assign security incidents to yourself or to other members of your security team.

When they are populated, you can view the following related lists on SIR security incidents with the Security Incident Response Mobile app:

- Configuration Item
- Affected User
- Affected Services
- Child Security Incidents
- Similar Security Incidents (not support by Now Platform)
- Observables
- Response Tasks
- Tasks
- Task SLA
- Attachments (not support by Now Platform)

The following figure illustrates how you log into your Now Platform instance from your mobile device and the structure of the landing screen of the Security Incident Response Mobile app that is displayed after you log in.

For step-by-step instructions about how to set up your Now Platform instance and install the Security Incident Response Mobile app, see Set up checklist for the Security Incident Response Mobile app. For instructions about how to log in, see Log in to the Security Incident Response Mobile app.
Applications

Applications are the ServiceNow® software components such as Security Incident Response (SIR), Vulnerability Response (VR),
Governance, Risk, and Compliance (GRC) that provide specific features and functionalities within your Now Platform instance. After you install the Security Incident Response core application and the Security Incident Response Mobile app on your Now Platform instance, the icon for the core application is displayed on the bottom of your Android or iOS mobile device after you log in.

Security Incident Response Mobile app (Security Incidents) icon

| ?                   | Security Incidents | Notification | Settings |

Folders

Each ServiceNow® mobile application contains folders that separate the applets by category. In the preceding image of the landing page, Security Incidents and Incident Response Tasks are folders.

Applets

Applets are the different options within the application. The icons under the Security Incidents and Incident Response Tasks sections are the available applets of the Security Incident Response Mobile app.

Set up checklist for the Security Incident Response Mobile app

The following checklist includes the set up tasks that you are required to complete in your Now Platform® instance and on your mobile device prior to using the Security Incident Response Mobile app.

Before you begin

As an option, print this checklist and use it to guide you through the set up tasks that are required for the Security Incident Response Mobile app. Verify that each item on the list is completed so that you can view and edit SIR security incidents on your mobile device.

The check list items are displayed in highlighted text. More information follows each item in the right column. Estimated time to complete this task: 15-20 minutes.

Roles required: admin, sn_si.analyst
## Mobile checklist

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| ☐    | **As a user with the admin role, verify that you have the Security Incident Response core application installed on a Now Platform instance. This is the Now Platform instance that you view on your mobile device.**  
   1. To verify the core application is installed on your instance, navigate to **Plugins** and search for Security Incident Response.  
   2. If the Security Incident Response core application is not already installed, click **Install** to install it.  
   For more information about installing the Security Incident Response core application, see [Install and configure Security Incident Response](#).  
   If the Security Incident Response core application is not visible in Plugins, for more information about installing core applications and entitlements to applications, see Security Operations and the ServiceNow Store. |

| ☐    | **As a user with the admin role, verify that you have the Security Incident Response Mobile app installed on the Now Platform instance that you want to view on your mobile device.**  
   1. Note: the Security Incident Response Mobile app and the Now Platform instance should be from the same family release.  
   Download and install the Security Incident Response Mobile app from the ServiceNow Store on your Now Platform instance.  
   When you install the Security Incident Response Mobile app, its dependencies, `com.glide.sg` and `com.glide.sg.agent_native_client`, are also installed.  
   To verify that these dependencies are installed: |
Mobile checklist (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to <strong>Plugins</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Search for the plugin IDs (com.glide.sg and com.glide.sg.agent_native_client).</td>
</tr>
<tr>
<td>3.</td>
<td>If they are not activated, activate these plugins. These plugins are required for the Security Incident Response Mobile app.</td>
</tr>
</tbody>
</table>

For more information about installing applications and entitlements to applications, see Security Operations and the ServiceNow Store.

- As a user with the Now Platform admin role, verify that you have assigned mobile users with the required roles in your Now Platform instance.

  1. To view the roles that are assigned to a user, navigate to **Users and Groups > Users**.
  2. Select the user name followed by the roles related list. All roles assigned to this user are displayed.
  3. Verify a user is assigned, or assign a user with the IT Infrastructure Library role (itil). Users with the itil role can create, open, update and close security incidents. Only users with the itil role can have tasks assigned to them.
  4. Verify a user is assigned, or assign a user with the security analyst role (sn_si.analyst). Users with the sn_si.analyst role can read and edit security incident records. This role is automatically added when you assign the itil role.
  5. Verify you have created any required assignment groups and assigned mobile users to these groups.

  **Note:** If you have a large number of users for the mobile application, you alternatively can assign the sn_si.analyst role to a group. Each user you add to the group inherits this role.

For more information about security analysts, see Assigning security analysts.
Mobile checklist (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For more information on users and assigning roles to users and groups, see Create a user, Assign a role to a user and Assign a role to a group on the ServiceNow Product Documentation website.</td>
</tr>
</tbody>
</table>
| ☐   | As a user with the sn_si.analyst role, download the most current ServiceNow® Agent app on your mobile device.  
The most current version of the Agent app is available on the Apple iOS App Store and the Google Play Store. |
| ☐   | As a user with the sn_si.analyst role, verify notifications are enabled on your mobile device and in your Now Platform instance.  
Notifications inform you when critical security incidents are assigned to you or to your assignment group. To assist you with timely remediation, after you enable notifications, click on a notification in the Security Incident Response Mobile app to navigate directly to the security incident.  
To enable notifications in your Now Platform instance so they are displayed on your mobile device, follow these steps.  
1. Verify you have downloaded and installed the Security Incident Response Mobile app on your Now Platform instance.  
2. In System Settings in your Now Platform instance, under Notifications, verify you have enabled the ServiceNow Mobile Application.  
   For more information about setting notifications, see User notification preferences in UI16 on the ServiceNow documentation website. |
Mobile checklist (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Now Platform notifications are also displayed on the messages screen on your mobile device. Verify that notifications are also enabled in the settings of your mobile device.</td>
</tr>
</tbody>
</table>

You have successfully set up your mobile device and the Now Platform for the Security Incident Response Mobile app. The next step is to log in to your Now Platform instance with your mobile device.

Log in to the Security Incident Response Mobile app

Open the Security Incident Response Mobile app and add a Now Platform® instance with Security Incident Response to your mobile device.

About this task
Time to complete this task: 5-10 minutes.
Verify that you have completed the setup steps described in Set up checklist for the Security Incident Response Mobile app.
Role required: security incident analyst (sn_si.analyst)
**Procedure**

1. On your mobile device, tap the **ServiceNow Agent** app to open it.

   ![ServiceNow Agent](image)

   If you are not already logged in to a Now Platform instance, the Instances screen is displayed.

2. If the Now Platform instance with the Security Incident Response core application is not already added to your mobile device, follow these steps to add it.

   a. On the Instances screen that is displayed, tap the **+**.

      A screen is displayed that prompts you to enter and save an address of a Now Platform instance.

   b. Fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the instance address</td>
<td>Choose one to continue:</td>
</tr>
<tr>
<td>or scan a QR code.</td>
<td>• Before the .service-now.com, enter the name of your Now Platform instance, for example, sirmobileparis.</td>
</tr>
<tr>
<td></td>
<td>• Enter an address. This address is the URL of your Now Platform instance that you want to view on your mobile device.</td>
</tr>
<tr>
<td></td>
<td>• Scan a QR code.</td>
</tr>
<tr>
<td>(Optional) Enter nickname</td>
<td>Enter a nickname for this instance. If you have multiple instances added to the device, nicknames can help you quickly locate a Now Platform instance.</td>
</tr>
</tbody>
</table>

   c. Tap **Save and Login**.

3. On the ServiceNow login screen that is displayed, enter the User name and Password for the Now Platform instance that you want to add and tap **Login**. The Security Incidents landing screen is displayed. You have successfully logged in to the Security Incident Response Mobile app!
4. After you log in, verify notifications are enabled in the Security Incident Response Mobile app.

   a. On the landing screen on the bottom, tap **Notification**.

   b. On the Notifications screen, tap **Enable Notifications** if not enabled. Notifications from the Now Platform are displayed on the Notifications screen in the Security Incident Response Mobile app.

5. After you log in to an instance on your mobile device, it is the default Now Platform instance on the device. If you want to view another Now Platform on the device, you are required to log out of the default instance. To log out:

   a. Tap the settings icon.

   b. Tap **Logout**.

      The Instances screen is displayed with any Now Platform instances you have added to the mobile device.

   c. **Optional:** Tap another instance to log in to it, or, alternatively, follow the preceding steps to add another instance.

   If the instances screen for the Security Incident Response Mobile app is not displayed after you tap the **ServiceNow Agent** app on your device, verify that the **ServiceNow Agent** is permitted as a trusted app on your device. To permit access as a trusted app, navigate to the settings and general device management on your device and tap the option (**Trust app**, etc.) to permit access.

   If an error message is displayed after you enter your credentials in the log in screen, verify that your User name and password for the Now Platform instance is correct.

   If you have problems viewing the landing screen, verify your network connection.

   If you cannot view the Instances screen after you tap the **ServiceNow Agent** app, try uninstalling it from your device. Verify you have the most current version of the app from the Apple iOS App Store or the Google Play Store and try reinstalling it.
View, edit, and assign open security incidents with the Security Incident Response Mobile app

As a security incident analyst, view, edit, and assign open Security Incident Response (SIR) security incidents from your mobile device. View related lists and the audit trail of work notes for more details about incidents.

Before you begin
Role required: sn_si.analyst

About this task
From the list of records, assign an open security incident to yourself, or reassign it. Alternatively, view the details and related lists of the record or add a work note prior to assignment. Time to complete this task: 5-10 minutes.

Procedure
1. If you are not logged in to your Now Platform instance on your mobile device, see Log in to the Security Incident Response Mobile app.
2. With the Security Incidents landing page displayed, tap Open Incidents.

If you navigate away from the Security Incident Response Mobile app after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.
The Open Incidents screen is displayed with a list of open security incident records.
3. **Optional:** Refer to Search for security incidents with the Security Incident Response Mobile app to search for security incidents that match specific criteria. Alternatively, with the filter icon (🔍) displayed, set filters to limit the number of records on the list. Filtering records on screens in the mobile app works like filtering with a condition builder on the Now Platform.

4. To assign an incident to yourself or reassign it directly from the list of open security incidents, swipe left on a record to open the menu.
5. Choose one from the menu that is displayed to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign to Me</td>
<td>Assign the security incident to yourself. If the security incident is already assigned to you, this option is not displayed.</td>
</tr>
</tbody>
</table>
| Reassign | To assign or reassign the assignment group:  
  a. Tap Assignment group.  
  b. Tap a group from the list that is displayed, or enter text in the search field. The group must be a security-related assignment group. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To assign or reassign the security incident to a member of the assignment group:</td>
</tr>
<tr>
<td>a.</td>
<td>Tap <strong>Assigned to</strong>.</td>
</tr>
<tr>
<td>b.</td>
<td>Tap a name from the list that is displayed, or enter text in the search field.</td>
</tr>
</tbody>
</table>

Tap the send icon (➡️) or **Submit** to save and submit your changes.

6. Alternatively, to view the details of an open security incident record and to see more associated records and related lists, with the Open Incidents screen displayed, tap a record on the list.

7. On the open record that is displayed, choose one option from the following table to continue.
From the menu that is displayed, choose from the following options.

- Tap **Edit**. With the Edit Security Incident screen displayed, tap a field to expand it and choose one or more of the options that are displayed. Alternatively, tap the search icon and enter text.

- To reassign the incident, tap **Reassign** or **Assign to Me**. Follow the instructions described in the previous table.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>After you complete your</td>
<td>After you complete your edits, tap</td>
</tr>
<tr>
<td>edits, tap the send</td>
<td>the send icon (▶️) or <strong>Submit</strong> to save your changes and update the</td>
</tr>
<tr>
<td>icon (▶️) or Submit</td>
<td>security incident.</td>
</tr>
<tr>
<td>Activity Stream tab</td>
<td>With the Activity Stream tab selected, review the audit trail of work notes,</td>
</tr>
<tr>
<td></td>
<td>activities, and additional comments of the record. Tap the plus icon (+)</td>
</tr>
<tr>
<td></td>
<td>to add a work note or attach a file.</td>
</tr>
<tr>
<td>Related List tab</td>
<td>With the Related List tab selected, view the items of any Related Lists of</td>
</tr>
<tr>
<td></td>
<td>the security incident that are populated.</td>
</tr>
<tr>
<td></td>
<td>Tap an item on the list that is displayed to view the details for a related</td>
</tr>
<tr>
<td></td>
<td>list. From the lists of items that are displayed, tap an item to continue</td>
</tr>
<tr>
<td></td>
<td>to view the activity streams and related lists associated with the parent</td>
</tr>
<tr>
<td></td>
<td>security incident.</td>
</tr>
<tr>
<td>Screen icons at the</td>
<td>On the bottom of the screen, choose one to continue.</td>
</tr>
<tr>
<td>bottom of the screen</td>
<td>• Tap the Security Incidents icon to return to the landing screen.</td>
</tr>
<tr>
<td></td>
<td>• If displayed, tap an icon to open another ServiceNow® mobile app.</td>
</tr>
<tr>
<td></td>
<td>• Tap <strong>Notification</strong> to view notifications from the Now Platform and the</td>
</tr>
<tr>
<td></td>
<td>Security Incident Response Mobile app.</td>
</tr>
<tr>
<td></td>
<td>• Tap <strong>Settings</strong> and choose one to continue.</td>
</tr>
<tr>
<td></td>
<td>◦ View information about the Now Platform instance on your device.</td>
</tr>
<tr>
<td></td>
<td>◦ Log out of the current Now Platform instance.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
View, edit, and reassign security incidents assigned to you with the Security Incident Response Mobile app

As a security incident analyst, view, edit, and reassign Security Incident Response (SIR) incidents that are assigned to you. View related lists and the audit trail of work notes for more details about incidents.

Before you begin
Role required: sn_si.analyst

About this task
Reassign an open security incident to another analyst in your group from the list of records. Alternatively, view the details and related lists of the record or add a work note prior to assignment. Time to complete this task: 5-10 minutes.

Procedure
1. If you are not logged in to your Now Platform instance on your mobile device, see Log in to the Security Incident Response Mobile app.
2. With the Security Incidents landing screen displayed, tap My Incidents.
   If you navigate away from the Security Incident Response Mobile app after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.
The My Incidents screen is displayed with a list of open security incident records that are assigned to you.
3. **Optional:** Refer to Search for security incidents with the Security Incident Response Mobile app to search for security incidents that match specific criteria. Alternatively, with the filter icon (🔍) displayed, Set filters to limit the number of records on the list. Filtering records on screens in the mobile app works like filtering with a condition builder on the Now Platform.

4. To reassign an incident directly from the list, with the list of open security incident records displayed, swipe left on a record to open the menu.
5. Edit the Assignment group or the Assigned to fields from the menu that is displayed.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reassign</td>
<td>To reassign the assignment group:</td>
</tr>
<tr>
<td></td>
<td>a. Tap <strong>Assignment group</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. Tap a group from the list that is displayed, or enter text in the search</td>
</tr>
<tr>
<td></td>
<td>field. The group must be a security-related assignment group.</td>
</tr>
<tr>
<td></td>
<td>To assign or reassign the security incident to a member of the assignment</td>
</tr>
<tr>
<td></td>
<td>group:</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Tap <strong>Assigned to.</strong></td>
<td>b. Tap a name from the list that is displayed, or enter text in the search field. Tap the send icon (&gt;) or Submit to save and submit your changes.</td>
</tr>
</tbody>
</table>

6. Alternatively, to view the details of the open security incident record, with the My Incidents screen displayed, tap a record on the list.

7. On the open record that is displayed, choose one option from the following table to continue.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Tap the menu icon (⋮) on the upper right of the screen. | From the menu that is displayed, choose from the following options.  
• Tap **Edit**. With the Edit Security Incident screen displayed, tap a field to expand it and choose one or more of the options that are displayed. Alternatively, tap the search icon and enter text.  
• To reassign the incident, tap **Reassign**. Follow the instructions described in the previous table.  
After you complete your edits, tap the send icon (▶) or **Submit** to save your changes and update the security incident. |
| Activity Stream tab                        | With the Activity Stream tab selected, review the audit trail of work notes, activities, and additional comments of the record. Tap the plus icon (+) to add a work note or attach a file. |
| Related List tab                           | With the Related List tab selected, view the items on any Related Lists that are populated on the security incident.  
Tap an item on the list that is displayed to view the details for a related list. From the lists of items that are displayed, tap an item to continue to view the activity streams and related lists associated with the parent security incident. |
| Screen icons at the bottom of the screen.  | On the bottom of the screen, choose one to continue.                                              |
View, edit and assign unassigned security incidents with the Security Incident Response Mobile app

From your mobile device, view, edit, and assign unassigned Security Incident Response (SIR) incidents. View related lists and the audit trail of work notes for more details about incidents.

Before you begin
Role required: sn_si.analyst

About this task
From the list of records, assign an open, unassigned security incident to yourself or to another analyst in your group. Alternatively, view the details and related lists of the record or add a work note prior to assignment. Time to complete this task: 5-10 minutes.

Procedure
1. If you are not logged in to your Now Platform instance on your mobile device, for more information see Log in to the Security Incident Response Mobile app.
2. With the Security Incidents landing screen displayed, tap Unassigned Incidents.

If you navigate away from the Security Incident Response Mobile app after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.
The Unassigned Incidents screen is displayed with a list of unassigned security incident records.
3. Optional: Refer to Search for security incidents with the Security Incident Response Mobile app to search for security incidents that match specific criteria. Alternatively, with the filter icon (��) displayed, set filters to limit the number of records on the list. Filtering records on screens in the mobile app works like filtering with a condition builder on the Now Platform.

4. To assign or reassign an open security incident record directly from the list, with the list of open unassigned security incident records displayed, swipe left on a record to open the menu.
5. Choose one from the menu to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign to Me</td>
<td>Assign the security incident to yourself. If the security incident is already assigned to you, this option is not displayed.</td>
</tr>
<tr>
<td>Reassign</td>
<td>To assign or reassign the assignment group:</td>
</tr>
<tr>
<td></td>
<td>a. Tap <strong>Assignment group</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. Tap a group from the list that is displayed, or enter text in the search field. The group must be a security-related assignment group.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>To assign or reassign the security incident to a member of the assignment group:</td>
</tr>
<tr>
<td>a. Tap</td>
<td><strong>Assigned to.</strong></td>
</tr>
<tr>
<td>b. Tap a name from the list that is displayed, or enter text in the search field.</td>
<td></td>
</tr>
<tr>
<td>Tap the send icon (▶) or <strong>Submit</strong> to save and submit your changes.</td>
<td></td>
</tr>
</tbody>
</table>

6. Alternatively, with the Unassigned Incidents screen displayed, tap a record on the list.

7. On the open record that is displayed, choose one option from the following table to continue.
Tap the menu icon (≡) on the upper right of the screen.

From the menu that is displayed, choose from the following options.

- Tap **Edit**. With the Edit Security Incident screen displayed, tap a field to expand it and choose one or more of the options that are displayed. Alternatively, tap the search icon and enter text.

- To assign or reassign the incident, tap **Reassign** or **Assign to Me**. Follow the instructions described in the previous table.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>After you complete your edits, tap the send icon (&gt;) or <strong>Submit</strong> to save your changes and update the security incident.</td>
<td></td>
</tr>
<tr>
<td><strong>Activity Stream tab</strong></td>
<td>With the Activity Stream tab selected, review the audit trail of work notes, activities, and additional comments of the record. Tap the plus icon (+) to add a work note or attach a file.</td>
</tr>
<tr>
<td><strong>Related List tab</strong></td>
<td>With the Related List tab selected, view the items on any of the Related Lists that are populated on the security incident. Tap an item on the list that is displayed to view the details for a related list. From the lists of items that are displayed, tap an item to continue to view the activity streams and related lists associated with the parent security incident.</td>
</tr>
<tr>
<td><strong>Screen icons at the bottom of the screen.</strong></td>
<td>On the bottom of the screen, choose one to continue.</td>
</tr>
<tr>
<td>• Tap the Security Incidents icon to return to the landing screen.</td>
<td></td>
</tr>
<tr>
<td>• If displayed, tap an icon to open another ServiceNow® mobile app.</td>
<td></td>
</tr>
<tr>
<td>• Tap <strong>Notification</strong> to view notifications from the Now Platform and the Security Incident Response Mobile app.</td>
<td></td>
</tr>
<tr>
<td>• Tap <strong>Settings</strong> and choose one to continue.</td>
<td></td>
</tr>
<tr>
<td>◦ View information about the Now Platform instance on your device.</td>
<td></td>
</tr>
<tr>
<td>◦ Log out of the current Now Platform instance.</td>
<td></td>
</tr>
</tbody>
</table>
**View, edit, and assign high priority incidents with the Security Incident Response Mobile app**

From your mobile device, view, edit, and assign high priority Security Incident Response (SIR) incidents. View related lists and the audit trail of work notes for more details about incidents.

**Before you begin**
Role required: sn_si.analyst

**About this task**
From the list of records, assign an open, critical security incident to yourself or to another analyst in your group. Alternatively, view the details and related lists of the record or add a work note prior to assignment. Time to complete this task: 5-10 minutes.

**Procedure**

1. If you are not logged in to your Now Platform instance on your mobile device, for more information see Log in to the Security Incident Response Mobile app.

2. With the Security Incidents landing screen displayed, tap **High Priority Incidents**.

   If you navigate away from the Security Incident Response Mobile app after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.
The High Priority Incidents screen is displayed with a list of critical (high priority) security incidents.
3. **Optional:** Refer to Search for security incidents with the Security Incident Response Mobile app to search for security incidents that match specific criteria. Alternatively, with the filter icon (фиолетовый круглый значок) displayed, Set filters to limit the number of records on the list. Filtering records on screens in the mobile app works like filtering with a condition builder on the Now Platform.

4. With the list of open high priority security incident records displayed, swipe left on a record to open the menu.
5. Choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign to Me</td>
<td>Assign the security incident to yourself. If the security incident is already assigned to you, this option is not displayed.</td>
</tr>
</tbody>
</table>
| Reassign        | To assign or reassign the assignment group:  
|                 | a. Tap **Assignment group**  
<p>|                 | b. Tap a group from the list that is displayed, or enter text in the search field. The group must be a security-related assignment group. |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To assign or reassign the security incident to a member of the assignment group:</td>
</tr>
<tr>
<td>a. Tap <strong>Assigned to</strong>.</td>
<td></td>
</tr>
<tr>
<td>b. Tap a name from the list that is displayed, or enter text in the search field.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tap the send icon (&gt;) or <strong>Submit</strong> to save and submit your changes.</td>
</tr>
</tbody>
</table>

6. To view the details of an open security incident record and to see more associated records and related lists, with the High Priority Incidents screen displayed, tap a record on the list.

7. On the open record that is displayed, choose one option from the following table to continue.

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Tap the menu icon (≡) on the upper right of the screen.

From the menu that is displayed, choose from the following options.

- Tap **Edit**. With the Edit Security Incident screen displayed, tap a field to expand it and choose one or more of the options that are displayed. Alternatively, tap the search icon and enter text.

- To reassign the incident, tap **Reassign** or **Assign to Me**. Follow the instructions described in the previous table.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>After you complete your edits, tap the send icon (🚀) or <strong>Submit</strong> to save your changes and update the security incident.</td>
<td><strong>Activity Stream tab</strong></td>
</tr>
<tr>
<td>With the Activity tab selected, review the audit trail of work notes, activities, and additional comments of the record. Tap the plus icon (➕) to add a work note or attach a file.</td>
<td><strong>Related List tab</strong></td>
</tr>
<tr>
<td>With the Related List tab selected, view the items on any of the Related Lists that are populated on the security incident. Tap an item on the list that is displayed to view the details for a related list. From the lists of items that are displayed, tap an item to continue to view the activity streams and related lists associated with the parent security incident.</td>
<td>On the bottom of the screen, choose one to continue.</td>
</tr>
<tr>
<td>Tap a screen icon at the bottom of the screen.</td>
<td>• Tap the Security Incidents icon to return to the landing screen.</td>
</tr>
<tr>
<td>• If displayed, tap an icon to open another ServiceNow® mobile app.</td>
<td></td>
</tr>
<tr>
<td>• Tap <strong>Notification</strong> to view notifications from the Now Platform and the Security Incident Response Mobile app.</td>
<td></td>
</tr>
<tr>
<td>• Tap <strong>Settings</strong> and choose one to continue.</td>
<td></td>
</tr>
<tr>
<td>◦ View information about the Now Platform instance on your device.</td>
<td></td>
</tr>
<tr>
<td>◦ Log out of the current Now Platform instance.</td>
<td></td>
</tr>
</tbody>
</table>
View, edit, and assign security incidents with a risk score greater than 60 with the Security Incident Response Mobile app

From your mobile device, view and edit Security Incident Response (SIR) incidents with a value in the risk score field that is greater than 60. View related lists and the audit trail of work notes for more details about incidents.

Before you begin
Role required: sn_si.analyst

About this task
From the list of records, assign an open security incident that has a risk score that is greater than 60 to yourself or to another analyst in your group. Alternatively, view the details and related lists of the record or add a work note prior to assignment. Time to complete this task: 5-10 minutes.

Procedure

1. If you are not logged in to your Now Platform instance on your mobile device, for more information see Log in to the Security Incident Response Mobile app.

2. With the Security Incidents landing screen displayed, tap Risk Score > 60.

   If you navigate away from the Security Incident Response Mobile app after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.
The Incident Risk Score screen is displayed with a list of security incidents.
3. **Optional:** Refer to Search for security incidents with the Security Incident Response Mobile app to search for security incidents that match specific criteria. Alternatively, with the filter icon ( ), displayed, Set filters to limit the number of records on the list. Filtering records on screens in the mobile app works like filtering with a condition builder on the Now Platform.

4. To assign a security incident to yourself or reassign it directly from the list of open security incident records displayed, swipe left on a record to open the menu.
5. Choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assign to Me</strong></td>
<td>Assign the security incident to yourself. If the security incident is already assigned to you, this option is not displayed.</td>
</tr>
</tbody>
</table>
| **Reassign**     | To assign or reassign the assignment group:  
|                  | a. Tap **Assignment group**.  
<p>|                  | b. Tap a group from the list that is displayed, or enter text in the search field. The group must be a security-related assignment group. |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To assign or reassign the security incident to a member of the assignment group:</td>
</tr>
<tr>
<td>a.</td>
<td>Tap <strong>Assigned to</strong> and</td>
</tr>
<tr>
<td>b.</td>
<td>Tap a name from the list that is displayed, or enter text in the search field.</td>
</tr>
<tr>
<td></td>
<td>Tap the send icon (▶) or <strong>Submit</strong> to save and submit your changes.</td>
</tr>
</tbody>
</table>

6. Alternatively, to view the details of an open security incident record and to see more associated records and related lists, with the Incident Risk Score screen displayed, tap a record on the list.

7. On the open record that is displayed, choose one option from the following table to continue.
From the menu that is displayed, choose from the following options.

- **Tap Edit.** With the Edit Security Incident screen displayed, tap a field to expand it and choose one or more of the options that are displayed. Alternatively, tap the search icon and enter text.

- **To reassign the incident, tap Reassign** or **Assign to Me.** Follow the instructions described in the previous table.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>After you complete your edits, tap the send icon (✓) or Submit to save your changes and update the security incident.</td>
<td></td>
</tr>
<tr>
<td>Activity Stream tab</td>
<td>With the Activity Stream tab selected, review the audit trail of work notes, activities, and additional comments of the record. Tap the plus icon (+) to add a work note or attach a file.</td>
</tr>
<tr>
<td>Related List tab</td>
<td>With the Related List tab selected, view the items on any of the Related Lists that are populated on the security incident. Tap an item on the list that is displayed to view the details for a related list. From the lists of items that are displayed, tap an item to continue to view the activity streams and related lists associated with the parent security incident.</td>
</tr>
<tr>
<td>Screen icons at the bottom of the screen.</td>
<td>On the bottom of the screen, choose one to continue.</td>
</tr>
<tr>
<td>• Tap the Security Incidents icon to return to the landing screen.</td>
<td></td>
</tr>
<tr>
<td>• If displayed, tap an icon to open another ServiceNow® mobile app.</td>
<td></td>
</tr>
<tr>
<td>• Tap Notification to view notifications from the Now Platform and the Security Incident Response Mobile app.</td>
<td></td>
</tr>
<tr>
<td>• Tap Settings and choose one to continue.</td>
<td></td>
</tr>
<tr>
<td>◦ View information about the Now Platform instance on your device.</td>
<td></td>
</tr>
<tr>
<td>◦ Log out of the current Now Platform instance.</td>
<td></td>
</tr>
</tbody>
</table>
Search for security incidents with the Security Incident Response Mobile app

Search for Security Incident Response (SIR) security incidents on a Now Platform® instance. Only incidents that match the specific search criteria that you enter are displayed.

Before you begin
Role required: sn_si.analyst

About this task
Time to complete this task: 5-10 minutes.

Procedure
1. If you are not logged in to your Now Platform instance on your mobile device, for more information see Log in to the Security Incident Response Mobile app.
2. With the Security Incidents landing screen displayed, tap Search Incidents.
   If you navigate away from the Security Incident Response Mobile app after you have logged in, tap the Now Agent at any time to return to the last screen you had displayed.
3. To limit the number of search results that are returned, you may prefer to fill out as many fields on the form as you can. To add search criteria, refer to the following table. Follow the instructions after the table to edit existing search criteria, clear search criteria, or submit a search.

<table>
<thead>
<tr>
<th>Tap this field</th>
<th>To add an entry on Android devices</th>
<th>To add an entry on iOS devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Enter an alpha-numeric value for a security incident, for example, SIR0010004. This number</td>
<td>Enter an alpha-numeric value for a security incident, for example, SIR0010004. This number</td>
</tr>
<tr>
<td>Tap this field</td>
<td>To add an entry on Android devices</td>
<td>To add an entry on iOS devices</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td></td>
<td>is displayed in the upper right of the security incident. The feature searches on numeric strings and partial numeric strings. For more refined searches, enter more digits. Wild cards (*) are not accepted. Tap a new field to enter more criteria or &gt; to submit a search.</td>
<td>is displayed in the upper right of the security incident. The feature searches on numeric strings and partial numeric strings. For more refined searches, enter more digits. Wild cards (*) are not accepted. Tap a new field to enter more criteria or Search to submit a search.</td>
</tr>
<tr>
<td>Short Description</td>
<td>Enter text in the field for example, malware. The feature searches on text strings and partial text strings from the Short Description field. For more refined searches, enter more text. Wild cards (*) are not accepted. Tap a new field to enter more criteria or &gt; to submit a search.</td>
<td>Enter text in the field for example, malware. The feature searches on text strings and partial text strings from the Short Description field. For more refined searches, enter more text. Wild cards (*) are not accepted. Tap a new field to enter more criteria or Search to submit a search.</td>
</tr>
<tr>
<td>Priority</td>
<td>To add an entry, tap one or more items or tap the search icon and type an entry in the search field. Tap the check mark icon to return to the Search Incidents screen.</td>
<td>To add an entry, tap one or more items or tap the search icon and type an entry in the search field. Tap Done to return to the Search Incidents screen.</td>
</tr>
<tr>
<td>Category</td>
<td>To add an entry, tap one or more items or tap the search icon</td>
<td>To add an entry, tap one or more items or tap the search icon</td>
</tr>
<tr>
<td>Tap this field</td>
<td>To add an entry on Android devices</td>
<td>To add an entry on iOS devices</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td></td>
<td>and type an entry in the search field. Tap the check mark icon to return to the Search Incidents screen.</td>
<td>and type an entry in the search field. Tap <strong>Done</strong> to return to the Search Incidents screen.</td>
</tr>
<tr>
<td>State</td>
<td>To add an entry, tap one or more items or tap the search icon and type an entry in the search field. Tap the check mark icon to return to the Search Incidents screen.</td>
<td>To add an entry, tap one or more items or tap the search icon and type an entry in the search field. Tap <strong>Done</strong> to return to the Search Incidents screen.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>Select one from the list or tap the search icon and type an entry in the search field. To clear a value for the Assignment group and Assigned to fields, for no entry, select <strong>None</strong>.</td>
<td>Select one from the list or tap the search icon and type an entry in the search field. To clear a value for the Assignment group and Assigned to fields, for no entry, select <strong>None</strong>.</td>
</tr>
<tr>
<td>Assignment group</td>
<td>Select one from the list or tap the search icon and type an entry in the search field. To clear a value for the Assignment group and Assigned to fields, for no entry, select <strong>None</strong>.</td>
<td>Select one from the list or tap the search icon and type an entry in the search field. To clear a value for the Assignment group and Assigned to fields, for no entry, select <strong>None</strong>.</td>
</tr>
</tbody>
</table>

For Android devices, with the Search Incidents screen displayed and all your criteria entered, choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Clear or modify search criteria prior to executing a search</strong></td>
<td>To clear all entered criteria, with the Search Incidents screen displayed, tap the back arrow to clear all the fields and return to the Security Inci-</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Clear or modify search criteria prior to executing a search | To clear all criteria and return to the landing screen, tap the close icon (X). Any entered search criteria are not saved. Alternatively, to edit a field:  
• With the Search Incidents screen displayed, tap a field with search criteria to expand it.  
• Tap an item on the list to deselect it, or tap **Clear All**. To clear a value for the Assignment group and Assigned to fields, for no entry, select **None**.  
• Tap the check mark icon to save the changes and return to the Search Incidents screen. |

4. For iOS devices, with the Search Incidents screen displayed, choose one to continue.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>signed to fields, for no entry, select None.</td>
<td></td>
</tr>
<tr>
<td>• Tap Done to save the changes and return to the Search Incidents screen.</td>
<td></td>
</tr>
<tr>
<td>Submit a search</td>
<td>With the Search Incidents screen displayed with your entered search criteria, tap Search.</td>
</tr>
<tr>
<td></td>
<td>The security incidents that match your search criteria are displayed. After the search is completed, the search criteria are not saved.</td>
</tr>
</tbody>
</table>

5. Optional: If your search returns multiple records, you can Filter records with the Security Incident Response Mobile app to refine the search results.

View, edit, and assign open response tasks with the Security Incident Response Mobile app

View, edit, and assign open response tasks. Your changes are saved on the Security Incident Response Task of the parent security incident.

Before you begin
Role required: sn_si.analyst

About this task
From the list of records, assign an open, unassigned response task to yourself or to another analyst in your group. Alternatively, view the details of the record or add a work note prior to assignment. Time to complete this task: 5-10 minutes.

Procedure
1. If you are not logged in to your Now Platform instance on your mobile device, for more information see Log in to the Security Incident Response Mobile app.
2. With the Security Incidents landing screen displayed, tap Open Response Tasks.

If you navigate away from the Security Incident Response Mobile app after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.
The Open Response Tasks screen is displayed with a list of open tasks.
### Optional:

Refer to Search for security incidents with the Security Incident Response Mobile app to search for tasks that match specific criteria.

Alternatively, with the filter icon (-filter icon) displayed, set filters to limit the number of records on the list. Filtering records on screens in the mobile app works like filtering with a condition builder on the Now Platform.

4. With the list of open response tasks displayed, to assign or reassign directly from the list, swipe left on a record to open the menu.
5. Choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign to Me</td>
<td>Assign the response task to yourself. If the task is already assigned to you, this option is not displayed.</td>
</tr>
<tr>
<td>Reassign</td>
<td>To assign or reassign the assignment group:</td>
</tr>
<tr>
<td></td>
<td>a. Tap <strong>Assignment group</strong></td>
</tr>
<tr>
<td></td>
<td>b. Tap a group from the list that is displayed, or enter text in the search field. The group must be a security-related assignment group.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>To assign or reassign the task to a member of the assignment group:</td>
</tr>
<tr>
<td><strong>a.</strong></td>
<td>Tap <strong>Assigned to</strong> and</td>
</tr>
<tr>
<td><strong>b.</strong></td>
<td>Tap a name from the list that is displayed, or enter text in the search field.</td>
</tr>
<tr>
<td></td>
<td>A message is displayed that confirms the record is updated. The task on the parent security incident is assigned to a new user and updated in your Now Platform instance.</td>
</tr>
<tr>
<td></td>
<td>Tap the send icon (🔗) or <strong>Submit</strong> to save and submit your changes.</td>
</tr>
</tbody>
</table>

6. Alternatively, to view the details of an open response task record, with the Open Response Tasks screen displayed, tap a record on the list.

7. With the tabs on the response task record displayed, choose one in the following table to continue.
Submit attachment to malware sandbox and review the results

State: Assigned

Details tab

With the Details tab selected, review the fields on the response task. To edit fields or assign the task, tap the menu icon (⋮). From the menu that is displayed, choose from the following options.

- Tap Edit. With the Edit Response Task screen displayed, tap a field to expand it and choose one or more of the options that are displayed.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alternatively, tap the search</td>
<td>• To reassign the task, tap <strong>Reassign</strong> or <strong>Assign to Me</strong>.</td>
</tr>
<tr>
<td>icon and enter text.</td>
<td>After you complete your edits, tap the send icon (👉) or <strong>Submit</strong> to save your changes and update the record. The Security Incident Response Task on the parent security incident in your Now Platform instance is updated.</td>
</tr>
<tr>
<td><strong>Activity Stream tab</strong></td>
<td>With the Activity Stream tab selected, choose one to continue.</td>
</tr>
<tr>
<td></td>
<td>• View the audit trail created by the Work notes on the record. To add a work note or attach a file, tap the plus icon (➕).</td>
</tr>
<tr>
<td></td>
<td>• Tap the menu icon (⋮) to edit or reassign the task.</td>
</tr>
<tr>
<td><strong>Screen icons at the bottom of</strong></td>
<td>On the bottom of the screen, choose one to continue.</td>
</tr>
<tr>
<td>the screen.</td>
<td>• If displayed, tap an icon to open another ServiceNow® mobile app.</td>
</tr>
<tr>
<td></td>
<td>• Tap <strong>Notification</strong> to view notifications for critical security incidents that are assigned to you or to your assignment group.</td>
</tr>
<tr>
<td></td>
<td>• Tap <strong>Settings</strong> and choose one to continue.</td>
</tr>
<tr>
<td></td>
<td>◦ View information about the Now Platform instance.</td>
</tr>
<tr>
<td></td>
<td>◦ Log out of the current instance. To log out of a Now Platform in-</td>
</tr>
</tbody>
</table>
View, edit, and reassign your response tasks with the Security Incident Response Mobile app

View, edit, and reassign response tasks that are assigned to you. Your changes are saved on the Security Incident Response Task of the parent security incident.

Before you begin
Role required: sn_si.analyst

About this task
From the list of records, reassign an open response task that is assigned to you to another analyst in your group. Alternatively, view the details of the record or add a work note prior to reassignment. Time to complete this task: 5-10 minutes.

Procedure
1. If you are not logged in to your Now Platform instance on your mobile device, for more information see Log in to the Security Incident Response Mobile app.
2. With the Security Incidents landing screen displayed, tap My Response Tasks.

   If you navigate away from the Security Incident Response Mobile app after you have logged in, tap the Now Agent (Fulfiller) app at any time to return to the last screen you had displayed.
The My Response Tasks screen is displayed with a list of the response tasks that are assigned to you.
3. **Optional:** Refer to Search for security incidents with the Security Incident Response Mobile app to search for tasks that match specific criteria.

Alternatively, with the filter icon (▼) displayed, set filters to limit the number of records on the list. Filtering records on screens in the mobile app works like filtering with a condition builder on the Now Platform.

4. To reassign a task directly from the list of task records that are assigned to you, swipe left on a record to open the menu.
5. Tap **Reassign**.

6. On the **Assign Response Task to Another** screen that is displayed, tap a field to expand it and select another group or user for the task.

7. Tap the send icon or **Submit** to save your changes and update the response task.

   A message is displayed that confirms the record is updated. The task is assigned to a new user on the parent security incident and your Now Platform instance is updated.

8. To view the details of an open response task and to see the work notes, with the **My Response Tasks** screen displayed, tap a record on the list.

9. With the fields on the response task displayed, choose one in the following table to continue.
With the Details tab selected, review the fields on the response task. To edit fields or reassign the task, tap the menu icon (···). From the menu that is displayed, choose from the following options.

- Tap Edit. With the Edit Response Task screen displayed, tap a field to expand it and choose one or more of the options that is displayed. Al-
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alternatively, tap the search icon and enter text.</td>
<td>• To reassign the task, tap <strong>Assign to Another</strong>. After you complete your edits, tap the send icon (&gt;&gt;) or <strong>Submit</strong> to save your changes and update the record. The Security Incident Response Task on the parent security incident in your Now Platform instance is updated.</td>
</tr>
<tr>
<td>Activity Stream tab</td>
<td>With the Activity Stream tab selected, choose one to continue.</td>
</tr>
<tr>
<td></td>
<td>• View the audit trail created by the Work notes on the task record. To add a work note or attach a file, tap ( ).</td>
</tr>
<tr>
<td></td>
<td>• Tap ( ) to edit or reassign the task.</td>
</tr>
<tr>
<td>Tap a screen icon at the bottom of the screen.</td>
<td>On the bottom of the screen, choose one to continue.</td>
</tr>
<tr>
<td></td>
<td>• If displayed, tap another icon to open another ServiceNow® core application to open it.</td>
</tr>
<tr>
<td></td>
<td>• Tap <strong>Notification</strong> to view notifications for critical security incidents that are assigned to you or to your assignment group.</td>
</tr>
<tr>
<td></td>
<td>• Tap <strong>Settings</strong> and choose one to continue.</td>
</tr>
<tr>
<td></td>
<td>◦ View information about the Now Platform instance.</td>
</tr>
</tbody>
</table>
|                               | ◦ Log out of the current instance. To log out of a Now Platform instance...
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>

stance on your device, with the details page displayed, tap Log out.

Filter records with the Security Incident Response Mobile app

Set additional filters to limit the number of records that are displayed on a screen. Filtering records in the mobile app works like filtering with a condition builder on the Now Platform.

**Before you begin**
Role required: sn_si.analyst

**About this task**
Time to complete this task: 5 minutes.

**Procedure**

1. To further refine your search results, or to enter additional filter criteria on any list of records that is displayed, tap the filter icon ( ▼ ).
2. With the Filters screen displayed, tap a field to expand it.
3. From the options that are displayed, tap the check box or tap an item for your filter. For many of the filters, you can select more than one option.
4. Tap the Back arrow ( ▼ ) or DONE to save your changes to a field. The criteria you chose are displayed on the Filters screen. The number of records that match your criteria is also displayed at the top of the screen. Tap RESET to remove any filters and restore the default setting.
5. **Optional:** Repeat steps 1 - 4 with the Filters screen displayed to continue setting your filter criteria.
6. Tap the intersection icon ( ▼ ) to create AND conditions. Alternatively, tap the intersection icon ( ▼ ) to create OR conditions.
7. After you have added all the criteria you want, with the Filters screen displayed, tap DONE. On the screen, only the records that match your filter criteria are displayed.
Security Incident Response Orchestration

Security Incident Response Orchestration activities allow users to interact with and retrieve data from Windows or UNIX-based systems and environments using workflow orchestration.

Set up Security Incident Response Orchestration

Prior to using Security Incident Response Orchestration, perform steps to set up various parts of the system, including populating the CMDB, configuring the mid-server, and configuring credentials.

Before you begin
Role required: admin
To use Security Incident Response, you need a fully populated CMDB with domain names. For more information, see .

About this task

Procedure
1. Activate Security Incident Response plugin.
2. Configure the mid-server.
3. Configure credentials.

Understand Security Incident Response Orchestration workflows and workflow templates

The Security Incident Response base system includes a series of workflows and workflow templates designed to work with security incident records.

Before you begin
You can tailor all workflows and workflow templates to better suit your needs, assuming you have the appropriate role: sn_sec_cmn.admin. Workflows are used throughout the Security Operations system to perform a variety of tasks. Workflow templates, however, are triggered by selecting a value in the Category field in a security incident. When this occurs, the workflow template associated with the selection kicks off a workflow template that instructs the security analysts how to deal with a specific type of threat.

For example, if you select Denial of Service from the Category field in a security incident, the Security Incident - Denial of Service - Template is executed and the analyst is directed to determine whether the target of the DOS is business critical. If so, the next task causes the priority of the security incident to be set to 1 - Critical, and then executes the next task. And so on.
So Security Incident Response workflows and workflow templates are essentially the same, except the templates are used for a specific set of functions within a security incident.

Role required: sn_si.basic

Procedure

2. A list of the workflows and workflow templates shipped in the base system are displayed. Any new workflows that you have created in the Security Operations application suite are also included in the list.
3. Click the name of the workflow or workflow template you want to view.

⚠️ Note: Workflows can be triggered in several different ways. Be aware that associating a workflow with a workflow trigger does not necessarily mean the workflow is active.

Security Incident Response Orchestration workflows and activities

Several workflows and activities are included with Security Incident Response Orchestration.

Only users with the sn_sec_cmn.admin role can add and edit Security Operations workflows.

Create Lookup Request for IoC Changes workflow

The Security Incident Response - Create Lookup Request for IoC Changes workflow is triggered by a business rule to run automatically when an IoC is added or changed. Malware scans are triggered only when new data is entered and only the new data is scanned.

Before you begin

Role required: sn_si.basic

About this task

If the IoC is empty, the workflow does not run. Historical scans are retained and viewable in the Security Scan Requests tab and work notes of the security incident.

Existing security incidents are automatically updated.

Workflow process activities include:
Run Audit Log script.

Create IoC Lookup Request activity

Create IoC Lookup Request activity

The **Create IoC Lookup Request** activity can be used with any workflow to create a malware lookup request for added or modified IoC fields.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Lookup request created.</td>
</tr>
<tr>
<td>Failure</td>
<td>Lookup request not created.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>iocString</td>
<td>JSON formatted IoC information. IP, hash, url.</td>
</tr>
<tr>
<td>siId</td>
<td>Security incident system identifier</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scnReqID</td>
<td>Lookup request identifier</td>
</tr>
</tbody>
</table>

Security Incident Response - Get Network Statistics workflow

The Security Incident Response > Get Network Statistics workflow retrieves the network statistics for an affected Windows-based resource when added to a security incident in the Analysis state.

Before you begin
Role required: sn_si.analyst

About this task
For new security incidents that contain configuration items, the workflow runs automatically when the state changes to Analysis.

Existing security incidents are automatically updated when you are in the Analysis state and you add a new configuration item.
Workflow process activities include:

- Get Configuration Item FQDN activity
- Determine Shell Script by OS
- If statement is executed by Powershell
- Execution Tracking - Begin activity
- Get Network Statistics via netstat activity
- Capability Execution Tracking - Failure activity
- Create Enrichment Data records activity
- Capability Execution Tracking - Failure activity - Returns enrichmentID.
- Capability Execution Tracking - Complete activity

Procedure
1. Open a security incident.
2. Update the State to Analysis, if necessary.
3. Add a configuration item (computer, server, or similar).
4. Click Update.

Security Incident Response Orchestration provides network statistics information in the Related Links > Security Incident Enrichments tab. For more information see, Security Operations enrichment data mapping.

Activities specific to this workflow are described here. For more information on other activities, see Common integration workflow activities.

Security Operations System Command Integration - Get Running Processes workflow
The Security Operations System Command Integration - Get Running Processes workflow retrieves the running processes of a configuration item when added or updated to a Windows or Unix-based security incident in the Analysis state.

Before you begin
Role required: sn_si.analyst

About this task
For new security incidents, the workflow runs automatically when you submit the incident with a selected configuration item, when the state automatically changes to Analysis. If it remains in the Draft state, then it does not run.
Existing security incidents are automatically updated when you are in the **Analysis** state and you add a new configuration item.

**Workflow process activities include:**

- Get Configuration Item FQDN activity
- Determine Shell Script by OS activity
- Execution Tracking - Begin activity
- Get Running Processes via PowerShell
- Execute Shell Script activity
- Capability Execution Tracking - Failure activity
- Extract Shell Script from MID Script activity
- Combine Results and return values in an array
- Create Enrichment Data records activity
- Capability Execution Tracking - Complete activity

**Procedure**

1. Open a security incident.
2. Update the **State** to **Analysis**, if necessary.
3. Add a configuration item (computer, server, or similar).
4. Click **Update**.
Security Incident Response Orchestration provides running process information in the Related Link > Security Incident Enrichments tab. For more information, see Security Operations enrichment data mapping.

Activities specific to this workflow are described here. For more information on other activities, see Common integration workflow activities.

Security Incident Response - Get Running Services workflow

The Security Incident Response - Get Running Services workflow retrieves a list of running services from Windows-based, ServiceNow, configuration items (CIs). This workflow is used for incident enrichment during investigations.

Before you begin
Role required: sn_si.analyst

About this task

The Security Incident Response - Get Running Services workflow runs automatically when you add a new configuration item to a Windows security incident after the state changes to Analysis. The information this workflow obtains appears on the Show Enrichment Data tabs for the security incident.

Note: If the security incident remains in the Draft state, the Security Incident Response - Get Running Services workflow workflow does not run.

Workflow activities include:

- Audit Log Enrichment Script activity
- Get Configuration Item FQDN activity
- Determine Shell Script by OS activity
- Is Execution via PowerShell activity
- Get Running Services - WMI Enrichment activity
- Create Enrichment Data records activity
Procedure

1. Open a security incident.
2. Update the State to Analysis, if necessary.
3. Add a Windows-based configuration item (server, laptop, or similar).
4. Click Update.

   Security Incident Response provides running services information in the Related Links > Security Incident Enrichments tab. For more information, see Security Operations enrichment data mapping.

Get Configuration Item FQDN activity

The Security Common Orchestration > Get Configuration Item FQDN workflow activity retrieves the fully qualified domain name (FQDN) of a configuration item. This activity can accelerate the investigation and remediation process.

The Get Configuration Item FQDN activity can be used with any workflow to retrieve the fully qualified domain name (FQDN) of a configuration item.

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cmddb_ci.id</td>
<td>The system identifier (sys_id) of a configuration item record.</td>
</tr>
</tbody>
</table>
Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fqdn</td>
<td>The fully qualified domain name (FQDN) of the configuration item.</td>
</tr>
</tbody>
</table>

Additional Notes

The fqdn field on the configuration item must be populated.

Determine Shell Script by OS activity

The Determine Shell Script by OS workflow activity determines which operating system to use in the workflow.

The Determine Shell Script by OS activity can be used with any workflow to determine which shell script to run based on the operating system running on the system containing the configuration item.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Found operating system.</td>
</tr>
<tr>
<td>Failure</td>
<td>No operating system found. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ciSysId</td>
<td>System identifier of the configuration item.</td>
</tr>
<tr>
<td>processType</td>
<td>Internal identifier that defines which script to pull from the table.</td>
</tr>
</tbody>
</table>
Output variables
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>processScript</td>
<td>ECC agent that gathers the running process.</td>
</tr>
<tr>
<td>executionTemplate</td>
<td>Determines whether the script is run through a probe or using PowerShell.</td>
</tr>
<tr>
<td>enrichmentMappingId</td>
<td>System identifier of the enrichment mapping used to transform the response data.</td>
</tr>
</tbody>
</table>

Get Running Services - WMI Enrichment
The Security Incident Response - Get Running Services workflow gathers running services on a configuration item added to a security incident.

The Get Running Services - WMI Enrichment activity is launched automatically to retrieve running services information for a Windows host.

Input variables
Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>The fully qualified domain name (FQDN) of the target system.</td>
</tr>
</tbody>
</table>

Output variables
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>response</td>
<td>A JSON string representing the current running services on the target system.</td>
</tr>
<tr>
<td></td>
<td>JSON data includes:</td>
</tr>
<tr>
<td></td>
<td>name</td>
</tr>
</tbody>
</table>
Output variables (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The name of the service</td>
<td></td>
</tr>
<tr>
<td><strong>pid</strong></td>
<td>The process identifier of the running service</td>
</tr>
<tr>
<td>Also, if available:</td>
<td></td>
</tr>
<tr>
<td><strong>service_type</strong></td>
<td>The type of running service</td>
</tr>
<tr>
<td><strong>start_name</strong></td>
<td>The system name for the service</td>
</tr>
<tr>
<td><strong>path</strong></td>
<td>The file path of the running service executable</td>
</tr>
<tr>
<td><strong>start_mode</strong></td>
<td>The start mode of the running service.</td>
</tr>
<tr>
<td><strong>display_name</strong></td>
<td>The name of the running service as it appears to the user</td>
</tr>
</tbody>
</table>

Restrictions
The MID Server must support **PowerShell**.
SHA-256 hash requires PowerShell V4.

Create Enrichment Data records activity
The **Create enrichment data records** workflow activity creates or updates enrichment records to use in the workflow.

The **Create Enrichment Data records** activity can be used with any workflow to update enrichment records in the workflow.

Results
Possible results for this activity are:
Results

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Enrichment record updated.</td>
</tr>
<tr>
<td>Failure</td>
<td>Enrichment record not updated. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>task_id</td>
<td>Task identifier.</td>
</tr>
<tr>
<td>content</td>
<td>Raw content (running processes data).</td>
</tr>
<tr>
<td>enrichment_mapping_id</td>
<td>Enrichment mapping identifier.</td>
</tr>
<tr>
<td>ci_id</td>
<td>Configuration item identifier.</td>
</tr>
<tr>
<td>reference_value</td>
<td>Unused.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>GlideRecords created using the enrichmentUtils script.</td>
</tr>
</tbody>
</table>

Run procdump workflow

The Run procdump workflow runs a process dump on a specified process and saves it to a file that can be targeted by security analysts.

About this task

This workflow is triggered when enriched processes are selected and a Run procdump UI action is executed.
Workflow process activities include:

- **Run Script (Audit log enrichment):** Runs a script to add an audit log to the security incident.

- **Execute procdump activity**

- **Run Script (Success - Add SI work note):** Runs a script to add a work note when the procdump succeeds.

- **Run Script (Failed - Add SI work note):** Runs a script to add a work note when the procdump fails. Reasons the procdump can fail includes:
  - Invalid dump path
  - Invalid file share path
  - Unable to fetch the fully-qualified domain name of the Windows machine the procdump is running on
  - The process name is not specified
  - The PROCDUMP environment variable not found
  - A copy of the dump file fails to copy from the dump path to the file share path
Execute procdump activity

**Execute procdump** is a powershell activity that runs the procdump on the selected processes, dumps the data into a file, and posts it to a shared site on an internal network. An analyst can then view a deny listed process, highlighted in red in a security incident, and perform additional analysis on the file.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The procdump executed successfully on the process_name, and the details are available in activityOutput.response.</td>
</tr>
<tr>
<td>Failure</td>
<td>The procdump failed to execute on the process_name, and the details are available in activityOutput.response.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables are used to create the requested outputs.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>targetId</td>
<td>[Mandatory] The target ID to run the procdump on.</td>
</tr>
<tr>
<td>process_name</td>
<td>[Mandatory] The process name for the procdump.</td>
</tr>
<tr>
<td>dump_path</td>
<td>[Mandatory] The local file path to which the generated dump file will be saved.</td>
</tr>
<tr>
<td>dump_filename</td>
<td>[Mandatory] The filename of the file generated by the procdump. All special characters will be replaced with hyphens (-) from the dump file name when the file is generated.</td>
</tr>
<tr>
<td>file_share_path</td>
<td>[Mandatory] The file share path to which the dump file will be copied.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.
Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>share_path</td>
<td>The file share path to which the dump file was copied.</td>
</tr>
<tr>
<td>response</td>
<td>A JSON representation of the result of the procdump.</td>
</tr>
<tr>
<td>result</td>
<td>The result of the procdump.</td>
</tr>
</tbody>
</table>

Security Incident - Evaluate response task outcome workflow

Security Incident - Evaluate Response task outcome workflow determines the task to use, invokes a chosen workflow and evaluation script based on the outcome evaluator record provided as input to the chosen workflow.

Before you begin
Role required: sn_si.write ??

About this task
This workflow is intended to run at the same time as the create task activity to be evaluated. The evaluation script queries the artifacts (such as sightings search records, or running processes) of the configured capability using context information from the response task (such as its parent security incident) to determine the appropriate outcome for the response task. The outcome could potentially be workflow activity dependent, but is generally yes or no. When creating an outcome evaluator record only capabilities that have a configured workflow, with the Is task based capability box checked, and a task input variable set are available to select.

Workflow process activities include:

- Run script to determine response task
- Should Run Workflow
- Parallel Flow Launcher Launch Capability Workflow
- Create Evaluation Event
Security Incident Response workflow templates

Workflow templates are provided with Security Incident Response Orchestration to allow you to perform basic security operation-related analysis procedures. The templates can be used as is or you can customize them to create workflows to better suit your specific needs. The workflow templates are deactivated by default.

Only users with the sn_sec_cmn.admin role can add and edit Security Operations workflows.

Security Incident Confidential Data Exposure workflow template

The Security Incident - Confidential Data Exposure - Template allows you to perform a series of tasks designed to handle the exposure of sensitive data.

Before you begin
Role required: sn_si.write

About this task
The workflow is triggered when the Category in a security incident is set or changed to Confidential personal identity data exposure. This action causes a response task to be created for the first activity in the workflow.
Procedure

1. Open the security incident for which you want to handle the exposure to sensitive data, or create a new security incident.

2. In Category, select Confidential personal identity data exposure.

3. Save the record.

4. Scroll down and open the Response Tasks related list. The first of a series of response tasks appears. Each time the record is saved, your response to the previous task either causes the next response task to be created or the flow to end.

<table>
<thead>
<tr>
<th>Response task</th>
<th>Description</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the data sensitive?</td>
<td>Determine whether the data associated with this security incident is sensitive or confidential. In the task, select Yes or No in Outcome.</td>
<td>If you selected Yes, the next response task is executed. If you selected No, the flow ends.</td>
</tr>
<tr>
<td>Determine root cause and</td>
<td>Determine the root cause of the attack and add egress filtering to stop the exfiltration,</td>
<td>If you change the state of the task to Closed Complete or Cancelled, the next response task is executed.</td>
</tr>
<tr>
<td>Response task</td>
<td>Description</td>
<td>Results</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>prevent egress</td>
<td>updating the <strong>State</strong> field in the task as appropriate.</td>
<td>If you change the state of the task to <strong>Closed Complete</strong> or <strong>Cancelled</strong>, the next response task is executed.</td>
</tr>
<tr>
<td>Eliminate exposure related to root cause</td>
<td>Based on the root cause, perform the steps to eliminate the exposure, updating the <strong>State</strong> field in the task as appropriate.</td>
<td>If you change the state of the task to <strong>Closed Complete</strong> or <strong>Cancelled</strong>, the next response task is executed.</td>
</tr>
<tr>
<td>Quarantine residual artifacts</td>
<td>Perform the steps to quarantine any residual artifacts, updating the <strong>State</strong> field in the task as appropriate.</td>
<td>If you change the state of the task to <strong>Closed Complete</strong> or <strong>Cancelled</strong>, the next response task is executed.</td>
</tr>
<tr>
<td>Legal process</td>
<td>Perform the steps to satisfy the legal requirements of this analysis, updating the <strong>State</strong> field in the task as appropriate.</td>
<td>If you change the state of the task to <strong>Closed Complete</strong> or <strong>Cancelled</strong>, the next response task is executed.</td>
</tr>
<tr>
<td>PR process</td>
<td>Perform the steps to satisfy the PR requirements of this analysis, updating the <strong>State</strong> field in the task as appropriate.</td>
<td>If you change the state of the task to <strong>Closed Complete</strong> or <strong>Cancelled</strong>, the next response task is executed.</td>
</tr>
<tr>
<td>Set state to review</td>
<td>No action required.</td>
<td>The <strong>State</strong> of the security incident is automatically changed to <strong>Review</strong>.</td>
</tr>
<tr>
<td>Lessons learned meeting</td>
<td>Conduct a lessons learned meeting to triage the work performed on this sensitive data, updating the <strong>State</strong> field in the task as appropriate.</td>
<td>If you change the state of the task to <strong>Closed Complete</strong> or <strong>Cancelled</strong>, the security incident remains in the <strong>Review</strong> state until you close it.</td>
</tr>
</tbody>
</table>

**Security Incident Denial of Service workflow template**

The Security Incident - Denial of Service - Template allows you to perform a series of tasks designed to handle Denial of Service (DOS) attacks.

**Before you begin**
Role required: sn_si.write
About this task
The workflow is triggered when the Category in a security incident is set to Denial of Service. This action causes a response task to be created for the first activity in the workflow.

Procedure
1. Open the security incident for this denial of service occurrence, or create a new security incident.
2. In Category, select Denial of Service.
3. Save the record.
4. Scroll down and open the Response Tasks related list.
   The first of a series of response tasks appears. Each time the record is saved, your response to the previous task either causes the next response task to be created or the flow to end.

Response tasks in Denial of Service Template

<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is target business critical?</td>
<td></td>
<td>Determine if the target of this DOS attack is business critical.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In the task, select Yes or No in Outcome.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you select Yes, the Set priority to critical task is executed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you select No, the Is a vulnerability being exploited? task is executed.</td>
</tr>
<tr>
<td>Response task</td>
<td>Action</td>
<td>Results</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Set priority to critical</td>
<td>No action required.</td>
<td>The <strong>Priority</strong> of the security incident is changed automatically to <strong>Critical</strong>, and the <strong>Is a vulnerability being exploited?</strong> task is executed.</td>
</tr>
<tr>
<td>Is a vulnerability being exploited?</td>
<td>Determine whether this DOS attack exploits a software vulnerability.</td>
<td>If you select <strong>Yes</strong>, the <strong>Emergency patch request</strong> task is executed.</td>
</tr>
<tr>
<td></td>
<td>In the task, select <strong>Yes</strong> or <strong>No</strong> in <strong>Outcome</strong>.</td>
<td>If you select <strong>No</strong>, the <strong>Internal attacker?</strong> task is executed.</td>
</tr>
<tr>
<td>Emergency patch request</td>
<td>Issue an emergency patch request for the system(s) being attacked.</td>
<td>If you changed the state of the task to <strong>Closed Complete</strong> or <strong>Cancelled</strong>, the next response task is executed.</td>
</tr>
<tr>
<td></td>
<td>Update the <strong>State</strong> field in the task as appropriate.</td>
<td></td>
</tr>
<tr>
<td>Internal attacker?</td>
<td>Determine if the source of this DOS attack is internal to your organization.</td>
<td>If you select <strong>Yes</strong>, the <strong>Isolate attacking host(s)</strong> task is executed.</td>
</tr>
<tr>
<td></td>
<td>In the task, select <strong>Yes</strong> or <strong>No</strong> in <strong>Outcome</strong>.</td>
<td>If you select <strong>No</strong>, the <strong>Notify DOS protection provider and/or ISP</strong> task is executed.</td>
</tr>
<tr>
<td>Isolate the attacking host(s)</td>
<td>Perform the steps necessary to isolate the internal host(s) responsible for the attack.</td>
<td>After you complete this step, the <strong>Validate system integrity of attacked systems</strong> task is executed.</td>
</tr>
<tr>
<td></td>
<td>Update the <strong>State</strong> field in the task as appropriate.</td>
<td></td>
</tr>
<tr>
<td>Notify DOS protection provider and/or ISP</td>
<td>Perform the steps necessary to contact your Denial of Service protection provider and/or your Internet Service Provider to notify them of the attack.</td>
<td>If you changed the state of the task to <strong>Closed Complete</strong> or <strong>Cancelled</strong>, the next response task is executed.</td>
</tr>
<tr>
<td></td>
<td>Update the <strong>State</strong> field in the task as appropriate.</td>
<td></td>
</tr>
<tr>
<td>Validate system integrity of</td>
<td>Perform the steps necessary to assess and validate the integrity of the attacked computers.</td>
<td>If you changed the state of the task to <strong>Closed Complete</strong></td>
</tr>
<tr>
<td>Response task</td>
<td>Action</td>
<td>Results</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>attacked systems</td>
<td>Update the <strong>State</strong> field in the task as appropriate.</td>
<td>or <strong>Cancelled</strong>, the next response task is executed.</td>
</tr>
<tr>
<td>Review DOS protections</td>
<td>Conduct a review of your existing DOS protections and procedures. Make any necessary changes. Update the <strong>State</strong> field in the task as appropriate.</td>
<td>If you changed the state of the task to <strong>Closed Complete</strong> or <strong>Cancelled</strong>, the next response task is executed.</td>
</tr>
<tr>
<td>Set state to review</td>
<td>No action required.</td>
<td><strong>State</strong> of the security incident is changed automatically to <strong>Review</strong>. The <strong>Lessons learned meeting</strong> task is executed.</td>
</tr>
<tr>
<td>Lessons learned meeting</td>
<td>Conduct a lessons learned meeting to triage the work performed for this Denial of Service incident. Update the <strong>State</strong> field in the task as appropriate.</td>
<td>If you change the state of the task to <strong>Closed Complete</strong> or <strong>Cancelled</strong>, the flow ends.</td>
</tr>
</tbody>
</table>

**Security Incident Lost Equipment workflow template**

The Security Incident - Lost Equipment - Template allows you to perform a series of tasks designed to handle lost equipment.

**Before you begin**
Role required: sn_si.write

**About this task**
The workflow is triggered when the **Category** in a security incident is set to **Equipment loss**. This action causes a response task to be created for the first activity in the workflow.
Procedure

1. Open the security incident for the equipment loss, or create a new security incident.

2. In Category, select Equipment loss.

3. Save the record.

4. Scroll down and open the Response Tasks related list. The first of a series of response tasks appears. Each time the record is saved, your response to the previous task either causes the next response task to be created or the flow to end.

Response tasks in Lost Equipment Template

<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did the equipment contain sensitive data?</td>
<td>Determine whether the equipment associated with this security incident contained any sensitive or confidential information.</td>
<td>If you select Yes the Was the data encrypted? task is executed.</td>
</tr>
<tr>
<td></td>
<td>In the task, select Yes or No in Outcome as appropriate.</td>
<td>If you select No, the flow ends.</td>
</tr>
<tr>
<td>Was the data encrypted?</td>
<td>Determine if the sensitive data on the lost device was encrypted.</td>
<td>If you select Yes, the Remote wipe created? response task is executed.</td>
</tr>
<tr>
<td></td>
<td>In the task, select Yes or No in Outcome as appropriate.</td>
<td>If you select No, the Create potential data response task is created.</td>
</tr>
<tr>
<td>Response task</td>
<td>Action</td>
<td>Results</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Create potential data loss incident</td>
<td>Perform the steps necessary to create a potential data loss incident.</td>
<td>The Remote wipe created? response task is executed.</td>
</tr>
<tr>
<td></td>
<td>After you have finished, set the state of the task to Complete or Incomplete as appropriate.</td>
<td></td>
</tr>
<tr>
<td>Remote wipe created?</td>
<td>Perform the steps necessary to execute a remote wipe of the lost equipment.</td>
<td>The Legal process - Disclosure required task is executed.</td>
</tr>
<tr>
<td></td>
<td>In the task, select Yes or No in Outcome as appropriate.</td>
<td></td>
</tr>
<tr>
<td>Legal process - Disclosure required?</td>
<td>Perform the steps to satisfy the legal requirements of this analysis.</td>
<td>The Lessons learned meeting task is executed.</td>
</tr>
<tr>
<td></td>
<td>Select Yes if a legal disclosure is required, No if it is not.</td>
<td></td>
</tr>
<tr>
<td>PR process</td>
<td>Perform the steps necessary to satisfy the PR requirements of this analysis.</td>
<td>The Set state to review task is executed.</td>
</tr>
<tr>
<td></td>
<td>After you have finished, set the state of the task to Complete or Incomplete as appropriate.</td>
<td></td>
</tr>
<tr>
<td>Set state to review</td>
<td>No action is necessary.</td>
<td>The State of the security incident is changed automatically to Review.</td>
</tr>
<tr>
<td>Lessons learned meeting</td>
<td>Conduct a lessons learned meeting to triage the work performed for this lost equipment incident.</td>
<td>The flow ends.</td>
</tr>
<tr>
<td></td>
<td>After you have finished, set the state of the task to Complete or Incomplete as appropriate.</td>
<td></td>
</tr>
</tbody>
</table>

**Security Incident Malicious Software workflow template**

The Security Incident - Malicious Software - Template allows you to perform a series of tasks designed to handle malicious software on your network.
Before you begin
Role required: sn_si.write

About this task
The workflow is triggered when the Category in a security incident is set to Malicious Software. This action causes a response task to be created for the first activity in the workflow.

Procedure
1. Open the security incident for this potential attack, or create a new security incident.
2. In Category, select Malicious code activity.
3. Save the record.
4. Scroll down and open the Response Tasks related list.
   The first of a series of response tasks appears. Each time the record is saved, your response to the previous task either causes the next response task to be created or the workflow to end.
### Response tasks in Malicious Software Template

<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Endpoint - Malware Found?</td>
<td>After running a scan, determine whether malware was found.</td>
<td>If you select <strong>Yes</strong>, the <strong>Remove Malware - Success?</strong> task is executed.</td>
</tr>
<tr>
<td></td>
<td>In the task, select <strong>Yes</strong> or <strong>No</strong> in <strong>Outcome</strong>.</td>
<td>If you select <strong>No</strong>, the flow ends.</td>
</tr>
<tr>
<td>Remove Malware - Success?</td>
<td>Determine whether the malware was successfully removed.</td>
<td>If you select <strong>Yes</strong>, the <strong>Was there a larger breach?</strong> task is executed.</td>
</tr>
<tr>
<td></td>
<td>In the task, select <strong>Yes</strong> or <strong>No</strong> in <strong>Outcome</strong>.</td>
<td>If you select <strong>No</strong>, the <strong>Wipe &amp; Reimage</strong> task is executed.</td>
</tr>
<tr>
<td>Wipe &amp; Reimage</td>
<td>If you did not successfully remove the malware found, this task instructs you to perform a wipe and reimage on the computers infected with the malware.</td>
<td>After the task is complete, the <strong>Set State to Review</strong> task is executed.</td>
</tr>
<tr>
<td>Was there a larger breach?</td>
<td>Determine whether the breach caused by the malicious software is larger than first believed.</td>
<td>If you select <strong>Yes</strong>, the following tasks are executed in parallel:</td>
</tr>
<tr>
<td></td>
<td>In the task, select <strong>Yes</strong> or <strong>No</strong> in <strong>Outcome</strong>.</td>
<td>• Legal Review</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HR Review</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Law Enforcement Review</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you select <strong>No</strong>, the flow ends.</td>
</tr>
<tr>
<td>Legal Review</td>
<td>Perform the steps necessary for each of these departments to review the process you followed to eradicate the malicious software.</td>
<td>When the tasks are complete, the <strong>Set State to Review</strong> task is executed.</td>
</tr>
<tr>
<td>HR Review</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Law Enforcement Review</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set State to Review</td>
<td>No action required.</td>
<td>The <strong>State</strong> of the security incident is changed automatically to <strong>Review</strong>, and the flow ends.</td>
</tr>
</tbody>
</table>

**Security Incident Phishing workflow template**

The Security Incident - Phishing - Template allows you to perform a series of tasks designed to handle spear phishing emails on your network.

**Before you begin**
Role required: sn_si.write

**About this task**
The workflow is triggered when the **Category** in a security incident is set to **Spear Phishing**. This action causes a response task to be created for the first activity in the workflow.
Procedure

1. Open the security incident for this potential spear phishing attack, or create a new security incident.

2. In Category, select Spear Phishing.

3. Save the record.

4. Scroll down and open the Response Tasks related list.
   The first of a series of response tasks appears. Each time the record is saved, your response to the previous task either causes the next response task to be created or the workflow to end.
<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is this a Phishing attack?</td>
<td>Determine if this is a phishing attack.</td>
<td>If you select <strong>Yes</strong>, the following tasks are executed in parallel:</td>
</tr>
<tr>
<td></td>
<td>In the task, select <strong>Yes</strong> or <strong>No</strong> in <strong>Outcome</strong>.</td>
<td>• Scan Endpoint - Malware Found?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Update Email Protection Software</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Remove Unread Phishing Email in Queue - For All Users</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you select <strong>No</strong>, the flow ends.</td>
</tr>
<tr>
<td>Scan Endpoint - Malware Found?</td>
<td>After running a scan, determine whether malware was found.</td>
<td>If you select <strong>Yes</strong>, the <strong>Remove Malware - Success?</strong> task is executed.</td>
</tr>
<tr>
<td></td>
<td>In the task, select <strong>Yes</strong> or <strong>No</strong> in <strong>Outcome</strong>.</td>
<td>If you select <strong>No</strong>, the <strong>Set State to Review</strong> task is executed.</td>
</tr>
<tr>
<td>Remove Malware - Success?</td>
<td>Determine whether the malware was successfully removed.</td>
<td>If you select <strong>Yes</strong>, the <strong>Set State to Review</strong> task is executed.</td>
</tr>
<tr>
<td></td>
<td>In the task, select <strong>Yes</strong> or <strong>No</strong> in <strong>Outcome</strong>.</td>
<td>If you select <strong>No</strong>, the <strong>Wipe and reimage</strong> task is executed.</td>
</tr>
<tr>
<td>Wipe and reimage</td>
<td>If you did not successfully remove the malware found, this task instructs you</td>
<td>After the task is complete, the <strong>Set</strong></td>
</tr>
<tr>
<td>Response task</td>
<td>Action</td>
<td>Results</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>to perform a wipe and reimage on the computers infected with the malware.</td>
<td><strong>State to Review</strong> task is executed.</td>
<td></td>
</tr>
<tr>
<td>Update Email Protection Software</td>
<td>If it was determined that this is a phishing attack, you are prompted to update your email protection software accordingly.</td>
<td>When the task is complete, the <strong>Set State to Review</strong> task is executed.</td>
</tr>
<tr>
<td>Remove Unread Phishing Email in Queue - For All Users</td>
<td>Perform the steps necessary to remove the phishing email still in the queue for all of your users.</td>
<td>When the task is complete, the <strong>Set State to Review</strong> task is executed.</td>
</tr>
<tr>
<td>Set State to Review</td>
<td>No action required.</td>
<td>The <strong>State</strong> of the security incident is changed automatically to <strong>Review</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The <strong>Schedule Security Awareness Training</strong> task is executed.</td>
</tr>
<tr>
<td>Schedule Security Awareness Training</td>
<td>Schedule training to heighten security awareness by your employees. Update the <strong>State</strong> field in the task as appropriate.</td>
<td>When the task is complete, the flow ends.</td>
</tr>
</tbody>
</table>

**Security Incident Policy Violation workflow template**

The Security Incident - Policy Violation - Template allows you to perform a series of tasks designed to handle security policy violations.

**Before you begin**
Role required: sn_si.write

**About this task**
The workflow is triggered when the **Category** in a security incident is set to **Policy violation**. This action causes a response task to be created for the first activity in the workflow.
Procedure

1. Open the security incident for the policy violation, or create a new security incident.

2. In Category, select Policy violation.

3. Save the record.

4. Scroll down and open the Response Tasks related list. The first of a series of response tasks appears. Each time the record is saved, your response to the previous task either causes the next response task to be created or the workflow to end.

Response tasks in Policy Violation Template

<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classify violation</td>
<td>Classify how this infraction violates your organization's security policies. Update the State field in the task after you have completed it.</td>
<td>The Advise violator of infraction response task is executed.</td>
</tr>
<tr>
<td>Advise violator of infraction</td>
<td>Communicate the nature of the infraction to the violator. Update the State field in the task after you have communicated it.</td>
<td>The Obtain acknowledgement from violator response task is executed.</td>
</tr>
<tr>
<td>Obtain acknowledgement from violator</td>
<td>Obtain an acknowledgement from the violator of the infraction.</td>
<td>The HR process response task is executed.</td>
</tr>
<tr>
<td>Response task</td>
<td>Action</td>
<td>Results</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Update the State field in the task as appropriate.</td>
<td>HR process Communicate all necessary information about this violation to HR. Update the State field in the task as appropriate.</td>
<td>The Set state to review response task is executed.</td>
</tr>
<tr>
<td>Set state to review No action is necessary.</td>
<td>Schedule security awareness training Conduct a security awareness training to educate staff on how to prevent similar security violations in the future. Update the State field in the task as appropriate.</td>
<td>The State of the security incident is changed automatically to Review. If you change the state of the task to Closed Complete or Cancelled, the flow ends.</td>
</tr>
</tbody>
</table>

**Security Incident Reconnaissance workflow template**

Reconnaissance is usually a preliminary step toward a further attack seeking to exploit a device or system. The Security Incident - Reconnaissance - Template allows you to perform a series of tasks designed to handle reconnaissance on your network.

**Before you begin**

Role required: sn_si.write

**About this task**

The workflow is triggered when the Category in a security incident is set to **Reconnaissance activity**. This action causes a response task to be created for the first activity in the workflow.
Procedure

1. Open the security incident for this potential attack, or create a new security incident.

2. In Category, select **Reconnaissance activity**.

3. Save the record.

4. Scroll down and open the **Response Tasks** related list.
   The first of a series of response tasks appears. Each time the record is saved, your response to the previous task either causes the next response task to be created or the workflow to end.

### Response tasks in Reconnaissance Template

<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconnaissance activity verified?</td>
<td>Determine whether any observed reconnaissance has been verified.</td>
<td>If you select <strong>Yes</strong>, the <strong>Identify impacted systems</strong> task is executed. If you select <strong>No</strong>, the flow ends.</td>
</tr>
<tr>
<td></td>
<td>In the task, select <strong>Yes</strong> or <strong>No</strong> in Outcome.</td>
<td></td>
</tr>
<tr>
<td>Identify impacted systems</td>
<td>Determine the systems impacted by the reconnaissance.</td>
<td>When this task is complete, the <strong>Allow reconnaissance for law enforcement analysis?</strong> task is executed.</td>
</tr>
<tr>
<td>Response task</td>
<td>Action</td>
<td>Results</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow reconnaissance for law enforcement analysis?</td>
<td>Determine whether you want the reconnaissance to be analyzed by law enforcement agencies. In the task, select <strong>Yes</strong> or <strong>No</strong> in Outcome.</td>
<td>If you select <strong>Yes</strong>, the <strong>Law enforcement process</strong> task is executed. If you select <strong>No</strong>, the <strong>Update system(s) to prevent reconnaissance</strong> task is executed.</td>
</tr>
<tr>
<td>Law enforcement process</td>
<td>Perform the law enforcement process as defined by your company.</td>
<td>When this task is complete, the <strong>Update system(s) to prevent reconnaissance</strong> task is executed.</td>
</tr>
<tr>
<td>Update system(s) to prevent reconnaissance</td>
<td>Perform the steps necessary to update the systems affected by the reconnaissance.</td>
<td>When this task is complete, the <strong>Set state to review</strong> task is executed.</td>
</tr>
<tr>
<td>Set state to review</td>
<td>No action required.</td>
<td>The <strong>State</strong> of the security incident is changed automatically to <strong>Review</strong>, and the <strong>Lessons learned meeting</strong> task is executed.</td>
</tr>
<tr>
<td>Lessons learned meeting</td>
<td>Conduct a lessons learned meeting to triage the work performed for this reconnaissance incident. Update the <strong>State</strong> field in the task as appropriate.</td>
<td>When this task is complete, the flow ends.</td>
</tr>
</tbody>
</table>

**Security Incident Rogue Server or Service workflow template**

The Security Incident - Rogue Server or Service - Template allows you to perform a series of tasks designed to handle activity from rogue servers or services affecting your network.

**Before you begin**
Role required: sn_si.write
About this task
The workflow is triggered when the Category in a security incident is set to Rogue server or service. This action causes a response task to be created for the first activity in the workflow.

Procedure
1. Open the security incident for this potential attack, or create a new security incident.
2. In Category, select Rogue server or service activity.
3. Save the record.
4. Scroll down and open the Response Tasks related list. The first of a series of response tasks appears. Each time the record is saved, your response to the previous task either causes the next response task to be created or the workflow to end.

Response tasks in Rogue Server or Service Template

<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rogue server or service verified?</td>
<td>Determine whether a connection with a rogue server or service has been verified on your network. In the task, select Yes or No in Outcome.</td>
<td>If you select Yes, the following two tasks are executed in parallel: • Identify impacted system(s) • Potential data loss? If you select No, the flow ends.</td>
</tr>
<tr>
<td>Response task</td>
<td>Action</td>
<td>Results</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Identify impacted system(s)</td>
<td>Determine the systems impacted by contact with the rogue server or service.</td>
<td>When this task is complete, the <strong>Update system(s) - Remove rogue connections</strong> task is executed.</td>
</tr>
<tr>
<td>Potential data loss?</td>
<td>Determine whether the connection with the rogue server or service caused potential data loss. In the task, select <strong>Yes</strong> or <strong>No</strong> in Outcome.</td>
<td>If you select <strong>Yes</strong>, the <strong>Create potential data loss incident</strong> task is executed. If you select <strong>No</strong>, the <strong>Update system(s) - Remove rogue connections</strong> task is executed.</td>
</tr>
<tr>
<td>Create potential data loss incident</td>
<td>Perform the steps necessary to create a security incident for the potential data loss.</td>
<td>When this task is complete, the <strong>Update system(s) - Remove rogue connections</strong> task is executed.</td>
</tr>
<tr>
<td>Update system(s) - Remove rogue connections</td>
<td>Perform the steps necessary to remove the rogue connections.</td>
<td>When this task is complete, the <strong>Set state to review</strong> task is executed.</td>
</tr>
<tr>
<td>Set state to review</td>
<td>No action required.</td>
<td>The <strong>State</strong> of the security incident is changed automatically to <strong>Review</strong>, and the <strong>Lessons learned meeting</strong> task is executed.</td>
</tr>
<tr>
<td>Lessons learned meeting</td>
<td>Conduct a lessons learned meeting to triage the work performed for this rogue server or service incident. Update the <strong>State</strong> field in the task as appropriate.</td>
<td>When this task is complete, the flow ends.</td>
</tr>
</tbody>
</table>

**Security Incident Spam workflow template**

The Security Incident - Spam - Template allows you to perform a series of tasks designed to handle email spam on your network.

**Before you begin**
Role required: sn_si.write
About this task
The workflow is triggered when the Category in a security incident is set or changed to Spam source. This action causes a response task to be created for the first activity in the workflow.

Procedure
1. Open the security incident for which you want to handle email spam, or create a new security incident.
2. In Category, select Spam source.
3. Save the record.
4. Scroll down and open the Response Tasks related list.
   The first of a series of response tasks appears. Each time the record is saved, your response to the previous task either causes the next response task to be created or the workflow to end.

Response tasks in Spam Template

<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
</table>
| Spam contains malicious content?    | Determine whether the spam contains malicious software. In the task, select **Yes** or **No** in Outcome. | If you selected **Yes**, the following response tasks are executed:  
   - Quarantine email message  
   - Create malicious software incident  
   If you selected **No**, the **Update email software** is executed. |
<p>| Create malicious                    | Perform the steps to create a security incident, updating | If you change the state of the task to <strong>Closed Complete</strong> or <strong>Cancelled</strong>, this response task waits until the next three |</p>
<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>software incident</td>
<td>the State field in the task as appropriate.</td>
<td>response tasks have been completed. The state of the security incident then transitions to Review.</td>
</tr>
<tr>
<td>Quarantine email</td>
<td>Perform the steps to quarantine the spam, updating the State field in the task as appropriate.</td>
<td>If you change the state of the task to Closed Complete or Cancelled, the next response task is executed.</td>
</tr>
<tr>
<td>Quarantine email</td>
<td>Perform the steps to quarantine the spam, updating the State field in the task as appropriate.</td>
<td>If you change the state of the task to Closed Complete or Cancelled, the next response task is executed.</td>
</tr>
<tr>
<td>Block source on firewall</td>
<td>Perform the steps to block the email address on the firewall, updating the State field in the task as appropriate.</td>
<td>If you change the state of the task to Closed Complete or Cancelled, the next response task is executed.</td>
</tr>
<tr>
<td>Update email software</td>
<td>Add the email address to your block list, updating the State field in the task as appropriate.</td>
<td>If you change the state of the task to Closed Complete or Cancelled, the next response task is executed.</td>
</tr>
<tr>
<td>Set state to review</td>
<td>No action required.</td>
<td>The State of the security incident is automatically changed to Review.</td>
</tr>
</tbody>
</table>

**Note:** This response task is also executed if you answered No to the Spam contains malicious content? response task.

**Security Incident Unauthorized Access workflow template**

The Security Incident - Unauthorized Access - Template allows you to perform a series of tasks designed to handle unauthorized access to your network.

**Before you begin**
Role required: sn_si.write

**About this task**
The workflow is triggered when the Category in a security incident is set to Unauthorized access. This action causes a response task to be created for the first activity in the workflow.

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Procedure

1. Open the security incident for this potential attack, or create a new security incident.

2. In Category, select Unauthorized access.

3. Save the record.

4. Scroll down and open the Response Tasks related list. The first of a series of response tasks appears. Each time the record is saved, your response to the previous task either causes the next response task to be created or the workflow to end.

Response tasks in Unauthorized Access Template

<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>User credentials compromised?</td>
<td>Determine whether any users credentials have been compromised.</td>
<td>If you select Yes, the following two tasks are executed in parallel:</td>
</tr>
<tr>
<td></td>
<td>In the task, select Yes or No in Outcome.</td>
<td>• Malicious software?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Deactivate user account</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you select No, the Contact user and determine intent task is executed.</td>
</tr>
<tr>
<td>Response task</td>
<td>Action</td>
<td>Results</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Malicious software?</td>
<td>Determine whether the unauthorized access resulted in the introduction of malicious software. In the task, select <strong>Yes or No</strong> in <strong>Outcome</strong>.</td>
<td>If you select <strong>Yes</strong>, the <strong>Create malicious software incident</strong> task is executed. If you select <strong>No</strong>, the <strong>Set state to review</strong> task is executed.</td>
</tr>
<tr>
<td>Create malicious software incident</td>
<td>Perform the steps necessary to create a security incident for the unauthorized access.</td>
<td>When this task is complete, the <strong>Set state to review</strong> task is executed.</td>
</tr>
<tr>
<td>Deactivate user account</td>
<td>Perform the steps necessary to deactivate the compromised user account.</td>
<td>When this task is complete, the <strong>Set state to review</strong> task is executed.</td>
</tr>
<tr>
<td>Contact user and determine intent</td>
<td>Perform the steps necessary to contact the user who responsible for the unauthorized access and determine the reason for the access attempt.</td>
<td>When this task is complete, the <strong>HR process</strong> task is executed.</td>
</tr>
<tr>
<td>HR process</td>
<td>Perform the steps necessary to contact human resources to implement disciplinary action if necessary.</td>
<td>When this task is complete, the <strong>Set state to review</strong> task is executed.</td>
</tr>
<tr>
<td>Set state to review</td>
<td>No action required.</td>
<td>The <strong>State</strong> of the security incident is changed automatically to <strong>Review</strong>, and the flow ends.</td>
</tr>
</tbody>
</table>

**Security Incident Web/BBS Defacement workflow template**

The Security Incident - Web/BBS Defacement - Template allows you to perform a series of tasks designed to handle vandalism directed against one of your organization's BBS or web sites.
Before you begin
Role required: sn_si.write

About this task
The workflow is triggered when the Category in a security incident is set to Web/BBS defacement. This action causes a response task to be created for the first activity in the workflow.

Procedure
1. Open the security incident for this occurrence of web or BBS defacement, or create a new security incident.
2. In Category, select Web/BBS defacement.
3. Save the record.
4. Scroll down and open the Response Tasks related list.
   The first of a series of response tasks appears. Each time the record is saved, your response to the previous task either causes the next response task to be created or the workflow to end.
<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security incident assignment</td>
<td>Create a security incident for each reported incident of website or BBS defacement.</td>
<td>The next response task is executed.</td>
</tr>
<tr>
<td>Defacement verified?</td>
<td>Determine whether the website or BBS has in fact been defaced.</td>
<td>If you select <strong>Yes</strong>, the following response tasks are executed:</td>
</tr>
<tr>
<td></td>
<td>In the task, select <strong>Yes</strong> or <strong>No</strong> in <strong>Outcome</strong>.</td>
<td>• <strong>PR process</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Law enforcement process</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Determine and eradicate root cause</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you select <strong>No</strong>, the flow ends.</td>
</tr>
<tr>
<td>PR process</td>
<td>Perform the steps necessary to notify the public that the website or BBS has been defaced.</td>
<td>The <strong>Lessons learned meeting</strong> task is executed.</td>
</tr>
<tr>
<td></td>
<td>When you are finished with the PR process, set the state of the task to <strong>Complete</strong> or <strong>Incomplete</strong> as appropriate.</td>
<td></td>
</tr>
<tr>
<td>Law enforcement process</td>
<td>Perform the steps required to engage the appropriate law enforcement agencies regarding the attack.</td>
<td>The <strong>Lessons learned meeting</strong> task is executed.</td>
</tr>
<tr>
<td></td>
<td>When you are finished, set the state of the task to <strong>Complete</strong> or <strong>Incomplete</strong> as appropriate.</td>
<td></td>
</tr>
<tr>
<td>Determine and eradicate root cause</td>
<td>Perform the steps necessary to discover and eliminate the root cause of the defacement.</td>
<td>If you changed the state of the task to <strong>Closed Complete</strong> or <strong>Cancelled</strong>, the next response task is executed.</td>
</tr>
<tr>
<td></td>
<td>Update the <strong>State</strong> field in the task as appropriate.</td>
<td></td>
</tr>
<tr>
<td>Response task</td>
<td>Action</td>
<td>Results</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Restore site from backup</td>
<td>Perform the steps required to back up and restore the website or BBS. Update the <strong>State</strong> field in the task as appropriate.</td>
<td>If you changed the state of the task to <strong>Closed Complete</strong> or <strong>Cancelled</strong>, the next response task is executed.</td>
</tr>
<tr>
<td>Test and verify site is restored</td>
<td>Verify that the site is restored. When you are finished, set the state of the task to <strong>Complete</strong> or <strong>Incomplete</strong> as appropriate.</td>
<td>The <strong>Lessons learned meeting</strong> task is executed.</td>
</tr>
<tr>
<td>Lessons learned meeting</td>
<td>Conduct a lessons learned meeting to triage the work performed for this website/BBS defacement incident. Update the <strong>State</strong> field in the task as appropriate.</td>
<td>If you change the state of the task to <strong>Closed Complete</strong> or <strong>Cancelled</strong>, the <strong>Set state to review</strong> task is executed.</td>
</tr>
<tr>
<td>Set state to review</td>
<td>No action required.</td>
<td>The <strong>State</strong> of the security incident is changed automatically to <strong>Review</strong>. The flow ends.</td>
</tr>
</tbody>
</table>

**Security Incident Response flow templates**

The Security Incident Response base system includes a series of flow templates created using the Flow Designer that work with security incident records.

Only users with the `sn_sec_cmn.admin` role can add or edit Security Operations flow templates.

The flow templates are created using the `.Flows` and the associated actions are described in this section.

Before you can use the Flow Designer templates, you must activate the Security Operations Spoke plugin.

**Important activation information**

The workflow templates created with the Workflow Editor and the flow templates created with the Flow Designer are both deactivated by default. The workflow templates can be activated using `Workflow Triggers`. Flow Designer templates can be activated using the Flow Designer.
Note: You must be careful not to activate the same template of each type. For example, avoid activating the Security Incident Confidential Data Exposure workflow template and the Security Incident Confidential Data Exposure flow template. Doing so may cause the execution of both the workflow and flow, and the creation of duplicate information.

Security Incident Confidential Data Exposure flow template

The Security Incident - Confidential Data Exposure - Template allows you to perform a series of tasks designed to handle the exposure of sensitive data.

Before you begin
Role required: sn_si.write

About this task
This flow is triggered when the Category in a security incident is set or changed to Confidential personal identity data exposure.

Procedure
1. Open the security incident for which you want to handle the exposure to sensitive data, or create a new security incident.
2. In Category, select Confidential personal identity data exposure.
3. Save the record.
4. Scroll down and open the Response Tasks related list.
   The first of a series of response tasks appears. Each time the record is saved, your response to the previous task either causes the next response task to be executed or the flow to end.

<table>
<thead>
<tr>
<th>Response task</th>
<th>Description</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the data sensitive?</td>
<td>Determine whether the data associated with this security incident is sensitive or confidential. In the task, select Yes or No in Outcome.</td>
<td>If you selected Yes, the next response task is executed. If you selected No, the flow ends.</td>
</tr>
<tr>
<td>Determine root cause and prevent egress</td>
<td>Determine the root cause of the attack and add egress filtering to stop the exfiltration, updating the State field in the task as appropriate.</td>
<td>If you change the state of the task to Closed Complete or Cancelled, the next response task is executed.</td>
</tr>
<tr>
<td>Response task</td>
<td>Description</td>
<td>Results</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Eliminate exposure related to root cause</td>
<td>Based on the root cause, perform the steps to eliminate the exposure, updating the State field in the task as appropriate.</td>
<td>If you change the state of the task to <strong>Closed Complete</strong> or <strong>Cancelled</strong>, the next response task is executed.</td>
</tr>
<tr>
<td>Quarantine residual artifacts</td>
<td>Perform the steps to quarantine any residual artifacts, updating the State field in the task as appropriate.</td>
<td>If you change the state of the task to <strong>Closed Complete</strong> or <strong>Cancelled</strong>, the next response task is executed.</td>
</tr>
<tr>
<td>Legal process</td>
<td>Perform the steps to satisfy the legal requirements of this analysis, updating the State field in the task as appropriate.</td>
<td>If you change the state of the task to <strong>Closed Complete</strong> or <strong>Cancelled</strong>, the next response task is executed.</td>
</tr>
<tr>
<td>PR process</td>
<td>Perform the steps to satisfy the PR requirements of this analysis, updating the State field in the task as appropriate.</td>
<td>If you change the state of the task to <strong>Closed Complete</strong> or <strong>Cancelled</strong>, the next response task is executed.</td>
</tr>
<tr>
<td>Set state to review</td>
<td>No action required.</td>
<td>The State of the security incident is automatically changed to <strong>Review</strong>.</td>
</tr>
<tr>
<td>Lessons learned meeting</td>
<td>Conduct a lessons learned meeting to triage the work performed on this sensitive data, updating the State field in the task as appropriate.</td>
<td>If you change the state of the task to <strong>Closed Complete</strong> or <strong>Cancelled</strong>, the security incident remains in the Review state until you close it.</td>
</tr>
</tbody>
</table>

**Security Incident Denial of Service flow template**

The Security Incident - Denial of Service - Template allows you to perform a series of tasks designed to handle Denial of Service (DOS) attacks.

**Before you begin**
Role required: sn_si.write

**About this task**
This flow is triggered when the Category in a security incident is set to Denial of Service.
Procedure

1. Open the security incident for this denial of service occurrence, or create a new security incident.

2. In Category, select Denial of Service.

3. Save the record.

4. Scroll down and open the Response Tasks related list.

   The first of a series of response tasks appears. Each time the record is saved, your response to the previous task either causes the next response task to be created or the workflow to end.

### Response tasks in Denial of Service Template

<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is target business critical?</td>
<td>Determine if the target of this DOS attack is business critical. In the task, select Yes or No in Outcome.</td>
<td>If you select Yes, the Set priority to critical task is executed. If you select No, the Is a vulnerability being exploited? task is executed.</td>
</tr>
<tr>
<td>Set priority to critical</td>
<td>No action required.</td>
<td>The Priority of the security incident is changed automatically to Critical, and the Is a vulnerability being exploited? task is executed.</td>
</tr>
<tr>
<td>Is a vulnerability being exploited?</td>
<td>Determine whether this DOS attack exploits a software vulnerability. In the task, select Yes or No in Outcome.</td>
<td>If you select Yes, the Emergency patch request task is executed. If you select No, the Internal attacker? task is executed.</td>
</tr>
<tr>
<td>Emergency patch request</td>
<td>Issue an emergency patch request for the system(s) being attacked. Update the State field in the task as appropriate.</td>
<td>If you changed the state of the task to Closed Complete or Cancelled, the next response task is executed.</td>
</tr>
<tr>
<td>Internal attacker?</td>
<td>Determine if the source of this DOS attack is internal to your organization.</td>
<td>If you select Yes, the Isolate attacking host(s) task is executed.</td>
</tr>
<tr>
<td>Response task</td>
<td>Action</td>
<td>Results</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Isolate the attacking host(s)</td>
<td>Perform the steps necessary to isolate the internal host(s) responsible for the attack. Update the State field in the task as appropriate.</td>
<td>After you complete this step, the Validate system integrity of attacked systems task is executed.</td>
</tr>
<tr>
<td>Notify DOS protection provider and/or ISP</td>
<td>Perform the steps necessary to contact your Denial of Service protection provider and/or your Internet Service Provider to notify them of the attack. Update the State field in the task as appropriate.</td>
<td>If you changed the state of the task to Closed Complete or Cancelled, the next response task is executed.</td>
</tr>
<tr>
<td>Validate system integrity of attacked systems</td>
<td>Perform the steps necessary to assess and validate the integrity of the attacked computers. Update the State field in the task as appropriate.</td>
<td>If you changed the state of the task to Closed Complete or Cancelled, the next response task is executed.</td>
</tr>
<tr>
<td>Review DOS protections</td>
<td>Conduct a review of your existing DOS protections and procedures. Make any necessary changes. Update the State field in the task as appropriate.</td>
<td>If you changed the state of the task to Closed Complete or Cancelled, the next response task is executed.</td>
</tr>
<tr>
<td>Set state to review</td>
<td>No action required.</td>
<td>The State of the security incident is changed automatically to Review. The Lessons learned meeting task is executed.</td>
</tr>
<tr>
<td>Lessons learned meeting</td>
<td>Conduct a lessons learned meeting to triage the work</td>
<td>If you change the state of the task to Closed Complete or Cancelled, the flow ends.</td>
</tr>
</tbody>
</table>
Security Incident Lost Equipment flow template

The Security Incident - Lost Equipment - Template allows you to perform a series of tasks designed to handle lost equipment.

Before you begin
Role required: sn_si.write

About this task
This flow is triggered when the Category in a security incident is set to Equipment loss.

Procedure
1. Open the security incident for this denial of service occurrence, or create a new security incident.
2. In Category, select Equipment loss.
3. Save the record.
4. Scroll down and open the Response Tasks related list. The first of a series of response tasks appears. Each time the record is saved, your response to the previous task either causes the next response task to be created or the flow to end.

<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did the equipment contain sensitive data?</td>
<td>Determine whether the equipment associated with this security incident contained any sensitive or confidential information. In the task, select Yes or No in Outcome as appropriate.</td>
<td>If you select Yes the Was the data encrypted? task is executed. If you select No, the flow ends.</td>
</tr>
<tr>
<td>Was the data encrypted?</td>
<td>Determine if the sensitive data on the lost device was encrypted.</td>
<td>If you select Yes, the Remote wipe</td>
</tr>
<tr>
<td>Response task</td>
<td>Action</td>
<td>Results</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>In the task, select <strong>Yes</strong> or <strong>No</strong> in Outcome</td>
<td><strong>created?</strong> response task is executed. If you select <strong>No</strong>, the <em>Create potential data loss incident</em> response task is executed.</td>
<td></td>
</tr>
<tr>
<td>Create potential data loss incident</td>
<td>Perform the steps necessary to create a potential data loss incident. After you have finished, set the state of the task to <strong>Complete</strong> or <strong>Incomplete</strong> as appropriate.</td>
<td>The <em>Remote wipe created?</em> response task is executed.</td>
</tr>
<tr>
<td>Remote wipe created?</td>
<td>Perform the steps necessary to execute a remote wipe of the lost equipment. In the task, select <strong>Yes</strong> or <strong>No</strong> in Outcome as appropriate.</td>
<td>The <em>Legal process - Disclosure required?</em> task is executed.</td>
</tr>
<tr>
<td>Legal process - Disclosure required?</td>
<td>Perform the steps to satisfy the legal requirements of this analysis. Select <strong>Yes</strong> if a legal disclosure is required, <strong>No</strong> if it is not.</td>
<td>The <em>Lessons learned meeting</em> task is executed.</td>
</tr>
<tr>
<td>PR process</td>
<td>Perform the steps necessary to satisfy the PR requirements of this analysis. After you have finished, set the state of the task to <strong>Complete</strong> or <strong>Incomplete</strong> as appropriate.</td>
<td>The <em>Set state to review</em> task is executed.</td>
</tr>
<tr>
<td>Set state to review</td>
<td>No action is necessary.</td>
<td>The <em>State</em> of the security incident is changed automatically to <strong>Review</strong>.</td>
</tr>
<tr>
<td>Lessons learned meeting</td>
<td>Conduct a lessons learned meeting to triage the work performed for this lost equipment incident. After you have finished, set the state of the task to <strong>Complete</strong> or <strong>Incomplete</strong> as appropriate.</td>
<td>The flow ends.</td>
</tr>
</tbody>
</table>
Security Incident Malicious Software flow template

The Security Incident - Malicious Software - Template allows you to perform a series of tasks designed to handle malicious software on your network.

Before you begin
Role required: sn_si.write

About this task
This flow is triggered when the Category in a security incident is set to Malicious code activity.

Procedure
1. Open the security incident for this potential attack, or create a new security incident.
2. In Category, select Malicious code activity.
3. Save the record.
4. Scroll down and open the Response Tasks related list. The first of a series of response tasks appears. Each time the record is saved, your response to the previous task either causes the next response task to be created or the flow to end.

Response tasks in Malicious Software Template

<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Endpoint - Malware Found?</td>
<td>After running a scan, determine whether malware was found. In the task, select Yes or No in Outcome.</td>
<td>If you select Yes, the Remove Malware - Success? task is executed. If you select No, the flow ends.</td>
</tr>
<tr>
<td>Remove Malware - Success?</td>
<td>Determine whether the malware was successfully removed. In the task, select Yes or No in Outcome.</td>
<td>If you select Yes, the Was there a larger breach? task is executed. If you select No, the Wipe &amp; Reimage task is executed.</td>
</tr>
<tr>
<td>Wipe &amp; Reimage</td>
<td>If you did not successfully remove the malware found, this task instructs you</td>
<td>After the task is complete, the Set</td>
</tr>
<tr>
<td>Response task</td>
<td>Action</td>
<td>Results</td>
</tr>
<tr>
<td>---------------</td>
<td>--------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>to perform a wipe and reimage on the computers infected with the malware.</td>
<td><strong>State to Review</strong> task is executed.</td>
</tr>
<tr>
<td>Was there a larger breach?</td>
<td>Determine whether the breach caused by the malicious software is larger than first believed.</td>
<td>If you select <strong>Yes</strong>, the following tasks are executed in parallel:</td>
</tr>
<tr>
<td></td>
<td>In the task, select <strong>Yes</strong> or <strong>No</strong> in <strong>Outcome</strong>.</td>
<td>• Legal Review</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HR Review</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Law Enforcement Review</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you select <strong>No</strong>, the flow ends.</td>
</tr>
<tr>
<td>Legal Review</td>
<td>Perform the steps necessary for each of these departments to review the process you followed to eradicate the malicious software.</td>
<td>When the tasks are complete, the <strong>Set State to Review</strong> task is executed.</td>
</tr>
<tr>
<td>HR Review</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Law Enforcement Review</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set State to Review</td>
<td>No action required.</td>
<td>The <strong>State</strong> of the security incident is changed automatically to <strong>Review</strong>, and the flow ends.</td>
</tr>
</tbody>
</table>

**Security Incident Phishing flow template**

The Security Incident - Phishing - Template allows you to perform a series of tasks designed to handle spear phishing emails on your network.

**Before you begin**
Role required: sn_si.write

**About this task**
This flow is triggered when the **Category** in a security incident is set to **Spear Phishing**.
Procedure

1. Open the security incident for this potential spear phishing attack, or create a new security incident.

2. In Category, select Spear Phishing.

3. Save the record.

4. Scroll down and open the Response Tasks related list.

   The first of a series of response tasks appears. Each time the record is saved, your response to the previous task either causes the next response task to be created or the flow to end.

**Response tasks in Spear Phishing Template**

<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is this a Phishing attack?</td>
<td>Determine if this is a phishing attack.</td>
<td>If you select Yes, the following tasks are executed in parallel:</td>
</tr>
<tr>
<td></td>
<td>In the task, select Yes or No in Outcome.</td>
<td>• Scan Endpoint - Malware Found?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Update Email Protection Software</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Remove Unread Phishing Email in Queue - For All Users</td>
</tr>
<tr>
<td>Scan Endpoint - Malware Found?</td>
<td>After running a scan, determine whether</td>
<td>If you select Yes, the Remove Malware - Success? task is executed.</td>
</tr>
<tr>
<td></td>
<td>malware was found.</td>
<td>If you select No, the Set State to Review task is executed.</td>
</tr>
<tr>
<td></td>
<td>In the task, select Yes or No in Outcome.</td>
<td></td>
</tr>
<tr>
<td>Response task</td>
<td>Action</td>
<td>Results</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Remove Malware - Success?</td>
<td>Determine whether the malware was successfully removed.</td>
<td>If you select Yes, the Set State to Review task is executed. If you select No, the Wipe and reimage task is executed.</td>
</tr>
<tr>
<td></td>
<td>In the task, select Yes or No in Outcome.</td>
<td></td>
</tr>
<tr>
<td>Wipe and reimage</td>
<td>If you did not successfully remove the malware found, this task instructs you to perform a wipe and reimage on the computers infected with the malware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>After the task is complete, the Set State to Review task is executed.</td>
<td></td>
</tr>
<tr>
<td>Update Email Protection Software</td>
<td>If it was determined that this is a phishing attack, you are prompted to update your email protection software accordingly.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When the task is complete, the Set State to Review task is executed.</td>
<td></td>
</tr>
<tr>
<td>Remove Unread Phishing Email in Queue - For All Users</td>
<td>Perform the steps necessary to remove the phishing email still in the queue for all of your users.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When the task is complete, the Set State to Review task is executed.</td>
<td></td>
</tr>
<tr>
<td>Set State to Review</td>
<td>No action required.</td>
<td>The State of the security incident is changed automatically to Review. The Schedule Security Awareness Training task is executed.</td>
</tr>
<tr>
<td>Schedule Security Awareness Training</td>
<td>Schedule training to heighten security awareness by your employees.</td>
<td>When the task is complete, the flow ends.</td>
</tr>
<tr>
<td></td>
<td>Update the State field in the task as appropriate.</td>
<td></td>
</tr>
</tbody>
</table>
Security Incident Policy Violation flow template

The Security Incident - Policy Violation - Template allows you to perform a series of tasks designed to handle security policy violations.

Before you begin
Role required: sn_si.write

About this task
This flow is triggered when the Category in a security incident is set to Policy violation.

Procedure
1. Open the security incident for the policy violation, or create a new security incident.
2. In Category, select Policy violation.
3. Save the record.
4. Scroll down and open the Response Tasks related list.
   The first of a series of response tasks appears. Each time the record is saved, your response to the previous task either causes the next response task to be created or the flow to end.

Response tasks in Policy Violation Template

<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classify violation</td>
<td>Classify how this infraction violates your organization’s security policies. Update the State field in the task after you have completed it.</td>
<td>The Advise violator of infraction response task is executed.</td>
</tr>
<tr>
<td>Advise violator of infraction</td>
<td>Communicate the nature of the infraction to the violator. Update the State field in the task after you have communicated it.</td>
<td>The Obtain acknowledgement from violator response task is executed.</td>
</tr>
<tr>
<td>Obtain acknowledgement from violator</td>
<td>Obtain an acknowledgement from the violator of the infraction.</td>
<td>The HR process response task is executed.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
## Security Incident Reconnaissance flow template

Reconnaissance is usually a preliminary step toward a further attack seeking to exploit a device or system. The Security Incident - Reconnaissance - Template allows you to perform a series of tasks designed to handle reconnaissance on your network.

### Before you begin
Role required: sn_si.write

### About this task
This flow is triggered when the **Category** in a security incident is set to **Reconnaissance activity**.

### Procedure
1. Open the security incident for this potential attack, or create a new security incident.
2. In **Category**, select **Reconnaissance activity**.
3. Save the record.
4. Scroll down and open the **Response Tasks** related list. The first of a series of response tasks appears. Each time the record is saved, your response to the previous task either causes the next response task to be created or the flow to end.

### Response tasks in Reconnaissance Template

<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconnaissance activity verified?</td>
<td>Determine whether any observed reconnaissance has been verified.</td>
<td>If you select <strong>Yes</strong>, the <strong>Identify impacted systems</strong> task is executed. If you select <strong>No</strong>, the flow ends.</td>
</tr>
<tr>
<td></td>
<td>In the task, select <strong>Yes</strong> or <strong>No</strong> in <strong>Outcome</strong>.</td>
<td></td>
</tr>
<tr>
<td>Identify impacted systems</td>
<td>Determine the systems impacted by the reconnaissance.</td>
<td>When this task is complete, the <strong>Allow reconnaissance for law enforcement analysis?</strong> task is executed.</td>
</tr>
<tr>
<td>Allow reconnaissance for law enforcement analysis?</td>
<td>Determine whether you want the reconnaissance to be analyzed by law enforcement agencies. In the task, select <strong>Yes</strong> or <strong>No</strong> in <strong>Outcome</strong>.</td>
<td>If you select <strong>Yes</strong>, the <strong>Law enforcement process</strong> task is executed. If you select <strong>No</strong>, the <strong>Update system(s) to prevent reconnaissance</strong> task is executed.</td>
</tr>
<tr>
<td>Law enforcement process</td>
<td>Perform the law enforcement process as defined by your company.</td>
<td>When this task is complete, the <strong>Update system(s) to prevent reconnaissance</strong> task is executed.</td>
</tr>
<tr>
<td>Update system(s) to prevent reconnaissance</td>
<td>Perform the steps necessary to update the systems affected by the reconnaissance.</td>
<td>When this task is complete, the <strong>Set state to review</strong> task is executed.</td>
</tr>
<tr>
<td>Set state to review</td>
<td>No action required.</td>
<td>The <strong>State</strong> of the security incident is changed automatically to <strong>Review</strong>, and the <strong>Lessons learned meeting</strong> task is executed.</td>
</tr>
</tbody>
</table>
Security Incident Rogue Server or Service flow template

The Security Incident - Rogue Server or Service - Template allows you to perform a series of tasks designed to handle activity from rogue servers or services affecting your network.

**Before you begin**
Role required: sn_si.write

**About this task**
This flow is triggered when the Category in a security incident is set to Rogue server or service.

**Procedure**

1. Open the security incident for this potential attack, or create a new security incident.
2. In Category, select Rogue server or service activity.
3. Save the record.
4. Scroll down and open the Response Tasks related list.
   The first of a series of response tasks appears. Each time the record is saved, your response to the previous task either causes the next response task to be created or the flow to end.

### Response tasks in Rogue Server or Service Template

<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lessons learned</td>
<td>Conduct a lessons learned meeting to triage the work performed for this reconnaissance incident. Update the State field in the task as appropriate.</td>
<td>When this task is complete, the flow ends.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify impacted system(s)</td>
<td>Determine the systems impacted by contact with the rogue server or service.</td>
<td>If you select No, the flow ends. When this task is complete, the Update system(s) - Remove rogue connections task is executed.</td>
</tr>
<tr>
<td>Potential data loss?</td>
<td>Determine whether the connection with the rogue server or service caused potential data loss.</td>
<td>If you select Yes, the Create potential data loss incident task is executed. If you select No, the Update system(s) - Remove rogue connections task is executed.</td>
</tr>
<tr>
<td>Create potential data loss incident</td>
<td>Perform the steps necessary to create a security incident for the potential data loss.</td>
<td>When this task is complete, the Update system(s) - Remove rogue connections task is executed.</td>
</tr>
<tr>
<td>Update system(s) - Remove rogue connections</td>
<td>Perform the steps necessary to remove the rogue connections.</td>
<td>When this task is complete, the Set state to review task is executed.</td>
</tr>
<tr>
<td>Set state to review</td>
<td>No action required.</td>
<td>The State of the security incident is changed automatically to Review, and the Lessons learned meeting task is executed.</td>
</tr>
<tr>
<td>Lessons learned meeting</td>
<td>Conduct a lessons learned meeting to triage the work performed for this rogue server or service incident. Update the State field in the task as appropriate.</td>
<td>When this task is complete, the flow ends.</td>
</tr>
</tbody>
</table>

**Security Incident Spam flow template**

The Security Incident - Spam - Template allows you to perform a series of tasks designed to handle email spam on your network.

**Before you begin**
Role required: sn_si.write
About this task
This flow is triggered when the **Category** in a security incident is set or changed to **Spam source**.

Procedure

1. Open the security incident for which you want to handle email spam, or create a new security incident.
2. In **Category**, select **Spam source**.
3. Save the record.
4. Scroll down and open the **Response Tasks** related list.
   The first of a series of response tasks appears. Each time the record is saved, your response to the previous task either causes the next response task to be created or the flow to end.

Response tasks in Spam Template

<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam contains malicious content?</td>
<td>Determine whether the spam contains malicious software. In the task, select <strong>Yes</strong> or <strong>No</strong> in <strong>Outcome</strong>.</td>
<td>If you selected <strong>Yes</strong>, the following response tasks are executed: • Quarantine email message • Create malicious software incident</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you selected <strong>No</strong>, the <strong>Update email software</strong> is executed.</td>
</tr>
<tr>
<td>Create malicious software incident</td>
<td>Perform the steps to create a security incident, updating the <strong>State</strong> field in the task as appropriate.</td>
<td>If you change the state of the task to <strong>Closed Complete</strong> or <strong>Cancelled</strong>, this response task waits until the next three response tasks have been completed. The state of the security incident then transitions to <strong>Review</strong>.</td>
</tr>
<tr>
<td>Quarantine email message</td>
<td>Perform the steps to quarantine the spam, updating the <strong>State</strong> field in the task as appropriate.</td>
<td>If you change the state of the task to <strong>Closed Complete</strong> or <strong>Cancelled</strong>, the next response task is executed.</td>
</tr>
<tr>
<td>Block source on firewall</td>
<td>Perform the steps to block the email address on the firewall, updating</td>
<td>If you change the state of the task to <strong>Closed Complete</strong> or <strong>Cancelled</strong>, the next response task is executed.</td>
</tr>
<tr>
<td>Response task</td>
<td>Action</td>
<td>Results</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Update email software</td>
<td>Add the email address to your block list, updating the State field in the task as appropriate.</td>
<td>If you change the state of the task to Closed Complete or Cancelled, the next response task is executed. Note: This response task is also executed if you answered No to the Spam contains malicious content? response task.</td>
</tr>
<tr>
<td>Set state to review</td>
<td>No action required.</td>
<td>The State of the security incident is automatically changed to Review.</td>
</tr>
</tbody>
</table>

Security Incident Unauthorized Access flow template

The Security Incident - Unauthorized Access - Template allows you to perform a series of tasks designed to handle unauthorized access to your network.

Before you begin
Role required: sn_si.write

About this task
This flow is triggered when the Category in a security incident is set to Unauthorized access.

Procedure
1. Open the security incident for this potential attack, or create a new security incident.
2. In Category, select Unauthorized access.
3. Save the record.
4. Scroll down and open the Response Tasks related list.
   The first of a series of response tasks appears. Each time the record is saved, your response to the previous task either causes the next response task to be created or the flow to end.
<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>User credentials compromised?</td>
<td>Determine whether any users credentials have been compromised.</td>
<td>If you select <strong>Yes</strong>, the following two tasks are executed in parallel:</td>
</tr>
<tr>
<td></td>
<td>In the task, select <strong>Yes</strong> or <strong>No</strong> in <strong>Outcome</strong>.</td>
<td>• Malicious software?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Deactivate user account</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you select <strong>No</strong>, the Contact user and determine intent task is executed.</td>
</tr>
<tr>
<td>Malicious software?</td>
<td>Determine whether the unauthorized access resulted in the introduction of malicious software.</td>
<td>If you select <strong>Yes</strong>, the Create malicious software incident task is executed.</td>
</tr>
<tr>
<td></td>
<td>In the task, select <strong>Yes</strong> or <strong>No</strong> in <strong>Outcome</strong>.</td>
<td>If you select <strong>No</strong>, the Set state to review task is executed.</td>
</tr>
<tr>
<td>Create malicious software incident</td>
<td>Perform the steps necessary to create a security incident for the unauthorized access.</td>
<td>When this task is complete, the Set state to review task is executed.</td>
</tr>
<tr>
<td>Deactivate user account</td>
<td>Perform the steps necessary to deactivate the compromised user account.</td>
<td>When this task is complete, the Set state to review task is executed.</td>
</tr>
<tr>
<td>Contact user and determine intent</td>
<td>Perform the steps necessary to contact the user who responsible for the unauthorized access and determine the reason for the access attempt.</td>
<td>When this task is complete, the HR process task is executed.</td>
</tr>
<tr>
<td>HR process</td>
<td>Perform the steps necessary to contact human resources to implement disciplinary action if necessary.</td>
<td>When this task is complete, the Set state to review task is executed.</td>
</tr>
</tbody>
</table>
Security Incident Web/BBS Defacement flow template

The Security Incident - Web/BBS Defacement - Template allows you to perform a series of tasks designed to handle vandalism directed against one of your organization’s BBS or web sites.

Before you begin
Role required: sn_si.write

About this task
This flow is triggered when the Category in a security incident is set to Web/BBS defacement.

Procedure
1. Open the security incident for this occurrence of web or BBS defacement, or create a new security incident.
2. In Category, select Web/BBS defacement.
3. Save the record.
4. Scroll down and open the Response Tasks related list. The first of a series of response tasks appears. Each time the record is saved, your response to the previous task either causes the next response task to be created or the flow to end.

Response tasks in Web/BBS Defacement Template

<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security incident assignment</td>
<td>Create a security incident for each reported incident of website or BBS defacement.</td>
<td>The next response task is executed.</td>
</tr>
<tr>
<td>Defacement verified?</td>
<td>Determine whether the website or BBS has in fact been defaced.</td>
<td>If you select Yes, the following response tasks are executed:</td>
</tr>
<tr>
<td>Response task</td>
<td>Action</td>
<td>Results</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| In the task, select **Yes** or **No** in **Outcome**. | • PR process  
• Law enforcement process  
• Determine and eradicate root cause  
If you select **No**, the flow ends. | The **Lessons learned meeting** task is executed. |
| **PR process**                      | Perform the steps necessary to notify the public that the website or BBS has been defaced.  
When you are finished with the PR process, set the state of the task to **Complete** or **Incomplete** as appropriate. | The **Lessons learned meeting** task is executed. |
| **Law enforcement process**         | Perform the steps required to engage the appropriate law enforcement agencies regarding the attack.  
When you are finished, set the state of the task to **Complete** or **Incomplete** as appropriate. | The **Lessons learned meeting** task is executed. |
| **Determine and eradicate root cause** | Perform the steps necessary to discover and eliminate the root cause of the defacement.  
Update the **State** field in the task as appropriate. | If you changed the state of the task to **Closed Complete** or **Cancelled**, the next response task is executed. |
| **Restore site from backup**        | Perform the steps required to back up and restore the website or BBS.  
Update the **State** field in the task as appropriate. | If you changed the state of the task to **Closed Complete** or **Cancelled**, the next response task is executed. |
| **Test and verify site is restored** | Verify that the site is restored.  
When you are finished, set the state of the task to **Complete** or **Incomplete** as appropriate. | The **Lessons learned meeting** task is executed. |
<table>
<thead>
<tr>
<th>Response task</th>
<th>Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lessons learned meeting</td>
<td>Conduct a lessons learned meeting to triage the work performed for this website/BBS defacement incident. Update the State field in the task as appropriate.</td>
<td>If you change the state of the task to Closed Complete or Cancelled, the Set state to review task is executed.</td>
</tr>
<tr>
<td>Set state to review</td>
<td>No action required.</td>
<td>The State of the security incident is changed automatically to Review. The flow ends.</td>
</tr>
</tbody>
</table>

Vulnerability Response

The National Vulnerability Database (NVD) and other sources collect information about known vulnerabilities. These vulnerabilities can include weaknesses in software, operating systems that malware can exploit, and other attacks. The ServiceNow® Vulnerability Response application aids you in tracking, prioritizing, and resolving these vulnerabilities.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Explore

- Vulnerability Response release notes
- Upgrade to Paris.
- Understanding the Vulnerability Response application

Note: Application Vulnerability Response documentation can be found here: Application Vulnerability Response.

Set up

- Install and configure Vulnerability Response
- Install the Solution Management for Vulnerability Response application
- Configure installed solution integrations for Vulnerability Solution Management using Setup Assistant
- Install the Qualys Vulnerability Integration

Administer

- Vulnerability Response remediation overview
- Managing NVD, CWE, and third-party data libraries
<table>
<thead>
<tr>
<th>Use</th>
<th>Develop</th>
<th>Integrate</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Domain separation and Vulnerability Response</td>
<td>• Install and configure the Rapid7 Vulnerability Integration</td>
<td>• Understanding the Qualys Vulnerability Integration</td>
</tr>
<tr>
<td>• Getting started with Vulnerability Response (video)</td>
<td>• Install and configure the Shodan Exploit Integration for Security Operations</td>
<td>• Understanding the Rapid7 Vulnerability Integration</td>
</tr>
<tr>
<td>• Security Operations videos</td>
<td>• Installation of Vulnerability Response and supported applications</td>
<td>• Understanding the Shodan Exploit Integration</td>
</tr>
<tr>
<td></td>
<td>• Install and configure the Performance Analytics for Vulnerability Response [PA] application</td>
<td>• Understanding the Tenable Vulnerability Integration</td>
</tr>
<tr>
<td></td>
<td>• Managing NVD, CWE, and third-party data libraries</td>
<td>• Understanding the Microsoft Security Response Center Solution Integration</td>
</tr>
</tbody>
</table>

- **Use**
  - Machine Learning solutions for Vulnerability Response
  - Vulnerability Solution Management
  - ServiceNow Tenable Vulnerability Integration
  - Vulnerability Response assignment rules overview
  - Vulnerability Response groups and group rules overview
  - Configure and manage Qualys vulnerability scanners and scans
  - Vulnerability Response calculators and vulnerability calculator rules
  - Remediate Vulnerability Response groups

- **Develop**
  - Developer training
  - Developer documentation
  - Find components installed with an application
  - Vulnerability Response Orchestration

- **Integrate**
  - Understanding the Qualys Vulnerability Integration
  - Understanding the Rapid7 Vulnerability Integration
  - Understanding the Shodan Exploit Integration
  - Understanding the Tenable Vulnerability Integration
  - Understanding the Microsoft Security Response Center Solution Integration
  - Manually create a vulnerability integration
  - Tips for writing integrations
Understanding the Vulnerability Response application

The ServiceNow® Vulnerability Response application imports and automatically groups vulnerable items according to group rules allowing you to remediate vulnerabilities quickly. Vulnerability data is pulled from internal and external sources, such as the National Vulnerability Database (NVD) or third-party integrations.

Compare vulnerability data pulled from internal and external sources. For any vulnerable items, create change requests and security incidents using vulnerability groups to remediate issues and mitigate risk.

Watch an overview of the typical vulnerability response within an enterprise versus the vulnerability response with ServiceNow®. It defines vulnerable items, vulnerability groups, and their lifecycles.

- Mobile experience for Vulnerability Response
- Change management for Vulnerability Response
- Software exposure assessment using Software Asset Management (SAM)
- Enhanced exception management
- Vulnerability Response personas and granular roles
- Configure the vulnerable item key

Troubleshoot and get help

- Ask or answer questions in the Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support
Overview of the typical vulnerability response within an enterprise versus the vulnerability response with ServiceNow, and defines vulnerable items, vulnerability groups and their lifecycles.

Vulnerability Response and the Now Platform®

Vulnerability Response is one member of the Security Operations application suite. Together these applications connect security to your IT department, increase the speed and efficiency of your response, and give you a definitive view of your security posture.

Vulnerability Response flow

You use Vulnerability Response to follow the flow of information, from integration through investigation, and then on to resolution.

- Work with an implementation specialist to achieve your desired business outcomes. To learn more, visit the Customer Success Center.
- Take a Vulnerability Response course to build expertise and realize ROI faster. To sign up, see ServiceNow training and certification.
Available versions for Paris

<table>
<thead>
<tr>
<th>Release version</th>
<th>Release Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Response v14.0</td>
<td>Vulnerability Response release notes</td>
</tr>
<tr>
<td>Vulnerability Response v13.0</td>
<td>For compatibility information, see KB0856498</td>
</tr>
<tr>
<td>Vulnerability Response v12.2</td>
<td>Vulnerability Response Compatibility Matrix and Release Schema Changes</td>
</tr>
<tr>
<td>Vulnerability Response v12.1</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Response v12.0</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Response v11.0</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Response v10.3</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Response v10.0 (platform upgrade only)</td>
<td></td>
</tr>
</tbody>
</table>

Integrate your Vulnerability scanner

After vulnerability data is imported, you can compare the data to CIs and software identified in the ServiceNow® Asset Management application. You can perform the following tasks.

- Compare vulnerability-related data, if a vulnerability is found on a configuration item.

- Escalate issues by creating change requests, and security incident records (if the ServiceNow® Security Incident Response application is activated).

- Manage vulnerable items grouped by the vulnerability, or CI, or individually. Each vulnerability represents a vulnerability entry in the NVD, Common Weakness Enumeration (CWE), or third-party libraries.

- Relate a single third-party vulnerability to multiple Common Vulnerabilities and Exposure (CVE) entries.

- Use CWE records, downloaded from the CWE database, for reference when deciding whether a vulnerability must be escalated. Each CWE record also includes an associated knowledge article that describes the weakness. You cannot escalate a vulnerability from the Common Weakness Enumerations page. That page is for reference only.

Multi-source support

You can have multiple deployments of the Qualys Vulnerability Integration, Rapid7 InsightVM integrations, and, starting with v12.1, the Tenable Vulnerability Integration developed for the Now Platform.

Assets, identified by multiple third-party deployments and their vulnerabilities, are consolidated and reconciled with your CMDB. This consolidation happens
even when scan processes overlap between the multiple deployments. Data sourced from each deployment is identified and available in a single instance of Vulnerability Response.

Qualys Vulnerability Integration KnowledgeBase records are normalized across deployments, ensuring that instances of the same vulnerability across deployments are treated as the same vulnerability. Setup for multi-source integrations for the Qualys Vulnerability Integration and the Tenable Vulnerability Integration is available within the Setup Assistant.

**Prioritize vulnerabilities**
Vulnerability Response data correlation is performed using groups, calculators, and libraries. You can perform the following tasks.

- Create vulnerability groups to contain vulnerable items from NVD, CWE, and third-party integrations.
- Assign prioritization, rules, and access.
- Create assignment and remediation target rules.
- Create vulnerability group rules based on vulnerabilities, filters, filter conditions, and group keys.
- Use calculator groups to determine business impact, specify varying conditions using filters, apply simple calculations, or use a script.
- View ungrouped vulnerable items and vulnerabilities.

**Create change requests and coordinate planning**
Vulnerability Response remediation is primarily a manual process performed at the group level. There are multiple ways to remediate vulnerability groups.

Create emergency, standard, and normal change requests directly from vulnerability groups to expedite your investigation and remediation of vulnerabilities with Change management for Vulnerability Response. Create change requests that contain pre-populated information imported directly from a vulnerability group, filter out a subset of vulnerable items and create a new vulnerability group, or associate vulnerability groups to existing change requests.

If the vulnerability is a security incident and Security Incident Response is activated, you can create security incident records.

Assignment rules are used to automate vulnerable item or vulnerability assignments. Due to the large volume in data imports, care should be taken with automated vulnerable item assignment.
Confirm vulnerability resolution
Vulnerability Solution Management contains solution integrations such as the Microsoft Security Response Center Solution Integration.

Starting with v10.3, Red Hat Solution Integration is also available.

Automatically correlate the vulnerabilities in your environment with the solutions that would remediate them. Identify the remediation actions that apply to your environment and prioritize them by the greatest reduction in vulnerability risk.

Vulnerability Response provides several useful reports, charts, and an Explorer dashboard for you to analyze and monitor data before and after remediation. You can also return Vulnerability Response-related information using the global search feature.

Automated rescan confirms that your changes have taken effect or the need to reschedule.

Mobile experience for Vulnerability Response
Access the Vulnerability Response application on your Now Platform® instance directly from your mobile device.

View and search vulnerabilities, vulnerability groups, and assignments using the Vulnerability Response mobile application.

This mobile application gives you the flexibility to reassign, edit fields, and begin remediation without being tied to the desktop.

Vulnerability Response terminology
The following terms are used in Vulnerability Response.

Common Vulnerability and Exposure (CVE)
Dictionary of publicly known information-security vulnerabilities and exposures.

Common Vulnerability Scoring System (CVSS)
Open framework for communicating the characteristics and severity of software vulnerabilities. CVSS v3 was not available prior to 2015.

Common Weakness Enumeration (CWE)
List of community-developed software weakness types.

Discovery models
Software models used to help normalize the software you own by analyzing and classifying models to reduce duplication.

National Vulnerability Database (NVD)

**Vulnerability Response calculators and vulnerability calculator rules and Vulnerability Response Rollup Calculators**

Calculators used to prioritize and categorize vulnerabilities based on user-defined criteria.

**Vulnerability Response groups and group rules overview**

Used to group vulnerable items based on vulnerability, vulnerable item conditions, or filter group.

**Vulnerability Integrations**

Scheduled jobs that pull report data from NVD, CWE, or a third-party system, such as the Qualys Cloud Platform, to retrieve vulnerability data.

**Vulnerabilities**

Records of potentially vulnerable software downloaded from the National Institute of Standards and Technology (NIST) NVD, CWE, or third-party integrations.

**Vulnerable items**

Pairings of vulnerable entries, downloaded from the NIST NVD or third-party integrations, and potentially vulnerable configuration items and software in your company network.

**Vulnerability Response personas and granular roles**

Before you can successfully remediate vulnerabilities with the Vulnerability Response application, you must assign personas and roles to your users and groups in Setup Assistant.

One of the first configuration steps required for the Vulnerability Response application is to assign roles to users and groups. Roles define what users and groups can see and do in Vulnerability Response, Performance Analytics for Vulnerability Response, and all third party integrations with Vulnerability Response.

Starting with v10.3, you assign persona roles to existing users and groups in Setup Assistant. See Assign the Vulnerability Response persona roles using Setup Assistant.
Note:

If you are an upgrade customer, you can continue using your existing roles for the Vulnerability Response application. Access for users and groups assigned with the sn_vul.vulnerability_read and sn_vul.vulnerability_write permissions and remediation owner prior to v10.3 has not changed.

However, for more control over what users and groups can do and see in the Vulnerability Response application at the task level, you may prefer using granular roles. For more information, see Manage persona and granular roles for Vulnerability Response.

If you have already assigned roles using Setup Assistant and you want to manage granular role assignments for all users and groups from the User Administration module, see Manage persona and granular roles for Vulnerability Response for more information.

Persona roles and granular roles starting with v10.3

Key terms

Role

Roles define what users and groups can see and do in the Vulnerability Response application.

Group

A set of users who share certain roles and a common purpose.

Persona role

A pre-configured role in the application that is made up of multiple granular roles. The persona roles in Setup Assistant, Vulnerability Admin, Vulnerability Analyst, Remediation Owner, Configuration Item Manager, and Exception Manager, are designed to correspond to common job titles for managers, analysts, and service owners in an IT organization or vulnerability remediation group.

Inherited roles

A term that describes roles that users automatically acquire when they are assigned other roles. For example, any users or groups assigned with the sn_vul.remediation_owner persona role also inherit the sn_vul.read_assigned,sn_vul.write_assigned granular roles.

Access control list (ACL)

Access control lists restrict access to data by requiring users to pass a set of requirements before they can interact with it.
Starting with v10.3, you assign groups and users to persona roles in Setup Assistant.

**Note:** In Setup Assistant, the system admin role (admin) is required for the tasks in the first section, assigning roles and installing integrations. After you assign persona roles in Setup Assistant and install integrations, you may prefer to assign a user or group with the sn_vul.vulnerability_admin role to finish any remaining tasks in Setup Assistant and to manage the Vulnerability Response application.

The following table lists Vulnerability Response roles prior to v10.3 and compares them to the persona roles installed with the application starting with v10.3.

<table>
<thead>
<tr>
<th>Prior to v10.3</th>
<th>Starting with v10.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you assigned sn_vul.admin</td>
<td>You may prefer to assign sn_vul.vulnerability_admin - Vulnerability Admin to users or groups. Users with this role have complete access to the Vulnerability Response (VR) application and its records. Users with this role configure all VR applications and rules and install third party integrations.</td>
</tr>
<tr>
<td>If you assigned sn_vulnerability_write for users and groups.</td>
<td>You may prefer to assign sn_vul.vulnerability_analyst - Vulnerability Analyst to users and groups. Users and groups with this role view and update all records for VI remediation.</td>
</tr>
<tr>
<td>If you assigned sn_vul.remediation_owner</td>
<td>You may prefer to assign sn_vul.remediation_owner - Remediation Owner to users and groups. Users and groups with this role remediate vulnerabilities assigned to them or to a group they belong to. Groups or users with this role view and update the records assigned to them or to a group they belong to.</td>
</tr>
<tr>
<td>Prior to v10.3</td>
<td>Starting with v10.3</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>If you assigned sn_vul.admin for management of unmatched configuration items (CIs)</td>
<td>You may prefer to assign sn_vul.ci- CI Manager to users and groups.</td>
</tr>
<tr>
<td></td>
<td>Users and groups with this role manage unmatched configuration items (CIs) not found in the Configuration Management Database (CMDB). Groups or users with this role update discovered items.</td>
</tr>
<tr>
<td>If you assigned sn_vul.admin for deferrals and exception approvals.</td>
<td>You may prefer to assign sn_vul.exception_approver - Exception Approver to users and groups.</td>
</tr>
<tr>
<td></td>
<td>Users and groups with this role approve exceptions, deferrals, and closures of vulnerability groups and vulnerable items.</td>
</tr>
<tr>
<td>If you assigned sn_vul.vulnerability_read to provide visibility into vulnerability management.</td>
<td>You may prefer to assign read access to specific areas in the application by task.</td>
</tr>
<tr>
<td></td>
<td>For example, assign sn_vul.read_all so a user can view all VR records. For read access to view vulnerability group rules, assign sn_vul.read_group_rules. Users and groups with this role do not update records.</td>
</tr>
</tbody>
</table>

**Granular roles and persona roles**

One way to think about persona roles is to consider how their descriptions may relate to job descriptions for various IT or vulnerability remediation positions in your organization. The following figure illustrates a possible job description for a remediation specialist in IT, and how the tasks associated with this job relate to the tasks of a remediation owner persona role in the Vulnerability Response application.
Both the job description and the remediation owner persona role could be defined as a series of remediation tasks. In the preceding image, a job description and a persona role in green blocks sit atop the tasks that describe them. In this example, some of the typical job requirements for a specialist in a remediation group correspond directly to the tasks that make up the remediation owner persona in Vulnerability Response: Review and update records, track the remediation status of vulnerabilities, prioritize items for remediation, and apply fixes and patches with IT.

Sometimes, however, the jobs in your organization may not directly correspond to the tasks that make up one of the five persona roles in the Vulnerability Response application. For various reasons, such as protecting sensitive data, or complying with regulations, you must limit the broad access some of the persona roles provide to your users and groups. Or, conversely, you are required to provide users and groups with more access so they can perform their jobs. Using granular roles, you can easily customize roles and control the access users and groups have to Vulnerability Response, Performance Analytics for Vulnerability Response, and third party integrations.

**The granular roles define the tasks**

The names for the granular roles in Vulnerability Response usually describe what users can do and see in the Vulnerability Response application. For
example, in the previous image, users and groups with the Remediation owner persona assigned have the sn_vul.read_assigned and sn_vul.write_assigned granular roles. These granular roles permit users or groups to view and update vulnerable items and vulnerability group records that are assigned to them. To view descriptions of specific granular roles, as a user with the system admin role, navigate to User Administration > Roles and locate the role that you want. Roles that are automatically inherited when a role is assigned are listed. Also, when a role depends on other role assignments, any required roles are also listed.

In the following image, the granular roles of both the remediation owner persona role and the vulnerability analyst persona are illustrated. Note that the remediation owner persona does not include the read_all and write_all permissions of the vulnerability analyst persona. The granular roles, read_all and write_all, are required before users and groups can read and edit all of the vulnerable item and vulnerability group records. To customize these roles, simply add or remove granular roles to expand or limit access.
Granular roles and the remediation owner and vulnerability analyst personas

Remediation owner persona

- Read assigned
- Write assigned
- Update assignment group
- Update assigned to
- Update state

Vulnerability analyst persona

- Read all
- Write all
- Update state
- Update assignment group
- View stats
- Bulk edit
- Read assignment rules
- Read remediation target rules
- Risk score configuration
- Risk score configuration
- Create SI
- Approver
- Update discovered item
- Manually initiate rescan
- Manage solutions

If you want your users and groups to have more access than the persona roles permit, you can add more granular roles to users and groups. Conversely, if you want to limit access for specific users and groups at the task level, you can remove granular roles.

Note: To assign and edit granular roles in the User Administration module, the system admin role is required.
Granular roles in the User Administration module

For an example of how to manage granular roles for a user or group, see Manage persona and granular roles for Vulnerability Response.

To assign persona roles, see Assign the Vulnerability Response persona roles using Setup Assistant.

Vulnerability Response assignment rules overview

Define the criteria by which vulnerable items (VIs) are automatically assigned to an assignment group for remediation.

A default assignment rule, Assign to CI support group, is included in the base system assigning vulnerable items to the CI Support Group.

Note: The assignment rules do not reevaluate manually created assignments.

Assignment type, whether Manual or Rule is available from the VI form and the list view. Any VI that was originally assigned by a rule but subsequently manually reassigned contains a reference to the original rule.

Use Assignment rule and Assignment type information to identify cases where the assignment rules did not find a correct match for the intended recipient. Or which rules had the most reassignments.

The Assignment groups set by Assignment Rules are used by Vulnerability Group Rules (VGR) to assign owners to vulnerability groups (VG).

Note: To make Rapid7 InsightVM asset tags available for use in the Condition filter for Assignment Rules, you must run the Rapid7 InsightVM Asset List integration before the other Rapid7 InsightVM integrations.

Starting with v13.0, case sensitivity for the search text you enter in the condition builder is not supported on this record or form. Prior to v 13.0, case sensitivity is supported for the search text you enter in the condition builder.

Assigning vulnerable items automatically

There are three different ways to assign vulnerable items using Assign using:

• Assignment Group: This option allows you to select any of the existing Now Platform® user groups.

• Assignment Group Field: This option allows you to choose any assignment group field available using the cmdb_ci table. By default you see the following three group fields:
None: Indicates no default value for this mandatory field
Configuration Item: Approval Group
Configuration Item: Assignment Group
Configuration Item: Support Group

Script: This option allows you to define the conditions using a script. This option requires coding or advanced ServiceNow expertise.

Run high priority rules (items that need special handling, where risk is critical, or a VI should be handled by regulatory compliance) first. Next, run your general rules, where no special handling is required, and you know who should be responsible for them. Finally, create a default rule to assign VIs to the group that will figure out what assignment group it should belong to. This group could add another rule to cover their decisions. This default rule would run last.

Assignment rule evaluation process
When a new vulnerable item (VI) is created, imported, or reopened after being closed, the assignment rules are evaluated against it. A VI is only evaluated once, unless it is reopened after being closed. You can manually reapply rules after changes.

The following process is used for each new, updated or reopened VI:

• For each vulnerability assignment rule, the VI is compared to the assignment filter, lowest order rule first.
• Where the condition matches, the VI is assigned an assignment group. The lookup stops.
• Where the conditions do not find a match among all the other rules, the VI is assigned to the default assignment group, if a default rule exists.

Once the vulnerable item has been assigned, the appropriate vulnerability group rule uses assignment as one of its criteria for placing the vulnerable items into a vulnerability group. See Vulnerability Response groups and group rules overview and Filtering within Vulnerability Response for more information.

Note: If there is no default rule then the VI remains unassigned when the vulnerability group rule makes the group assignment.

Reapplying assignment rules
When you change an assignment rule, use the Apply Changes button on the Assignment Rules list page to rerun all the changed rules on all active Open VIs, except those that were manually assigned.
Note:

If the **Reapply all vulnerability assignment rules** scheduled job has not run before the first time you use **Apply Changes**, then it runs all the assignment rules on all Open VIs except those VIs that were manually assigned. After that, all subsequent uses of **Apply Changes** rerun only the changed rules and any dependent rules. Changes to one rule may result in a VI matching a different unmodified rule. Reapplying assignment rules does not regroup the vulnerable items.

The scheduled job [**Reapply all assignment rules**] is inactive, by default. When activated, it applies all the rules to all open VIs except those manually assigned. It can run **Daily**, **Weekly**, **Monthly**, **Periodically**, **Once**, or **On Demand**. Depending on how many active VIs you have in your environment, remember to set the **Run** field appropriately following the initial run to prevent performance impacts.

Upgrade customers to Vulnerability Responsev10.0 or later, should refer to the [Vulnerability Response release notes](#) for information regarding the impact of this feature on existing VIs.

**Assignment rules and vulnerability group assignment**

In most cases, you would assign your vulnerability group to the same assignment group as the vulnerable items in it. That is what vulnerability group rules do, by default. When you create a VGR, it groups the vulnerable items by the assignment group in addition to whatever other key columns you have selected. For example, if your VGR groups by configuration item class (laptop, Oracle Database, Linux Server and so on), the vulnerability group created is broken apart by the different assignment groups — an Oracle Database VG assigned to Group 1, and an Oracle Database VG assigned to Group 2.

If you want the VGR to create groups and assign them differently, you can. There is an Advanced Assignment view in VGRs that display your assignment options. See [Create or edit Vulnerability Response group rules](#) for more information vulnerability group rule options.

**Vulnerability Response groups and group rules overview**

Configure vulnerability groups (VG) to help analysts and remediation specialists organize vulnerable items (VI) and analyze them in bulk. The criteria by which groups are formed is configured so that you do not have to manually assign vulnerable items into groups. Using vulnerability groups, you can monitor progress and drive the remediation process more efficiently.
Understanding vulnerability groups

Vulnerability groups represent a set of vulnerable items to remediate. Grouping vulnerable items has many advantages. You can move vulnerable items through the remediation states, mark them under investigation, defer them, mark them resolved in bulk by using groups. You can create conditions to automatically group all items with specified vulnerabilities, departments, locations, and any other data related to the vulnerable item. Vulnerable items can belong to more than one vulnerability group giving you the flexibility to actively work with one group and monitor another. It all depends on your organizational needs. For example, you could group by department, and also create a group containing all currently exploitable vulnerabilities.

Vulnerability groups are created as follows.

- Manually, using one of three options, to add vulnerable items to the group.
  - Add vulnerable items to the group by hand.
  - Use a **Condition** filter that automatically adds vulnerable items to the vulnerability group.
  - Use a **Filter group** that automatically adds vulnerable items to the vulnerability group.

  **Note:** Manually added vulnerable items are not automatically removed from vulnerability groups by vulnerability group rules or group conditions.

- Automatically, using vulnerability group rules (VGR). This option is the easiest option, once configured, vulnerability group rules create all desired vulnerability groups.

From a vulnerability group, the group of vulnerable items may be assigned to a user, deferred until later, used to create a **Change Request**, and so on.

Starting with version 10.0, when a group is formed based on a specific vulnerability, that vulnerability is listed on the VG form.

When it is determined that a new vulnerable item can be added to a group, the vulnerability item is included in the **Vulnerable Items** list of the vulnerability group. Conversely, the vulnerability group appears in the **Vulnerability Group** list of **Vulnerable Items**.

When updating the state of a vulnerability group, associated vulnerable items can have their state updated to match this vulnerability group. See **Vulnerability Response group and vulnerable item states** for more information on state changes.

You can create security incidents and change requests from vulnerability groups, as needed.
Refreshing vulnerable items automatically

**Note:** Vulnerable item refresh automation applies only to groups created using the condition filter or filter group. Automation does not apply to VIs that were added manually or grouped using vulnerability group rules (VGRs).

When the **Automatically refresh vulnerable items** check box is selected, new VIs matching the vulnerability group filter criteria are automatically added to the group. Vulnerable items in the group that no longer match the filter criteria are automatically removed from the group.

By default, when the group leaves the **Open** state, the check box is cleared. If you want vulnerable items to continue being added to the group, regardless of state, disable the **Set auto refresh vulnerable items** business rule.

You can select the check box again manually from the Under Investigation state. **Automatically refresh vulnerable items** is not disabled when the group moves into the **Awaiting Implementation** state. Once in the Awaiting Implementation state, no new vulnerable items can be added to the existing group, nor can existing vulnerable items be removed from the group.

**Note:** When a group is created manually, and VIs are added using the **Condition** filter or **Filter Group**, the check box is unchecked. You have the choice to select the box or not.

Refreshing vulnerable items manually

For manually created vulnerability groups with a **Filter Group** or **Condition** filter, when you click the **Re-scan vulnerable items** related link on the **Vulnerability Group** page, any vulnerable items that match the filter criteria are added. Items no longer matching the criteria are removed. This action allows an immediate update of the list of vulnerable items and is used whether the **Automatically refresh vulnerable item** check box is selected or not.

Manually created vulnerability groups using **Condition** or **Filter Group** filter types are refreshed once an hour.

Understanding vulnerability group rules

Vulnerability groups rules allow you to define how vulnerable items are automatically grouped and assigned. A default rule, **Vulnerability**, is included in the base system grouping vulnerable items based on its vulnerability. However, you can group by any other set of values in columns accessible from the VI. These values could include configuration item (CI) support group, vulnerability severity, and, so on.
You can create any number of conditions. Once you set a Group by selection, another row appears. You can have up to six Group by selections. You can automate group assignment, as well. See Create or edit Vulnerability Response group rules and Filtering within Vulnerability Response for more information.

**Note:** To make Rapid7 InsightVM asset tags available for use in the Condition filter for Vulnerability Group Rules, you must run the Rapid7 InsightVM Asset List integration before the other Rapid7 InsightVM integrations.

For example, you can group your vulnerable items by the cost center of the vulnerable CI, or by the attack vector of the vulnerability. You can have one group rule for low severity vulnerabilities or low risk CIs. You can have another group rule for critical servers, and vulnerabilities with exploits — vulnerable items that expose the company to more risk.

A different set of rules can be used for vulnerable items that expose the company to more risk. The VGR name is appended to the VGR Group by values to make the short description of the new vulnerability group. See Create a Vulnerability Response group for more information on available fields.

Starting with v13.0, by default, *(Case sensitive check box disabled)*, the search text you enter in the condition builder on group rules records and forms is not case-sensitive. You have the option to enable case-sensitive searches on group records and forms.
When a new vulnerable item is created, imported, or reopened after being closed, the vulnerability rules are evaluated against it. A VI is only evaluated once, automatically, unless it is reopened after being closed or the rules are reapplied manually.

The following process is used for each new or reopened VI:

- For each vulnerability group rule, the VI is compared to the VGR filter.
- For each rule where the VGR condition matches, the rule pulls the data from the Group by selections on the VI. It builds a group name and field. In this case, High Risk: QID-32342:Summary of QID-3242 (Name:vulnerability ID:vulnerability summary).

Note: The short description field is limited to 160 characters. Longer vulnerability summaries are truncated.

The rule checks to see if there is a matching Open vulnerability group that is assigned to the same assignment group as the VI.
- If the group is found, the VI is added to the existing group in the Open state.
- If no group in the Open state is found, the rule creates a High Risk: QID-32342 group, assigns it to the same assignment group as the VI, and places the VI in the vulnerability group.

More than one VGR can be defined, to group different kinds of vulnerabilities. Since each vulnerability is compared with the VGR conditions before putting it in a group, too many rules may have a performance impact.

By default, VGRs use the assignment group set by the Assignment Rules on the vulnerable item when grouping the items, and assigns the vulnerability group to match the vulnerable items.

As part of the default group rule, the assignment of these vulnerability groups is controlled by the rules in the Assignment Rules module. For more information on assignment rules, see Vulnerability Response assignment rules overview.

When a group rule is deleted, from the form or list view, you have the option to delete all Open groups created by that rule. Groups not in the Open are excluded.

Reapplying vulnerability group rules

When you want to change a vulnerability group rule, use the Reapply button on the vulnerability group rule page to rerun the changed rule on all active Open vulnerability groups created by that rule. It deletes and recreates vulnerability groups based on the changed rule automatically.
Machine Learning solutions for Vulnerability Response

Vulnerability Assignment Recommendations uses ServiceNow® Predictive Intelligence and machine learning to recommend assignment groups for vulnerable items (VIs) and vulnerability groups (VGs). You can reduce the time that you spend on identifying the owners for unassigned or incorrectly assigned vulnerability findings. Also, you can see a system-generated confidence score that evaluates if the recommended assignment group is suited to resolve the vulnerability.

The Predictive Intelligence capabilities are used in Vulnerability Response to provide better work experiences by creating and training a solution definition model that can predict the assignment group based on existing data.

For more information, see Predictive Intelligence.

Vulnerability Assignment Recommendations

With the Vulnerability Assignment Recommendations application (com.snc.vulnerability.recom), the system can assign recommendations in Vulnerability Response using ServiceNow Predictive Intelligence. This plugin requires:

- Vulnerability Response (com.snc.vulnerability)
- Predictive Intelligence (com.glide.platform_ml)

For more information, see Predictive Intelligence.

Confidence scores

Use the Vulnerability Assignment Recommendations application to generate the confidence score that reports the confidence level of the recommended assignment groups for the selected VGs or VIs. The confidence score evaluates whether the system is confident that the recommended assignment group is suited to resolve the vulnerability. Up to 10 recommendations appear. These recommendations are based on the highest probability for successful assignments. The first recommendation in the list means that the system has the highest confidence that it is the correct assignment group.

For example, on a scale of 0-100, for each assignment group, the confidence score suggests the probability of a VI or VG belonging to that particular group.

Related information

- Predictive Intelligence
- Create and train a classification solution
- Create and train a similarity solution
CI Lookup Rules for identifying configuration items from Vulnerability Response third-party vulnerability integrations

When data is imported from a third-party integration, Vulnerability Response automatically uses host data to search for matches in the Configuration Management Database (CMDB). It does this using CI Lookup Rules. These rules are used to identify configuration items (CIs) and add them to the vulnerable item record to aid in remediation.

As assets are imported, a lookup is performed first on the Discovered Items list using third-party IDs to find matches to configuration item (CIs) from prior imports. When a host ID match is found, it is used as the Configuration item field in the vulnerable item record.

You can see how imported assets are mapped to CIs using the Discovered Items list. If a match is not found, or the host ID field is empty, the rules use the other host information to attempt to correctly identify the CI. If a match is still not found, a placeholder CI is created and is designated as an Unmatched CI. See Unmatched CIs for more information on how those CIs are handled.

⚠️ Note: CI lookup rules are available only for the Qualys and Rapid7 vulnerability integrations.

CI lookup rules can be domain separated and are source-specific. Each source can have multiple deployments. For example, the Rapid7 Vulnerability Integration, can have both Data Warehouse and InsightVM deployments. Qualys can have multiple deployments of the Qualys Vulnerability Integration. Each deployment has its own set of CI Lookup Rules.

⚠️ Note: CI lookup rules are shared by all deployments of the vulnerability integration. If a rule is deleted or modified, the deletion or changes affect all deployments of the vulnerability integration.

When attempting a match, the first step is a vendor ID lookup for an exact match across source, source_instance, and vendor ID. Then, lookup rules are run in order, from lowest to highest and stop when a rule returns just a single CI as a match. If a rule is created in such a way that it returns more than one CI, only the first match is used.

⚠️ Note: To avoid matching on low-level networking elements, if a matched CI is one of dscy_switchport, cmdb_ci_network_adapter, cmdb_ci_nic, or cmdb_ci_ip_address, the parent CI is returned.
A system property to exclude CI classes is available. This property is not available with upgrade. See [Ignore CI classes](#) for upgrade information and instructions on setting the property.

To make it easier to find matching issues, when a match is found, the CI lookup rule used to find it is added to the Discovered Item record in the **CI matching rule** field. Lookup rules are evaluated by lowest **Order** value first.

These Qualys CI lookup rules are shipped with the base system.

- QUALYS HOST ID
- FQDN
- NetBIOS
- DNS
- IP

These Rapid7 CI lookup rules are shipped with the base system.

- MacAddress
- FQDN
- HostName
- IP

**Note:** Rules, once removed, cannot be recovered. Rather than removing existing rules, deactivate them when creating new ones.

Importing vulnerability data can be taxing on an instance and performance issues with resources can occur if rules are not carefully constructed. The logic used to iterate through and perform matching within the CMDB can result in lengthy processing times. To avoid any potential degradation of resources or performance complications, test any custom-written CI Lookup Rules or modifications to pre-defined **CI Lookup Rules**. See [Prevent duplicate or orphaned records after running Vulnerability Response CI lookup rules](#) for more information on preventing duplicate orphan records, deleting data, and cleaning up data.

**Reapplying updated CI lookup rules**

When you change a CI lookup rule, click **Apply Changes** on the CI Lookup Rules list page to rerun all the rules on the discovered items that:

- Were matched by the updated rules
- Are not matched by any rule
If the configuration item (CI) changes after reapplying the lookup rules, the discovered items are updated with the new CI. The impacted detections and vulnerable items are also updated. For more information, see CI changes for discovered items.

**Prevent duplicate or orphaned records after running Vulnerability Response CI lookup rules**

Take steps to prevent duplicate or orphan records resulting from matching (configuration items (CIs) within the CMDB.

Importing vulnerability data can be taxing on an instance and performance issues with resources can occur if rules are not carefully constructed. The logic used to iterate through and perform matching within the CMDB can result in lengthy processing times. Thorough testing and debugging of processing scripts in the rules helps alleviate the potential of issues later in the process.

**Preventing duplicate or orphaned records**

- Use small subsets of data that are specific to the CI Lookup Rule being tested.
  - Set all CI Lookup Rules, other than the one being tested, to **Inactive**.
  - Analyze the imported CIs to ensure that you are observing the expected behavior and matching is occurring properly.

- Review Matched CIs
  - Examine the count of matched vs unmatched CIs. Ensure that the percentage is acceptable. Don’t just look at the first page, that is likely the first one inserted.
  - Manually search for some CIs.
  - Check to see if there are any naming or field problems (such as searching for a specific domain).
  
    If it seems appropriate, add additional matching rules.

- Review Unmatched CIs
  - Navigate to the Unmatched CIs table.
  - Group by Configuration Item class.
  - Review any classes that don’t look right (certificates, network cards, images).
    - Figure out why didn’t they match the correct CI?
    - Should the class be excluded?
    - Should the class be elevated to a related class?

- Review CI states such as **Retired**.
• Remove Test Data
  ◦ Once you begin to observe the correct or expected behavior in CI matching, start over. Start over by:
    ■ Deleting the data used for testing: (see the **Deleting data from tables** section)
    ■ Discovered Items
    ■ Vulnerable Items
    ■ Vulnerability Groups
  ◦ Manually rerunning all the CI Matching rules.

For more information on CI Lookup Rules and Qualys, see the [KB0750656](#) article.
For more information on CI Lookup Rules and Rapid7, see the [KB0818096](#).

**Deleting data from tables**
Sometimes you have imported data and realize something is wrong. If something is wrong in a development or performance environment, you could reclone from a better environment, but that isn’t always an option.

⚠️ **Note:** Performing these actions requires ServiceNow expertise.

There are four options for deleting data from tables:

• **Using Delete All Records on Table Configuration.**

• Configure the **Table Cleaner** by navigating to **Auto Flushes** (sys_auto_flush.list) and creating a new **Auto-flush** record.

• Truncate the gs.truncateTable using a background script.

  Using `truncateTable` requires turning off the record for rollback check box in the background scripts. Otherwise, a copy of the table and related cascade tables are created, take too long, and most likely fail.

  ⚠️ **Note:** Never use `truncateTable` in a production environment. Consult your Support representative before executing large deletions in production or shared environments.

• Create a request in HI to have the data deleted.
Deduplicating existing configuration items

Whenever configuration items (CIs) are updated through a deduplication task, the discovered items (DIs) that are related to those CIs are also updated. The vulnerable items (VIs) and detections are also updated with the CI.

For more information, see CI changes for discovered items.

Related information

Remediate a de-duplication task

Creating CIs for Vulnerability Response using the Identification and Reconciliation engine

Starting with Vulnerability Response 12.1, you can create configuration items (CIs) in the Configuration Management Database (CMDB) using the Identification and Reconciliation engine (IRE) API. By using the IRE API to create CIs, you can prevent duplicate CIs from being created and you can reconcile CI attributes by allowing only authoritative data sources to write to CMDB.

A CI class (table) is the original table name in the instance database. CMDB contains base system classes that store data about CIs.

Using IRE for CI creation

Prior to version 12.1, if a matched CI was not found either in the Discovered Items list or CMDB, a CI was created in the Unmatched CI class (sn_sec_cmos_unmatched_ci).

For more information, see Unmatched CIs.

Starting with version 12.1, you can use the IRE API to create CIs in CMDB. Instead of using the Unmatched CI class, a CI is created in the Unclassed Hardware or Incomplete IP Identified Device class.

CMDB CI classes

⚠️ Note: To use the new classes, activate the CMDB CI Class Models plugin. Otherwise, CIs are created in the Unmatched CI class.

Starting with version 12.1, if the host that you imported from a third-party scanner can’t be found in the Discovered Items list or CMDB, it is stored in one of the following new CMDB CI classes.
## CMDB CI classes

<table>
<thead>
<tr>
<th>CMDB CI Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incomplete IP Identified Device</td>
<td>CI is created in this table if only the IP address is available in the host information that is received from the scanner.</td>
</tr>
<tr>
<td>(cmdb_ci_incomplete_ip)</td>
<td></td>
</tr>
<tr>
<td>Unclassed Hardware</td>
<td>CI is created in this table if any of the following information is available in the host information that is received from the scanner:</td>
</tr>
<tr>
<td>(cmdb_unclassed_hardware_ci)</td>
<td>• Host name</td>
</tr>
<tr>
<td></td>
<td>• IP address</td>
</tr>
<tr>
<td></td>
<td>• DNS</td>
</tr>
<tr>
<td></td>
<td>• NETBIOS</td>
</tr>
<tr>
<td></td>
<td>• MAC address</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the MAC address is available, the network adapter entry is created and related to the unclassed hardware CI. If both the IP and MAC addresses are available, the IP address CI is also created and related to the unclassed hardware CI.</td>
</tr>
</tbody>
</table>

The system automatically uses an Unmatched CI class if one of the following occurs:

- The CMDB CI Class plugin is not activated.
- IRE raises an exception while creating a new CI.
  
  For more information, see [Unmatched CIs](#).

### Related information

CMDB CI Class Models store app
Identification and Reconciliation engine (IRE)
Discovered Items

Assets are automatically matched to configuration items (CIs) using CI Lookup Rules, when they are imported using the host and vulnerable item integrations. Discovered Items give you visibility into how asset identification is mapped to CIs in the CMDB.

Discovered Items are considered **Matched**, **Unmatched**, or **Reclassified**. Identified CIs are in the **Matched** state.

To make it easier to find potential matching issues, the CI Lookup Rule that matched the CI appears in the **CI matching rule** field.

ℹ️ Note: **CI matching rule** field support is available only for the Qualys and Rapid7 vulnerability integrations.

If a match was not found, a CI is created in the **Unmatched CI** class [sn_sec_cmn_unmatched_ci] of the CMDB. If the original unmatched CI was reclassified, Discovered item records are updated to reflect that state. See **Unmatched CIs** and **View and reclassify unmatched configuration items** for more information.

By default, the **Security Operations > CMDB > Discovered Items** module lists unmatched configuration items. You can view all discovered items from an import by removing the filter.

For a description of the fields in Discovered Items, see **Discovered Items form fields**

### Discovered Items form fields

Assets are automatically matched to configuration items (CIs) in the Configuration Management Database (CMDB) when they are imported using CI Lookup Rules. Records for unmatched CIs are automatically created during third-part vulnerability integration imports and included in the discovered Items.

### Discovered Items fields

The information in these records are ingested from the third-party records and classified during import.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Identifier assigned to the record.</td>
</tr>
<tr>
<td>Configuration Item</td>
<td>Imported from the third-party source integration.</td>
</tr>
</tbody>
</table>
### Field Description

Starting from **v12.0**, this is the latest CI from the list of CIs after filtering the decommissioned ones.

**Class**
Class assigned the CI during import by Vulnerability Response.

**Source**
Imported from the third-party source integration.

**CI matching rule**
The CI matching rule that was used to create the item.

**Version 12.0: Other matched CIs**
List of the other configuration items matching the CI lookup rule.

**State**
Determined during import. Choices are:
- **Matched**: A matching configuration item was found in the CMDB.
- **Unmatched**: No match was found in the CMDB. A placeholder record is created.

**Created**
Date the Discovered Item record was created.

**Updated**
Date the Discovered Item record was updated.

**Updated by**
Who or what updated the data.

**Host tag**
Host tags assigned to this discovered item during import. You can have up to 31 host tags per discovered item.

**Fully qualified domain name**
Data associated with this CI found in the CMDB.

**MAC Address**
Data associated with this CI found in the CMDB.

**Operating System**
Operating system associated with this CI.

**NetBIOS**
Imported from the third-party source integration.

**IP address**
Data associated with this CI found in the CMDB.

**Source data**
Data associated with this CI from the source.

### CI changes for discovered items

When a configuration item (CI) on a discovered item (DI) changes, the impacted detections and vulnerable items (VIs) are updated. The risk score, assignment rules, group rules, and remediation target rule are reevaluated.
If a VI exists with the same vulnerability and CI, the detections are updated with the existing VI and the current VI is closed with the substate as invalidCI. Work notes are added for the following reasons:

- When detections are moved from one VI to another.
- When a duplicate VI is closed.

If you do not want to update the CI for the existing VI, set the property sn_sec_cmn.update_on_ci_change to false. Then, when a CI changes, a new VI is created and the existing one is closed as an invalidCI.

The default value of the property sn_sec_cmn.update_on_ci_change is true.

Reconcile unmatched discovered items

Create a scheduled job to reconcile unmatched discovered items. A vulnerable item (VI) consists of a vulnerability and a configuration item (CI). When a VI is created, the CI that is added to it at the time of creation might be an outdated one. Unmatched CI information is not reconciled if the information in the CMDB changes. To reconcile, apply configuration Item (CI) lookup rules on the items that are in an unmatched state when the CMDB is updated with the latest CIs.

About this task

You can run a scheduled job demand to reapply the CI matching rule for the discovered items in an unmatched state. If the CI changes after reapplying the lookup rules, the discovered items are updated with the new CI. Impacted detections and vulnerable items are also updated. For details, see CI changes for discovered items.

Procedure

2. On the Background Jobs page, click Create reconciliation job.
3. On the form, fill in the fields.

   Note: You can only edit the Parameters field.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Unique job number.</td>
</tr>
<tr>
<td>Created by</td>
<td>User who created the job.</td>
</tr>
<tr>
<td>Parameters</td>
<td>Parameters to reconcile the unmatched discovered items:</td>
</tr>
</tbody>
</table>
Field | Description
---|---
• limit: Maximum number of discovered items to be reconciled. If you do not enter a value, 10,000 discovered items are reconciled.
• firstDiscoveredItem: First discovered item that must be reconciled. If you do not enter a value, the reconciliation process starts from the first discovered item.
State | Current state of the background job.
State description | Description of the current state of the background job.
Job type | Type of job. The value is Reconcile unmatched discovered items.
Started at | Time when the job started.
Ended at | Time when the job was completed.
Job duration | Total time taken to complete the job.
Substate | Substate for the selected state.
Notes | Number of records that were processed.

4. Click Submit.

ℹ️ Note: To stop running the job, click Cancel.

ℹ️ Note: You can’t reconcile unmatched CIs or reapply CI lookup rules while you are importing hosts or vulnerable items.

Reapply CI lookup rules on selected discovered items
Reapply the configuration item (CI) lookup rules on selected discovered items from the discovered item list view select actions. If the CI changes after you reapply the rules, the discovered items are updated with the new CI and impacted detections. Vulnerable items are also updated.

About this task
For more information, see CI changes for discovered items.
Procedure

1. Navigate to Security operations > CMDB > Discovered Items.

2. Select the required discovered items and click Action on selected rows.

3. From the list, select Reapply CI lookup rules.
   The rules are reapplied on these discovered items.

Vulnerability Response group and vulnerable item states

Vulnerability Response offers a state model for the status of the vulnerability group, at any given time. Knowing how each state relates to and affects each other helps you to determine when and how to remediate your vulnerable items (VI).

Vulnerability group states

Complex use cases can sometimes result in a vulnerable item being in a different state than its group. Understanding how states work helps to explain this behavior and can help with creating vulnerability groups and, creating or editing vulnerability group rules.

Vulnerability groups have many possible states.
Note: Each group form contains **Follow** and **Update** buttons which are standard for ServiceNow tasks.

Starting with Vulnerability Response v10.0, third-party integrations import vulnerable item detection data that create new VIs or update existing VIs. Detection states update VI states in so far as they are **Open** or **Closed**. For more information, see the section below titled, Detections, vulnerability groups, and vulnerable items.

With **Change management for Vulnerability Response**, there is a synchronized relationship between the State fields of vulnerability groups (VG) and the State fields of change requests (CHG) in the Vulnerability Response product. As a change request moves through its life cycle, it also moves the state of any related vulnerability groups automatically. After a change request is implemented, the vulnerability group is automatically resolved. See **State synchronization between change requests and vulnerability groups** for more information.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
</table>
| Open     | State upon creation. From this state you can:  
**Start Investigation**  
Assign this vulnerability group to a person or group to start investigating.  
**Mark as false positive**  

## Vulnerability Response state flow diagram prior to V10.3

Diagram showing the state flow of vulnerability responses, with states including **Open**, **Awaiting Implementation**, **Under Investigation**, **Resolved**, **Deferred**, and **Closed**. Each state has associated actions and notes, such as the ability to start investigation or mark as false positive.
<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting with v10.3, mark an item or group as false positive if the scanner reports that a vulnerability exists in the system, but in reality there is no vulnerability.</td>
<td></td>
</tr>
<tr>
<td><strong>Request exception</strong></td>
<td>Starting with v10.3, request an exception, a reopen (Until) date, a reason, and optionally, provide addition information. Defers the remediation of the item or group until the date till which an exception is requested.</td>
</tr>
<tr>
<td><strong>Resolve</strong></td>
<td>Starting with v10.3, mark as Resolved to move the item or group to a resolved state.</td>
</tr>
<tr>
<td><strong>Create Change</strong></td>
<td>Create a change request or associate a vulnerability group to an existing change request. See Create a change request from a vulnerability group and Associate a vulnerability group to an existing change request.</td>
</tr>
<tr>
<td><strong>Split Group</strong></td>
<td>For a group with more than one vulnerable item, use a set of conditions to filter out a subset of vulnerable items and split a vulnerability group. The items that you select are automatically moved to a new VG. See Split a vulnerability group.</td>
</tr>
<tr>
<td><strong>Defer</strong></td>
<td>Select the Deferred state, a reopen date, a reason and, optionally, provide addition information. Defers the group state until the reopen date.</td>
</tr>
<tr>
<td><strong>Close</strong></td>
<td>Select the Closed state, a reason and provide addition information. Closes the group.</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Confirm the deletion. Removes the group.</td>
</tr>
<tr>
<td>State</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Under Investigation</td>
<td>Triggered by the <strong>Start Investigation</strong> button. From this state you can:</td>
</tr>
<tr>
<td></td>
<td><strong>Create a Security Incident</strong></td>
</tr>
<tr>
<td></td>
<td>See Create a security incident for more information.</td>
</tr>
<tr>
<td></td>
<td><strong>Create Change</strong></td>
</tr>
<tr>
<td></td>
<td>Create a change request or associate a vulnerability group to an existing change request. See Create a change request from a vulnerability group and Associate a vulnerability group to an existing change request.</td>
</tr>
<tr>
<td></td>
<td><strong>Split Group</strong></td>
</tr>
<tr>
<td></td>
<td>For a group with more than one vulnerable item, use a set of conditions to filter out a subset of vulnerable items and split a vulnerability group. The items that you select are automatically moved to a new VG. See Split a vulnerability group.</td>
</tr>
<tr>
<td></td>
<td><strong>Create a Change Request</strong></td>
</tr>
<tr>
<td></td>
<td>See Create a change request from a vulnerability group for more information.</td>
</tr>
<tr>
<td></td>
<td><strong>Awaiting Implementation</strong></td>
</tr>
<tr>
<td></td>
<td>Changes state to Awaiting Implementation. This state indicates that the group remediation has been referred outside Vulnerability Response.</td>
</tr>
<tr>
<td></td>
<td><strong>Deferred</strong></td>
</tr>
<tr>
<td></td>
<td>Select the Deferred state, a reopen date, a reason and, optionally, provide addition information. Defers the group state until the reopen date.</td>
</tr>
<tr>
<td></td>
<td><strong>Close</strong></td>
</tr>
<tr>
<td></td>
<td>Select the Closed state, a reason and provide addition information. Closes the group.</td>
</tr>
<tr>
<td></td>
<td><strong>Delete</strong></td>
</tr>
<tr>
<td></td>
<td>Confirm the deletion. Removes the group.</td>
</tr>
<tr>
<td>State</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Deferred</td>
<td>Starting with v10.3, this is triggered by the <strong>Request Exception</strong> button. Prior to v10.3, it was triggered by the <strong>Close/Defer</strong> button. As part of the approval workflow, the Deferred state is In Review and cannot be closed until approved. From this state you can:</td>
</tr>
<tr>
<td></td>
<td><strong>Create Change</strong></td>
</tr>
<tr>
<td></td>
<td>- Create a change request or associate a vulnerability group to an existing change request. See Create a change request from a vulnerability group and Associate a vulnerability group to an existing change request.</td>
</tr>
<tr>
<td></td>
<td><strong>Split Group</strong></td>
</tr>
<tr>
<td></td>
<td>- For a group with more than one vulnerable item, use a set of conditions to filter out a subset of vulnerable items and split a vulnerability group. The items that you select are automatically moved to a new VG. See Split a vulnerability group.</td>
</tr>
<tr>
<td></td>
<td><strong>Create a Security Incident</strong></td>
</tr>
<tr>
<td></td>
<td>- See Create a security incident for more information.</td>
</tr>
<tr>
<td></td>
<td><strong>Reopen</strong></td>
</tr>
<tr>
<td></td>
<td>- Transitions back to an Open state.</td>
</tr>
<tr>
<td></td>
<td><strong>Delete</strong></td>
</tr>
<tr>
<td></td>
<td>- Confirm the deletion. Removes the group.</td>
</tr>
<tr>
<td></td>
<td><strong>Close</strong></td>
</tr>
<tr>
<td></td>
<td>- Select the Closed state, a reason and provide addition information. Closes the group.</td>
</tr>
<tr>
<td></td>
<td>Deferment information appears under the <strong>Close/Defer</strong> tab. On the defer date, the group reopens for remediation.</td>
</tr>
<tr>
<td>Awaiting Implementation</td>
<td>Triggered by the <strong>Awaiting Implementation</strong> button. From this state you can:</td>
</tr>
<tr>
<td></td>
<td><strong>Create a Security Incident</strong></td>
</tr>
<tr>
<td></td>
<td>- See Create a security incident for more information.</td>
</tr>
<tr>
<td>State</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Create Change</td>
<td>Create a change request or associate a vulnerability group to an existing change request. See Create a change request from a vulnerability group and Associate a vulnerability group to an existing change request.</td>
</tr>
<tr>
<td>Split Group</td>
<td>For a group with more than one vulnerable item, use a set of conditions to filter out a subset of vulnerable items and split a vulnerability group. The items that you select are automatically moved to a new VG. See Split a vulnerability group.</td>
</tr>
<tr>
<td>Create a Change Request</td>
<td>See Create a change request from a vulnerability group for more information.</td>
</tr>
<tr>
<td>Defer</td>
<td>Select the Deferred state, a reopen date, a reason and, optionally, provide addition information. Defers the group state until the reopen date.</td>
</tr>
<tr>
<td>Close</td>
<td>Select the Closed state, a reason and provide addition information. Closes the group.</td>
</tr>
<tr>
<td>Resolve</td>
<td>Add notes. The state becomes Resolved. Notes appear under the Resolution tab.</td>
</tr>
<tr>
<td>Delete</td>
<td>Confirm the deletion. Removes the group.</td>
</tr>
</tbody>
</table>

**Resolved**

Triggered from the Resolve button. From this state you can:

- **Create a Security Incident**
  - See Create a security incident for more information.
- **Create Change**
<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Create a change request or associate a vulnerability group to an existing change request. See Create a change request from a vulnerability group and Associate a vulnerability group to an existing change request.</td>
</tr>
<tr>
<td>Reopen</td>
<td>Transitions back to an Open state.</td>
</tr>
<tr>
<td>Close</td>
<td>Select the Closed state, a reason, and provide addition information. Closes the group.</td>
</tr>
<tr>
<td>Delete</td>
<td>Confirm the deletion. Removes the group.</td>
</tr>
</tbody>
</table>

Notes appear under the Notes tab. Resolution information appears under the Resolution tab.

<table>
<thead>
<tr>
<th>State</th>
<th>Triggered from the Close button. From this state you can:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Create a Security Incident</strong></td>
</tr>
<tr>
<td></td>
<td>See Create a security incident for more information.</td>
</tr>
<tr>
<td></td>
<td><strong>Reopen</strong></td>
</tr>
<tr>
<td></td>
<td>Transitions back to an Open state.</td>
</tr>
<tr>
<td></td>
<td><strong>Delete</strong></td>
</tr>
<tr>
<td></td>
<td>Confirm the deletion. Removes the group.</td>
</tr>
<tr>
<td></td>
<td>Closure information appears under the Close/Defer tab.</td>
</tr>
</tbody>
</table>

- Prior to v10.3, if the vulnerability group was manually marked Closed, with the reason, Result Invalid, the state of the vulnerable items in the group is updated to match the vulnerability group. It has been removed in v10.3.
- The remediation owner can only mark a vulnerable item or vulnerability group as resolved. Based on the confirmation from the scanner, this resolved item or group can be marked as Closed, or reopened.
- While the Close option is available only for the vulnerability analyst, Delete is available for the admin. These are used when there are multiple vulnerable items created manually, and these need to be closed or deleted.
• If you determine that the items are a low risk, waiting for a change window, or a patch, you can change their group to the Defer state for a defined amount of time, or immediately close the group. Starting with v10.3, you can request an exception using the Request Exception option.

**Note:** When vulnerability groups are deferred or closed, you can specify resolutions to further define the reasons for doing so.

• When a VI that is reopened, either manually or automatically, the following happens:
  ◦ The VI state changed to Open. (The original VG state does not update.)
  ◦ The VI is reevaluated and put into a new or existing group based on the active Vulnerability Group Rules.
This preserves its history while allowing for further remediation.

**Detections, vulnerability groups, and vulnerable item states**

Starting with v10.0, third-party Integrations retrieve vulnerable item detection data. Detections are distinct occurrences of vulnerabilities as reported by the scanners. Detection data are paired with vulnerable items and VI state is updated based on the state of the detections. If a VI is not found, a new one is created. Detections are only opened or closed by data found directly by a scanner.

If all detections are closed for a vulnerable item, that vulnerable item is closed. On the VI record, the state is Closed/ Fixed. When all VIs are closed for a VG, the VG is closed. (State flow otherwise remains the same. )

**Vulnerability groups and vulnerable item states**

Vulnerability groups and vulnerable items states can affect each other. Most of the time, a vulnerability group state updates the vulnerable item state, with the highest precedence group state used to update the vulnerable items in the group.

The state precedence is as follows.

Closed/Result Invalid > Deferred > Resolved > Awaiting Implementation > Under Investigation > Open

• When a group of vulnerable items are in one vulnerability group and are not altered at an individual level, they have the same state as their group.

• When the vulnerability group goes from the Open state to Awaiting Implementation, all the VIs in the group move to the Awaiting Implementation state.

• When the vulnerability group is deferred, the VI is likewise deferred.
Vulnerable items updated only by groups

Items match the state of the group (provided they have not been updated individually) with these exceptions:

- If the group changes its state to be Closed and its resolution to Canceled or Fixed with Exceptions, the item is not affected and takes on the state of any other group containing it. If the vulnerable item is in no other group, it reverts to the Open state.

- If the vulnerable item state is Closed/Fixed (updated by a scan or import), then when the group changes its state, the vulnerable item remains in the Closed/Fixed state. This condition is true no matter what state the group is in.

Vulnerable items in states set individually

Vulnerable items, in a state updated on the item, such as those items closed or deferred individually, do not match the state of the group automatically. Instead it compares its state to all associated groups to find the state with the highest precedence to apply.

Note: The Closed/Fixed state is a special case. For vulnerable items set to the Closed/Fixed state, if all vulnerable items within a group are set to Closed/Fixed — such as when a scanner finds that all the vulnerabilities have been remediated — the vulnerability group is automatically marked Closed/Fixed.

Vulnerability groups contain empty assignment fields

If the state of the VIs in a VG changes from Resolved to Open, the state of the VG is also updated from Resolved to Under Investigation.

However, if both the Assigned to and Assignment group fields in the VG are empty, the VG remains in Resolved state and does not move to Under Investigation.

Vulnerability group state for VIs in multiple groups

When a VI is in multiple groups, and its own state has not been set, the higher precedence group state determines the state of that VI, as illustrated in the following table.

Vulnerable item states examples

<table>
<thead>
<tr>
<th>Vulnerability groups state</th>
<th>Vulnerable item state</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group A: Open &gt; Under Investigation</td>
<td>Under Investigation</td>
</tr>
</tbody>
</table>
### Vulnerable item states examples (continued)

<table>
<thead>
<tr>
<th>Vulnerability groups state</th>
<th>Vulnerable item state</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group B: Open</strong></td>
<td><strong>Under Investigation</strong></td>
</tr>
<tr>
<td><strong>Group A:</strong> Under Investigation</td>
<td><strong>Group B:</strong> Open &gt; Under Investigation</td>
</tr>
<tr>
<td><strong>Group A:</strong> Under Investigation</td>
<td><strong>Awaiting Implementation</strong></td>
</tr>
<tr>
<td><strong>Group B:</strong> Under Investigation &gt; Awaiting Implementation</td>
<td><strong>Deferred</strong></td>
</tr>
<tr>
<td><strong>Group A:</strong> Under Investigation &gt; Deferred</td>
<td><strong>Closed/Result Invalid</strong></td>
</tr>
<tr>
<td><strong>Group B:</strong> Awaiting Implementation</td>
<td><strong>Deferred</strong></td>
</tr>
<tr>
<td><strong>Group A:</strong> Deferred</td>
<td><strong>Closed/Result Invalid</strong></td>
</tr>
<tr>
<td><strong>Group B:</strong> Awaiting Implementation &gt; Closed (Result Invalid)</td>
<td><strong>Deferred</strong></td>
</tr>
</tbody>
</table>

When Group A is Under Investigation and Group B is Open, the VI changes to Under Investigation. After the search, between Group A and Group B, Group A has the state with the highest precedence.

When Group B is Under Investigation and Group A is Under Investigation, the VI stays as Under Investigation. After the search, between Group A and Group B, they have the state with the same precedence.

When Group B is Awaiting Implementation and Group A is Under Investigation, the VI changes to Awaiting Implementation. After the search, between Group A and Group B, Group B has the state with the highest precedence.

When Group A is Deferred and Group B is Awaiting Implementation, the VI changes to Deferred. After the search, between Group A and Group B, Group A has the state with the highest precedence.

When Group B is Closed and the reason is Result Invalid, and Group A is Deferred, the VI changes to Closed/Result Invalid. After the search, between Group A and Group B, Group B has the state with the highest precedence.
Vulnerable item states examples (continued)

<table>
<thead>
<tr>
<th>Vulnerability groups state</th>
<th>Vulnerable item state</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group B: <strong>Closed (Result Invalid) &gt; Open</strong> (via Reopen)</td>
<td>When Group B is reopened and its state changes to Open, and Group A is Deferred, the VI changes to Deferred. After the search, between Group A and Group B, Group A has the state with the highest precedence.</td>
</tr>
</tbody>
</table>

Vulnerable item in multiple groups special cases

<table>
<thead>
<tr>
<th>Vulnerability Group State</th>
<th>Vulnerable Item State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group A: <strong>Under Investigation</strong></td>
<td><strong>Under Investigation</strong></td>
</tr>
<tr>
<td>Group B: <strong>Awaiting Implementation &gt; Closed (Fixed or Cancelled)</strong></td>
<td>When Group B is Closed/Fixed or Closed/Cancelled, and Group A is Under Investigation, the VI changes from Awaiting Implementation (previously the highest precedence) to Under Investigation (currently the highest precedence).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group A: any state</th>
<th>Group B: any state</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>If the vulnerable item source status is Fixed (updated by a scan or import), then when the group changes its state, the vulnerable item changes its state to Closed/Fixed. This condition is true no matter what states the other associated groups are in. The vulnerable item search for group state does not occur.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When a VI state is set individually, its state is considered when evaluating precedence, as with any other group. When a VI belongs to more than one group, the following updates are made.

**Vulnerable item state set individually special cases**

<table>
<thead>
<tr>
<th>Vulnerability item state within a group</th>
<th>Vulnerable item final state</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group A state: <strong>Under Investigation</strong></td>
<td><strong>Awaiting Implementation</strong></td>
</tr>
<tr>
<td>Group B state: <strong>Under Investigation &gt; Awaiting Implementation</strong></td>
<td>When Group B moved to Awaiting Implementation, and Group A remained</td>
</tr>
</tbody>
</table>
Vulnerable item state set individually special cases (continued)

<table>
<thead>
<tr>
<th>Vulnerability item state within a group</th>
<th>Vulnerable item final state</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original VI state: <strong>Under Investigation</strong> &gt; (set on the VI)</td>
<td>Under Investigation, the VI changes to Awaiting Implementation (the highest precedence).</td>
</tr>
<tr>
<td>Group A: <strong>Under Investigation</strong></td>
<td><strong>Deferred</strong></td>
</tr>
<tr>
<td>Group B: <strong>Under Investigation</strong> &gt; Awaiting Implementation</td>
<td>When Group B moved to Awaiting Implementation, and Group A remained Under Investigation, the VI remains in the Deferred state (the highest precedence).</td>
</tr>
<tr>
<td>Original VI state: <strong>Deferred</strong> &gt; (set on the VI)</td>
<td></td>
</tr>
</tbody>
</table>

When two groups with common vulnerable items are deferred, the state is deferred until the latest date is reached.

Vulnerable item deferred state special cases

<table>
<thead>
<tr>
<th>Vulnerability item state within a group</th>
<th>Vulnerable item final state</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group A state: <strong>In Review</strong> (until April 10)</td>
<td><strong>Deferred</strong> (until April 30)</td>
</tr>
<tr>
<td>Group B state: <strong>Under Investigation</strong> &gt; In Review (until April 30)</td>
<td>When Group B moved to Deferred (until Apr-30), and Group A remains Deferred (until Apr-10), the VI changes from Deferred (until Apr-05) to Deferred state (until Apr-30).</td>
</tr>
<tr>
<td>Original VI state: In Review (until April 10) &gt; (set on the VI)</td>
<td></td>
</tr>
<tr>
<td>Group A: <strong>In Review</strong> (until July 15)</td>
<td><strong>Deferred</strong> (until July 15)</td>
</tr>
<tr>
<td>Group B: <strong>Under Investigation</strong> &gt; In Review (until July 10)</td>
<td>When Group B moved to Deferred (until Jul-10), and Group A remains Deferred (until Jul-15), the VI remains in Deferred (until Jul-15).</td>
</tr>
<tr>
<td>Original VI state: <strong>Deferred</strong> &gt; (until July 15)</td>
<td></td>
</tr>
</tbody>
</table>

Vulnerable item age calculation and display

Starting with version 10.0, the age of vulnerable items (VIs) is displayed in the Vulnerability Response application with more detail.

**Overview**

Starting with version 10.0, the vulnerable item (VI) age is displayed in Days/Hours/Minutes format in the Age column on the Vulnerable Items list view, and in the
Age and Age closed fields on VI (VIT) records. Age displayed in more significant digits may help you more accurately perform the following activities:

- Configure rules in the Auto Delete Rules module to target and delete specific VI records by Days/Hours/Minutes. Removing records with more accuracy may increase your performance, especially if you have a very large number of VI records in your instance.
- View reports with more specific details in the Performance Analytics for the Vulnerability Response application.
- Create filters that identify only the VIs you want.
- Prune list views to display only the VIs you want.
- Dot-walk more easily.

Prior to v10.0, a scheduled job calculated age and updated all active VIs. In instances with very large numbers of VI records, this process could be slow and negatively impact performance. Starting with v10.0, VI age is calculated more efficiently on-demand and displayed with more significant digits with an enhanced Age column. The enhanced Age column is automatically added when you install or upgrade the Vulnerability Response application.

Note: If you perform an upgrade to v10.0 and the VI age is not displayed in the Vulnerable Items list view and in the Age and Age closed fields on active VI (VIT) records in Days/Hours/Minutes (9 Days, 18 Hours, 29 Minutes) format, the age column is not current in your instance. For more information about how to resolve this issue after an upgrade, see KB0749231.

The age column and fields are not editable. A vulnerability manager with the sn_vul.vulnerability_read permission or the Vulnerability admin persona can view this value, and IT remediation owners with the sn_vul.remediation_owner role can view it on records assigned to them.

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

VI age is displayed as shown in the following images.

**Vulnerable items list**

As shown in the following figure, on the Vulnerable Items list view, Age is displayed in the Age column in Days/Hours/Minutes (21 Days 17 Hours 17
minutes) only for active VIs. Active VIs are VIs in any states other than ‘Closed’. This age value represents the number of days the VI has been active.

The age is not displayed for VIs in the ‘Closed’ state. For VIs previously in a ‘Closed’ state and then reopened, the value represents the number of days the VI has been active since the date it was last opened.

### Age on VI records

On the VI records, the value of Age column in the list view is visible for active VIs in the Age field.

The value of the Age column is not displayed for VI records in the ‘Closed’ state.

### Age on the Vulnerable items list and VI records when a VI is updated

When a VI is in the ‘Closed’ state, the Age field is not displayed. When the VI transitions to ‘Closed’, the value in number of days from the Age column is displayed in the Aged closed field (9) as shown in the following figure. This value represents the number of days the VI was active before it transitioned to ‘Closed.’ For example, in the following image, this VI was active for 9 days, 18
hours, and 29 minutes, but only the number of days (9) is displayed on the closed record.

If this VI is reopened, when the VI state transitions back to ‘Open’, the Age closed field is reset to 0. Because the VI is active again, the age in Days/Hours/Minutes is displayed in the list view in the Age column and on the Age field on the VIT.

**Vulnerability Response calculators and vulnerability calculator rules**

Vulnerability calculators automate calculating initial values for the fields on vulnerable items. The condition for each calculator is evaluated in order, and the first matching calculator is used.

**Vulnerability Calculators**
The Vulnerability Response base system includes two vulnerability calculators that set the base **Risk Score** on the vulnerable item.

- **Default Risk Calculator**
- **Vulnerability Severity**

Vulnerability calculators can be built to prioritize and rate the impact of vulnerable items based on any criteria by using condition filters. Whether it is the business impact of the vulnerability, the class of the configuration item (CI), or the age of the vulnerable item, you can create additional vulnerability
calculators to set other fields on vulnerable items. Or you can customize the existing vulnerability calculators. A calculator can be written to reflect any set of priorities. See Create a Vulnerability Response calculator and Filtering within Vulnerability Response for more information.

Each calculator contains a list of calculator rules, with a condition determining when to apply it. When the calculator is run, the condition for each calculator rule is evaluated in order, and the first matching calculator rule is used.

The **Vulnerability Severity** calculator calculates **Risk Score** for vulnerable items using the normalized vulnerability severity.

> **Note:** Only one calculator per target field (Risk Score) can be active at a time. **Vulnerability Severity** is disabled by default.

All enabled vulnerability calculators set the selected fields each time a vulnerable item is created, when an associated CI or vulnerability changes, or when the **Calculate Risk Score** related link in a vulnerable item is used. As an example, the Risk Score is automatically updated on vulnerable item records when the severity value is updated on a vulnerability that is imported. After a vulnerability import has updated a vulnerability score, the recalculate flag is enabled for that vulnerability. The risk scores for the vulnerable items that have the recalculate flag enabled (true) with that vulnerability are recalculated.

From an existing vulnerable item, if you click the **Calculate Risk Score** related link and either of the calculators is enabled, the **Risk Score** field in the vulnerable item is updated.

> **Note:** The **Calculate Risk Score** related link is only visible when at least one vulnerability calculator is enabled.

**Vulnerability Calculator Rules**

The base system **Default Risk Calculator** calculator contains the **Default Risk Rule** rule, a specialized vulnerability calculator rule called a **Risk Rule**. It calculates **Risk Score** based on multiple values:

- Vulnerability severity
- Exploit information,
- Criticality
- External exposure of the CI with the vulnerability

You can adjust the values to use in the **Default Risk Rule** and how much weight to give each of these values. Weights are used to adjust how much each element counts when setting the base **Risk Score**.
Starting with v14.0 of Vulnerability Response, you can customize the criteria for the default risk rule. For more information, see .

Assigning a weightage percentage

Starting with v14.0 of Vulnerability Response, you can also assign weightage percentage (0-100) at the field value level, for example, you can assign a weightage percentage to each level of Severity (None to Critical).

If the severity weightage is 50 for the risk rule, and the following weightage values are assigned for the Severity level:

<table>
<thead>
<tr>
<th>Vulnerability severity</th>
<th>Risk score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>100</td>
</tr>
<tr>
<td>High</td>
<td>50</td>
</tr>
<tr>
<td>Medium</td>
<td>20</td>
</tr>
<tr>
<td>None</td>
<td>0</td>
</tr>
</tbody>
</table>

If the severity is critical, the equivalent weightage is 50. If the severity is high, the equivalent weightage is 25, and if the severity is medium, the equivalent weightage is 10. If the severity is None, the equivalent weightage is 0. For more information, see the .

Vulnerability calculator rule settings

Each rule has an Order setting however, the first one to match the conditions updates the Risk score field in the vulnerable item. For more information on vulnerability calculator rule settings, see Create a Vulnerability Response calculator. Non-scripted calculator rules typically create less of a performance impact than scripted calculator rules.

The base system Vulnerability Severity calculator contains calculator rules that assign each level of severity (None to Critical) a value (0-100) for Risk Score based on severity. Unknown Severity is automatically assigned a risk score of 100. These values can be adjusted and, like Default Risk Calculator, new calculator rules or new risk rules can be created.

**Tenable Vulnerability Integration and the Tenable Risk Rule**

Starting with v12.1 of Vulnerability Response, the Tenable Risk Rule is available. The Vulnerability Priority Rating (VPR) is an attribute from the Tenable product that is imported and used with a new default risk calculator in Vulnerability Response. The Tenable Risk Rule is installed with the Tenable Vulnerability Integration application as part of the Default Risk Calculator in the Vulnerability Calculators from Vulnerability Response.
This risk rule is disabled by default. See Configure the Tenable Vulnerability Integration using Setup Assistant.

Vulnerability Response Rollup Calculators

Configure how the cumulative risk score is computed for vulnerability groups and imported vulnerabilities with the vulnerability rollup calculators.

Vulnerability Response Rollup Calculators

Use the vulnerability rollup calculators to configure how the cumulative risk score is computed for vulnerability groups and imported vulnerabilities. Two rollup calculators are shipped with the base system:

- **Vulnerability Group Rollup**: Rolls up the risk scores for all vulnerable items in a vulnerability group, to provide an overall risk score for the entire group of vulnerable items.

- **Vulnerability Entry Rollup**: Rolls up the risk scores for all vulnerable items with the same vulnerability entry, to provide an overall risk score for the vulnerability entry.

Configure the rollup calculator to specify how much weight to give each of those computed values in setting the cumulative risk score. The higher the weight, the more that value is used to determine the rolled up risk score in the vulnerability or vulnerability group.

⚠️ **Note**: When Include deferred is selected, all deferred vulnerable items are included in the rollup calculation for the vulnerable group. Be sure that you understand the impact on the total calculation before selecting this option.

Rollup calculators are scheduled jobs that run every 15 minutes to pick up changes. These scheduled jobs also calculate cumulative values for the number of VIs, maximum risk score, as well as, remediation target date, and status for vulnerability group.

⚠️ **Note**: Calculated values for vulnerability entries do not include remediation target data.
In the Vulnerability rollup calculator example, the formula for determining the Vulnerability Group Risk Score is:

\[(\text{Maximum risk score/100}) \times 80 + (\text{Average risk score/100}) \times 5 + (\text{factor} \times 15)\]

The factor is determined as follows:

<table>
<thead>
<tr>
<th>VI count</th>
<th>Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;10</td>
<td>0.2</td>
</tr>
<tr>
<td>1 - 99</td>
<td>0.4</td>
</tr>
<tr>
<td>100 - 1000</td>
<td>0.6</td>
</tr>
<tr>
<td>1001 - 9999</td>
<td>0.8</td>
</tr>
<tr>
<td>&gt; 10000</td>
<td>1</td>
</tr>
</tbody>
</table>

So, for vulnerability group, VUL324567, with three vulnerable item Risk scores:
- 30 (Ignored)
- 40 (Average risk score)
- 50 (Maximum risk score)

the vulnerability group, VUL32456, Risk Score would be 45

\[(50/100) \times 80 + (40/100) \times 5 + 0.2 \times 15 = 40 + 2 + 3 = 45\]
Vulnerability Response vulnerable item detections from third-party integrations

Starting with v10.0, view all of the information that is gathered by third-party scans in your Now Platform® instance. View the returned results of the scans on detection and vulnerable item (VI) records in your instance as these results are viewed on the scanners.

Overview

Starting with v10.0, the Vulnerability Response application supports third-party Integrations that retrieve vulnerable item data from your enterprise environment. Detailed data about detections, that is, single, distinct occurrences of vulnerabilities as reported by the scanners of your third-party integrations, are imported and displayed on both the detection and the vulnerable item records in your Now Platform instance.

Third-party Integrations retrieve vulnerable item detection data. Detections are distinct occurrences of vulnerabilities as reported by the scanners. Detection data are paired with vulnerable items and VI state is updated based on the state of the detections. If a VI is not found, a new one is created. Detections are only opened or closed by data found directly by a scanner.

Prior to v10.0 vulnerable item detections, the relationship between a CI (asset) in your environment and an imported vulnerability from a third-party scanner created a unique vulnerable item in your Now Platform instance. Starting with v10.0, the granularity of the original data provided by the scanner is preserved. With detections, the detection data is paired with vulnerable items. During an ingestion, if a vulnerable item is not found, a new VI is created.

Supported versions of Vulnerability Response

Vulnerable item detections are supported by the Vulnerability Response application for v10.0 for the Madrid, New York, and Orlando family releases. For more information about installing or updating the Vulnerability Response application to v10.0, see Install and configure Vulnerability Response.

Supported third-party integrations

A supported third-party integration with your Vulnerability Response application is required for vulnerable item detections. Starting with v10.0, the following third-party integrations are supported by the Vulnerability Response application for vulnerable item detections:

• Qualys Host Detection Integration
• Rapid7 Data Warehouse:
Vulnerable Item Integration
Vulnerable Item Resolution Integration

• Rapid7# Vulnerable Item Resolution Integration (InsightVM)
  • Insight VM integration
  • Vulnerable Item Integration - API

These third-party integrations are available with a separate subscription from the ServiceNow Store. For more information about these integrations, see Vulnerability Response integrations and Security Operations and the ServiceNow Store for more information about obtaining entitlement.

To verify that your third-party scanner is configured for import, see Install and configure the Rapid7 Integration for Security Operations application and Install the Qualys Vulnerability Integration.

Key terms for vulnerable item detections

Vulnerability
Data about weaknesses in software, operating systems, and assets imported from internal and external sources. This data is imported and compared to existing assets (configuration items, CIs) listed in the CMDB.

Vulnerable item
A vulnerable item is created or updated when an imported vulnerability matches a CI in the CMDB.

Detection
A single, distinct occurrence of a vulnerability as reported by a scanner referred to as a Vulnerable Item Detection within the Now Platform environment. A detection includes enriched data about a vulnerability and any corresponding vulnerable items. This data is displayed on the Detection record (VID#) and the vulnerable item list view that includes the following details:

• First found (data)
• Last found (date)
• DNS name
• Net BIOS name
• IP address
• Port
• Protocol
• Proof
• SSL
• Times found

Detection key

A hashed combination of fields that provided a way to identify and tie a detection to a vulnerable item. Starting with v14.0 of Vulnerability Response, detection keys are integration-specific.

Detection key configurations

<table>
<thead>
<tr>
<th>Scanner</th>
<th>Vulnerability</th>
<th>Port</th>
<th>Protocol</th>
<th>Asset ID</th>
<th>Proof</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualys</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Tenable</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Rapid7</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (it is not case sensitive)</td>
</tr>
</tbody>
</table>

Note: If the detection key is not specified, or for versions earlier than Vulnerability Response 14.0, the detection key is a combination of vulnerability entry, port, protocol, asset ID, and proof.

De dup

The process used by the Vulnerability Response application of collapsing of individual detections into a single VI when the data meets certain hard-coded criteria.

VI External ID

The value stored in the External ID field of the VI table. This value is a hash comprised of the combination of keys within a VI that represents what makes it unique within the application. It is composed of a CI and a vulnerable entry.

Reopen resolved vulnerable items not closed by scans

Starting with v10.3, vulnerable items set to 'Resolved' in your Now Platform instance but not transitioned to 'Closed/Fixed' by the subsequent integration runs are reopened if they are detected during rescans.
For Rapid7 detections, an option is now available on the Rapid7 configuration page in your instance to reopen resolved VIs by age. If enabled, VIs set to 'Resolved' but then not transitioned to 'Closed/Fixed' by subsequent scans transition back to 'Open' after the number of days you enter.

For Qualys detections, if the scanner continues to find VIs that were set to 'Resolved' but then not transitioned to 'Closed/Fixed' by subsequent scans, these VIs move back to 'Open' when the last found date is later than the Resolved date.

**View detection data**

You view the data imported from vulnerable item detections on the VI record. For more information, see View Vulnerability Response vulnerable item detection data and Verify Vulnerability Response vulnerable item detection data on integration run (VINTRUN) records.

**Vulnerability Response remediation target rules**

Remediation target rules define the expected timeframe for remediating a vulnerable items (VI), much like SLAs provide a timeframe for remediating the vulnerability itself. For example, if an asset contains PCI data (credit card data) then the vulnerability on that item needs to be fixed within 30 days according to PCI DSS.

Vulnerability managers can create remediation target rules by defining:

- The remediation target
- The reminder target
- The reminder and notification recipients — Who should be notified when the vulnerable items (VIs) are past the reminder or remediation target date and have not been remediated.

Vulnerability analysts and managers can see the remediation target date in the vulnerability item form and list views, as long as the vulnerable items are not in **Deferred, Resolved,** or **Closed** state. Starting with version 12.0, remediation target rules are run on import and rerun if a VI is reopened.

The **Remediation target date** is color-coded on the VI list view as dots, as follows:

- Vulnerable items that have not reached their notification date are shown in green.
- Vulnerable items approaching the remediation target date are shown in orange.
- Vulnerable items past the remediation target date are shown in red.
A summary email, per remediation target rule, is sent when one or more VIs are either approaching their remediation target date or the remediation target date has passed.

Remediation target rules can be deactivated or deleted

Starting with v12.0, when a rule is deactivated, the current remediation target dates for the VIs it was applied to are cleared. If a VI satisfies any active rule that rule is applied, otherwise the VI has no rule or target date, and its status is **No Target**.

When rules are deleted, the Remediation target date and related fields on closed, deferred or resolved VIs are preserved. The Remediation target date and related fields on non-closed VIs are cleared and any dependent rules are reapplied.

Prior to v12.0, Remediation target rules could be deactivated but not deleted. When a rule was deactivated, it is no longer applied to new vulnerable items. However, the remediation target rule scheduled job, **Evaluate remediation targets** continued tracking existing vulnerable items, to which the rule was applied. If the rules are subsequently reactivated, any **Open** VI with an empty **Remediation Target Date** field was evaluated against the rules. This includes VIs created while the rules were deactivated.

Remediation target rule scenario

- When multiple remediation target rules are applied to the same vulnerable item, the most restrictive rule is applied.

  Note: Remediation targets are calculated from the Last Opened date plus the number of days (measured as 24-hour increments).

For example, if a vulnerable item meets the condition for two remediation target rules:

**Scenario:** Vulnerable item last opened on 03/01/2018 at 10:00:00.

- Remediation target rule 1: Last opened on 03/07/2018; remediation target is 15 days since it was last opened; calculated remediation target date is 03/16/2018 10:00:00.
- Remediation target rule 2: Last opened on 03/10/2018; remediation target is 10 days since it was last opened; calculated remediation target date is 03/11/2018 10:00:00.

In this scenario, the Remediation target rule 2 applies to the vulnerable item since it has the more restrictive date. 10 days since the vulnerable item was first identified versus 15 days.
Note: Once the Remediation target rule is defined, remediation target
dates are calculated by the *Evaluate remediation targets* scheduled job.

About the Evaluate remediation targets scheduled job

*Evaluate remediation targets* runs once at 4:00:00 daily.

It iterates through all active vulnerability rules, starting with those rules with the
earliest remediation target date. It looks at all vulnerable items that:

- Are not in a **Closed**, **Deferred**, or **Resolved** state.
- Have no remediation target date.
- Have a remediation target date that is later than the date in the remediation
target rule.

*Evaluate remediation targets* adds a remediation target date, if one does
not exist, or if a rule results in an earlier date than the one in the record, it
updates the existing target date. Finally, it updates the **Remediation target** and
**Remediation status** fields in the vulnerable item form.

Once the *Evaluate remediation targets* runs, available notifications are sent.
Starting with v12.0, *Evaluate remediation targets* clears the remediation fields on
the VI and stops sending notifications.

Reapplying remediation target rules

Starting with v12.0, when you change a remediation target rule, use the **Apply
Changes** button on the Remediation Target Rules list page to rerun all the
changed rules on all active Open VIs except those in the **Closed**, **Deferred** or
**Resolved** state. Depending on how many VIs you have, this may take time.

Note:

If the scheduled job, *Evaluate remediation targets* is running, you cannot
initiate a reapply process. However, if a reapply process is already running,
and the scheduled job it triggered, they run in parallel.

The reapply processes in Vulnerability Response and Application
Vulnerability Response are independent and can run in parallel.

Related information

- Create or edit Vulnerability Response remediation target rules
- View the remediation target status of a Vulnerability Response vulnerable item
- Create or edit remediation target notifications
Vulnerability Solution Management

Automatically correlate your vulnerability findings with the solutions that address them. Easily view and identify the remediation actions of highest impact to your organization and orchestrate their completion.

Vulnerability Solution Management

Security and IT teams often spend a significant amount of time researching vulnerability findings in order to identify the most effective treatments for their environment. Given the volume and complexity of vulnerabilities in large organizations, translating vulnerability findings into remediation tasks is a manual, tedious, and error-prone process.

With Vulnerability Solution Management, you can automatically correlate your vulnerability findings with the solutions that remediate them. Identify the software patches, configuration updates, and other controls that have the highest impact for your organization without the manual overhead.

Vulnerability Solution Management requirements

Vulnerability Solution Management is a feature available within the Vulnerability Response application. Vulnerability Solution Management requires a separate subscription.

For more information about getting entitlements for applications from the ServiceNow Store, see Get entitlement for a Security Operations product or application. See Install the Solution Management for Vulnerability Response application for more information about installing the application after you have downloaded it onto your instance.

After it is installed, Vulnerability Solution Management provides you access to Microsoft Security Response Center data from within Vulnerability Response. Starting with v10.3 of Vulnerability Response, the Red Hat solution data is also available.

Note:

You can configure both solution applications from within Setup Assistant. See Configuring Vulnerability Response using the Setup Assistant.

See Understanding the Microsoft Security Response Center Solution Integration and Understanding the Red Hat Solution Integration for more information on the imported solutions.

Available versions

For the most current version of Vulnerability Solution Management, verify you have the most current version of Vulnerability Response installed.
Understanding solutions and supersedence

A superseded update is a complete replacement of a previous release or releases. For example, a hotfix update may be superseded by a Service Pack. Solutions are related to vulnerabilities. Solutions can also relate to other solutions in a supersedence chain. Solutions address vulnerabilities in preceding solutions as well since they’re cumulative. Vulnerability Solution Management automatically associates vulnerabilities from preceding solutions with superseding solutions. If an older vulnerability is found, any higher superseding solution can address it, but the highest supersedence solution is preferred, since it is the most cumulative.

Potential versus Preferred Solutions

A potential solution is one that could address a vulnerability. Vulnerabilities often have many potential solutions. A preferred solution is the single solution targeted for remediating a vulnerability or vulnerable item (VI). It communicates intention, and enables more detailed deployment metrics.

Preferred Solutions

Vulnerability Solution Management automatically sets the most effective solution (Preferred Solution) for the detected vulnerability based on highest-supersedence when only one highest-supersedence solution exists. If more than one highest-supersedence exists for the vulnerability, no value is set. In Vulnerability Response, Preferred Solution is the Microsoft Security Response Center or Red Hat solution with the highest supersedence derived from the solutions associated with the vulnerability.

Preferred Solution values can be set on the vulnerable item or the vulnerability. When set directly on the vulnerability, all vulnerable items associated with
the vulnerability inherit that solution. Change the **Preferred Solution** values for multiple vulnerable items using the bulk edit feature. When bulk edited, only the **Preferred Solution** on the vulnerable item is updated since setting the **Preferred solution** at the vulnerability entry level would set the **Preferred solution** for all new VIs going forward. Bulk editing only applies to current vulnerable items.

**Note:** If multiple highest-supersedence solutions exist for a vulnerability, **Preferred Solution** values at the vulnerability level are cleared, since that solution depends on the affected asset. When multiple highest-supersedence solutions exist for a vulnerability, set a **Preferred Solution** on the vulnerable item. You can set a different solution using the **Lookup** list on the **Vulnerable Item** form.

All preferred solutions for the vulnerable items in a vulnerability group are in a related list on the **Vulnerability Group** form.

Not all solution imports result in full data refreshes. The supersedence process updates when:

- A vulnerable item is created.
- Data has changed on an active VI.
- New solution data was released since last import.

**What does Vulnerability Solution Management do?**

- Automatically associates new vulnerable items and vulnerability groups with solutions during Microsoft Security Response Center Solution Integration and Red Hat Solution Integration import. MSRC solutions are associated with the latest bulletin the solution appears in.
- Automatically associates vulnerable items and vulnerability groups with solutions when vulnerability records are associated manually with solutions.

**Note:** Vulnerable items manually re-assigned to another solution are not automatically updated with solution changes at the vulnerability level.

- MSRC: Creates supersedence chains during import that you can view in the solution's related list.
- Indicates whether a solution is a highest-supersedence solution or not.
- Lists the Solution **Risk score** associated with each solution to provide you with the biggest opportunities for risk reduction.

- Maintains **Remediation Status** for solutions on **Third-party Vulnerability Entries**, **Vulnerability Groups**, and **Vulnerability Solution** records so you can track remediation progress.
It contains:

- Vulnerable item counts by percent remediated, for those VIs with Preferred Solutions, with and without those VIs in the Deferred state.
- Configuration Item (CI) counts by percent remediated, for those VIs with Preferred Solutions, with and without those VIs in the Deferred state.
- Vulnerable item counts by percent remediated, for those VIs with Potential Solutions, with and without those VIs in the Deferred state.
- Configuration Item counts by percent remediated, for those VIs with Preferred Solutions, with and without those VIs in the Deferred state.

**What can you do with Vulnerability Solution Management?**

- Create, update, view, or delete solutions associated with vulnerabilities, so that you can track vulnerability solutions that are not covered by third-party solution content.
- Associate third-party vulnerabilities and NVD entries with a solution record.
- Remove and reassociate vulnerable items and vulnerability groups with a solution.
- View the **Preferred Solution** applicable to a given vulnerability on the vulnerability and vulnerable item forms.
- View a **Preferred Solutions** related list on vulnerability group forms that lists all the solutions that have been preferred by at least one active VI within that group.
- View the **Remediation Status** details on a solution that show the risk reduction associated with deploying the **Preferred Solution** on vulnerability, vulnerable item, vulnerability group, and solution forms.
- View vulnerabilities applicable to a given solution on the solution form.
- MSRC: View the superseding solutions for a given solution on a vulnerability, to find the latest update to deploy, or an earlier, more focused, efficient update.
- View lists of solutions sorted for different characteristics.
  - All: Solutions sorted by Date published and Number.
  - MSRC: Highest Supersedence: Solutions with active, non-deferred vulnerable items. Sorted by **Highest supersedence**, **Date published**, and **Number**.
  - With Vulnerable Items: Solutions with active, non-deferred vulnerable items. Sorted by **Highest supersedence** or **Preferred, Risk Score**, and **Number**. If deployed, the top entries in the list provide the largest risk reduction for the assets in your environment.
Solution record Risk score and Risk rating

Note: The Solution record Risk score and Risk rating are distinct from those fields used for vulnerabilities, vulnerable items, and vulnerability groups.

The Solution record Risk score is a weighted calculation based on the vulnerable item Risk score and a count of active vulnerable items with this solution as their Potential Solution. Solution Risk score provides an estimation of the reduction in risk that the solution is expected to accomplish.

Solution record Risk score is calculated as follows:

- It starts by taking 85% of the highest or maximum Risk score of an active vulnerable item with that potential solution.
- Solution record Risk score then tabulates the total number of vulnerable items with that potential solution. For each range of the number of vulnerable items, it adds some points and arrives at a total.
  - 0–09 vulnerable items adds no points
  - 10–99 vulnerable items adds 5 points
  - 100–999 vulnerable items adds 10 points
  - 1000 and beyond vulnerable items adds 15 points

For example, for a vulnerable item Risk score of 80, the Solution record Risk score would start at 68. If there were 200 active total vulnerable items with that potential solution, then the final Solution Risk score would be 78.

The Solution record Risk rating separates the Solution record Risk score into ranges from Critical to None. Solution Risk rating rates the risk reduction for the vulnerable items that this solution remediates.

Risk ratings separate the resulting Solution Risk score into the following ranges:

- 1 — Critical (90+ Solution Risk score)
- 2 — High (70-89 Solution record Risk score)
- 3 — Medium (30-69 Solution record Risk score)
- 4 — Low (1-29 Solution record Risk score)
- 5 — None (0 Solution record Risk score)

Use Cases

View the status deployment progress of a current patch cycle using the highest-supersedence module, sorted by date.
View highest value solutions using the With Vulnerable Items module, sorted by risk score.

Solution lists communicate key solution details, risk scores, and deployment metrics. Use Risk score and active VI counts for prioritization. See which solutions in the current patch cycle are not progressing, possibly an indication of a missed deployment prerequisite.

**Note:** Add \%Vi remediated(percent_nd_pref_vis_remediated) from the Personalize List Columns menu for remediation progress on the Vulnerability Solutions form.

Understanding the Microsoft Security Response Center Solution Integration

Review and implement proposed remediation solutions provided by the Microsoft Security Response Center Solution Integration.

Microsoft Security Response Center Solution Integration is included in the Vulnerability Solution Management feature of Vulnerability Response. Vulnerability Solution Management is available by separate subscription. See Vulnerability Solution Management for more information on how Vulnerability Response incorporates solutions.

Microsoft Security Response Center investigates reports of security vulnerabilities affecting Microsoft products and services, and provides solution information to help manage security risks. Solutions are known remediations imported into your Microsoft Security Response Center Solution Integration from the Microsoft Security Response Center product.

The Microsoft Security Response Center Solution Integration contains entry points to Microsoft Security Response Center product, invoked as scheduled jobs. Scheduled jobs simplify the vulnerability remediation lifecycle by keeping the instance synchronized with other vulnerability management systems. Scheduled jobs run automatically and in the order specified. You can also execute individual scheduled jobs manually.

There is a configured run-as user for each integration record. The default value for this user is **VR.System**. Do not change this value.

Available versions for Paris

For the most current version of Vulnerability Solution Management and Microsoft Security Response Center solutions, verify you have the most current version of Vulnerability Response installed.

For more information about installing Vulnerability Solution Management, Install the Solution Management for Vulnerability Response application.
<table>
<thead>
<tr>
<th>Release version of Vulnerability Response</th>
<th>Version of Vulnerability Solution Management</th>
<th>Release Notes</th>
</tr>
</thead>
</table>
For compatibility information, see KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes |

**Roles**

Microsoft Security Response Center Solution Integration tasks involve the following roles.

- v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated): Can read, write, and delete records.
- sn_vul.vulnerability_write: Can read and write records.
- sn_vul.vulnerability.read: Can read records.
- sn_vul.remediation_owner: Can read and write internal notes on records assigned to the remediation specialist group or individual. (Contained in the itil role.)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

**Microsoft Security Response Center Solution Integration**

To view the Microsoft Security Response Center Solution Integration, navigate to Vulnerability Response > Administration > Integrations.

The following integration is included in the base system.
Microsoft Security Response Center Solution Integration

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Security Response Center Solution Integration</td>
<td>Retrieves solutions and National Vulnerability Database (NVD) mapping to associate solutions with vulnerabilities, vulnerable items, and vulnerability groups.</td>
</tr>
</tbody>
</table>

Note: The Microsoft Security Response Center Solution Integration does not provide solutions prior to 2016.

Solutions
To view imported solutions in a list, see View a solution.

Understanding the Red Hat Solution Integration
Starting with V10.3 of Vulnerability Response, you can review and implement proposed remediation solutions provided by the Red Hat Solution Integration.

Red Hat Solution Integration is included in the Vulnerability Solution Management feature of Vulnerability Response, available by separate subscription. See Vulnerability Solution Management for more information on how Vulnerability Response incorporates solutions.

Red Hat Solution Integration investigates reports of security vulnerabilities affecting Red Hat products and services, and provides solution information to help manage security risks. Solutions known as remediations are imported into your Red Hat Solution Integration from Red Hat.

Red Hat Solution Integration contains entry points to the Red Hat product, invoked as a scheduled job. The scheduled job simplifies the vulnerability remediation life cycle by keeping the instance synchronized with other vulnerability management systems. It runs automatically. You can also execute the scheduled job manually.

There is a configured run-as user for each integration record. The default value for this user is VR.System. Do not change this value.

Available versions for Paris
For the most current version of Vulnerability Solution Management and Red Hat solutions, verify you have the most current version of Vulnerability Response installed.

For more information about installing Vulnerability Solution Management, Install the Solution Management for Vulnerability Response application.
Roles

Red Hat Solution Integration tasks involve the following role.

- sn_vul.configure_rhsa_integration

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Red Hat Solution Integration

To view the Red Hat Solution Integration, navigate to Vulnerability Response > Administration > Integrations.

The following integration is included in the base system.

### Red Hat integration

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Solution Integration</td>
<td>Retrieves solutions and National Vulnerability Database (NVD) mapping to associate solutions with vulnerabilities, vulnerable items, and vulnerability groups.</td>
</tr>
</tbody>
</table>

Solutions

To view imported solutions in a list, see View a solution.
Exception Management overview

When your organization can’t comply with a published vulnerability management or security policy, standard, or guideline, you can request an exception. Exception management entails requesting, reviewing, approving, or rejecting exceptions to a vulnerable item (VI) or vulnerability group (VG) that cannot be remediated according to the policy.

Some vulnerabilities might not have an existing patch, fix, or solution. When an exception is approved, it also means that you’re accepting a risk because you’re acknowledging and agreeing to the consequences of not remediating the vulnerability.

Life cycle of an exception

Definition of an exception

An exception is a request to defer the remediation of a VI or VG for a specified period. For example, as a remediation owner, you can request an exception if a patch is not available for a machine.

Requesting an exception

As the remediation owner, you can ask for an exemption for a VI or VG using the exception management process. After the exception approver approves this request, the VI or VG moves to a Deferred state.

Approving an exception request

VIs or VGs that can’t be remediated immediately are reviewed by vulnerability analysts, assessed for risk, and approved for deferral until they can be remediated. Approving an exception request can be a two-level workflow. If only the first-level approver is present, the exception can be requested and approved. However, if there’s no first-level approver, an exception can’t be requested. See Add an exception approver for more information.

Once an exception request for a VI or VG is approved, you can perform the following actions:

• Reopen
• Delete
• Update the Assignment to or Assignment groups fields

Note: Rejection comments are shown in the Work notes for a VI or VG. If an exception request is not approved, this VI or VG reverts to its previous state.

Tracking an exception request
After raising the exception, you can track its status by using the **State Change Approvals** tab of the VI or VG. If an action is taken on a VG, you can't track the status of the individual VIs in that VG.

**Expiry of an exception request**

When an exception request for a particular VI or VG expires, the impacted VI or VG reverts to its **Open** state.

### Exception management approval process

<table>
<thead>
<tr>
<th>Remediaion Owner</th>
<th>Exception Approver L1</th>
<th>Exception Approver L2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>State:</strong> Open</td>
<td><strong>Assess Exception requested?</strong></td>
<td><strong>Assess Exception requested?</strong></td>
</tr>
<tr>
<td>Under Investigation</td>
<td>Accepts</td>
<td>Rejects</td>
</tr>
<tr>
<td>Awaiting Implementation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reverts</td>
<td>Changes to previous state</td>
</tr>
<tr>
<td></td>
<td>to 'In Review'</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Accepts</td>
<td></td>
</tr>
<tr>
<td>VIs/VG state changes to 'In Review'</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If a single VI or all the VIs in a VG pass in the next scan, then the VIs and, where applicable, the VG **State** field changes to **Closed** with the substate **Fixed**.

**Exception rules overview**

Starting with version 12.0, exception rules for Vulnerability Response enable you to automate the deferral process for vulnerable items (VIs). You can request an exception for the vulnerable items (VIs) that can't be remediated or deferred immediately, by identifying the impacted vulnerabilities, configuration items (CIs), or VIs. By automating the VI deferral process, you can defer the matching VIs based on the rule when the system identifies them.

**Using exception rules in your organization**

Use exception rules to automatically defer new and existing VIs for a specific period if they match the approved rule condition. Automation minimizes the risk of missing service level agreements and makes it easier to manage multiple items, because you are eliminating manual intervention.
Deferral rules support ordering, that is, the rule with the highest priority is run first. When a high-priority rule is applied on a VI, no subsequent rules are applied on it again even if the condition matches the VI.

**Note:** You can only create rules if you select Vulnerability Response in the Exception Management configuration. For details, see Configure Exception Management for a vulnerability response.

The life cycle of an exception rule is as follows:

- Creating an exception rule
- Approving an exception rule request
- Activating an exception rule
- Deferring an exception rule
- Expiry of an exception rule

**Creating an exception rule**

You can create an exception rule to automatically defer the VIs that match the defined conditions for the specified period. After you create an exception rule, submit it for approval.

**Approving an exception rule request**

Approving an exception rule request is a two-level process. If only the first-level approver is present, the exception rule can be assessed and approved by a single approval. However, if there's no first-level approver, an exception rule approval can't be approved. After the rule is approved, a vulnerability group (VG) is created. See Approve an exception rule request for more information.

After an exception rule request is approved, you can perform the following actions:

- Cancel
- Delete

**Activating an exception rule**

After an exception rule is approved, a VG is created in a Deferred state by default. Starting from the "Valid from" date, the exception rule runs on all the VIs that are created and also on the ones that are moved from the Closed to the Open state.

**Note:** If you enable the Execute on existing data option, a scheduled job runs once on the existing data on the "Valid from" date.
Deferring an exception rule

You can defer VIs that match the conditions defined in this exception rule, up to the “Deferred until” date that is defined for the rule. On this date, the VG that you created for the exception rule is closed and all the VIs in this group move back to the Open state. Group rules are applied on them again to allocate them to the required VGs.

Expiry of an exception rule

After the exception rule expires, it no longer runs on new or reopened VIs. The associated VG remains in the Deferred state until the "Deferred until" date.

Exception rules work flow

Exception rules for Vulnerability Response

- **Start**
  - Admin creates a rule to request an exception for a specific condition (using a rule/condition builder) for a VI.
  - The rule goes to the approver with state In review.
  - Approver assesses the rule.
    - Rejects
      - The state of the rule changes to Rejected.
    - Approves
      - The state of the rule changes to Approved.
      - The rule is applied from the “Valid from” date.

- **Yes**
  - If user selects to run the rule on existing data.
    - Once the rule becomes active on the “Valid from” date, a VG with the provided details is created in the Deferred state.

- **No**
  - The rule will run on all the newly created/reopened VIs from “Valid from” date to “Valid to” date. The matching VIs will automatically get deferred and placed in this VG.
  - On the “Valid to” date the rule expires and stops running on the new VIs.
  - The exception expires on the “Deferred until” date. The VG is closed and the VIs in this VG move to the Open state. Group rules are applied again on these VIs.

- **End**
  - Run the exception rules on the existing data based on user input. The VIs matching the condition are also moved to this VG and state changes to Deferred.

**VI = Vulnerability Item**
**VG = Vulnerability Group**
False Positive overview
A false positive is a condition wherein the scanner reports that a vulnerability exists in the system, but in reality there is no vulnerability. There can be multiple reasons like incorrect classification, improper logic or algorithm in the scanner. The remediation owner can mark vulnerable items (VIs) or vulnerability groups (VGs) as false positives.

Life cycle of a false positive

Meaning of false positive
The scanner sometime gives a warning, when in reality there is no vulnerability. For example, if a configuration item has been decommissioned but the scanner is still raising an issue related to it, mark it as a false positive.

Marking as a false positive
For details on marking a VI or VG as a false positive, see Mark as a false positive.

Working with the false positive
Once a VI or VG is marked as a false positive, the state is updated to Closed and the substate is changed to False Positive. The following actions can be performed:
• Reopen
• Delete
• Update the date in the Until field. This date is then used as the expiry date for the false positive.

Note: If not approved, the VI or VG reverts to its previous state.

Approving a false positive
The approver can approve the false positive from their approval workflow.

Reopening a false positive
A VI or VG in a false positive substate can be reopened anytime.

Tracking a false positive
Use the State Change Approvals section to track the status of the false positive. Once approved, the state of the VI or VG is updated to Closed and the reason is False Positive.

Expiry of a false positive
Only the false positive approver can set an Until date for the false positive, for the VI or VG to expire. Also, only false positives for which the approver has provided an Until date can expire. This date can be provided after the false positive is approved.

A false positive without an Until date is a permanent false positive. After the false positive expires, the state of the VI or VG moves back to Open.

**False positive approval process**

<table>
<thead>
<tr>
<th>Remediation Owner</th>
<th>Vulnerability Analyst</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start</strong></td>
<td></td>
</tr>
<tr>
<td><strong>State:</strong></td>
<td></td>
</tr>
<tr>
<td>Open</td>
<td></td>
</tr>
<tr>
<td>Under Investigation</td>
<td></td>
</tr>
<tr>
<td>Awaiting Implementation</td>
<td></td>
</tr>
<tr>
<td>Flag VIs/VG as False Positive</td>
<td></td>
</tr>
<tr>
<td>VIs/VG state changes to &quot;In Review&quot;</td>
<td></td>
</tr>
<tr>
<td>Provides a date on the VIs/VG form</td>
<td></td>
</tr>
<tr>
<td>When Date is over</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Limit the duration?</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
</tr>
<tr>
<td>VIs/VG state changes to &quot;Closed&quot; with sub-state as &quot;False Positive&quot;</td>
<td></td>
</tr>
<tr>
<td>Approves</td>
<td></td>
</tr>
<tr>
<td>Assess False Positive?</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>VIs/VG state changes to &quot;Open&quot;</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
</tr>
<tr>
<td>VIs/VG state changes to &quot;Closed&quot; with sub-state as &quot;False Positive&quot;</td>
<td></td>
</tr>
<tr>
<td>Rejects</td>
<td></td>
</tr>
<tr>
<td>Set the state and substate of VIs/VG to the previous state</td>
<td></td>
</tr>
</tbody>
</table>

The approval process is automatic if all VIs pass the next scan. The VIs auto-close regardless of the current state. The VIs or, where applicable, the VG **State** fields change to **Closed** with the substate **Fixed**.

**Change management for Vulnerability Response**

As an IT remediation owner, you can create and manage change requests (CHG) directly from vulnerability groups (VG) in the Vulnerability Response application. Change requests help you initiate and track change activities on your assets so that you can remediate your vulnerability groups and their corresponding vulnerable items.
Change requests and the vulnerability workflow

If you are not familiar with the Vulnerability Response application, for more information see Understanding the Vulnerability Response application.

The following image illustrates the flow of information for Vulnerability Response, from integration (scanner) set up through automated triage and into investigation.

Change requests and change management are part of the remediation process (Assess/Fix state) in the Vulnerability Response workflow shown in the following figure. During this phase, you might use change requests to initiate and track the remediation of vulnerabilities. You can create and manage change requests directly from the vulnerability group and list investigation and remediation tasks that include solutions for impacted assets for the configuration items (CI) in your CMDB.

When to use change requests in vulnerability response

As an IT remediation owner, you might create change requests from a vulnerability group if a manual and controlled process of any kind is required for modification or removal of supported configuration items (CIs) in your CMDB. Creating and managing change requests directly from a vulnerability group record helps you investigate and resolve vulnerabilities quickly. The VIs of a resolved vulnerability group can be scanned and verified during the next scheduled scan in your Now Platform and returned to the automated triage of the Vulnerability Response workflow. Manual interventions that might require change requests include the following examples:
• A software patch, fix, or other task by IT that is required on vulnerable items prior to VG resolution.
• You determine a subset of the vulnerable items in a vulnerability group requires further investigation or reassignment to another department.
• You determine that a subset of vulnerable items in a VG with a large set of vulnerable items can be moved into a new vulnerability group.
• You might associate a vulnerability group to an existing change request to avoid duplication of remediation tasks.

Types of change requests for a VG

The Vulnerability Response application utilizes the three types of service changes supported by the ITSM Change Management product on your Now Platform® instance — standard, emergency, and normal. The type of change you select determines which state model is invoked and the change process that must be followed. Change requests record the detailed information about the change, such as the reason of the change, the priority, the risk, the type of change, and the change category. See Change types.

As a Vulnerability Response IT remediation owner, you have the following options for creating normal, standard, and emergency change requests directly from a vulnerability group:

• You can create change requests that contain pre-populated information from the vulnerability group to streamline the process and save time.
• You can associate a vulnerability group to an existing change request to avoid creating duplicate change requests that share similar information and vulnerable items.
• Using a set of conditions, you can filter out a subset of vulnerable items and split a vulnerability group. The items that you select are automatically moved to a new VG.

You can filter vulnerable items using values from any fields from a vulnerability group and apply the change request to only those items that match your filter criteria.

Related information

Create a change request from a vulnerability group
Associate a vulnerability group to an existing change request
Split a vulnerability group
State synchronization between change requests and vulnerability groups
Software exposure assessment using Software Asset Management (SAM)

Use the ServiceNow® Exposure Assessment application to determine your total installed software count for a specific software package on your assets. When used with the ServiceNow® ITSM Software Asset Management application, evaluate your exposure, create vulnerable items, and manage remediation for the vulnerable software you discover.

Overview

Determine your exposure to vulnerable software by providing the vulnerable software information (publisher, product, edition and version) without using the Common Vulnerabilities and Exposures (CVE) database. Assess cases of a zero-day (current day) vulnerabilities to software for the following cases:

- When products do not yet have CVE data.
- When there is a lag between the time a vulnerability becomes publicly known and the CVE data with the vulnerability is updated in the NVD.
- When you learn about the vulnerability in-between the scheduled scans of your vulnerability scanner.

With the Exposure Assessment application, if you know the publisher and product for the vulnerable software, using the records that list the installed software in your network created by the SAM application, you can assess your exposure to potentially malicious software packages on-demand.

Knowing the scale of your exposure to this type of vulnerability permits you to proactively respond by implementing a red alert and uninstalling the software, or informing your security operations center (SOC) to look for a specific patch. You can create vulnerable items and assign tasks to the remediation specialist for further investigation remediation. View a vulnerability group (VG) list to verify that the vulnerable items you want are created and associated correctly to the VG.

The Exposure Assessment application for the Vulnerability Response application is compatible with the New York v10.0 and Orlando family releases.

Related information

Configure Exposure Assessment
Assess your exposure to vulnerable software

Domain separation and Vulnerability Response

This is an overview of domain separation and Vulnerability Response. Domain separation enables you to separate data, processes, and administrative tasks.
into logical groupings called domains. You can then control several aspects of this separation, including which users can see and access data.

Support level: Standard

- Includes **Basic** level support.
- Business logic: Processes can be created or modified per customer by the service provider (SP). The use cases reflect proper use of the application by multiple SP customers in a single instance.
- The owner of the instance needs to be able to configure the minimum viable product (MVP) business logic and data parameters per tenant as expected for the specific application.

Use case: An admin needs to be able to make comments mandatory when a record closes for one tenant, but not for another.

How domain separation works in Vulnerability Response

With domain separation you can standardize VR (Vulnerability Response) procedures, across the customer base you serve, with lowered operational costs and a higher quality of service.

Separate customer work spaces for workflows, dashboards, reports, and so on, ensures that customer data is separated and never exposed to other clients.

<table>
<thead>
<tr>
<th>Release</th>
<th>Support level</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>New York</td>
<td>Level 2 (Data, Requestor, Fulfiller)</td>
<td><strong>New features:</strong> Rapid7 Vulnerability Integration enabled with multiple instances but all instances still live under a single domain.</td>
</tr>
<tr>
<td>Orlando</td>
<td>Standard</td>
<td>Support standards and terminology for domain separation changed starting with this release. For more information about support levels, see Application support for domain separation</td>
</tr>
<tr>
<td>Paris</td>
<td>Standard</td>
<td></td>
</tr>
</tbody>
</table>
Domain separation for the Vulnerability Response application covers the following product functionality:

- Ingests the vulnerable items from third-party scanners (Qualys, Rapid 7 or Tenable) in the correct domain
  - The data ingests in the same domain as that of the integration user, whose credentials are used for integration.
- Re-scans specific assets from Vulnerability Response in the domain from which it was requested.
- Uses the CMDB CI lookup process to ensure that the CI information from the scanners matches the CIs in CMDB of the integration user’s domain.
- Calculates risk scores at the vulnerable item level as per the risk score calculator defined in the same domain as that of the integration user.
- Remediation target rules are executed on vulnerable items as per the remediation target rules defined in the same domain as that of the integration user.
- Vulnerability group rule(s) can be defined, and stay in, the same domain as the domain of the integration user.
- Vulnerability groups created using the vulnerability group rules stay in the same domain as where the group rules are created.
- Deferral workflow goes through the approval process in the same domain for which the deferral is requested.
- Reports and dashboards display the vulnerable item-states such as age of vulnerable item, open vulnerable items by CI, vulnerabilities by impact, and remediation target date status in the domain to which it belongs.
- Knowledge from third-party scanners or the National Vulnerability database (NVD) can be ingested in the global domain and data can be shared across multiple clients.

**Note:** In all the above cases the overarching principles of visibility in separated domains separation in the NOW Platform apply.

**Use cases**

The Vulnerability Response application manages the life cycle of a vulnerability item end to end. The following use cases are domain-separation aware:
• **Ingest** vulnerable items (vulnerabilities on asset) from either Qualys, Rapid 7 or Tenable
  ◦ Ingest data from multiple instances
  ◦ De-duplicate the vulnerable item
  ◦ Match up with CMDB CI

• **Enrichment** of vulnerable item with risk scores and remediation target dates
  ◦ Asset enrichment (CMDB)
  ◦ Risk score and remediation target date enrichment

• **Group** vulnerable items and assign the vulnerability group
  ◦ Automatically group the vulnerable items
  ◦ Automatically assign the vulnerability group

• **Remediate**
  ◦ Vulnerability group assigned as a remediation task
  ◦ Comprehensive remediation life cycle
  ◦ Deferral workflow

• **Measure** the security posture of the organization and vulnerability management program
  ◦ Vulnerability trend, most vulnerable asset, vulnerability by age
  ◦ Remediation status by the remediation target date

**Setup**

Setting up domain separation for Vulnerability Response does not require any additional steps. All Vulnerability Response tables acquire the Domain column after the instance is domain separated. You can direct vulnerability integration import data to specific domains. See Create domain-separated imports for the Qualys Host Detection Integration for more information.

**Domain-separated data**

Data can be domain separated, which means:

• Vulnerable item ingested from third-party scanners stays in the same domain as the domain of the integration user, and is not accessible from any other domain.

• Vulnerabilities, vulnerable items (instances) or assets in one domain cannot be viewed from other domains.
• The risk scoring algorithm, the vulnerability group rules and the remediation target rules cannot be viewed by anyone outside the domain.
• Vulnerability information from the NVD can exist in the global domain and be shared with all customers.
• Remediaion tasks in one domain cannot be viewed from another domain.
• Deferral workflows created in one domain are not visible in another domain.
• All email notifications are contained within the domain they belong to.

How vulnerability analysts manage their own application data
• Analysts create their own application installation, multi-source application management, and CI lookup rules.
• Analysts can configure specific integrations exclusively for use within the domain.
• Analysts can create their own deferral and change management workflows.
• Analysts can create their own vulnerability group rules, risk-scoring logic to accurately prioritize vulnerabilities, auto-assign vulnerability groups and assign to the correct assignment group.
• Domain users create a manual vulnerability item and then close the item.

Business logic and processes that can be domain-separated by instance owner
• Vulnerability Response users and groups
• Vulnerability Response integrations (starting with the Madrid release)
• Complete setup configuration (user and group management, application installation, multi-source application management, CI lookup rules, vulnerability group rules, risk calculators, remediation target rules etc.)
• Complete remediation life cycle including deferral
• Vulnerability Response Remediation Target Rules

Related information
Domian separation for service providers

Vulnerability Response implementation
Use the steps illustrated in the following images to download the Vulnerability Response application from the ServiceNow Store, install it on your Now Platform instance, and configure it using the Setup Assistant.
An installation and configuration example for installing the base system, the Vulnerability Response application and a third-party scanner application, the Qualys application, is illustrated in the two flows shown in the following images. Required roles and mandatory tasks, as well as optional steps, are also listed.

- For more information about each step illustrated in the following images and a checklist with links to supporting documentation, see Implementation checklist for the Vulnerability Response application.
- You can extend the concepts and sequence of steps presented in this example to installing and configuring other supported applications for Vulnerability Response. For a list of support applications, see Installation of Vulnerability Response and supported applications.

- The admin role is required to download and install the Vulnerability Response application and the Qualys Vulnerability application used for this example.
- The admin role also assigns the Vulnerability admin [sn_vul.vulnerability_admin] persona and other Vulnerability Response persona roles to users and groups.
The sn_vul.vulnerability_admin role configures the Vulnerability Response and Qualys applications in Setup Assistant and verifies expected results.

Follow the steps and prompts in Setup Assistant starting with the Vulnerability Response Settings section to continue with the installation and configuration. Reviewing these settings helps you understand and verify the processes of Vulnerability Response as you continue to set up your environment.

Role required: sn_vul.vulnerability_admin or, alternatively, admin
Vulnerability admin tasks

Review the descriptions, default settings, and demo data that you installed with the applications in the following sections:

- **Vulnerability Assignment Rules** - automatically assign vulnerable items (VIs) to
  the appropriate assignment group.
- **Vulnerability Group Rules** - automatically group vulnerable items (VIs) as they
  are imported based on certain conditions.
- **Risk Calculators** - Default Risk Calculator is enabled.
- **Remediation Target Rules** - Define remediation timelines for VIs and
  vulnerability groups (VGs).
- **Review and edit the settings** for the third-party applications and installed
  solutions you installed and define conditions for your data imports. Enter your
  third-party account information and configure import settings, and schedules,
  configuration item (CI) lookup rules, as well as other settings.

See **Implementation checklist for the Vulnerability Response application** for more
information.

**Implementation checklist for the Vulnerability Response application**

This checklist lists the steps required for a basic implementation of the
Vulnerability Response application on your Now Platform® instance. When
you have completed these tasks, the base system is ready for operation and
verification.
Before you begin
Consider creating and printing a PDF of this checklist topic. You can then check off tasks as you complete them. To generate a PDF, click the Save As PDF icon (⬇️) at the top of the topic and click Selected topic.
Roles required: admin, sn_vul.vulnerability_admin

Vulnerability Response basic implementation checklist tasks for admin

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| ☐    | As a user with the admin role, verify that you have the Vulnerability Response and the Qualys Integration for Security Operations applications downloaded onto your Now Platform instance.  
1. To verify the applications are available on your instance, navigate to System Applications > All Available Applications and search for Vulnerability Response [sn_vul] and [sn_vul_qualys].  
2. If the Vulnerability Response and Qualys Integration for Security Operation applications are not visible, see Security Operations and the ServiceNow Store for more information about getting entitlement and downloading the applications. |
| ☐    | As a user with the admin role, install the Vulnerability Response application along with its dependencies on your Now Platform instance. |
### Vulnerability Response basic implementation checklist tasks for admin (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| [ ]  | **Note:** During installation of the Vulnerability Response application, you have the option to install demo data. Demo data is required if you want to run automated tests to confirm that your instance works after installation. Run tests only on development, test, and other non-production instances to avoid data corruption and outage. If demo data or demo accounts are created, all demo data should be removed prior to using the instance in non-production or production.  

The Setup Assistant for Vulnerability Response is installed automatically along with the application. The Setup Assistant is required to configure the Vulnerability Response application. Additionally, it is used to install and configure the Qualys Integration for Security Operations application used in this example, as well as other applications that are compatible with Vulnerability Response.  

For more information about installing the Vulnerability Response application, see [Install and configure Vulnerability Response](#). |
| [ ]  | **As a user with the admin role, navigate Vulnerability Response > Administration > Setup Assistant > Integration Application Installation and install the Qualys Integration for Security Operations application.**  

For more information, see [Install Vulnerability Response third-party applications using Setup Assistant](#). |
| [ ]  | **(Optional) As a user with the admin role, if you installed demo data with the Vulnerability Response application, you can run the Vulnerability Response ATF Test Suite to verify the applications successfully installed.**  

**Note:** Run tests only on development, test, and other non-production instances to avoid data corruption and outage.  

For more information, see [Run the Automated Test Framework (ATF) test suite for Vulnerability Response](#). |
Vulnerability Response basic implementation checklist tasks for admin (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For more information about automated tests, see Automated Test Framework (ATF).</td>
</tr>
<tr>
<td></td>
<td><strong>As a user with the admin role, in Setup Assistant, navigate to Vulnerability Response Users and Groups and assign users with the required Vulnerability Response persona roles.</strong></td>
</tr>
<tr>
<td></td>
<td>1. From within Setup Assistant, you can view existing users and any roles that are already assigned by clicking the User Administration module link.</td>
</tr>
<tr>
<td></td>
<td>2. From the list, click a user name to open the record and click the Roles related list. All the roles assigned to this user are displayed.</td>
</tr>
<tr>
<td></td>
<td>3. Navigate back to Vulnerability Response Users and Groups in Setup Assistant and follow the prompts to assign the sn_vul.vulnerability_admin role.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The sn_vul.vulnerability_admin role is required to continue with the configuration. Alternatively, you can continue with the configuration as a user with the admin role.</td>
</tr>
<tr>
<td></td>
<td>(Optional) You can also assign the Configuration Item (CI) Manager [sn_vul.ci_manager] and Exception Approver [sn_vul.exception_approver] roles, but these personas are not required for the remaining setup tasks.</td>
</tr>
<tr>
<td></td>
<td>For more information about assigning the persona roles using the Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant.</td>
</tr>
<tr>
<td></td>
<td>For more information on users and assigning roles to users and groups, see Create a user, Assign a role to a user and Assign a role to a group on the ServiceNow Product Documentation website.</td>
</tr>
</tbody>
</table>

Continue with the configuration of the applications starting in the Vulnerability Response Settings section. Reviewing these settings helps you understand how Vulnerability Response works as you continue to set up your environment. For the scanner integration used in this example, you are required to edit the settings.
The concepts you use in this configuration example for the Qualys product apply to other scanner applications.

**Before you begin**

Obtain your Qualys credentials. Verify you have any account names, passwords, and other service information required by Qualys products so that you have access to them. They are required to configure the application.

Roles required: sn_vul.vulnerability_admin or, alternatively, admin

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| ☐   | Review the Vulnerability Assignment Rules.  
Assignment rules automatically assign vulnerable items (VIs) to the appropriate assignment group. For more information, see, [Vulnerability Response assignment rules overview](#).  
For more information about configuring Vulnerability Response using the Setup Assistant, see [Configuring Vulnerability Response using the Setup Assistant](#). |
| ☐   | Review the Vulnerability Group Rules.  
Vulnerability group rules automatically group vulnerable items (VIs) as they are imported based on certain conditions. For more information, see [Vulnerability Response groups and group rules overview](#). |
| ☐   | Review the Risk Calculators.  
Risk calculators score vulnerable items for prioritization. You can configure calculators to incorporate characteristics of the configuration item (CI), exploit availability, and vulnerability severity reported by your vulnerability assessment (scanner) vendor. For more information, see [Vulnerability Response calculators and vulnerability calculator rules](#). |
| ☐   | Review the Remediation Target Rules.  
Remediation Target Rules define remediation timelines for VIs and VGs. For more information, see [Vulnerability Response remediation target rules](#). |
| ☐   | In the Integration Configuration section, review the Qualys application settings and define and schedule your data imports. |
Vulnerability Response basic implementation checklist tasks for vulnerability admin (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Click <strong>Scanner Integrations</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>On the Installed Applications page, click <strong>Edit</strong>.</td>
</tr>
<tr>
<td>3.</td>
<td>Enter your credentials and click <strong>Next</strong>.</td>
</tr>
<tr>
<td>4.</td>
<td>Read the descriptions for the KnowledgeBase Configuration.</td>
</tr>
<tr>
<td>5.</td>
<td>Review the Host Detection Configuration page for Import Settings, CI Lookup Rules, and Import Schedules.</td>
</tr>
<tr>
<td>6.</td>
<td>After you are satisfied with the settings on this page, click <strong>Execute Now</strong> to import data. Click the <strong>View details</strong> link that is displayed to view vulnerability integration run status.</td>
</tr>
<tr>
<td>7.</td>
<td>(Optional) Continue to edit configuration settings.</td>
</tr>
<tr>
<td>8.</td>
<td>Click <strong>Finish</strong> to complete the installation and configuration in Setup Assistant.</td>
</tr>
</tbody>
</table>

For more information about configuring the Qualys application, see Configure the Qualys Vulnerability Integration using Setup Assistant.

What to do next

Congratulations! You successfully installed the Vulnerability Response application and configured it and a scanner application using the Setup Assistant. The base system is now ready for operation.

To download, install, and configure other applications for Vulnerability Response, follow the same steps and concepts you completed for the preceding checklist. Refer to specific topics provided for each application for more information.

For more information about supported applications available that are available to you from the ServiceNow Store for Vulnerability Response, see Installation of Vulnerability Response and supported applications.

For more information about how to use Vulnerability Response, see Understanding the Vulnerability Response application.

Installation of Vulnerability Response and supported applications

Setup for Vulnerability Response consists of several tasks. Setup Assistant is designed to streamline basic configuration for Vulnerability Response and a third-party integration. More options are available to extend this basic setup.
Tasks for basic setup
The following list includes applications and integrations supported by the Vulnerability Response application you can install for the basic setup.

• The Vulnerability Response application is required. For more information about installing it, see Install the Vulnerability Response application. For an overview and step-by-step instructions for how to download, install, and configure the Vulnerability Response application and a third-party integration using the Setup Assistant, see Vulnerability Response implementation.

• After installation is completed, Configure Vulnerability Response using Setup Assistant.
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

• Select, install, and configure one or more supported third-party integrations. These integrations retrieve vulnerability data from external systems and vendors. For more information about how integrations work, see Vulnerability Response integrations.
  ◦ [Optional] Install the Qualys Vulnerability Integration. The Qualys Vulnerability Integration is available to configure within Setup Assistant.
  ◦ [Optional] Install and configure the Rapid7 Vulnerability Integration.

  Note: You can install the Rapid7 Vulnerability Integration from Setup Assistant, but configuration is not supported for this integration in Setup Assistant. See Install and configure the Rapid7 Vulnerability Integration for more information.

  ◦ [Optional] Install and configure the Vulnerability Response Integration with Tenable application using Setup Assistant. Installation and configuration for the Tenable Vulnerability Integration developed for the Now Platform is supported within Setup Assistant.

• Select an analytics application, when applicable. The Performance Analytics Content Pack for Vulnerability Response application contains reports that cover all stages of the vulnerability management lifecycle.
  ◦ [Optional] Install and configure the Performance Analytics for Vulnerability Response [PA] application application.
• Select a solutions application, when applicable. Solution management helps you correlate the vulnerabilities in your environment with the solutions that could remediate them.
  ◦ [Optional] Install the Solution Management for Vulnerability Response application.

⚠️ Note:
- When the Vulnerability Solution Management application is enabled, the Microsoft Security Response Center Solution Integration and the Red Hat Solution Integration are available to edit in Setup Assistant.

  The Red Hat Solution Integration is available starting with v10.3 of Vulnerability Response. Vulnerability Solution Management requires a separate subscription. For more information, see Vulnerability Solution Management.

• [Optional] Install the ServiceNow Agent app and the Vulnerability Response Mobile app for the Mobile experience for Vulnerability Response.

Additional tasks you can perform
These setup tasks are tasks that supplement remediation with reporting, native integration configuration, and working with vulnerable items manually.

• Manage persona and granular roles for Vulnerability Response
• Configure Exposure Assessment
• Define Vulnerability Response email notifications
• View Vulnerability Response SLAs for vulnerability groups
• Managing NVD, CWE, and third-party data libraries
• Manage individual vulnerable items manually

Optional tasks
Optional setup tasks are detailed tasks that can be revisited outside of Setup Assistant or tasks that fall outside of basic setup but that you might find useful.

• Configure the vulnerable item key
• Create a Vulnerability Response CI lookup rule
• Manually create a Vulnerability Response group
• Create or edit Vulnerability Response group rules
• View Vulnerability Response SLAs for vulnerability groups
Create a Vulnerability Response calculator
Create or edit Vulnerability Response remediation target rules
Configure and manage Qualys vulnerability scanners and scans
Manually create a vulnerability integration

Install and configure Vulnerability Response
Before you run the Vulnerability Response application in your Now Platform instance, you must get entitlement and download the application from the ServiceNow Store, install it on your Now Platform instance, and complete a few installation steps in Setup Assistant.

Before you begin
Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

Note: This process applies only to applications downloaded to production instances. If you’re downloading applications to sub-production or development instances, it’s not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

<table>
<thead>
<tr>
<th>Setup tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have the required ServiceNow roles assigned for your instance.</td>
<td>The admin role is required for installation. If not already assigned, the System Administrator [admin] also assigns the Vulnerability Admin [v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)] role.</td>
</tr>
</tbody>
</table>

Role required: admin
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.
Note:

If you are an upgrade customer, access for the users and groups you assigned with the `sn_vul.vulnerability_read` and `sn_vul.vulnerability_write` permissions prior to v10.3 has not changed. Users and groups remain assigned with these roles until you change them. However, starting with v10.3, you may prefer assigning granular roles for more control over what users and groups can do and see in the Vulnerability Response application. For an overview and more information about managing these roles, see Vulnerability Response personas and granular roles and Manage persona and granular roles for Vulnerability Response.

Procedure

1. To get entitlement and download the Vulnerability Response core application, navigate to the ServiceNow Store.

2. In the upper right of the page, click Log In.

3. In the dialog that is displayed, enter your Hi credentials and click Login.

4. On the page that is displayed, if not selected, click the ServiceNow Products tab.
5. To view the associated applications that you are eligible for with the Vulnerability Response application, on the product list page, click the **Vulnerability Response** product.

The Eligible tab lists all the applications you are eligible for if you opt-in. For more information on an application, click a link.

6. To get the Vulnerability Response core application, click **Opt-in**.

7. To agree to the terms and conditions, at the prompt, select the check box and click **Accept**.

A message is displayed that indicates you have successfully opted-in for the application.
With the ServiceNow Products tab selected and displayed, a green check mark replaces the plus sign to the right of the Vulnerability Response application, as shown in the following figure.

![Security Operations](image)

After you have accepted the terms and conditions and managed entitlements for any of the applications on the ServiceNow Products tab, on the Products List page, you can click the plus sign (+) to get entitlement and opt-in for the other applications on this page with a single click.

8. Skip to step 10 to install the application on your Now Platform instance.

9. Optional: Alternatively, to manage your entitlement for the Vulnerability Response application on other Now Platform instances, follow these steps.

   a. If the Manage Entitlement button is not displayed, click the Vulnerability Response application on the Product List to display it.

   b. With the Eligible tab selected, click Manage Entitlement.
c. In the Manage Entitlements for Vulnerability Response dialog that is displayed, choose one:

Manage Entitlements for Vulnerability Response

- Remove all existing entitlements
- Entitle all instances
- Entitle selected instances

d. Click OK or Cancel to continue.

You are ready to activate plugins and install the application on your Now Platform instance(s).

10. Log in to the Now Platform instance that you want to install the Vulnerability Response application on.

11. Navigate to System Applications > All Available Applications > All.
12. From the applications listed, locate the Vulnerability Response application (sn_vul), select a version from the choice list, and click Install. The Application installation dialog is displayed. Any dependencies that will be installed are displayed.

13. If you want demo data, select the Load demo data check box and click Install.

**Note:** If you do not select the Load demo data check box, demo data is not available to install from the Application Manager later. For information on how to install or reinstall demo data after the initial installation, see the Work around to install demo data if application is already installed [KB0722909] article in the Now Support Knowledge Base.
14. Click Close.

15. After installation is successfully completed, navigate to Vulnerability > Administration > Setup Assistant.

16. Follow the instructions on the forms in each section.
What to do next
For more information on Vulnerability Response settings, installing applications, configuration, integrations, group rules, risk calculators, and remediation target rules, see Configuring Vulnerability Response using the Setup Assistant.

Components installed with Vulnerability Response
Several types of components are installed with activation of the Vulnerability Response application, including tables, user roles, and scheduled jobs.

⚠️ Note: The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

Demo data is available for this feature.

Roles installed
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

⚠️ Note:
If you are an upgrade customer, access for the users and groups you assigned with the sn_vul.vulnerability_read and sn_vul.vulnerability_write permissions prior to v10.3 has not changed. Users and groups remain assigned with these roles until you change them. However, starting with v10.3, you may prefer assigning granular roles for more control over what users and groups can do and see in the Vulnerability Response application. For an overview and more information about managing these roles, see Vulnerability Response personas and granular roles and Manage persona and granular roles for Vulnerability Response.

<table>
<thead>
<tr>
<th>Role title [name]</th>
<th>Description</th>
<th>Contains roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability managers and senior analysts [v10.3</td>
<td>Update properties and vulnerability integrations. The v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated) role is required for Vulnerability</td>
<td>• sn_vul.vulnerability_write</td>
</tr>
<tr>
<td>sn_vul.vulnerability.admin or sn_vul.admin (deprecated)]</td>
<td></td>
<td>• Version 13.0: sn_vul.ciso_write</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• sn_sec_cmn.admin</td>
</tr>
<tr>
<td>Role title [name]</td>
<td>Description</td>
<td>Contains roles</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
<td>----------------</td>
</tr>
</tbody>
</table>
| Response administration including vulnerability integrations, vulnerability group rules, calculators, and remediation target rules and tasks, reports, and third-party integration configuration. | • sn_vul_qualys.admin (when the Qualys Vulnerability Integration is installed.)  
• sn_vul_r7.admin (when the Rapid7 Vulnerability Integration is installed.)  
• sn_vul_shodan.admin (when the Shodan Exploit Integration is installed.)  
• Version 12.1: sn_vul_tenable.admin (when the Tenable Vulnerability Integration is installed.)  
• Version 12.1: sn_vul_tenable.configure_integration (when the Tenable Vulnerability Integration is installed.)  
• Version 13.0: sn_vul.configure_nvd_integration (when the NVD integrations are installed.)  
• treemap_admin (when the Performance Analytics application is installed.) | |
| Vulnerability analysts [sn_vul.vulnerability_write] | The sn_vul.vulnerability_write role is required for managing vulnerability groups and vulnerable items, and monitoring remediation progress. | • sn_vul.vulnerability_read  
• sn_sc_cmn.write  
• sn_vul_qualys.user (when the Qualys Vulnerability Integration is installed.)  
• sn_vul_shodan.write (when the Shodan Exploit Integration is installed.) | |
| Others [sn_vul.vulnerability_read] | The sn_vul.vulnerability_read role is required for anyone needing visibility into vulnerability management. For example, IT and security | • sn_sec_cmn.read  
• sn_vul_qualys.read (when the Qualys Vulnerability Integration is installed.)  
• sn_vul_shodan.read (when the Shodan Exploit Integration is installed.) | |
<table>
<thead>
<tr>
<th>Role title [name]</th>
<th>Description</th>
<th>Contains roles</th>
</tr>
</thead>
</table>
  Note: This user is the default run-as user for each integration record. Do not change.                                                                                                                                                                                      | • import_admin  
  • sn_vul.vulnerability_write.                                                                                                       |                                                                                                                                                                      |
| Remediation owner [sn_vul.remediation_owner]                                    | View and update permission for vulnerable items, vulnerability groups assigned to you or your group. Can view all vulnerabilities and solutions. Has write access to the **Internal notes field** on the solution record.                                                                                      | Contained in the itil role.                                                                                                                                  |
| Version 13.0: CISOs and vulnerability executives [sn_vul.vulnerability_ciso]   | View the CISO dashboard in Performance Analytics for Vulnerability Response.                                                                                                                                                                                                 | • sn_vul.ciso_read  
  • sn_vul.read_all                                                                                                                      |                                                                                                                                                                      |

**Scheduled jobs installed**

<table>
<thead>
<tr>
<th>Scheduled job</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 12.0: Associate existing VIs with Auto Exception Rule</td>
<td>Automatically associates the Auto Exception Rule with existing VIs.</td>
</tr>
<tr>
<td>Scheduled job</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Version 10.3: Auto-Close Vulnerable Items</td>
<td>Version 10.3: Automatically closes the stale vulnerable items based on the configuration defined in the table ‘sn_vul_auto_close_config’.</td>
</tr>
<tr>
<td>Calculate Related VI Counts for Vulnerability and Vulnerability Group</td>
<td>Captures manual and VI import changes for the day. Reconciles vulnerability and solution relationships and recalculates totals.</td>
</tr>
<tr>
<td>Version 13.0: Check Mid-Server Timeout</td>
<td>Pings the Mid-Server and errors out after 30 seconds.</td>
</tr>
<tr>
<td>Check Run State WaitComplete</td>
<td>Marks an integration run as complete once they are verified as fully done.</td>
</tr>
<tr>
<td>Check Vulnerable Item and Groups Deferment Expiration</td>
<td>Sends notifications if vulnerable items or vulnerabilities have expired (and if they expire in one week).</td>
</tr>
<tr>
<td>Close cancel VIIs that do not have a CI associated</td>
<td>Automatically closes vulnerable items that do not have an associated configuration item (CI) and have not been updated for three days. State is set to Closed/Cancelled.</td>
</tr>
<tr>
<td>Close VI on exp record delete</td>
<td>Closes a VI when it is deleted.</td>
</tr>
<tr>
<td>CR State Synchronization</td>
<td>Script retrofits all existing VG-CHG relationships so they are synchronized. Enables synchronization going forward.</td>
</tr>
<tr>
<td>CWE Comprehensive 2000 Integration</td>
<td>Vulnerability integration that pulls in vulnerability information from the Common Weakness Enumeration (CWE) dataset, curated by the MITRE Corporation.</td>
</tr>
<tr>
<td>Disable VR solutions when solutions application not active</td>
<td>Disables and hides the Vulnerability Solution Management feature when the Solution Management for Vulnerability Response application is not installed.</td>
</tr>
<tr>
<td>Evaluate remediation targets</td>
<td>Sets or updates remediation target dates on all vulnerable items. Determines the status of remediation target dates against rules.</td>
</tr>
<tr>
<td>Scheduled job</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Version 14.0:</strong></td>
<td>Cleans up detection data automatically by an integration-specific scheduled job that is triggered post-upgrade to Vulnerability Response.</td>
</tr>
<tr>
<td>Microsoft Security Response Center Solution integration</td>
<td>Vulnerability Solution Management integration that retrieves solutions from the Microsoft Security Response Center.</td>
</tr>
<tr>
<td><strong>Removed in Version 13.0:</strong> NIST National Vulnerability Database</td>
<td>Vulnerability integration that retrieves the National Vulnerability Database (NIST) data feed.</td>
</tr>
<tr>
<td>Pick up throttled integration process</td>
<td>Creates the integration process for the Shodan Exploit Integration.</td>
</tr>
<tr>
<td>Populate affected products text</td>
<td>After upgrade, handles existing solutions to populate affected products text. This job runs only once.</td>
</tr>
<tr>
<td>Populate new CR Count Column</td>
<td>Automatically populates the new CR count column for customers with existing data in the Vulnerability Group [sn_vul_vulnerability] table.</td>
</tr>
<tr>
<td><strong>Version 10.3:</strong> Populate records in vulnerability vendor mapping table</td>
<td>Inserts records into vulnerability vendor mapping table for existing vulnerabilities.</td>
</tr>
<tr>
<td>Prior to v10.3: Populate records in vulnerability vendor mapping table for Rapid7 vulnerabilities</td>
<td></td>
</tr>
<tr>
<td>Re-open deferred vulnerability groups</td>
<td>Reopens deferred vulnerability groups when the deferment date has passed.</td>
</tr>
<tr>
<td>Reaply all vulnerability assignment rules</td>
<td>Reevaluates assignment rules against all Open VIs.</td>
</tr>
<tr>
<td><strong>Version 10.3:</strong> Red Hat Solution Integration</td>
<td>Vulnerability Solution Management integration that retrieves solutions from the Red Hat Security Advisory.</td>
</tr>
<tr>
<td>Refresh associated vulnerable items for non-VGR based VG</td>
<td>Updates the vulnerability group with vulnerable items matching the Filter Group and Condition groups criteria.</td>
</tr>
<tr>
<td>Scheduled job</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **Version 10.0:**
Repair erroneous Vulnerable Items Last Opened and Closed | Repairs existing UI data corrupted by defects previously fixed. |
| Rerun calculators | Reapplies the calculators to any vulnerable items affected by the change. This triggers a recalculation of the cumulative risk scores of their vulnerability groups.  

**Note:** Rerunning calculators can take a long time depending on your environment. |
| Retry Cancelled Integration Import Sets | Retries canceled integration import sets. Retries 5 times before returning an error. |
| Retry Integration Processes | Retries integration processes. Retries 5 times before returning an error. |
| Rollup vulnerable item values to vulnerability and group | Computes the risk score, number of vulnerable items, and remediation target status for vulnerability groups, using the rollup calculator. |
| Run severity calculator after vuln entry promotion | Runs the severity calculator after a previously missing vulnerability has been updated with its score and other data from a third-party provider, such as Qualys Cloud Platform, Rapid7 Nexpose. |
| Scheduled Vulnerability Data Source Processor | Checks the import queue for entries to process and assigns a scheduled import job based on available resources. |
| Scheduled Vulnerability integration process attachment cleanup | Removes integration XML attachments once they are 14 days old. This retention time is not configurable. |
| Scheduled Vulnerability Integration timeout checker | Cancels integration runs that take over 60 minutes to complete. |
| Set related CI services for VI | Once the integration import is complete, links affected business services to CIs connected to vulnerable items, at the specified time. |
| **Version 13.0:**
Trigger next integration | Triggers the next integration in a chained integration run. |
### Scheduled job

<table>
<thead>
<tr>
<th>Scheduled job</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update CI scan last found</td>
<td>Updates the <strong>Last vulnerability found</strong> field in the CMDB CI record after scan.</td>
</tr>
<tr>
<td>Update Ungrouped Vulnerable Items</td>
<td>Determines whether a vulnerable item is in a vulnerability group and adds or removes it from the <strong>Ungrouped Vulnerable Items</strong> list.</td>
</tr>
<tr>
<td><strong>Note:</strong> This job runs post-upgrade and, depending on your data set, can take a long time to complete.</td>
<td></td>
</tr>
<tr>
<td>Update Vulnerability on VG</td>
<td>Updates the <strong>Vulnerability</strong> field on the Vulnerability Group (sn_vul_vulnerabilty) table after upgrade. This job is triggered once and disabled afterward.</td>
</tr>
<tr>
<td>Removed in v10.0</td>
<td>Updates vulnerable item age based on how long the vulnerable item has been open.</td>
</tr>
<tr>
<td><strong>Note:</strong> Deprecated for versions prior to v10.0. Do not use.</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Import Template</td>
<td>Engine that processes the import queue. One of 10.</td>
</tr>
<tr>
<td>Vulnerability Response Age Closed Update</td>
<td>Updates Age closed column on VI table.</td>
</tr>
<tr>
<td>Vulnerability Response CI count</td>
<td>Calculates the number of CIs scanned by third-party scanners in the last 30 days.</td>
</tr>
<tr>
<td>Vulnerability Response Risk and Remediation Status Upgrade</td>
<td>Updates the risk rating on data when you upgrade.</td>
</tr>
</tbody>
</table>

### Tables installed

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessed Vulnerable Items [sn_vul_m2m_exp_sw_vi]</td>
<td>Assigns a vulnerability group to an assignment group during vulnerability group creation.</td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assignment Rule [sn_vul_vgr_assignment_rule]</td>
<td>Assigns a vulnerability group to an assignment group during vulnerability group creation.</td>
</tr>
<tr>
<td>Associate Change Request [sn_vul_action_associate_cr]</td>
<td>Staging table used to process new VG-CHG associations.</td>
</tr>
<tr>
<td>Removed in v10.0: Associated IP Addresses [sn_vul_vi_ip_address]</td>
<td>IP addresses associated with a vulnerable item.</td>
</tr>
<tr>
<td>Note: Deprecated for versions prior to v10.0. Do not use.</td>
<td></td>
</tr>
<tr>
<td>Asynchronous Vulnerable Item Job [sn_vul_async_vi_job]</td>
<td>Contains background jobs that process vulnerable items. Only one job type is supported; used to edit vulnerabilities in bulk.</td>
</tr>
<tr>
<td>Asynchronous Vulnerable Item Job Type [sn_vul_async_vi_job_type]</td>
<td>Contains the types of background jobs, and references the relevant script. Only has one processor, the <strong>VulnerabilityBulkEditProcessor</strong></td>
</tr>
<tr>
<td>Version 10.3: Auto-Close Stale Vulnerable Items [sn_vul_auto_close_config]</td>
<td>Version 14.0: Stores the configuration for how stale detections are automatically closed.</td>
</tr>
<tr>
<td>Version 13.0: Stores the configuration for how stale vulnerable items are automatically closed.</td>
<td></td>
</tr>
</tbody>
</table>
| CI Scan [sn_vul_ci_scan] | Contains data on when CIs were last scanned.  
Data includes:  
- last scan date (if available)  
- scanner used for the last scan |
<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
</table>
| • date of the last vulnerability found for the CI  
• scanner last used for a found vulnerability | |
| Version 10.3:  
Configure Vulnerable Item Granularity  
[sn_vul_action_vi_granularity_config] | Stores the UI form used to enable or disable Include Port from the configuration page in the Configure VI Granularity module. |
| Create change request  
[sn_vul_action_create_cr] | Used to create change requests from VG. |
| Create Vulnerable Items  
[sn_vul_action_create_vi] | A staging table which is used as a place holder for information. This table does not store any records. |
| CWE  
[sn_vul_cwe] | Catalog of Common Weakness and Enumeration (CWE) software vulnerabilities. |
| Version 12.0:  
CWE Applicable Platform  
[sn_vul_cwe_m2m_cwe_platform] | Contains the imported CWE applicable platform data. |
| Version 12.0:  
CWE Category  
[sn_vul_cwe_category] | Contains the imported CWE category data. |
| Version 12.0:  
CWE Common Consequence  
[sn_vul_cwe_consequence] | Contains the imported CWE common consequence data. |
| Version 12.0:  
CWE External Reference  
[sn_vul_cwe_reference] | Contains the imported CWE external reference data. |
| Version 12.0:  
CWE Observed Example  
[sn_vul_m2m_cwe_cve] | Contains the imported CWE CVE data. |
<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 12.0: CWE Platform</td>
<td>Contains the imported CWE platform data.</td>
</tr>
<tr>
<td>[sn_vul_cwe_platform]</td>
<td></td>
</tr>
<tr>
<td>Version 12.0: CWE External Reference</td>
<td>Contains the imported CWE related external reference data.</td>
</tr>
<tr>
<td>[sn_vul_cwe_reference]</td>
<td></td>
</tr>
<tr>
<td>Version 12.0: CWE Relationship</td>
<td>Contains the imported CWE relationship data.</td>
</tr>
<tr>
<td>[sn_vul_m2m_cwe_relation]</td>
<td></td>
</tr>
<tr>
<td>Version 12.0: CWE View</td>
<td>Contains the imported CWE view data.</td>
</tr>
<tr>
<td>[sn_vul_cwe_view]</td>
<td></td>
</tr>
<tr>
<td>Version 12.0: CWE Weakness</td>
<td>Contains the imported CWE weakness data.</td>
</tr>
<tr>
<td>[sn_vul_cwe_weakness]</td>
<td></td>
</tr>
<tr>
<td>Discovery Model Vulnerable Software Match</td>
<td>Supplements the matching of vulnerable software to a discovery model.</td>
</tr>
<tr>
<td>[sn_vul_discovery_model_software_match]</td>
<td></td>
</tr>
<tr>
<td>Version 10.3: Exception Management Configuration</td>
<td>Stores the configuration settings for the exception management feature.</td>
</tr>
<tr>
<td>[sn_vul_exception_config]</td>
<td></td>
</tr>
<tr>
<td>Version 12.0: Exception Rule</td>
<td>Contains the set of rules evaluated for Exception Management.</td>
</tr>
<tr>
<td>[sn_vul_auto_exception_rule]</td>
<td></td>
</tr>
<tr>
<td>Exploit</td>
<td>Contains the definitions of exploits: publicly available code that takes advantage of a vulnerability.</td>
</tr>
<tr>
<td>[sn_vul_exploit]</td>
<td></td>
</tr>
<tr>
<td>Exploit Framework</td>
<td>Contains the names of exploit frameworks: full software packages that are capable of running many exploits.</td>
</tr>
<tr>
<td>sn_vul_exploit_framework</td>
<td></td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Exposed Discovery Models</td>
<td>Stores the mapping between the Discovery model and Exposure Assessment.</td>
</tr>
<tr>
<td>[sn_vul_m2m_exp_sw_model]</td>
<td></td>
</tr>
<tr>
<td>Exposure Assessment</td>
<td>Stores the records for exposure assessment.</td>
</tr>
<tr>
<td>[sn_vul_exp_by_sw]</td>
<td></td>
</tr>
<tr>
<td>Exposure Vulnerability Entries</td>
<td>Stores the mapping between Vulnerability (sn_vul_entry) and Exposure Assessment.</td>
</tr>
<tr>
<td>[sn_vul_m2m_entry_exp]</td>
<td></td>
</tr>
<tr>
<td>Malware Kit</td>
<td>Contains the details of malware kits: pre-written tools that make it easy to run an exploit or set of related exploits without doing additional coding or configuration work</td>
</tr>
<tr>
<td>[sn_vul_malware_kit]</td>
<td></td>
</tr>
<tr>
<td>Microsoft Response Center Solution Update</td>
<td>Contains the last time that the solution data was updated by Microsoft. Used to compare against the nightly import to determine the delta data for download.</td>
</tr>
<tr>
<td>[sn_vul_msrc_update]</td>
<td></td>
</tr>
<tr>
<td>Microsoft Security Response Center Solution Import</td>
<td>Used by the Microsoft Security Response Center Solution integration to stage import data prior to processing.</td>
</tr>
<tr>
<td>[sn_vul_msrc_solution_import]</td>
<td></td>
</tr>
<tr>
<td>[sn_vul_msrc_integration]</td>
<td></td>
</tr>
<tr>
<td>National Vulnerability Database Entry</td>
<td>Documented vulnerability from the NIST National Vulnerability Database.</td>
</tr>
<tr>
<td>[sn_vul_nvd_entry]</td>
<td></td>
</tr>
<tr>
<td>NVD CVSS Import</td>
<td>Contains staging data that has not yet been transformed to the Vulnerability Response schema during NVD import.</td>
</tr>
<tr>
<td>[sn_vul_nvd_cvss_import]</td>
<td></td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Note:</strong> Deprecated for versions prior to v13.0. Do not use.</td>
<td></td>
</tr>
<tr>
<td>[sn_vul_nvd_repo]</td>
<td></td>
</tr>
<tr>
<td>Product category</td>
<td>Contains the imported product category data.</td>
</tr>
<tr>
<td>[sn_vul_product_category]</td>
<td></td>
</tr>
<tr>
<td>Version 10.3: Red Hat Security Advisory</td>
<td>Compares the Red Hat solutions against the nightly job to determine the delta data for import.</td>
</tr>
<tr>
<td>[sn_vul_rhsa_update]</td>
<td></td>
</tr>
<tr>
<td>Version 10.3: Red Hat Solution Imports</td>
<td>Used by the Red Hat Solution Integration to stage import data prior to processing.</td>
</tr>
<tr>
<td>[sn_vul_rh_solution_import]</td>
<td></td>
</tr>
<tr>
<td>[sn_vul_rh_integration]</td>
<td></td>
</tr>
<tr>
<td>Related Business Services</td>
<td>Links CIs to Business Services for impacted services lookup. Contains a flag indicating whether it was added by Service Mapping.</td>
</tr>
<tr>
<td>[sn_vul_m2m_ci_services]</td>
<td></td>
</tr>
<tr>
<td>Remediation Target Rule</td>
<td>Defines the expected time frame for remediating a vulnerable item. Extends Application File.</td>
</tr>
<tr>
<td>[sn_vul_ttr_rule]</td>
<td></td>
</tr>
<tr>
<td>Version 13.0: REST Integration</td>
<td>Extends the Vulnerability Integration [sn_vul_integration] table for the REST-based Integrations.</td>
</tr>
<tr>
<td>[sn_vul_rest_integration]</td>
<td></td>
</tr>
<tr>
<td>SAM NVD Vulnerability Detection</td>
<td>Contains which CI and Vulnerabilities are monitored with SAM NVD and whether SAM NVD vulnerability detection is enabled or not.</td>
</tr>
<tr>
<td>[sn_vul_sam_config]</td>
<td></td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Scheduled Import Pool</td>
<td>Collection of scheduled import set records used to facilitate simultaneous data source imports.</td>
</tr>
<tr>
<td>[sn_vul_sched_import_pool]</td>
<td></td>
</tr>
<tr>
<td>Select Vulnerable Item</td>
<td>Base staging table used to handle split VG, create CHGs, and associate CHGs</td>
</tr>
<tr>
<td>[sn_vul_action_select_vi]</td>
<td></td>
</tr>
<tr>
<td>Setup Status</td>
<td>Internal only: Used by the Setup Assistant. Whenever Setup Assistant is opened, it shows the status of the steps Completed, and the percentage on the right top corner comes from this table.</td>
</tr>
<tr>
<td>[sn_vul_setup_status]</td>
<td></td>
</tr>
<tr>
<td>Severity Map</td>
<td>Contains the mappings from source severity to normalized severity.</td>
</tr>
<tr>
<td>[sn_vul_severity_map]</td>
<td></td>
</tr>
<tr>
<td>Version 12.1: Solution Scanner Mapping</td>
<td>Maps vendor, scanner, and keywords for exclusion or inclusion.</td>
</tr>
<tr>
<td>[sn_vul_solution_scanner_mapping]</td>
<td></td>
</tr>
<tr>
<td>Split vulnerability group</td>
<td>Staging table used to split vulnerability groups.</td>
</tr>
<tr>
<td>[sn_vul_action_split_vg]</td>
<td></td>
</tr>
<tr>
<td>Third Party Vulnerability Entry</td>
<td>Documented vulnerability from a third-party source.</td>
</tr>
<tr>
<td>[sn_vul_third_party_entry]</td>
<td></td>
</tr>
<tr>
<td>Update Manifest</td>
<td>List of Vulnerability Groups that have been updated and require recalculation by the rollup calculator.</td>
</tr>
<tr>
<td>[sn_vul_update_manifest]</td>
<td></td>
</tr>
<tr>
<td>VR Configuration Item Count</td>
<td>Contains the 90-day rolling cumulative average of configuration items imported from third-party integrations.</td>
</tr>
<tr>
<td>[sn_vul_vr_configuration_item_count]</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Assignment Rule</td>
<td>Contains the set of rules evaluated to set the assignment group on VIs.</td>
</tr>
<tr>
<td>[sn_vul_assignment_rule]</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Calculator</td>
<td>Contains the vulnerability calculator rules. The order of the</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>[sn_vul_calculator_group]</td>
<td>calculator determines which calculator is evaluated first, and in each calculator, one calculator rule, at most, is used.</td>
</tr>
<tr>
<td>Vulnerability Calculator Rule</td>
<td>Contains the rules for all of the calculators. For each calculator, the calculator rules are reviewed in order. The first calculator matching the condition uses the values within that rule.</td>
</tr>
<tr>
<td>[sn_vul_calculator]</td>
<td></td>
</tr>
<tr>
<td>Vulnerability CVEs</td>
<td>Links NVD Common Vulnerability Exposures (CVE) data to vulnerable entries.</td>
</tr>
<tr>
<td>[sn_vul_m2m_entry_cve]</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Data Source Import Queue Entry</td>
<td>Queue for attachments before they are processed by a data source. Utilized by vulnerability integrations.</td>
</tr>
<tr>
<td>[sn_vul_ds_import_q_entry]</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Entry</td>
<td>Documented vulnerability.</td>
</tr>
<tr>
<td>[sn_vul_entry]</td>
<td></td>
</tr>
<tr>
<td>Version 12.1:</td>
<td>Stores the relationship between a scan and vulnerability entry.</td>
</tr>
<tr>
<td>Vulnerability Entry Scan</td>
<td></td>
</tr>
<tr>
<td>[sn_vul_entry_scan]</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Exploit Framework</td>
<td>Contains the relationship between Exploit frameworks and vulnerabilities.</td>
</tr>
<tr>
<td>[sn_vul_m2m_framework_vul]</td>
<td></td>
</tr>
<tr>
<td>Version 10.3:</td>
<td>Stores and maintains the state of include or exclude Port for the Configure VI Granularity module.</td>
</tr>
<tr>
<td>Vulnerability Granularity Configuration</td>
<td></td>
</tr>
<tr>
<td>[sn_vul_granularity_config]</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Group</td>
<td>Collection of vulnerable items organized for remediation.</td>
</tr>
<tr>
<td>[sn_vul_vulnerability]</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Group Change Requests</td>
<td>Stores the association of VGs and CHG requests.</td>
</tr>
<tr>
<td>[sn_vul_m2m_vg_change_request]</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Group Item</td>
<td>Association of vulnerability groups and vulnerable items.</td>
</tr>
<tr>
<td>[sn_vul_vulnerability]</td>
<td></td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>[sn_vul_m2m_vul_group_item]</td>
<td>Contains the rules that define the criteria with which groups are automatically created for a set of vulnerable items.</td>
</tr>
<tr>
<td>Vulnerability Group Rule</td>
<td></td>
</tr>
<tr>
<td>[sn_vul_grouping_rule]</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Integration</td>
<td>Schedulable record to import vulnerability data from an external source. Extends Scheduled Script Execution.</td>
</tr>
<tr>
<td>[sn_vul_integration]</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Integration Data Source</td>
<td>Data source to use with a vulnerability integration.</td>
</tr>
<tr>
<td>[sn_vul_int_data_src]</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Integration Log</td>
<td>Records log information output by vulnerability integration runs.</td>
</tr>
<tr>
<td>[sn_vul_integration_log]</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Integration Process</td>
<td>Single process occurrence for a vulnerability integration.</td>
</tr>
<tr>
<td>[sn_vul_integration_process]</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Integration Queue</td>
<td>Queues the import requests for an integration run when all the Data Sources are in use.</td>
</tr>
<tr>
<td>[sn_vul_integration_queue]</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Integration Run</td>
<td>Vulnerability integration invocations.</td>
</tr>
<tr>
<td>[sn_vul_integration_run]</td>
<td></td>
</tr>
<tr>
<td>Version 10.3:</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Integration Run Stats</td>
<td>Stores the breakdown of each step: for example, REST API time, VI creation time, etc. for an integration run</td>
</tr>
<tr>
<td>[sn_vul_integration_stats]</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Item Task</td>
<td>Vulnerable items associated with problems, changes, and security incidents.</td>
</tr>
<tr>
<td>[sn_vul_m2m_item_task]</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Malware Kit</td>
<td>Contains the relationships between vulnerabilities and malware kits.</td>
</tr>
<tr>
<td>[sn_vul_m2m_malware_kit_vul]</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Prerequisite Solution</td>
<td>Contains the source-specific prerequisites to applying a solution, when available.</td>
</tr>
<tr>
<td>[sn_vul_m2m_solution_prerequisite]</td>
<td></td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Vulnerability Rate limit [sn_vul_rate_limit]</td>
<td>Defines a rate limit to be used on a scanner.</td>
</tr>
<tr>
<td>Vulnerability Reference [sn_vul_reference]</td>
<td>External references for known vulnerabilities.</td>
</tr>
<tr>
<td>Vulnerability Remediation Status [sn_vul_m2m_ttr_status]</td>
<td>Status of the vulnerable item against the closest applied remediation target rule.</td>
</tr>
<tr>
<td>Vulnerability Risk Rule [sn_vul_calc_risk]</td>
<td>Specialized calculator rule used with the Risk Score calculators. Takes weights indicating which values, related to a VI, to use to calculate the Risk Score.</td>
</tr>
<tr>
<td>Vulnerability Rollup Calculator [sn_vul_rollup]</td>
<td>List of vulnerability rollup calculators.</td>
</tr>
<tr>
<td>Vulnerability Scan [sn_vul_scan]</td>
<td>Vulnerability scan. Contains what to scan, with what scanner, and a summary of the scan results.</td>
</tr>
<tr>
<td>Vulnerability Scan Configuration Item [sn_vul_m2m_scan_configuration_item]</td>
<td>Associates CMDB CIs that are queued to be scanned.</td>
</tr>
<tr>
<td>Vulnerability Scan Queue Entry [sn_vul_scan_q_entry]</td>
<td>Scan record queued for scanning or processing. Facilitates the requests within stated rate limits.</td>
</tr>
<tr>
<td>Vulnerability Scan Source [sn_vul_m2m_scan_source]</td>
<td>Associates sources to a scan record and signifies all the records that are queued to be scanned.</td>
</tr>
<tr>
<td>Vulnerability Scan Task [sn_vul_m2m_scan_vulnerability]</td>
<td>Associates vulnerability tasks for the sources of a scan record.</td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Vulnerability Software [sn_vul_m2m_entry_software]</td>
<td>Contains associations between vulnerabilities and vulnerable software.</td>
</tr>
<tr>
<td>Vulnerability Solution [sn_vul_solution]</td>
<td>Contains the relationship data between the vulnerability and the possible solutions for it.</td>
</tr>
<tr>
<td>Version 10.3: Vulnerability Solution [sn_vul_solution]</td>
<td>Contains the relationship data between the vulnerability and the possible solutions for it.</td>
</tr>
<tr>
<td>Version 10.0: Vulnerability Solution [sn_vul_m2m_vulnerability_solution]</td>
<td>Links the Vulnerability Entry (sn_vul_entry) table to the Vulnerability Solution (sn_vul_solution) table.</td>
</tr>
<tr>
<td>Vulnerability State Change Approval [sn_vul_change_approval]</td>
<td>Tracks the approval process for vulnerabilities.</td>
</tr>
<tr>
<td>Vulnerability Superseding Solution [sn_vul_m2m_solution_supersedence]</td>
<td>Contains the source-specific relationship between solutions.</td>
</tr>
<tr>
<td>Vulnerability Update Manifest [sn_vul_vuln_update]</td>
<td>Contains a list of vulnerabilities that need their rollup data updated after their vulnerable items are updated, closed, or have risk score changes.</td>
</tr>
<tr>
<td>Version 10.0: Vulnerability Vendor Mapping [sun_vul_vulnerability_vendor_mapping]</td>
<td>Contains a list of vulnerabilities and their vendors.</td>
</tr>
<tr>
<td>Vulnerable Item [sn_vul_vulnerable_item]</td>
<td>Contains the occurrence of a vulnerability on a configuration item.</td>
</tr>
<tr>
<td>Version 10.0: Vulnerable Item Detection [sn_vul_detection]</td>
<td>Contains the vulnerable item detections from third-party integrations.</td>
</tr>
<tr>
<td>Vulnerable Software [sn_vul_software]</td>
<td>Software that is known to have certain vulnerabilities.</td>
</tr>
</tbody>
</table>
Install the Solution Management for Vulnerability Response application

Before you can use the Solution Management for Vulnerability Response feature of Vulnerability Response in your instance, you must complete installation of the Vulnerability Solution Management application. This application is available as a separate subscription in the ServiceNow Store.

Before you begin

Complete the following setup checklist prior to installation. Perform these setup tasks for a smooth installation.

Note: This process applies only to applications downloaded to production instances. If you're downloading applications to sub-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Note: To verify that plugins and applications are installed and activated, navigate to Subscription Management > Subscriptions in your instance. The list displays the subscriptions your organization has purchased.

<table>
<thead>
<tr>
<th>Setup tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that the Vulnerability Response application is installed and activated.</td>
<td>Solution Management for Vulnerability Response requires the Vulnerability Response application. For the most current version of Vulnerability Solution Management, verify you have the most current version of Vulnerability Response installed. See Vulnerability Response and Configuration Compliance Compatibility Matrix for more compatibility information. If the application is not installed and activated see, Install and configure Vulnerability Response.</td>
</tr>
<tr>
<td>Verify that you have entitlement to the application.</td>
<td>To verify you have entitlement to the Vulnerability Solution Management application, navigate to Subscription Management &gt; Subscriptions in your instance. The list displays the</td>
</tr>
<tr>
<td>Setup tasks</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>.subscriptions your organization has purchased.</td>
<td>To get entitlement for the Vulnerability Solution Management application from the ServiceNow Store and download it onto your Now Platform instance, see Get entitlement for a Security Operations product or application.</td>
</tr>
<tr>
<td>Ensure that your NVD records are up-to-date for the last 10 years.</td>
<td>See Managing NVD, CWE, and third-party data libraries.</td>
</tr>
<tr>
<td>Ensure your third-party vulnerabilities are up-to-date.</td>
<td>See Vulnerability Response integrations for information on third-party vulnerability integrations.</td>
</tr>
<tr>
<td>Verify that you have the required Now Platform roles assigned for your instance.</td>
<td>The following roles are required for installation and verification of expected results:</td>
</tr>
<tr>
<td></td>
<td>Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.</td>
</tr>
<tr>
<td></td>
<td>• The System Administrator [admin] installs the application If not already assigned, the admin assigns the vulnerability admin [sn_vul.vulnerability_admin or sn_vul.admin (deprecated)] role.</td>
</tr>
<tr>
<td></td>
<td>• The vulnerability admin oversees configuration and verifies expected results.</td>
</tr>
</tbody>
</table>
Setup tasks | Description
---|---
| Prior to v10.3 of Vulnerability Response:  
- The System Administrator [admin] installs the app and assigns the Vulnerability Admin [sn_vul.admin] role.  
- The Vulnerability Admin [sn_vul.admin] oversees configuration and verifies expected results.

Roles required: admin install the Vulnerability Solution Management application and vulnerability to configure it.

**Procedure**

1. Navigate to the ServiceNow Store.
2. Click **Log in** and enter your HI credentials.
3. Click the **ServiceNow Products** tab to view the available ServiceNow products.
4. Click plus (+) sign next to **Vulnerability Solution Management** to view all the associated applications that you are eligible for.
5. Click **Opt-in** to verify you have entitlement to Vulnerability Solution Management to the application.
6. If you already have entitlement, skip to step 10 to install the application on your Now Platform instance.
7. Select the check box and click **Accept** to agree to the terms and conditions at the prompt.  
   A message is displayed that indicates you have successfully opted-in for the application.
8. **Optional:** Click **Manage Entitlement** if you want to manage your entitlement for Vulnerability Solution Management on other Now Platform instances.

⚠️ **Note:** If the **Manage Entitlement** button is not displayed, click the **Vulnerability Solution Management** application on the Product List to display it.
a. Choose an option

b. Click OK or Cancel to continue.
   You are ready to activate plugins and install the application on your instances.

9. Log in to the Now Platform instance that you want to install the Vulnerability Solution Management application on.

10. Navigate to System Applications > All Available Applications > All.

11. Locate the Vulnerability Solution Management application (sn_vul_solution) and click Install.
    The Application installation dialog displays the application dependency plugin status. Any required dependencies not already installed are automatically installed along with the application.

12. Click Install.
    This installation may take some time. A message is displayed in the Install dialog box after the application and its dependencies are successfully installed.
    The vulnerability admin can now configure the application from within the Setup Assistant.

13. Click Close.
    The Microsoft Security Response Center Solution Integration and Red Hat Solution Integration are the solution applications available in Solution Management for Vulnerability Response after you install Vulnerability Solution Management. The Red Hat Solution Integration is available starting with v10.3 of Vulnerability Response.
    View the Vulnerability Solutions by navigating to Vulnerability Response > Administration > Setup Assistant > Integration Configuration > Solution Integrations. See Configure installed solution integrations for Vulnerability Solution Management using Setup Assistant for more information.

**What to do next**
After you configure the application and the available solutions, check that the CVEs and Solutions agree using Vulnerability Solution [sn_vul_m2m_vulnerability_solution] table.

**Configuring Vulnerability Response using the Setup Assistant**
Setup Assistant walks you through setting up Vulnerability Response and certain third-party integrations for your environment. Setup Assistant provides almost
everything you need to install and set up your environment so that you can use Vulnerability Response.

Using Setup Assistant requires two different Now Platform® roles: admin and vulnerability admin.

Refer to the following sections to supplement the instructions and prompts provided in Setup Assistant.

**System Administration - assign users and groups and install integration applications**

Role required: admin

A list of users and integrations should be obtained from the Vulnerability Manager prior to beginning these tasks.
1. Navigate to **Vulnerability Response > Administration > Setup Assistant**.

![Setup Assistant](image)

2. In the first section, System Administration, the admin assigns roles to users and groups and installs supported integrations.

Starting with version 10.3 of Vulnerability Response and later, assign Vulnerability Response personas and roles to users and groups in Setup Assistant.

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see **Manage persona and granular roles for Vulnerability Response**.

**Note:**

If you are an upgrade customer, access for the users and groups you assigned with the `sn_vul.vulnerability_read` and `sn_vul.vulnerability_write` permissions prior to v10.3 has not changed. Users and groups remain assigned with these roles until you change them. However, starting with v10.3, you may prefer assigning granular roles for more control over what users and groups can do and see in the Vulnerability Response application. For an overview and more information about managing these roles, see **Vulnerability Response personas and granular roles** and **Manage persona and granular roles for Vulnerability Response**.

3. Alternatively, prior to v10.3 of Vulnerability Response, assign roles in Setup Assistant.

   - Assign the role of `sn_vul.admin` to users or groups.
   - Assign the `sn_vul.admin` role for Vulnerability Response administration and configuration including vulnerability integrations, vulnerability group rules, calculators, and time-to-remediate rules.
• Assign the `sn_vul_vulnerability_write` role for the creation and update of vulnerability groups and vulnerable items.

  **Note:** All other users automatically receive Write access only to vulnerability groups that are assigned to them.

• Assign the `sn_vul_vulnerability_read` role to view vulnerability groups, vulnerable items, and other vulnerability information.

  **Note:** Users with the `itil` role are automatically granted the `sn_vul.remediation_owner` role allowing them to see vulnerability groups and vulnerable items assigned to them, vulnerability entries, and, solutions in the Vulnerability Response application on their instance and in the ServiceNow Agent application. No additional assignment is needed.

4. Install third-party integration applications.

• The Qualys Vulnerability Integration can be installed and completely configured in Setup Assistant.

• Starting with v12.1 of Vulnerability Response, you can install and configure the Vulnerability Response Integration with Tenable application using Setup Assistant.

• See Installation of Vulnerability Response and supported applications and Vulnerability Response integrations for more information about applications that are supported by Vulnerability Response.

• For more information about using setup assistant to install supported apps, see Install Vulnerability Response third-party applications using Setup Assistant.

**Vulnerability Response Settings**

Role required: `sn_vul.vulnerability.admin` or `sn_vul.admin` (deprecated), or admin
In Vulnerability Response Settings, the vulnerability administrator defines application-wide settings and defines rules for Vulnerability Response. Alternatively, the admin can perform these tasks.

1. Create Vulnerability Assignment Rules.

Create rules that define the automatic assignment of vulnerability groups for remediation. At least one rule is shipped with the base system. See Vulnerability Response assignment rules overview for more information.

<i>Note:</i>

The reapply feature requires a baseline application of the rules. Once your rules are created, activate the Reapply all vulnerability assignment rules scheduled job to execute, at your convenience. Otherwise, you will be required to reapply all rules to all Open VIs prior to changing them.

When the job is complete, set the Run field in the scheduled job to fit your environment. Depending on the number of active VIs you have, evaluating and updating them daily can have non-trivial performance impact. For larger environments, consider updating once a week or even once a month.

Reapplying assignment rules does not regroup the vulnerable items.

2. Create Vulnerability Group Rules.

Create rules that define the automatic creation of vulnerability groups for remediation. At least one rule, Vulnerability, is shipped with the base system. You can reapply the rules from the form or list view.
• When a group rule is deleted, from the form or list view, you have the option to delete all Open groups created by that rule. Groups not in the Open state are excluded.

• See CI Lookup Rules for identifying configuration items from Vulnerability Response third-party vulnerability integrations for more information on creating rules for your environment.

• See Understanding the Vulnerability Response application for more information on using Vulnerability Response to remediate vulnerabilities.

3. Create and enable Risk Calculators.

Enable risk calculators that define how vulnerable items are scored for prioritization. Several risk calculators are shipped with the base system. See Vulnerability Response calculators and vulnerability calculator rules information on creating or editing risk calculators for your environment.

4. Create Remediation Target Rules.

Create remediation target rules for categories of remediation. At least one rule is shipped with the base system. See Vulnerability Response remediation target rules for more information on creating rules for your environment.

Integration Configuration

Role required: sn_vul.vulnerability.admin or sn_vul.admin (deprecated), or admin

In the Integration Configuration section, configure, schedule, edit, and launch on-demand the following third-party vulnerability scanner integrations and solution providers for the Vulnerability Solution Management application.

• See Configure the Qualys Vulnerability Integration using Setup Assistant for more information about configuring the Qualys Vulnerability Integration.

• Starting with v12.1 of Vulnerability Response, configuration of the Tenable Vulnerability Integration is supported. See Configure the Tenable Vulnerability Integration using Setup Assistant.
After you install the Vulnerability Solution Management application, the Solution Integrations option is displayed below Scanner Integrations. Click Solution Integrations to configure your installed vulnerability solution providers from this section of Setup Assistant. Starting with v10.3 of Vulnerability Response, the Red Hat Solution Integration is available.

See Vulnerability Solution Management for more information about installed solutions. See Install the Solution Management for Vulnerability Response application for more information about installation.

See Configure installed solution integrations for Vulnerability Solution Management using Setup Assistant for more information about configuring your installed solutions.

- If an integration is multi-sourced, you can have multiple deployments of the same third-party integration.
- The settings from your original third-party integration are used as a template for the settings of each new integration.

⚠️ Note: If you delete the original vulnerability integration, you have to select another integration to use as your template. See for more information. Consider disabling the integration instead of deleting it. Integrations created from disabled templates are disabled by default.

Data from each third-party integration is uniquely identified and available in a single instance of Vulnerability Response.

⚠️ Note: Multiple vulnerability integrations for Rapid7 InsightVM are not available within Setup Assistant. See Install and configure the Rapid7 Vulnerability Integration for information on configuring and creating multiple Rapid7 InsightVM integrations.

Additional tasks
Tasks, not covered by Setup Assistant, include, but are not limited to:

- Understanding the Rapid7 Vulnerability Integration
- Define Vulnerability Response email notifications
- Configure the scheduled job for updating CWE records
- Manage individual vulnerable items manually

See Additional Vulnerability Response setup tasks for more information on setup tasks not included in Setup Assistant.
Assign the Vulnerability Response persona roles using Setup Assistant

Assign the Vulnerability Response persona roles to groups or users with Setup Assistant.

Before you begin

If you have already assigned persona roles in Vulnerability Response using Setup Assistant and you want more information about editing and managing your granular roles and role assignments in the User Administration module, see Manage persona and granular roles for Vulnerability Response.

If you are an upgrade customer, you can continue using your existing roles for the Vulnerability Response application. Access for users and groups assigned with the sn_vul.vulnerability_read and sn_vul.vulnerability_write permissions and remediation owner roles prior to v10.3 has not changed.

However, for more control over what users and groups can do and see in the Vulnerability Response application at the task level, you may prefer using persona and granular roles.

If you have not already assigned the sn_vul.vulnerability_admin persona role using Setup Assistant, follow the steps below to assign it. Once assigned, the vulnerability administrator with this persona role has permission to complete the Setup Assistant tasks after the first section, and manage rules and third-party integrations in the Vulnerability Response application.

For an overview about persona roles and granular roles, see Vulnerability Response personas and granular roles.

If you are an upgrade customer, use the following table as a reference.

<table>
<thead>
<tr>
<th>Prior to v10.3</th>
<th>Starting with v10.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you assigned sn_vul.admin</td>
<td>You may prefer to assign sn_vul.vulnerability_admin - Vulnerability Admin to users or groups. Users with this role have complete access to the Vulnerability Response (VR) application and its records. Users with this role configure all VR applications and rules and install third-party integrations.</td>
</tr>
<tr>
<td>If you assigned sn_vulnerability_write for users and groups.</td>
<td>You may prefer to assign sn_vul.vulnerability_analyst - Vulnerability Analyst to users and groups.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Prior to v10.3</th>
<th>Starting with v10.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users and groups with this role view and update all records for VI remediation.</td>
<td>Users and groups with this role view and update all records for VI remediation.</td>
</tr>
</tbody>
</table>

If you assigned `sn_vul.remediation_owner`

Users and groups with this role remediate vulnerabilities assigned to them or to a group they belong to.

Groups or users with this role view and update the records assigned to them or to a group they belong to.

If you assigned `sn_vul.ci- CI Manager`

You may prefer to assign `sn_vul.ci- CI Manager` to users and groups.

Users and groups with this role remediate vulnerabilities assigned to them or to a group they belong to.

Groups or users with this role view and update the records assigned to them or to a group they belong to.

If you assigned `sn_vul.admin for management of unmatched configuration items (CIs)`

You may prefer to assign `sn_vul.ci- CI Manager` to users and groups.

Users and groups with this role remediate vulnerabilities assigned to them or to a group they belong to.

Groups or users with this role view and update the records assigned to them or to a group they belong to.

If you assigned `sn_vul.admin for deferrals and exception approvals.`

You may prefer to assign `sn_vul.ci- CI Manager` to users and groups.

Users and groups with this role remediate vulnerabilities assigned to them or to a group they belong to.

Groups or users with this role view and update the records assigned to them or to a group they belong to.

If you assigned `sn_vul.vulnerability_read`

You may prefer to assign read access to specific areas in the application by task.

For example, assign `sn_vul.read_all` so a user can view all VR records. For read access to view vulnerability group rules, assign `sn_vul.read_group_rules`. Users and groups with this role do not update records.
To view the granular roles a user or groups with a persona role inherits by default, navigate to **User Administration > Roles**. Locate the role you want, and click it to open the record. The Contains Roles tab lists all the granular roles of the persona role as well as any inherited roles.

You may prefer to verify that you have all your required users and groups created before you assign roles in Setup Assistant. Alternatively, to add new users and groups from inside Setup Assistant, click the **User Administration module** link in the form shown in the following figure.

For the following example, to limit access to the Vulnerability Response application, this example shows how to assign a user with the vulnerability admin persona. Usually, you may prefer to assign persona roles other than sn_vul.vulnerability_admin to groups.

**Role required**: admin  

**Procedure**

1. Navigate to **Vulnerability Response > Administration Setup Assistant**. The Setup Assistant page is displayed.

2. Click Vulnerability Response User and Groups. The System Administration Vulnerability Response Users and Groups page is displayed.

3. With Assign roles to a user selected, choose an existing user from the list. You can only assign a user or a group with one persona role.
On the right of the form, after you select a user or group, the default persona, Remediation owner [sn_vul.remediation_owner] is assigned by default and remains displayed in the list until you change it.

**Note:** If you are upgrading to v10.3 and you assigned the sn_vul.vulnerability_read or sn_vul.vulnerability_write role to a user or group prior to the upgrade, it is displayed along with the new persona roles, as shown in the following figure.

If you are an upgrade customer, you can keep using your existing roles for the Vulnerability Response application. Access for users and groups assigned with the sn_vul.vulnerability_read and sn_vul.vulnerability_write permissions and remediation owner prior to v10.3 has not changed.

Note that for existing users or groups currently assigned with the sn_vul.vulnerability_read or sn_vul.vulnerability_write roles, these roles are displayed along with the persona roles in the list. Once you assign a persona role, the old role is no longer available going forward. For example, as shown in following figure, the Write [sn_vul.vulnerability_write] role is no longer displayed as an option for this user or group after it is assigned one of the persona roles.

4. From the list on the right of the form, select **Vulnerability Admin [sn_vul.vulnerability_admin]**. A message is displayed that indicates the user or group is successfully assigned with the persona.
The following image shows the Remediation Owner persona assigned to a group, and the Vulnerability admin persona assigned to a user.

Assign one of the following Vulnerability Response personas to users or groups.
- **Vulnerability Analyst (sn_vul.vulnerability_analyst)**: Manages remediation of all vulnerable items. Views and updates records for VR remediation.
- **Remediation Owner (sn_vul.remediation_owner)**: Remediates vulnerabilities assigned to him or to a group he belongs to.
- **Vulnerability Admin (sn_vul.vulnerability_admin)**: Has complete access to the Vulnerability Response (VR) application and its records. Configures all VR applications and rules and installs third-party integrations. Assigns all VR personas and roles.
- **Configuration Item (CI) Manager (sn_vul.ci_manager)**: Manages unmatched configuration items (CIs) not found in the Configuration Management Database (CMDB). Updates discovered items.
- **Exception Approver (sn_vul.exception_approver)**: Approves exceptions, deferrals, and closures of vulnerability groups and vulnerable items.

**Note:** You can assign one persona at a time to a user or group from Setup Assistant. After you complete your initial configuration in Setup Assistant, manage any additional persona and granular role assignments to users and groups from the User Administration module in your instance.

### Vulnerability Response Users and Groups

**Assign roles to a user**

Select a User

- **Vulnerability Response**
  - 3 Members
  - [Alissa Mountjoy](alissa.mountjoy@example.com)

- **Remediation Owner (sn_vul.remediation)**

- **Vulnerability Admin (sn_vul.vulnerability)**

**5. Using the descriptions of the persona roles listed above, continue to assign any users and groups to the remaining persona roles: Remediation Owner, Vulnerability Analyst, CI Manager, and Exception Approver.**

You have successfully completed assigning persona roles to users and groups using Setup Assistant.

**6. Optional:** To edit the users in a group from Setup Assistant, follow these steps.

**a.** With the group displayed on the form, click the name of the group you want to edit.
   The Group record is displayed.

**b.** With the Group Members tab selected, click **Edit**.
   The Edit Members form is displayed.

**c.** Use the slushbucket to select or remove users.

**d.** Click **Save** to save your changes and return to the Group record.
e. Click **Update** to return to Setup Assistant.

f. On the Setup Assistant page, click **Vulnerability Response Users and Groups** to continue with your configuration in Setup Assistant.

**What to do next**
As system admin, continue with the configuration of Vulnerability Response in Setup Assistant. For more information about installing supported third-party applications for Vulnerability Response in Setup Assistant, see **Install Vulnerability Response third-party applications using Setup Assistant**. For more information about managing granular roles and examples, see **Manage persona and granular roles for Vulnerability Response**.

Note that after the first section is completed in Setup Assistant, you can have a user you assigned with the vulnerability admin persona role complete the configuration tasks.

**Install Vulnerability Response third-party applications using Setup Assistant**
Install the third-party integration applications you have entitlement for in Vulnerability Response using the Setup Assistant.

**Before you begin**
Setup Assistant supports the installation of most third-party integration applications with Vulnerability Response, but you continue with the configuration for some applications from configuration modules in your instance. See **Vulnerability Response integrations** for a list of applications that are supported by Vulnerability Response.

**Note:** This process applies only to applications downloaded to production instances. If you're downloading applications to sub-production or development instances, it's not necessary to get entitlements. Proceed to **Activate a ServiceNow Store application**.

- After it is installed, the Vulnerability Solution Management feature of Vulnerability Response provides you access to the Microsoft Security Response Center Solution Integration in Setup Assistant. Starting with v10.3 of Vulnerability Response, the Red Hat Solution Integration is also available.

- Vulnerability Solution Management is available by separate subscription. See **Vulnerability Solution Management** for more information on how Vulnerability Response incorporates solutions.
Before you can install and activate third-party applications from Setup Assistant, perform the following tasks to ensure a smooth installation:

<table>
<thead>
<tr>
<th>Setup Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have valid ServiceNow entitlements for the integration applications that you want to install.</td>
<td>To verify entitlements, navigate to Subscription Management &gt; Subscriptions in your instance. The list displays the subscriptions your organization has purchased. For more information about getting entitlements for a Security Operations application from the ServiceNow Store, see Get entitlement for a Security Operations product or application.</td>
</tr>
<tr>
<td>(Optional) If not already installed and activated, you may prefer to install the Vulnerability Response application prior to installing the third-party application.</td>
<td>For more information about installing and activating the Vulnerability Response application, see, Install and configure Vulnerability Response.</td>
</tr>
<tr>
<td>Verify you have completed any setup tasks required for the third-party integrations for Vulnerability Response.</td>
<td>Review the required setup tasks in the following topics: - Preparing for the Rapid7 Vulnerability Integration For Rapid7 installation, refer to the installation steps described in Install and configure the Rapid7 Vulnerability Integration for more setup requirements. - Preparing for the Qualys Vulnerability Integration - Preparing for the Tenable Vulnerability Integration - Understanding the Red Hat Solution Integration</td>
</tr>
</tbody>
</table>
Role required: admin

Procedure

1. To view the available applications you can install from Setup Assistant, navigate to **Vulnerability Response > Administration > Setup Assistant > System Administration > Integration Application Installation**.

After a few moments, the applications that are available for installation on your instance are displayed.

2. On the application tile you want to install, click **Install**.
The All Applications dialog is displayed with the name of the application tile you clicked, for example, Rapid7 Integration for Security Operations.

3. Locate the application you want to install, select a version from the choice list, and click Install.

   If an update is available for the application, the **Update** button is displayed.
The Application installation dialog displays the application dependency status. Any required dependencies not already installed are automatically installed along with the application.

4. In the Application installation dialog, click **Install**.

The Install dialog indicates when the installation is successfully completed.

5. Close the dialog.

The All Applications page is displayed that shows your application is successfully installed. After the first section is completed, you can have a
user you assigned with the vulnerability admin persona role complete the configuration tasks in Setup Assistant.

After installation and activation, you can configure, schedule, and launch the following applications directly from Setup Assistant:

- The Qualys Vulnerability Integration
- The Tenable Vulnerability Integration (built by ServiceNow® engineering).
- The Microsoft Security Response Center Solution Integration
- Starting with Vulnerability Response v10.3, the Red Hat Solution Integration

For other applications not listed above, navigate directly to the configuration module of the application to continue with the configuration and to enter any required third-party credentials. For example, the following image shows the location of the Configuration and module for the Rapid7 application.

For more information about configuring specific applications, see the installation and configuration product documentation by product name provided for each application.

**What to do next**

Continue with the configuration of your application in Setup Assistant if your application is supported.

If your application is not supported for configuration in Setup Assistant, navigate directly to the configuration module of the application to continue with the configuration. To view supported applications in Setup Assistant, see, *Installation of Vulnerability Response and supported applications*.

**Configure installed solution integrations for Vulnerability Solution Management using Setup Assistant**

After you install the Vulnerability Solution Management application, you can configure your vulnerability solution providers using Setup Assistant.
Before you begin
Roles required: sn_vul.vulnerability.admin or sn_vul.admin (deprecated), or admin

Use the following sections to supplement the instructions and prompts provided in Setup Assistant for installed solution integrations for Solution Management for Vulnerability Response.

- Verify you have already installed Vulnerability Solution Management and the solution integrations you want before you begin. For more information, see Install Vulnerability Response third-party applications using Setup Assistant.
- Verify you have any third-party account credentials available. They are required to edit some solution integrations.
- See Install the Solution Management for Vulnerability Response application for more information before you configure installed solutions.

Procedure
1. Navigate to Vulnerability Response > Administration > Setup Assistant > Integration Configuration > Solution Integrations.

The Microsoft Security Response Center Solution Integration requires an API key and URL from the Microsoft Security Response Center to configure it.

Note: Starting with v14.0, entering the API key is optional for MSRC. To obtain the MSRC key, you must have a Microsoft ID from a live.com, outlook.com, or Microsoft.com email account, a phone number registered with Microsoft, or a Skype login.

2. Optional: To generate the MSRC key:
   b. Click the Generate API Key button.
   c. Copy the key.
   d. In Setup Assistant, to the right of the Microsoft Security Response Center Solution Integration, click Edit.
   e. Enter the key for the Microsoft Security Response Center Solution Integration.

3. Click the Generate API Key button.
4. Copy the key.
5. In Setup Assistant, to the right of the Microsoft Security Response Center Solution Integration, click Edit.
6. Enter the key for the Microsoft Security Response Center Solution Integration.
7. Enter the URL. The URL in Setup Assistant for MSRC is https://api.msdc.microsoft.com.

8. Click Finish.

9. Optional: You can execute imports on-demand by clicking Execute Now on the configuration page after you enter your credentials.

10. Starting with v10.3 of Vulnerability Response, the Red Hat Solution Integration is also available. It does not require an API key.

11. In Setup Assistant, to the right of the Red Hat Solution Integration, click Edit.

12. Verify the URL in Setup Assistant for RHSI is https://acess.redhat.com/hydra/rest.

13. Optional: You can execute imports on-demand by clicking Execute Now on a configuration page.

14. Click Finish followed by Mark as Complete to complete the configuration. A check mark is displayed in the Setup Assistant for Solution Integrations when you have completed the configuration.

Configure the Qualys Vulnerability Integration using Setup Assistant

After you have installed the Qualys application, configure it using the Setup Assistant.

Before you begin

Roles required: System Admin (admin) for installation, Vulnerability Admin (sn_vul.vulnerability_admin) or sn_vul.admin (deprecated) for configuration.

Use the following sections to supplement the instructions and prompts provided in Setup Assistant for configuration of the Qualys Vulnerability Integration.

- Verify you have already installed the application before you begin. For more information, see Install Vulnerability Response third-party applications using Setup Assistant.

- See Preparing for the Qualys Vulnerability Integration for more information before you configure the Qualys Vulnerability Integration.

- Verify you have any third-party account credentials available. They are required to edit some third-party applications.

Procedure

1. Navigate to Vulnerability Response > Administration > Setup Assistant > Integration Configuration > Scanner Integrations. The installed integrations are displayed.
2. Click **Edit** to the right of the Qualys Vulnerability Integration you want to configure.

3. In the Account Credentials form, enter your Qualys Cloud Platform credentials. Your credentials are required to configure it.

4. Use the following notes as a guide as you continue with the configuration.

- If you have upgraded from an earlier version of Vulnerability Response with a version of the Qualys Vulnerability Integration you’ve already configured, that version, with its configuration settings preserved, is still available.

Under Import Settings in Host Detection Configuration for the Qualys Vulnerability Integration, there is an option to view fixed Qualys vulnerability detection records. If enabled, this permits you to create vulnerable items from detection records in a fixed status (state=**Fixed**). For more information on vulnerable item detections, see **Vulnerability Response vulnerable item detections from third-party integrations**.

Version 10.3: All host tags are imported as part of the Qualys Host List integration. Host tags are used primarily for filtering in Vulnerability Response Assignment and Vulnerability Group Rules. They are displayed in the Discovered Item form.

**Note:** The Qualys Host List integration should be run prior to creating Assignment or Vulnerability Group Rules in Vulnerability Response so that all tags can be present in the rules and before vulnerable items are imported and grouped.

Version 10.0: Qualys **Asset Tags** are stored in the Host Tags module under the Qualys Vulnerability Integration.

- The Qualys Vulnerability Integration supports multi-source. You can have multiple deployments of the same third-party integration. To add another integration, on the Scanner Integrations page, click **Add Integration**. The settings from your original third-party integration are used as a template for the settings of each new integration.

**Note:** If you delete the original vulnerability integration, you have to select another integration to use as your template. See for more information. Consider disabling the integration instead of deleting it. Integrations created from disabled templates are disabled by default.
Data from each third-party integration is uniquely identified and available in a single instance of Vulnerability Response.

- You can execute imports on-demand by clicking **Execute Now** on a configuration page.

5. Click **Finish** to complete the configuration in Setup Assistant.

**Configure the Tenable Vulnerability Integration using Setup Assistant**

After you have installed the Vulnerability Response Integration with Tenable application, configure it using the Setup Assistant.

**Before you begin**

Roles required: System Admin (admin) for installation, Vulnerability Admin (sn_vul.vulnerability_admin) or sn_vul.admin (deprecated), and Configure Integration (sn_vul_tenable.configure_integrations) for configuration

Use the following sections to supplement the instructions and prompts provided in Setup Assistant for the Vulnerability Response Integration with Tenable integration.

- Verify you have already installed the application before you begin. For more information, see **Install Vulnerability Response third-party applications using Setup Assistant**.

- See **Preparing for the Tenable Vulnerability Integration** for more information before you configure the application.

- Verify you have any third-party account credentials available. They are required to edit some third-party applications.

**Procedure**

1. If not displayed, navigate to **Vulnerability Response > Administration > Setup Assistant > Integration Configuration > Scanner Integrations**. The Tenable.io and Tenable.sc integrations are displayed.
Tenable is a multi-source integration, and you can have multiple deployments of the same third-party integration. The settings from your original third-party integration are used as a template for the settings of each new integration.

⚠️ Note: If you delete the original vulnerability integration, you have to select another integration to use as your template. See for more information. Consider disabling the integration instead of deleting it. Integrations created from disabled templates are disabled by default.

Data from each third-party integration is uniquely identified and available in a single instance of Vulnerability Response.

2. To the right of the Tenable integration you want to configure, click Edit.
3. In the Account Credentials form, fill in the fields.
   Enter your Tenable credentials.
   • Tenable.io requires Administrator access with a permission attribute greater than or equal to 64.
   • Tenable.sc requires Security Analyst or Manager access.
4. Click Next to save your changes and proceed to the first integration form. The Asset Import Configuration form is displayed.
5. On this form, enable or disable the Asset Import, determine the initial start date for the assets you want imported, and schedule when the Tenable asset import should run.
• For the Tenable.io integration, you also have the option to enable and disable the import of asset tags. Asset tags are imported by default and used for organizing and tracking the assets listed in your CMDB in the Tenable.io environment.

• Click CI Lookup rules to display the default configuration item (CI) lookup rules. CI Lookup Rules define how asset data from third-party sources are used to identify Configuration Items (CIs) in the Now Platform CMDB. You have the option to add lookup rules or modify the default CI lookup rules on this page. For more information, see CI Lookup Rules for identifying configuration items from Vulnerability Response third-party vulnerability integrations.

• Click Import Assets Now to import data on-demand.

• The Advanced Settings link points you to the Integration record.

6. Click Next to save your changes and proceed to the next form.

The Plugins Import Configuration form is displayed.

7. On this form, enable or disable the Plugins (Third-party Vulnerability Entries) Import determine the initial start date for the plugins you want imported, and schedule when the Tenable Plugins import should run. If you want to import all the plugins, vulnerabilities, and assets, leave the initial start date blank.

• Click Import Plugins Now to import data on-demand.

• The Advanced Settings link points you to the Integration record.

• For the vulnerabilities import, you can schedule and set severity levels for Tenable.io for the vulnerabilities that you want ingested. Determine a date so only the vulnerabilities created or updated starting with a specific date are imported.

• For the Tenable.sc integration, you can determine a query filter and a date so only the vulnerabilities created or updated starting with a specific date are imported.

8. Click Next to save your changes and proceed to the next form.

The Vulnerabilities Import Configuration form is displayed. Enable or disable the integration and determine the initial start date for the vulnerabilities you want imported.

Also, for Tenable.io:

• Import only the vulnerabilities and associated VIs that match the conditions you select with the Severity filter.

• Enable the Fixed Vulnerabilities option to view VIs for fixed detection records. If this flag is enabled in Setup Assistant, new VIs are created for
detections in the **Fixed** state that do not already exist in your instance. When enabled, this feature may negatively impact your ingestion performance.

- The **Advanced Settings** link points you to the Integration record.
- Click **Import Schedules** to configure how often vulnerabilities are ingested and enable the integration.

For Tenable.sc:

- Import only the vulnerabilities and associated VIs that match the condition filters set by a Tenable Query in the Tenable platform. See Tenable documentation for more information about Tenable queries.

- Enable the **Fixed Vulnerabilities** option to view VIs for fixed detection records. If this flag is enabled in Setup Assistant, new VIs are created for detections in the **Fixed** state that do not already exist in your instance. When enabled, this feature may negatively impact your ingestion performance.
- The **Advanced Settings** link points you to the Integration record.
- Click **Import Schedules** to configure how often vulnerabilities are ingested and enable the integration.

- The ServiceNow® Tenable.sc Scan Credential Integration is enabled (**Active**) automatically from within the Setup Assistant in your instance when you configure the Tenable.sc Vulnerabilities integrations (Tenable.sc Open and Fixed Vulnerabilities Integrations).

  This Integration imports and updates scanner credentials from the Tenable.sc product in your instance. This integration runs weekly to import and securely store your Tenable credentials data. Navigate to **Tenable Vulnerability Integration** > **Integrations** > **Tenable.sc Scan Credential Integration** to view more information about the Scan Credential Integration.

9. Click **Finish** to save your changes and complete the configuration in Setup Assistant.

**What to do next**

(Optional) Navigate to **Vulnerability Response** > **Administration** > **Vulnerability Calculators** > **Default Risk Calculator** > **Tenable Risk Rule** to enable the Tenable Risk Rule.

In the Vulnerability Calculator Rule form that is displayed, select the Active checkbox to enable it.

The Tenable Risk Rule is installed with the Vulnerability Response Integration with Tenable application as part of the Default Risk Calculator in the Vulnerability Calculators from Vulnerability Response. The Vulnerability Priority Rating (VPR) is an attribute from the Tenable product that is imported and used with the
new default risk calculator. This risk rule is disabled by default. By enabling the Tenable risk calculator rule, the imported VPR values are used to calculate the Risk Score for vulnerable items. The default weight distribution for this risk calculator: VPR = 70%, Asset=15%, and Business Criticality=15%. Enabling this Tenable Risk Calculator rule may impact your data ingestion performance.

See Vulnerability Response calculators and vulnerability calculator rules for more information about risk calculators.

**Install and configure the Performance Analytics for Vulnerability Response [PA] application**

Before you can use the Performance Analytics for Vulnerability Response application, you must get entitlement and download the application from the ServiceNow Store, install it on your Now Platform® instance, and complete a few installation and configuration steps. The PA application is not installed as part of the Vulnerability Response application. It is available as a separate subscription.

**Before you begin**

If you already have the application on your instance and you are updating to a newer version of the application, proceed to step 8 in the following steps to continue with the update and configuration.

For a fresh installation, complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

To verify that plugins and applications are installed and activated, navigate to **Subscription Management > Subscriptions** in your instance. The list displays the subscriptions your organization has purchased.

**Note:** This process applies only to applications downloaded to production instances. If you're downloading applications to sub-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

<table>
<thead>
<tr>
<th>Setup tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that the Vulnerability Response dependencies plugin (com.snc.vul_dep) is installed and activated.</td>
<td><strong>Vulnerability Response Dependencies</strong>&lt;br&gt;This plugin contains all the dependency plugins required to support the application.</td>
</tr>
<tr>
<td>Setup tasks</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>To verify that the plugin is installed and activated, in your instance you want the application navigate to <strong>System Applications &gt; All Available Applications &gt; All</strong>. If you are prompted to update other dependency plugins, Click the links in the dialogs and follow the prompts to continue.</td>
<td><strong>Vulnerability Response</strong> To verify that the plugin is installed and activated, in your instance you want the application navigate to <strong>System Applications &gt; All Available Applications &gt; All</strong>. If you are prompted to update other dependency plugins, Click the links in the dialogs and follow the prompts to continue. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
</tr>
<tr>
<td>Verify that you have the required ServiceNow roles for your instance. Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial</td>
<td>The following roles are required for installation, configuration, and verification of expected results:</td>
</tr>
<tr>
<td>Verify that the ServiceNow Vulnerability Response application (sn_vul) is installed and activated.</td>
<td>• The Performance Analytics Admin [pa_admin] or the system [admin] installs the application and verifies the expected results.</td>
</tr>
</tbody>
</table>
Setup tasks | Description
--- | ---
assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response. | • The Vulnerability Admin [v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)] oversees configuration and verifies expected results with the PA dashboards.
• The Remediation Owner [sn_vul.remediation_owner] oversees change management tasks and reads and updates assigned records. The sn_vul.remediation_owner role is also automatically assigned when any user is assigned the itil role.

Verify the versions of Performance Analytics and the Vulnerability Response application are compatible. | See Vulnerability Response and Configuration Compliance Compatibility Matrix for more information.

Role required: admin or pa_admin

Procedure

1. To get entitlement and download the application on your Now Platform instance, navigate to the ServiceNow Store.

2. In the upper right of the page, click Log in.

3. In the dialog that is displayed, enter your HI credentials and click Login.
4. On the page that is displayed, if not selected, click the ServiceNow Products tab.

5. On the product list page, click **Performance Analytics - Vulnerability Response**.

6. Enter the **Instance Name** and **Reason for the Instance**, and click **Validate Instance**.
   A page with the Opt-in button is displayed.

7. To get the Performance Analytics for Vulnerability Response application, click **Opt-in**.

8. To agree to the terms and conditions, at the prompt, select the check box and click **Accept**.

9. **Optional:** Alternatively, to manage your entitlement for the application on other Now Platform instances, follow these steps.

   a. If the Manage Entitlement button is not displayed, click the Performance Analytics for Vulnerability Response application on the Product List to display it.

   b. With the Eligible tab selected, click **Manage Entitlement**.
c. In the Manage Entitlements for Vulnerability Response dialog that is displayed, choose one:

- Entitlement Type
  - Remove all existing entitlements
  - Entitle all instances
  - Entitle selected instances

  ![Entitlement Selection Dialog](image)

  

  Cancel OK

  d. Click OK or Cancel to continue.

  You are ready to activate plugins and install the application on your Now Platform instance(s).

10. Log in to the Now Platform instance that you want to install the Vulnerability Response application on.

11. Navigate to System Applications > All Available Applications > All.

12. From the applications listed, locate the Performance Analytics - Content Pack - Vulnerability Response (sn_vul_analytics) application and click Install.

  Note: If you are updating to a new version, select the version you want from the choice list.
and click **Update**. The Application installation dialog is displayed. Any dependencies that will be installed automatically with the application are also displayed.

13. If you want demo data, select the Load demo data check box and click **Install**.

   **Note:** If you do not select the **Load demo data** check box, demo data is not available to install from the **Application Manager** later. For information on how to install or reinstall demo data after the initial installation, see the **Work around to install demo data if application is already installed** [KB0722909] article in the **Now Support Knowledge Base**.

This installation may take some time. A message is displayed in the Install dialog after the application is successfully installed.

14. Click **Close**.

15. **Optional:** If you anticipate a large number of active vulnerable items in your environment, you may prefer to change the default setting for the maximum number of collected records, enable scheduled jobs, and set collection times during off-hours. To change these and other settings for the application after it is installed, follow these steps.

   a. Navigate to **Performance Analytics > Admin console**.

   b. On the Advanced Configuration tile, click the **Performance Analytics Properties** link.

   c. On the Admin Console [Performance Analytics] page, scroll to the Performance Analytics Data Collector section. The default setting (50,000 records) is displayed for the Maximum number of rows that are allowed to be fetched from an Indicator Source.
Performance Analytics Data Collector

Maximum time in seconds a script is allowed to run during a Data Collection cycle

30

Maximum duration in minutes that a single query for a data collection job can run before a warning is logged

60

Maximum number of rows that are allowed to be fetched from an Indicator Source

50000

d. You may prefer to increase this number to a value that is roughly 20% more than the total number of active vulnerable items (VIs) you anticipate in your environment.

e. Click Save.

f. To activate scheduled jobs, navigate to Performance analytics > Data Collector > Jobs.
The Scheduled Data Collection list is displayed. In the Active column, the scheduled jobs listed in the Application column for Performance Analytics - Content Pack - Vulnerability Response by default are disabled (false).

Note: a scheduled job for historical data collection is not displayed on the list of jobs. For large sets of data, you may prefer to start collecting data and trends over time by enabling your daily jobs when you are setting up the Performance Analytics for Vulnerability Response application.

g. In the Name column, click a link to open a PA_VR job record.
h. If fields are not editable, click the here link to edit them.

i. In the Job parameters section, click the Active check box to schedule a job. The Time fields are displayed.

```
Job parameters
```

Specify when to run the scheduled data collection job.

<table>
<thead>
<tr>
<th>Run as</th>
<th>System Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run as tz</td>
<td>System (US/Pacific)</td>
</tr>
<tr>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>Run</td>
<td>Daily</td>
</tr>
<tr>
<td>Collect</td>
<td>Scores only</td>
</tr>
<tr>
<td>Time</td>
<td>Hours 05 30 00</td>
</tr>
<tr>
<td>Conditional</td>
<td></td>
</tr>
</tbody>
</table>

Update | Execute Now | Cancel Job | Delete |

j. Enter the start time for the job.
If you anticipate a large volume, you may prefer to set collection times during off-hours. If you anticipate 10 million active VIs or greater in your environment, contact your ServiceNow® implementation partner for more information on setting up your data collection environment.

For more information about the indicators used for data collection, see View the Performance Analytics indicators for Vulnerability Response[PA].

k. After you have enabled all the jobs you want, click Update.
The Scheduled Data Collection list is displayed.

What to do next
Navigate to Vulnerability Response > Overview to view the dashboard.

Additional Vulnerability Response setup tasks
To help with remediation, create or adjust reports, define email notifications, manage vulnerability libraries, or create custom vulnerability integrations in addition to your Setup Assistant configuration.

You can use the default reporting supplied with Vulnerability Response to oversee your security posture. You can edit those reports if they do not suit your environment, or use them as templates to create your own.
If the Performance Analytics for Vulnerability Response application is installed, you can create reports, responsive dashboards, and more. See Getting Started with reports for more information.

Email notifications increase productivity and smooth workflow.

National Vulnerability Database (NVD) and Common Weakness Enumeration (CWE) vulnerability imports are standard. Configure these imports so they can be used successfully within Vulnerability Response. These configurations are done manually.

**Note:** NVD vulnerability imports download JSON files instead of XML in anticipation of the switch to JSON by NVD.

With Software Exposure Assessment, look up the publisher, product name, and version number in Software Asset Management (SAM Foundation) to determine your exposure to vulnerable software.

Visibility into vulnerability libraries can provide flexibility with grouping and remediation tasks.

**Manage persona and granular roles for Vulnerability Response**

After you complete your initial assignment of persona roles using Setup Assistant, manage additional granular role assignments to users or groups from the User Administration module in your instance.

**Before you begin**

If you have not already completed your initial set up and configuration for Vulnerability Response using Setup Assistant, or assigned persona roles to users and groups, navigate to Vulnerability Response > Administration > Setup Assistant. See Assign the Vulnerability Response persona roles using Setup Assistant.

For key terms and an overview of persona roles, see Vulnerability Response personas and granular roles.

A persona role is pre-configured role in the application that is made up of multiple granular roles. The persona roles in Setup Assistant, Vulnerability Admin, Vulnerability Analyst, Remediation Owner, Configuration Item Manager, and Exception Manager, are designed to correspond to common job titles for managers, analysts, and service owners in an IT organization or vulnerability remediation group.

If you want your users and groups to have more access than one of the roles permits, you can add more granular roles to users and groups. Conversely, if you want to limit access for specific users and groups at the task level, you can remove granular roles. Also, you can build custom roles to suit your needs.
Role required: admin

Procedure

1. To manage granular roles for users and groups, choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Edit the granular roles for a user or group</strong></td>
<td>Assign or remove granular roles for users or groups, or edit granular roles so that only select users within a group have expanded or limited permissions. An example follows the table.</td>
</tr>
<tr>
<td><strong>Create a new role</strong></td>
<td>Create a new role using one or more granular roles from the library for a specific job title, or to fulfill a specific requirement. An example follows the table.</td>
</tr>
</tbody>
</table>

The names for the granular roles in Vulnerability Response usually describe what users can do and see. To view descriptions of specific granular roles, navigate to User Administration &gt; Roles and locate the role that you want. Role description, roles that are automatically inherited when a role is assigned, and any roles that depend on other roles are also listed.

2. To assign or remove a granular role for a user or a group, follow these steps. As an example, assume you want to assign an IT manager with a role that permits this manager to view records but not update or edit them. To view records in Vulnerability Response, Performance Analytics for Vulnerability Response, and for all third party integrations, you assign this user with the sn_vul.read_all granular role.

   a. Navigate to User Administration &gt; Users.

   b. Locate the user, and, in the Name column, click the record to open it. The user’s record is displayed.

   c. If not selected, select the Roles tab. The roles currently assigned to the user are displayed.

   d. Click Edit. The Edit members form is displayed.
e. In the Collection field of the slushbucket, enter the name of the role if you know it, or, enter *sn_vul to view only the granular roles available for Vulnerability Response.

f. Locate and move sn_vul.read_all to the Roles List.

Caution: Use the same process to remove specific granular roles from users in the slushbucket by moving the role from the Roles list to the Collection list.

g. Click Save.
The user record is displayed with the new granular role.

h. Click Update to save your changes and return to the Users list.
You have provided a user with permission to read but not update records in Vulnerability Response, Performance Analytics for Vulnerability Response, and for third party integrations.

3. To edit a group so that only specific members have expanded access with more granular roles, follow these steps.
As example, assume you want to permit certain users in the Remediation Owner (sn_vul.remediation_owner) group to create vulnerable items manually, but you don't want to expand that permission to all users in the group. The permission to create vulnerable items manually is granted by the sn_vul.create_vulnerable_items granular role. To grant this permission to only select users from this group, follow these steps.

a. Navigate to User Administration > Groups.

b. Locate the Remediation Owner group, and, in the Name column, click the group to open the record.
The group record is displayed.

c. If not selected, select the Group Members tab.
The current members of the group are displayed.

d. Click a name from the list you want to assign the granular role to and open the record.

e. On the record, scroll to the Roles tab and select it.
The roles assigned to the user are displayed.
f. Click Edit.
The Edit members form is displayed.

g. In the Collection field, enter the name of the role if you know it, or, enter *sn_vul* to view all the granular roles available for Vulnerability Response.

h. Locate and move sn_vul.create_vulnerable_items to the Roles List.

i. Click Save.
The user record is displayed with the new granular role.

j. Click the back arrow to return to view the users in the record for the Remediation Owner group.

k. Click names from the list you want to assign this granular role to, open their records, and use the slushbucket to assign the role.

l. After you complete your edits, Click Update to save your changes and return to the groups list. You have provided some users in the Remediation Owner (sn_vul.remediation_owner) group permission to create vulnerable items manually.
4. To create a new role using only granular roles you select, follow these steps. For this example, assume you want to create role for a compliance auditor. This role works closely with Governance, Risk, and Compliance (GRC), and the job requires the following permissions and tasks within Vulnerability Response:

- Manages remediation deadlines for vulnerable items and vulnerability groups
- Approves exception requests for extending deadlines or deferring remediation
- Manages the clean up of older vulnerable items with auto-delete
- Define risk scores
- Reads all records in Vulnerability Response but is not permitted to edit them.

a. Navigate to User Administration > Roles.

b. In the Roles list, click New.

c. In the Role record, fill out the fields. Create a name, select the application that contains this record, and enter a short description for your new role. For more information about the other fields on the form, see Create a role

Note: When creating a name for your new role, you may prefer to use a name that is easily recognized in the roles list and describes the functionality of the role. For this example, you may prefer a title such as, Compliance Auditor - GRC-VR.

d. Click Submit.
The Roles list is displayed.

e. Locate your new role and click it to open the record.

f. Click Edit.
The Edit Members form is displayed.

g. Use the slushbucket to add granular roles to your new role. For this example, the required roles for this new role are displayed in the right column in the following figure.
To display only the granular roles for Vulnerability Response, in the Collection field, enter sn_vul.
h. Click **Save**.
   The record for your new role is displayed. Starting with the Contains Roles tab, continue editing the role as required.

i. Click **Update** to save your changes.
   Your new role is displayed on the Roles list.

Add vulnerability significance charts to the Vulnerability Response homepage

You can add vulnerability significance definition charts and other visualizations to the Overview.

**Before you begin**

Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see **Assign the Vulnerability Response persona roles using Setup Assistant**. For more information about managing granular roles, see **Manage persona and granular roles for Vulnerability Response**.

The Vulnerability Analytics plugin must be activated.
Procedure

1. Navigate to **Vulnerability > Overview**.
   Some reports are added to the dashboard by default. For more information about these reports, see Using the default Vulnerability Response dashboards.

2. Near the dashboard header, click the plus sign icon **Add content** to open the dialog box to add more widgets.

3. From the lists in the **Add Widgets** dialog box, select **Reports** to display more Vulnerability Response reports.

<table>
<thead>
<tr>
<th>Content</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Group Details</td>
<td>Treemap &gt; Vulnerability Significance &gt; Vulnerability Significance</td>
</tr>
<tr>
<td>Vulnerability Significance score report</td>
<td>Performance Analytics &gt; Score &gt; Services with Vulnerability Significance</td>
</tr>
<tr>
<td>Vulnerable Entry</td>
<td>Reports &gt; Vulnerable Entry &gt; Vulnerabilities by Impact, Score, Week</td>
</tr>
<tr>
<td>Vulnerability Group</td>
<td>Reports &gt; Vulnerable Group &gt; Vulnerability Group by Time to Remediate Status</td>
</tr>
<tr>
<td>Vulnerability Group Item</td>
<td>Reports &gt; Vulnerable Group Item &gt; New Vulnerable Items</td>
</tr>
<tr>
<td>Vulnerability Integration Run</td>
<td>Reports &gt; Vulnerability Integration Run &gt; Last 30 Days Qualys Duplicates, New VIs, Results, Updated VIs, Qualys Integration Runs</td>
</tr>
<tr>
<td>Vulnerable Item</td>
<td>Reports &gt; Vulnerable Item &gt; An extensive list of vulnerable item filters including open Qualys VIs.</td>
</tr>
</tbody>
</table>

4. Click the location on the screen you want to add the gauge.

5. Close the **Add content** box.

**Define Vulnerability Response email notifications**

Email notifications can be useful when National Vulnerability Database (NVD) records are uploaded so that analysts are informed when new records have been imported. Creating an email notification involves specifying when to send it, who receives it, and what it contains.
Before you begin
Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure
1. Navigate to Vulnerability Response > Administration > Email Templates.
2. Click New.

   For detailed instructions for creating email notifications, see Create an email notification.

Define Vulnerability Response email templates
Creating an email notification involves specifying when to send it, who receives it, and what it contains.

Before you begin
Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure
1. Navigate to Vulnerability > Administration > Email Templates.
2. Click New.

   For detailed instructions for creating email templates, see Construct an email message with a template.

Create or edit remediation target notifications
Vulnerability administrators can edit the remediation target notification or add new ones, specifying when to send the notification, who receives the notification, and what content is in the notification.
Before you begin
Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure
1. Navigate to Vulnerability > Administration > Notifications.
2. Select the remediation target notification record or click New.
3. Fill in fields on the form, as appropriate. Fields are described in detail in Create an email notification.
4. Click Preview Notification.

Managing NVD, CWE, and third-party data libraries

Vulnerability data can be imported from the National Vulnerability Database (NVD), Common Weakness Enumeration (CWE), or third-parties and used to decide whether to escalate a vulnerability group. Once imported, you can update NVD records on-demand or configure a scheduled job to update them or CWE regularly. Vulnerability Response stores them under Libraries.

The Common Vulnerability Scoring System (CVSS), included in NVD and third-party entries, captures the main characteristics of a vulnerability. Vulnerability Response uses CVSS data to produce a normalized value reflecting vulnerability severity. When the severity is computed, the vulnerability provides a better understanding of the risk posed by this vulnerability to your organization. Severity helps you assess and prioritize vulnerability remediation.

If this is your first installation of Vulnerability Response, perform an initial import of CWE, and then NVD records when you configure your scheduled jobs. See Configure the scheduled job for updating CWE records and prior to Vulnerability Response v13.0, Configure the scheduled job for updating NVD records (Prior to v13.0) for more information.

By default, prior to v13.0, all data feeds for NVD Auto-update are disabled. To enable the feeds you want, see Configure the scheduled job for updating NVD records (Prior to v13.0).

Starting with v13.0, the NIST National Vulnerability Database Integration - API (CVE only) integration is pre-configured and activated. It runs daily. See or Understanding the NVD integrations for more information.
CWE updates are **On Demand**, by default, and must be enabled for a scheduled job. See Configure the scheduled job for updating CWE records.

The Vulnerable items in your system are grouped and are usually managed in bulk, but can be managed individually. Each vulnerability is represented by a vulnerability entry in the library, from the NVD, or a third-party source. For information on the vulnerability entry fields, see Vulnerability Response vulnerability form fields.

The following libraries are available:

<table>
<thead>
<tr>
<th>Libraries</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NVD</td>
<td>List of vulnerabilities found by NVD and includes security checklists,</td>
</tr>
<tr>
<td></td>
<td>security-related software flaws, misconfigurations, product names,</td>
</tr>
<tr>
<td></td>
<td>and impact metrics including exploits.</td>
</tr>
<tr>
<td>CWE</td>
<td>List of community-developed software weakness types.</td>
</tr>
<tr>
<td></td>
<td>Each CWE record also includes an associated knowledge article that</td>
</tr>
<tr>
<td></td>
<td>describes the weakness. You cannot escalate a vulnerability from the</td>
</tr>
<tr>
<td></td>
<td>Common Weakness Enumerations screen, it is for reference only.</td>
</tr>
<tr>
<td>Third-party</td>
<td>List of imported third-party vulnerabilities in your instance. Contains</td>
</tr>
<tr>
<td></td>
<td>a list of related references, vulnerable items, exploits, and CVEs.</td>
</tr>
<tr>
<td>Vulnerable</td>
<td>Deprecated: List of all vulnerable software in your instance.</td>
</tr>
<tr>
<td>Software</td>
<td></td>
</tr>
</tbody>
</table>

**Related information**

- View Vulnerability Response vulnerability libraries

**Configure the scheduled job for updating CWE records**

Use Common Weakness Enumeration (CWE) records downloaded from the CWE database for reference when deciding whether a vulnerability must be escalated. Update common weakness records from the Common Weakness Enumeration database on a regularly scheduled basis. You can also update the default script or write your own scripts, as needed.

**Before you begin**

Roles required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more
information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Each CWE record also includes an associated knowledge article that describes the weakness. You cannot escalate a vulnerability from the Common Weakness Enumerations page.

- If you have the admin role, you can add repositories to the scheduled job.
- If you have sn_vul.vulnerability_read, you can execute the scheduled job.
- If you have sn_vul.vulnerability_write, you can edit the details of the scheduled job.

Procedure

1. Navigate to Vulnerability > Administration > Integrations.
2. Select the CWE Comprehensive 2000 Integration scheduled job.
3. Modify the fields, as needed.

Vulnerability Integration form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the scheduled job.</td>
</tr>
<tr>
<td>Active</td>
<td>Whether the scheduled job is active. If you do not want the job to run for</td>
</tr>
<tr>
<td></td>
<td>a specific time period, you can set up the parameters you want to use and</td>
</tr>
<tr>
<td></td>
<td>deactivate the job.</td>
</tr>
<tr>
<td>Run</td>
<td>Frequency you want the job to run. Subsequent fields are displayed or hidden</td>
</tr>
<tr>
<td></td>
<td>based on your setting in this field.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
|       | 1 Note: The CWE update is On Demand by default. Set to a scheduled period that is prior to your NVD updates. Choices include:  
  • Daily: Choose a Time  
  • Weekly: (most common choice) Choose a Day and Time  
  • Monthly: Choose Day and Time  
  • Periodically: Choose a Repeat interval, Starting date and time  
  • Once: Choose a Starting date and time |
| Day   | The day you want the scheduled job to run.  
If you selected Weekly in the Run field, this field displays the days of the week. If you selected Monthly in the Run field, this field displays the days of the month.  
2 Note: Schedule the CWE update to run prior to the NVD database update. The default day for the NVD update is Weekly on Monday. |
| Time  | The time you want the scheduled job to start.  
3 Note: Schedule the CWE update to run prior to the NVD database update. The default time for the NVD update is 01:00:00 |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration script</td>
<td>The script for pulling data from the data sources specified in the <strong>Data Sources</strong> related list.</td>
</tr>
<tr>
<td>Application</td>
<td>[Read only] The name of the application for which you are running the scheduled job.</td>
</tr>
<tr>
<td>Repeat Interval</td>
<td>The number of days and hours before the scheduled job runs again. This field appears when <strong>Periodically</strong> is selected in the <strong>Run</strong> list.</td>
</tr>
<tr>
<td>Starting</td>
<td>The date and time to start the periodic updates. This field appears when <strong>Periodically</strong> is selected in the <strong>Run</strong> list.</td>
</tr>
<tr>
<td>Conditional</td>
<td>The check box to add conditional parameters.</td>
</tr>
<tr>
<td>Condition</td>
<td>The conditions to run the schedule job. This field appears when <strong>Conditional</strong> check box is selected.</td>
</tr>
<tr>
<td>Report processor strategy</td>
<td>The strategy for pulling data and processing the scheduled job.</td>
</tr>
<tr>
<td></td>
<td>- To pull data from the data sources in the <strong>Data Sources</strong> related list using the script in the <strong>Integration script</strong> field, select <strong>Data Source Attachment</strong>.</td>
</tr>
<tr>
<td></td>
<td>- To select a custom processor in the <strong>Report Processor script</strong> field, select the <strong>Custom Report Processor</strong>.</td>
</tr>
<tr>
<td>Report processor</td>
<td>The script to be executed when the scheduled job runs. This field appears when <strong>Custom Report Processor</strong> is selected in the <strong>Report processor strategy</strong> list.</td>
</tr>
</tbody>
</table>
| Processor factory script     | The script to build the report processor. This field appears when
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Custom Report Processor</strong> is selected in the <strong>Report processor strategy</strong> list.</td>
<td></td>
</tr>
</tbody>
</table>

4. Right-click in the header to **Save** your changes.

5. To run the scheduled job immediately, click **Execute Now**. You are returned to the Vulnerability Integrations view.

6. To watch the progress of the import, select the **CWE Comprehensive 2000 Integration** scheduled job again and select the **Vulnerability Integration Runs** tab.

   See [View Vulnerability Response vulnerability libraries](#) to see the imported entries.

---

**Configure the scheduled job for updating NVD records (Prior to v13.0)**

Identify the repositories that you want updated regularly. You can execute a scheduled job to update National Vulnerability Database (NVD) records on a nightly or weekly basis.

**Before you begin**

ℹ️ **Note:** This feature has been deprecated in favor of the Vulnerability Response integration with NVD available in the ServiceNow Store.

The NVD runs as a scheduled job weekly on Mondays at 01:00:00. This scheduled job is enabled by default, however if **Auto-update**, for each repository, is not set, an import is not initiated.

ℹ️ **Note:** If you receive a 'server overload' error for an NVD download, reset your time for 15 minutes, before or after 1:00:00 to avoid traffic on the NVD website.

NVD vulnerability imports download JSON files, instead of XML, in anticipation of the switch to JSON by NVD. The JSON download contains the CVSS v3 data. CVSS v3 data is not available prior to 2015.

If the NVD data feed you want to use for the scheduled job is not present, you can add it.

Roles required:

- If you have the admin role, you can add repositories to the scheduled job.
- If you have sn_vul.vulnerability_read, you can execute the scheduled job.
- If you have sn_vul.vulnerability_write, you can edit the details of the scheduled job.
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure

1. Navigate to Vulnerability > Administration > NVD Auto-Update.
2. For each NVD repository that you want to update automatically, change the Automatically update field to true.
3. Navigate to Vulnerability > Administration > Integrations.
4. Select the NIST National Vulnerability Database scheduled job.
5. Modify the fields as needed.

Vulnerability Integration form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the scheduled job.</td>
</tr>
<tr>
<td>Active</td>
<td>Specifies whether the scheduled job is active. If you have previously set up this job and then decided to use a different integration, you can uncheck this box to deactivate the job.</td>
</tr>
<tr>
<td>Run</td>
<td>Frequency you want the job to run. Subsequent fields are displayed or hidden based on your setting in this field.</td>
</tr>
<tr>
<td>Day</td>
<td>Day you want the scheduled job to run. If you selected Weekly in the Run field, this field displays the days of the week. If you selected Monthly in the Run field, this field displays the days of the month.</td>
</tr>
<tr>
<td>Time</td>
<td>Time you want the scheduled job to start.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Application</td>
<td>[Read only] Name of the application for which you are running the scheduled job.</td>
</tr>
<tr>
<td>Repeat Interval</td>
<td>Number of days and hours before the scheduled job runs again. This field appears when Periodically is selected from the Run list.</td>
</tr>
<tr>
<td>Starting</td>
<td>Date and time to start the periodic updates. This field appears when Periodically is selected from the Run list.</td>
</tr>
<tr>
<td>Conditional</td>
<td>Check box to add conditional parameters.</td>
</tr>
<tr>
<td>Condition</td>
<td>Conditions to run the scheduled job. This field appears when the Conditional check box is selected.</td>
</tr>
<tr>
<td>Integration Details</td>
<td></td>
</tr>
<tr>
<td>Integration script</td>
<td>Script for pulling data from the data sources in the Data Sources related list.</td>
</tr>
<tr>
<td>Integration factory script</td>
<td>Calls the Integration script.</td>
</tr>
<tr>
<td>Report processor strategy</td>
<td>Strategy for pulling data and processing the scheduled job.</td>
</tr>
<tr>
<td>Report processor</td>
<td>Script to execute when the scheduled job runs. This field appears when Custom Report Processor is selected.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>selected in the <strong>Report processor strategy</strong> list.</td>
<td>Processor factory script Script to build the report processor. This field appears when Custom Report Processor is selected in the Report processor strategy list.</td>
</tr>
</tbody>
</table>

**Related Lists**

<table>
<thead>
<tr>
<th>List</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Sources</td>
<td>Defines what data should be imported.</td>
</tr>
<tr>
<td>Vulnerability Integration Runs</td>
<td>Historical record of the integration executions.</td>
</tr>
</tbody>
</table>

6. To save your changes, click **Update**.

7. To run the scheduled job immediately, click **Execute Now**.

**Note:** When the scheduled job runs and new records are downloaded to the NVD, an email notification is sent to the members of the vulnerability response group.

**Related information**

- Report processor strategies
- Integration factory script fields

**Update NVD on-demand (Prior to v13.0)**

A scheduled job usually updates National Vulnerability Database (NVD) records but you can update the NVD library selectively.

**Before you begin**

**Note:** This feature has been deprecated in favor of the Vulnerability Response integration with NVD available in the ServiceNow Store

Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see **Assign the Vulnerability Response persona roles using Setup Assistant**. For more information about managing granular roles, see **Manage persona and granular roles for Vulnerability Response**.
About this task
This update includes both CVSS v2 and CVSS v3 data, where available. CVSS v3 data is not available prior to 2015. NVD vulnerability imports download JSON files, instead of XML, in anticipation of the switch to JSON by NVD.

Procedure
1. Navigate to Vulnerability > Administration > On-Demand Update.
2. Select the check boxes for the repositories you want to update.
3. Click Import.
   The Total entries, Last refreshed date, and Last import fields are updated.

What to do next
By default, the NVD update is set to run weekly, every Monday at 01:00:00.

Note:
If you receive a 'server overload' error for an NVD download, reset your time for 15 minutes, before or after 1:00:00 to avoid traffic on the NVD website. To change your default settings, see Configure the scheduled job for updating NVD records (Prior to v13.0).

The default value for the System Property > Import Export > Import Properties > JSON Format Maximum size for import (MB) is 100. Before updating an NVD feed, check the size of the files in the JSON .zip file and change the system property to 250 before import. Reset the value back to 100 after import to prevent memory issues in your environment.

Add new NVD data feeds (Prior to v13.0)
If the National Vulnerability Database (NVD) releases a new annual, modified, or recent feed you can add it, as needed, to your instance.

Before you begin
Note: This feature has been deprecated in favor of the Vulnerability Response integration with NVD available in the ServiceNow Store

Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.
Procedure

1. Navigate to **Vulnerability > Administration > NVD Auto-Update**.
2. Click **New**.
3. Fill in the fields, as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>Name for the data feed.</td>
</tr>
<tr>
<td>Total entries</td>
<td>This field is auto-filled with the total number of entries imported when this NVD data feed is updated.</td>
</tr>
<tr>
<td>Last refreshed</td>
<td>This field is auto-filled with the date of the last import when this NVD data feed is updated.</td>
</tr>
<tr>
<td>State</td>
<td>This field is auto-filled when this NVD data feed is updated.</td>
</tr>
<tr>
<td>Percent complete</td>
<td>This field is auto-filled with the percentage of when this NVD data feed is updated.</td>
</tr>
<tr>
<td>Automatically update</td>
<td>Check box to enable automatic updates of this data feed based on the scheduled job.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Note:</td>
<td>CVSS v3 data is not available prior to 2015.</td>
</tr>
<tr>
<td></td>
<td>The default value for the System Property &gt; Import Export &gt; Import Properties &gt; JSON Format Maximum size for import (MB) is 100. Before creating an NVD feed, check the size of the files in the JSON .zip file and change the system property to 250 before import. Reset the value back to 100 after import to prevent memory issues in your environment.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**View Vulnerability Response vulnerability libraries**

You can view vulnerability data imported from the National Vulnerability Database (NVD), Common Weakness Enumeration (CWE), or third-parties to decide whether to escalate a vulnerability group.

**Before you begin**

Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see **Assign the Vulnerability Response persona roles using Setup Assistant**. For more information about managing granular roles, see **Manage persona and granular roles for Vulnerability Response**.

**Procedure**

1. Navigate to **Vulnerability > Libraries**. For information on specific fields, see **Vulnerability Response vulnerability form fields**.

   The following libraries are available:
<table>
<thead>
<tr>
<th>Libraries</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NVD</td>
<td>List of vulnerabilities found by NVD and includes security checklists, security-related software flaws, misconfigurations, product names, and impact metrics including exploits.</td>
</tr>
<tr>
<td>CWE</td>
<td>List of community-developed software weakness types. Each CWE record also includes an associated knowledge article that describes the weakness. You cannot escalate a vulnerability from the Common Weakness Enumerations screen, it is for reference only.</td>
</tr>
<tr>
<td>Third-party</td>
<td>List of imported third-party vulnerabilities in your instance. Contains a list of related references, vulnerable items, exploits, and CVEs.</td>
</tr>
<tr>
<td>Vulnerable Software</td>
<td>Deprecated: List of all vulnerable software in your instance.</td>
</tr>
</tbody>
</table>
2. Choose a library to view vulnerabilities.

Vulnerability Response vulnerability form fields

Vulnerabilities are created automatically when records are downloaded from the National Vulnerability Database (NVD), Common Weakness Enumeration.
(CWE), or third-party integrations and stored under **Libraries** in Vulnerability Response.

**NVD entry fields**
The imported fields in this table are read-only. Vulnerable Items (VIs), Vulnerable Software, and Vulnerability References are automatically associated and entries can be manually added.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identifier for this vulnerability entry.</td>
</tr>
<tr>
<td>Risk rating</td>
<td>(Hidden when no VIs are associated with the vulnerability)</td>
</tr>
<tr>
<td></td>
<td>Quantified <strong>Risk Score</strong> separating vulnerable items into Critical, High, Medium, Low, and None. For more information on risk ratings, see Vulnerability Response calculators and vulnerability calculator rules.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This base <strong>Risk rating</strong> is not the same as the Solution record <strong>Risk rating</strong>.</td>
</tr>
<tr>
<td>Risk score</td>
<td>(Hidden when no VIs are associated with the vulnerability)</td>
</tr>
<tr>
<td></td>
<td>Calculated amount of risk the vulnerable item poses to your environment.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This base <strong>Risk score</strong> is not the same as the Solution record <strong>Risk score</strong>. For more information, see Vulnerability Response calculators and vulnerability calculator rules.</td>
</tr>
<tr>
<td>Severity</td>
<td>Normalized degree of severity of this vulnerability. Severity maps are provided for NVD and with ServiceNow third-party integrations. For more information on creating or adjusting severity maps, see Create a Vulnerability Response severity map.</td>
</tr>
<tr>
<td>Exploit exists</td>
<td>Yes, if at least one exploit is associated with this vulnerability.</td>
</tr>
<tr>
<td>Exploit skill level</td>
<td>Lowest skill level required to exploit this vulnerability.</td>
</tr>
<tr>
<td>Exploit attack vector</td>
<td>Most vulnerable attack vector of the exploits for this vulnerability.</td>
</tr>
<tr>
<td></td>
<td>Available when SAM NVD is enabled.</td>
</tr>
<tr>
<td>Active VIs</td>
<td>(Hidden when no VIs are associated with the vulnerability)</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Number of vulnerable items associated with this vulnerability, not in the Closed state. If there are no active VIs for this vulnerability, Risk Rating and Risk Score are not displayed.</td>
<td></td>
</tr>
<tr>
<td>CWE entry</td>
<td>Reference to the Common Weakness Enumeration element that this vulnerability best fits into.</td>
</tr>
<tr>
<td>Date published</td>
<td>Date the vulnerability was published.</td>
</tr>
<tr>
<td>Last modified</td>
<td>Date the vulnerability was last modified.</td>
</tr>
<tr>
<td>Summary</td>
<td>Description of the vulnerability.</td>
</tr>
</tbody>
</table>

**Vulnerability Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVSS v2</td>
<td>Imported CVSS v2 data</td>
</tr>
<tr>
<td>CVSS v3</td>
<td>Imported CVSS v3 data, not available prior to 2015.</td>
</tr>
<tr>
<td>Preferred solution</td>
<td>Solution of the highest-supersedence in the chain, derived from the solutions referenced in the vulnerability. If more than one highest-supersedence exists in the chain, no value is set. Any value set manually can be overwritten on subsequent imports. Setting this value manually should be done on the vulnerable item.</td>
</tr>
</tbody>
</table>

**Remediation Status**

(Hidden when no VIs are associated with the vulnerability)

**Excludes Deferred**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerable items</td>
<td>Number of active vulnerable items with this vulnerability. This count excludes deferred vulnerable items.</td>
</tr>
<tr>
<td>Total VIs</td>
<td>Total number of vulnerable items with this vulnerability. This count excludes deferred vulnerable items.</td>
</tr>
<tr>
<td>%VIs remediated</td>
<td>Percent complete for remediation of vulnerable items with this vulnerability. This count excludes deferred vulnerable items.</td>
</tr>
</tbody>
</table>

**Includes Deferred**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerable items</td>
<td>Number of active vulnerable items with this vulnerability.</td>
</tr>
<tr>
<td>Total VIs</td>
<td>Total number of vulnerable items with this vulnerability.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>%VIs remediated</td>
<td>Percent complete for remediation of vulnerable items with this vulnerability.</td>
</tr>
</tbody>
</table>

**Related Links**

<table>
<thead>
<tr>
<th>Prior to v13.0: Force software vulnerability import</th>
<th>(Deprecated) Re-calculates product mapping with ITSM Software Asset Management based on information from NVD. Updates the Vulnerable Software library.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> Removed in v13.0</td>
<td></td>
</tr>
</tbody>
</table>

| Version 10.0: Update status | Displays date and time of the last update.  
|                            | Updates the following:  
|                            |  • Vulnerability group state  
|                            |  • Risk score and rating  
|                            |  • Metrics such as Active VIs, Total VIs from the Remediation Status section |

**Related Lists**

<table>
<thead>
<tr>
<th>Vulnerable Items</th>
<th>(Hidden when no VIs are associated with the vulnerability) Vulnerable items associated with this vulnerability.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability References</td>
<td>Information about the vulnerability from external sources, cited by NVD.</td>
</tr>
<tr>
<td>Exploits</td>
<td>Exploits associated with this vulnerability.</td>
</tr>
<tr>
<td>Solutions</td>
<td>(Hidden when no VIs are associated with the vulnerability) All Vulnerability Solution Management integration solutions associated with this vulnerability.</td>
</tr>
<tr>
<td>Weaknesses</td>
<td>Imported <strong>Weakness</strong> data associated to a Common Vulnerabilities and Exposures (CVE).</td>
</tr>
<tr>
<td>Vulnerable Software</td>
<td>(Hidden when software is associated with the CVE) Imported Common Platform Enumeration (CPE) data associated with the vulnerability.</td>
</tr>
</tbody>
</table>
CWE vulnerability entry fields
The imported fields in this table are read-only.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-ID</td>
<td>Identifier for this vulnerability entry.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the vulnerability.</td>
</tr>
<tr>
<td>Knowledge</td>
<td>Knowledge base article associated with this vulnerability.</td>
</tr>
<tr>
<td>Name</td>
<td>Descriptive name assigned to this CWE-ID.</td>
</tr>
</tbody>
</table>

Third-party vulnerability entry fields
The imported fields in this table are read-only.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identifier for this vulnerability entry.</td>
</tr>
<tr>
<td>Source</td>
<td>Origin of the vulnerability — whether a scanner or physical test.</td>
</tr>
<tr>
<td>Risk rating</td>
<td>Quantified Risk Score separating vulnerable items into Critical, High, Medium, Low and None. For more information on risk ratings see, Vulnerability Response calculators and vulnerability calculator rules.</td>
</tr>
<tr>
<td>Risk score</td>
<td>Calculated amount of risk the vulnerable item poses to your environment, based on risk score.</td>
</tr>
<tr>
<td>Severity</td>
<td>Normalized degree of severity of this vulnerability. Severity maps are provided for NVD and with ServiceNow third-party integrations. For more information on creating or adjusting severity maps, see Create a Vulnerability Response severity map.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Exploit exists</td>
<td>Yes, if at least one exploit is associated with this vulnerability.</td>
</tr>
<tr>
<td>Exploit skill level</td>
<td>Lowest skill level required to exploit this vulnerability.</td>
</tr>
<tr>
<td>Exploit attack</td>
<td>Most vulnerable attack vector of the exploits for this vulnerability.</td>
</tr>
<tr>
<td>vector</td>
<td></td>
</tr>
<tr>
<td>Active VIs</td>
<td>Number of vulnerable items associated with this vulnerability, not in the Closed state.</td>
</tr>
<tr>
<td>Category</td>
<td>Classification provided by the third-party integration. Aids in assignment.</td>
</tr>
<tr>
<td>Remediation type</td>
<td>Types of remediation actions.</td>
</tr>
<tr>
<td></td>
<td>• Patch</td>
</tr>
<tr>
<td></td>
<td>• Configuration change</td>
</tr>
<tr>
<td></td>
<td>• Patch and Configuration change</td>
</tr>
<tr>
<td></td>
<td>• Countermeasure</td>
</tr>
<tr>
<td>CWE entry</td>
<td>Reference to the Common Weakness Enumeration element that this vulnerability best fits into.</td>
</tr>
<tr>
<td>PCI</td>
<td>When the checkbox is selected, the vulnerability is flagged for significant risk for exposure of payment information.</td>
</tr>
<tr>
<td>PCI severity</td>
<td>Level of risk for exposure of payment information. [Qualys only.]</td>
</tr>
<tr>
<td>Date published</td>
<td>Date the vulnerability was published.</td>
</tr>
<tr>
<td>Last modified</td>
<td>Date the vulnerability was last modified.</td>
</tr>
<tr>
<td>Summary</td>
<td>Description of the vulnerability.</td>
</tr>
</tbody>
</table>

**Vulnerability Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVSS v2</td>
<td>Imported CVS v2 data</td>
</tr>
<tr>
<td>CVSS v3</td>
<td>Imported CVSS v3 data, not available prior to 2015.</td>
</tr>
<tr>
<td>Threat</td>
<td>Description of the threat from this vulnerability.</td>
</tr>
<tr>
<td>Preferred Solution</td>
<td>Solution of the highest-supersedence in the chain, derived from the solutions referenced in the vulnerability. If more than one highest-supersedence exists in the chain, no value is set. Any value set manually can be overwritten on subsequent</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>imports. Setting this value manually should be done on the vulnerable item.</td>
<td></td>
</tr>
<tr>
<td>Remediation notes</td>
<td>Description of the remediation solution pulled from the vendor.</td>
</tr>
<tr>
<td><strong>Remediation Status</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Excludes Deferred</strong></td>
<td></td>
</tr>
<tr>
<td>Vulnerable items</td>
<td>Number of active vulnerable items with this vulnerability. This count excludes deferred vulnerable items.</td>
</tr>
<tr>
<td>Total VIs</td>
<td>Total number of vulnerable items with this vulnerability. This count excludes deferred vulnerable items.</td>
</tr>
<tr>
<td>%VIs remediated</td>
<td>Percent complete for remediation of vulnerable items with this vulnerability. This count excludes deferred vulnerable items.</td>
</tr>
<tr>
<td><strong>Includes Deferred</strong></td>
<td></td>
</tr>
<tr>
<td>Vulnerable items</td>
<td>Number of active vulnerable items with this vulnerability.</td>
</tr>
<tr>
<td>Total VIs</td>
<td>Total number of vulnerable items with this vulnerability.</td>
</tr>
<tr>
<td>%VIs remediated</td>
<td>Percent complete for remediation of vulnerable items with this vulnerability.</td>
</tr>
<tr>
<td><strong>Related Links</strong></td>
<td></td>
</tr>
<tr>
<td>Version 10.0:</td>
<td>Displays date and time of the last update.</td>
</tr>
<tr>
<td>Update status</td>
<td>Updates the following:</td>
</tr>
<tr>
<td></td>
<td>• Vulnerability group state</td>
</tr>
<tr>
<td></td>
<td>• Risk score and rating</td>
</tr>
<tr>
<td></td>
<td>• Metrics such as Active VIs, Total VIs from the Remediation Status section</td>
</tr>
<tr>
<td><strong>Related Lists</strong></td>
<td></td>
</tr>
<tr>
<td>Vulnerable Items</td>
<td>Vulnerable items associated with this vulnerability.</td>
</tr>
<tr>
<td>Vulnerability References</td>
<td>Information about the vulnerability from external sources, cited by NVD.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CVEs</td>
<td>Common Vulnerability Enumeration (CVE) record associated with this vulnerability.</td>
</tr>
<tr>
<td>Categories</td>
<td>Categories associated with this vulnerability.</td>
</tr>
<tr>
<td>Exploits</td>
<td>Exploits associated with this vulnerability.</td>
</tr>
<tr>
<td>Vulnerability Malware Kits</td>
<td>Malware kits associated with this vulnerability.</td>
</tr>
<tr>
<td>Solutions (Rapid7)</td>
<td>Solution information from the Rapid7 solution integrations. Displayed when available.</td>
</tr>
<tr>
<td>Exploit Frameworks</td>
<td>Exploit frameworks associated with this vulnerability.</td>
</tr>
<tr>
<td>Solutions</td>
<td>Vulnerability Solution Management solutions associated with this vulnerability.</td>
</tr>
</tbody>
</table>

**Add CVEs to third-party entries**

Common Vulnerability and Exposure (CVE) information can be related to a single third-party vulnerability. It is usually added during third-party integration import however, you can add multiple CVEs (vulnerabilities) manually.

**Before you begin**

Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated) Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

**Procedure**

1. Navigate to **Vulnerability > Libraries > Third-Party**.
2. Open a record.
3. Click on the **CVEs** related list tab.
4. Click **Edit**.

5. Choose which CVEs to add.

   🔄 **Note:** You can use condition filters to refine the CVE collection.

6. Click **Save**.

**Install Vulnerability Assignment Recommendations for Vulnerability Response**

Install Vulnerability Assignment Recommendations so that you can reduce the time that you spend on identifying owners for vulnerability findings that are unassigned or incorrectly assigned. This application is available as a separate subscription in the ServiceNow Store.

**Before you begin**

Before you run the Vulnerability Assignment Recommendations feature of Vulnerability Response in your Now Platform® instance, you must first download and install the Vulnerability Assignment Recommendations for Vulnerability Response application. Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

/jpeg

   🔄 **Note:** This process applies only to applications that are downloaded to production instances. If you’re downloading applications to non-production or development instances, it’s not necessary to get entitlements. For more information, see Activate a ServiceNow Store application.

<table>
<thead>
<tr>
<th>Setup tasks</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that the Vulnerability Response application (starting with v12.1) is installed and activated.</td>
<td>Navigate to <strong>System Applications &gt; All Applications &gt; Installed in your instance</strong>. Vulnerability Response is shown in this list if it is installed.</td>
</tr>
<tr>
<td>Setup tasks</td>
<td>Action</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>If the application is not installed and activated, see Install and configure Vulnerability Response.</td>
<td>If the application is not installed and activated, see Install and configure Vulnerability Response.</td>
</tr>
<tr>
<td>Verify that the Predictive Intelligence application is installed and activated.</td>
<td>Navigate to System Applications &gt; All Applications &gt; Installed in your instance. Predictive Intelligence is shown in this list if it is installed.</td>
</tr>
<tr>
<td>Verify that you have the required ServiceNow roles for your instance.</td>
<td>Check that you have these required roles for installation and verification of expected results:</td>
</tr>
<tr>
<td></td>
<td>• vulnerability_admin: Required to enable and configure Vulnerability Assignment Recommendations. You can also use it to view and select assignment recommendations for vulnerable items and vulnerability groups.</td>
</tr>
<tr>
<td></td>
<td>• ServiceNow admin: Required to install applications.</td>
</tr>
</tbody>
</table>

**Procedure**

1. Navigate to the ServiceNow Store.
2. Click Log In and enter your HI credentials.
3. To view the available ServiceNow products, click the ServiceNow Products tab.
4. To view all the associated applications that you are entitling for Vulnerability Assignment Recommendations, click the Vulnerability Response product.

The page lists all the applications that you are eligible for if you opt-in. For information on an application, click the link for the application.

5. To verify that you have entitlement to Vulnerability Assignment Recommendations, click Opt-in.

6. To agree to the terms and conditions, at the prompt, select the check box and click Accept.

A message appears that indicates you have successfully opted-in for the application.

7. Skip to step 10 to install the application on your Now Platform instance.

8. Optional: If you want to manage your entitlement for the Vulnerability Assignment Recommendations application on other Now Platform instances, click Manage Entitlement.

   Note:
   If the Manage Entitlement button is not displayed, click the Vulnerability Assignment Recommendations application on the Product List to display it.

a. Choose an option.

b. Click OK or Cancel to continue.

You are ready to activate plugins and install the application on your Now Platform instances.

9. Log in to the Now Platform instance that you want to install the Vulnerability Assignment Recommendations application on.

10. Navigate to System Applications > All Available Applications > All.

11. From the applications listed, locate the Vulnerability Assignment Recommendations application (sn_vul_recom) and click Install.

The Application installation dialog box is displayed and any dependencies that are installed are displayed.

12. Optional: If you want demo data, select the Load demo data check box and click Install.

   Note: If you do not select the Load demo data check box, demo data is not available to install from the Application Manager later. For information on how to install or reinstall demo data after the initial installation, see the Work around to install demo data if application is already installed [KB0722909] article in the Now Support Knowledge Base.
This installation may take some time. A message is displayed in the Install dialog box after the application and its dependencies are successfully installed.

13. Click Close.

14. To configure Vulnerability Assignment Recommendations, see Configure Vulnerability Assignment Recommendations for Vulnerability Response.

Configure Vulnerability Assignment Recommendations for Vulnerability Response

Enable Vulnerability Assignment Recommendations to reduce the time that you spend on identifying the owners for vulnerability findings that are unassigned or incorrectly assigned.

Before you begin
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Role required: sn_vul.manage_assignment_recom_config

About this task
This application is not enabled by default.

Procedure

1. Navigate to Vulnerability Response > Administration > Assignment Recommendations.

2. Select Enable Assignment Recommendations. The Predictive Intelligence solution definition field appears. The default value is Vulnerable Item Assignment.

3. Click Save.

Create and train a solution definition for Vulnerability Response

Create and train a solution definition model for Vulnerability Response by using Predictive Intelligence. You can use this model to predict the assignment group for a vulnerable item (VI) or vulnerability group (VG) based on existing data.

Before you begin
Role required: sn_vul.vulnerability_admin
Procedure

1. Navigate to **Predictive Intelligence > Classification > Solution Definitions**.
2. On the Classification Definitions form, click **Vulnerable Item Assignment**. This solution definition is the default one.

**Note:**

- The default Training Frequency is 30 days. This means that every 30 days, the model re-trains automatically using the VI dataset that matches the configured filter condition.

- Fields from the Vulnerable Item table can be used for training. The default solution definition trains on two VI fields: **Vulnerability.Summary** and **Configuration item.Name**. You can customize the fields used for training, depending on which fields you find helpful for predicting vulnerability ownership in your organization.

3. To create and train the classification solution, see **Create and train a classification solution**.

**Note:** You can also create and train a similarity or a clustering solution. For more information, see:

- Create and train a similarity solution.
- Create and train a clustering solution.

4. Click **Update & Retrain**.

**Note:** To configure advanced settings for ML solutions, see **Configuring advanced settings for your ML solutions**.

Configure Exposure Assessment

To assess the zero-day (current day) exposure of your assets to vulnerable software with the Exposure Assessment application, first verify that the ITSM Software Asset Management application is installed.

With the vulnerability write role, (sn_vulnerability_write), you can view the Exposure Assessment module and create and edit exposure assessment records on-demand for vulnerable software in your instance with the Vulnerability Response application.

Compatibility and system requirements

The Exposure Assessment module for the Vulnerability Response application is compatible with New York v10.0 and Orlando family releases. The Vulnerability Response application is available on the ServiceNow Store. The ITSM Software
Asset Management application (com.snc.asset_management) is required for the Exposure Assessment module. This application manages all your assets and software licenses, and the SAM Foundation version of this application is part of the Vulnerability Response application you download from the ServiceNow Store. The Exposure Assessment application works with either the SAM Foundation or the SAM Pro Now Platform® applications.

The SAM Pro application is not part of the core Vulnerability Response product from the ServiceNow Store and requires a separate subscription.

To verify the SAM Foundation application is installed on your instance, navigate to System Applications > All Available Applications > All and search for com.snc.asset_management. If the application is not installed, click Install.

Since the Exposure Assessment application requires access to the asset data on your Now Platform® instance, the asset management applications must have data to reference. The Software Discovery Models table (cmdb_sam_sw_discovery_model) and the Software installations (cmdb_sam_sw_install) require data.

Refer to the following topic for the steps to assess your exposure to vulnerable software.

Assess your exposure to vulnerable software

You can provide the publisher and product information in the Exposure Assessment module to assess your zero-day (current day) exposure of your assets to vulnerable software using the ITSM Software Asset Management application.

Before you begin
For more information on system requirements, see Configure Exposure Assessment.

Use case

View the software exposure assessment module and create and edit exposure assessment records on-demand for vulnerable software in your Now Platform® instance.

You manage the vulnerability response activities for a large operation responsible for many assets. The Security Operations Center (SOC) in your operation contacts you about a version of software that they have learned is vulnerable. You discover that a scan of your assets just recently completed and did not find this vulnerability. The SOC team learned about this vulnerability from a reliable source outside of the National Vulnerability Database (NVD), Common Weakness Enumeration (CWE), or the other third-party libraries in your instance, and you are concerned that your vulnerability scanner has not yet added the plugin for it.
You are confident that the data for this vulnerability will be updated in the NVD and imported soon so that your scanner can catch this vulnerability in the next scan, but because you are concerned about the scope of your potential exposure, you want to determine today if you have assets in your network that have this software installed.

Role required: vulnerability admin (sn_vulnerability_write)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Have the following information available about the vulnerable software you want to assess:

- Publisher
- Version
- Product
- Edition

Procedure

1. To create a new exposure assessment, navigate to **Vulnerability Scanning > Exposure Assessment**.
   
   The Exposure Assessments list is displayed.

   ![Exposure Assessments](image)

2. Click **New**.
   
   The Exposure Assessment form is displayed.
3. Fill out the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publisher</td>
<td>Name of the software publisher.</td>
</tr>
<tr>
<td>(Optional) Version</td>
<td>Enter the version number to help you narrow the search on your assets.</td>
</tr>
<tr>
<td>Product</td>
<td>Name of the software product.</td>
</tr>
<tr>
<td>(Optional) Edition</td>
<td>Enter the edition to help you narrow the search on your assets.</td>
</tr>
<tr>
<td>CI filter</td>
<td>Use the choice lists for the Configuration Item (CI) filter to limit your search to specific configuration items (assets). For example, you can submit a query for only active assets that may have this software installed:</td>
</tr>
</tbody>
</table>

Operational status is Operational

4. Click **Show Exposure**.

The Exposure Assessment record with your discovery model and the software installation count on your assets as of the specific date is displayed.
5. Choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Exposure</td>
<td>Add additional CI filter conditions and click <strong>Show Exposure</strong> to further refine your search results.</td>
</tr>
<tr>
<td>Create Vulnerable Items</td>
<td>Create vulnerable items for the configuration items from your search results. If vulnerable items are successfully created, a vulnerability group is created for all the vulnerable items and displayed on the exposure assessment record.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete this record and return to the Exposure Assessments list. A confirmation dialog is displayed.</td>
</tr>
</tbody>
</table>

6. Optional: Create vulnerable item for your search result. Alternatively, revise your filter conditions and further refine your search results.

⚠️ Note: After you create vulnerable items, you cannot alter the search criteria for this exposure record.

7. To create vulnerable items, follow these steps:

a. Click Create Vulnerable Items.
   The Create Vulnerable Items dialog is displayed.

b. Fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using</td>
<td>Form the choice list, choose one to continue.</td>
</tr>
<tr>
<td></td>
<td>• Existing vulnerability. To the right of the Vulnerability field, click the search icon. In the list that is displayed, select the CVE-ID, or enter search criteria to locate the existing CVE-ID, for example, CVE 2018-9120.</td>
</tr>
<tr>
<td></td>
<td>⚠️ Note: This can be a CVE-ID from a vulnerability database other than the NVD.</td>
</tr>
<tr>
<td></td>
<td>• New vulnerability. Enter the CVE-ID for your new vulnerability in xxxx-xxxx, xxxx-xxxxx, or xxxx-xxxxxxx format.</td>
</tr>
<tr>
<td>Vulnerability summary</td>
<td>Enter a summary for the new vulnerability, for example, An attacker can execute script on an unsuspecting user's browser.</td>
</tr>
<tr>
<td>(for new vulnerability only)</td>
<td></td>
</tr>
</tbody>
</table>

The following images show examples of the completed form for an existing vulnerability and a new vulnerability.
c. Click **Create Vulnerable items**.

   The Exposure Assessment record is displayed with a status message that indicates vulnerable items are being created.

   
   
   d. After a few seconds, at the top of the form, right-click in the gray banner to reload the page.

   The new vulnerable items are displayed as shown in the following figure on the Assessed Vulnerable Items tab (531). The new vulnerability group created for these vulnerable items is displayed on the Vulnerability Groups tab (1).
Note: For this example, a vulnerability group is created according to the group rules and conditions from the vulnerability group rule called, *Vulnerability*. This group rule is the default vulnerability group rule that is installed with the Vulnerability Response product in your Now Platform® instance. In this example, the conditions of this group rule placed all the vulnerable items into a single vulnerability group. If you prefer to create more than one vulnerability group for the vulnerable items that match your exposure assessment search results, you may prefer to set up additional vulnerability group rules. Creating more vulnerability groups may help you prevent creating vulnerability groups with large numbers of vulnerable items. For more information about vulnerability group rules, see *Vulnerability Response groups and group rules overview* and *Create or edit Vulnerability Response group rules*.

8. Choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerability Groups</strong></td>
<td>With the Vulnerability Groups tab selected, in the number column, click to open the record and review and assign the vulnerability group for</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>remediation. For more information on assignment groups, see.</td>
</tr>
<tr>
<td>Assessed Vulnerability Items</td>
<td>With the Assessed Vulnerable Items tab selected, in the Vulnerable item column, click to open the records and review and assign individual vulnerable items.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete the exposure assessment record. A confirmation dialog is displayed.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you delete the exposure record after you create vulnerability items, any vulnerable items that you create for this record that are not related to another exposure record are automatically moved to the Closed state. The reason for closure is Cancelled.</td>
</tr>
</tbody>
</table>

**Confirmation**

Deleting this record results in the following actions:

- Related exposed discovery models are deleted.
- All assessed vulnerable items are closed.

Are you sure you want to delete this record?

[Cancel] [Delete]

**What to do next**

Respond to any zero-day (current day) threats based on your exposure assessment. For more information about vulnerability groups and change management for Vulnerability Response, see [Vulnerability Response groups and group rules overview](#) and [Change management for Vulnerability Response](#).

**Manage individual vulnerable items manually**

Vulnerable items represent one configuration item (CI) with a given vulnerability. Vulnerable items are imported from third-party sources, or using the SAM NVD information (link) to compare vulnerability entries to software records retrieved from the Software Asset Management module.
Vulnerable items are contained in vulnerability groups defined by vulnerability rules. Typically vulnerability groups are the location where groups of vulnerable items are assigned and worked on.

Vulnerable items can be viewed and edited in bulk from the **Vulnerable Items** module. Vulnerable item records display information from the vulnerability in the **Vulnerability** tab of a vulnerability group. This tab can indicate whether there are public or active exploits for it. Also, whether it can be remediated via a patch, configuration change, or combination of both. If there are IP addresses that are found during de-duplication, they appear in a related list.

If a CI is removed from the CMDB, any associated vulnerable items are removed, as well.

When a vulnerable item is added to a vulnerability group, the group appears in the **Associated Vulnerability Group** list of **Vulnerable items**.

When a task is created that affects a vulnerable item, the task appears in the **Affected Tasks** related list of **Vulnerable items**.

Vulnerable items can be created manually. You can create security incidents or change requests and manually closed or defer them. Vulnerability group rules can be applied to manually created vulnerable items.

**Vulnerable Item** is no longer a task and no longer appears in the **My Work** common menu item. **Vulnerability Groups** and **Vulnerability Rules** have been enhanced to take over task functionality. Vulnerable items cannot be linked as a parent task.

### Create Vulnerability Response vulnerable items

Multiple methods create vulnerable items (VI). Most commonly, an integration to a vulnerability scanner is installed and configured to import results nightly. There are cases, like physical security vulnerabilities, when you may want to manually add vulnerable item records.

**Before you begin**

**Role required:** sn_vul.vulnerability_write

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see **Assign the Vulnerability Response persona roles using Setup Assistant**. For more information about managing granular roles, see **Manage persona and granular roles for Vulnerability Response**.
About this task
Manually created VIs are automatically added and removed from vulnerability groups, by vulnerability group rules and group conditions, just as automatically added vulnerable items are.

Procedure
1. Navigate to Vulnerability > Vulnerabilities > Vulnerable Items.
2. Click New.
3. Fill in the fields on the form, as appropriate. For information on the vulnerable items fields see, Vulnerability Response vulnerable item form fields.
4. Right-click in the form header and click Save.

The vulnerability group rules evaluate the vulnerable item and add it to an existing group or create a new group. If the evaluation fails, then the vulnerable item is added to Ungrouped Vulnerable Items list.

When you save a new vulnerable item, all the enabled calculators run.

Note: Only one calculator per Target field is allowed to be active at a time. When you activate one, any others with the same Target field are deactivated.

5. You can click any of the related lists to view additional information. For information on the related lists see, .

You can use the Related Link, Scan for Vulnerabilities to manually trigger a ServiceNow®-initiated scan. For information on how to configure a vulnerability scanner, see Configure and manage Qualys vulnerability scanners and scans.

For a Qualys Vulnerability Integration, a default scanner is pre-installed in the Vulnerability Scanners module. This scanner is disabled by default. Select the Active and Default check boxes to enable the Qualys scanner to work using the Scan for Vulnerabilities related link on the vulnerability group and vulnerable item forms.

The following editing and remediation options become available from the header bar:

- Update: Saves updates to the form.
- Create Security Incident: Creates a security incident.
- Close/Defer: Closes or defers the item. If all items in its group are closed, the Vulnerability Group automatically closes.
- Delete: Removes the vulnerable item.
Vulnerability Response vulnerable item form fields

Vulnerable items are automatically created during third-part vulnerability integration imports.

Vulnerable item fields

If you have enabled SAM NVD vulnerability scanning, vulnerable items are created automatically when records are downloaded from the NIST NVD. The records are compared to the software in your Configuration Management Database (CMDB) and matches are found with vulnerable software or configuration items (CIs).

Starting with v10.0, the information displayed on the Configuration Details tab in versions 8.0-9.0 is now displayed on the Initial Detections and Detection tabs along with other detection-related information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select security tag</td>
<td>Security tag to add metadata to the record or identify who should have access to this security incident record. This field appears only after the vulnerable item has been saved.</td>
</tr>
<tr>
<td>Number</td>
<td>Automatically generated vulnerable item number for this record.</td>
</tr>
<tr>
<td>Source</td>
<td>Scanner that found this vulnerable item.</td>
</tr>
<tr>
<td>Risk rating</td>
<td>Quantified Risk Score separating vulnerable items into Critical, High, Medium, Low, and None. For more information on risk ratings see, Vulnerability Response calculators and vulnerability calculator rules.</td>
</tr>
<tr>
<td>Note:</td>
<td>This base Risk rating is not the same as the Solution record Risk rating.</td>
</tr>
<tr>
<td>Risk score</td>
<td>Calculated amount of risk the vulnerable item poses to your environment.</td>
</tr>
<tr>
<td>Note:</td>
<td>This base Risk score is not the same as the Solution record Risk score.</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>ID of the vulnerability associated with this vulnerable item.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Configuration item</td>
<td>Affected asset.</td>
</tr>
<tr>
<td>State</td>
<td>This field defaults to <strong>Open</strong>, but you can change it to <strong>Under Investigation</strong> if the vulnerability is ready for immediate remediation.</td>
</tr>
<tr>
<td>Assignment group</td>
<td>Group selected to work on this vulnerability group.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>Individual from the selected assignment group that works on this vulnerability.</td>
</tr>
<tr>
<td>Created</td>
<td>Date this vulnerable item was created in your instance.</td>
</tr>
<tr>
<td>Last opened</td>
<td>Date the vulnerable item was most recently opened in your instance. Initially, this is the same as the creation date of the vulnerable item, however, if it was closed, then reopened the Last opened date contains the date and time reopened.</td>
</tr>
<tr>
<td>Updated</td>
<td>Date of the last scan.</td>
</tr>
<tr>
<td><strong>Vulnerability</strong></td>
<td></td>
</tr>
<tr>
<td>Summary</td>
<td>Description of the vulnerability.</td>
</tr>
<tr>
<td>Severity</td>
<td>Normalized degree of severity of this vulnerability. Severity maps are provided for NVD and with ServiceNow third-party integrations. For more information on creating or adjusting severity maps, see Create a Vulnerability Response severity map.</td>
</tr>
<tr>
<td>Vulnerability score (v3)</td>
<td>CVSS v3 score.</td>
</tr>
<tr>
<td>Vulnerability score (v2)</td>
<td>CVSS v2 score.</td>
</tr>
<tr>
<td>Exploit exists</td>
<td>Yes, if at least one exploit is associated with the vulnerabilities associated with this vulnerable item.</td>
</tr>
<tr>
<td>Exploit attack vector</td>
<td>Most vulnerable attack vector of the exploits for the vulnerabilities associated with this vulnerable item.</td>
</tr>
<tr>
<td>Exploit skill level</td>
<td>Lowest skill level required to exploit the vulnerabilities associated with this vulnerable item.</td>
</tr>
<tr>
<td>Date published</td>
<td>Date the vulnerability was published.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last modified</td>
<td>Date the vulnerability was last modified.</td>
</tr>
<tr>
<td>Threat</td>
<td>Relevant information about the threat. Pulled from the vulnerable entry record.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Any changes made here update the vulnerable entry record.</td>
</tr>
<tr>
<td>Remediation notes</td>
<td>Relevant solution to the threat, pulled from the vulnerable entry record.</td>
</tr>
<tr>
<td><strong>Remediation Steps</strong></td>
<td>Available only with Vulnerability Solution Management.</td>
</tr>
<tr>
<td>Preferred solution</td>
<td>Preferred solution imported from the vulnerability record.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Any manual changes made here do not change the vulnerability record and remain unchanged on the VI upon subsequent imports.</td>
</tr>
<tr>
<td>Summary</td>
<td>Imported Summary from the solution record.</td>
</tr>
<tr>
<td><strong>Initial Detection</strong></td>
<td><strong>(Information on Configuration Details tab displayed in Version 9.0 moved to Initial Detection and Detections tabs for Version 10.0 )</strong></td>
</tr>
<tr>
<td>DNS name</td>
<td>Name of the Domain Name Service name. If a CI is not provided, this field is used to look up a matching CI, if one exists.</td>
</tr>
<tr>
<td>NetBIOS name</td>
<td>Name of the NetBIOS. If a CI is not provided, this field is used to look up a matching CI, if one exists.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IPv4 or IPv6 address. If a CI is not provided, this field is used to look up a matching CI, if one exists.</td>
</tr>
<tr>
<td>Port</td>
<td>Address of the port</td>
</tr>
<tr>
<td>Protocol</td>
<td>Name of the protocol</td>
</tr>
<tr>
<td>SSL</td>
<td>Whether SSL encryption is used or not.</td>
</tr>
<tr>
<td><strong>Detections</strong></td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>State of the detection.</td>
</tr>
<tr>
<td>First found</td>
<td>Date the third-party source first found the detection on this asset.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last found</td>
<td>Date the third-party source last found the detection on this asset.</td>
</tr>
<tr>
<td>DNS name</td>
<td>Name of the Domain Name Service name. If a CI is not provided, this field is used to look up a matching CI, if one exists.</td>
</tr>
<tr>
<td>NetBIOS name</td>
<td>Name of the NetBIOS. If a CI is not provided, this field is used to look up a matching CI, if one exists.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IPv4 or IPv6 address. If a CI is not provided, this field is used to look up a matching CI, if one exists.</td>
</tr>
<tr>
<td>Port</td>
<td>Address of the port</td>
</tr>
<tr>
<td>Protocol</td>
<td>Name of the protocol.</td>
</tr>
<tr>
<td>SSL</td>
<td>Whether SSL encryption is used or not.</td>
</tr>
<tr>
<td>Times found</td>
<td>Number of times this vulnerability has been detected on this asset by the third-party source.</td>
</tr>
<tr>
<td>Integration run</td>
<td>Integration run that imported the detection.</td>
</tr>
<tr>
<td><strong>Close</strong></td>
<td></td>
</tr>
<tr>
<td>Closed by</td>
<td>Who closed the vulnerable item.</td>
</tr>
<tr>
<td>Closed</td>
<td>Date the vulnerable item was closed.</td>
</tr>
<tr>
<td>Close notes</td>
<td>Information included in the closure.</td>
</tr>
<tr>
<td>Age closed</td>
<td>Time period after which the VI was closed. If the VI is reopened, the value of the Age closed field is set to zero.</td>
</tr>
<tr>
<td><strong>Notes</strong></td>
<td></td>
</tr>
<tr>
<td>Additional comments/Work notes</td>
<td>Any relevant information. Select the check box for Work notes.</td>
</tr>
<tr>
<td>Activity</td>
<td>Only appears when a work note has been created.</td>
</tr>
<tr>
<td><strong>Related Links</strong></td>
<td></td>
</tr>
<tr>
<td>Calculate Risk Score</td>
<td>When either the Vulnerability Severity or Risk Score calculators is enabled, the Risk Score field is updated.</td>
</tr>
</tbody>
</table>
The following are the vulnerable items related lists.

<table>
<thead>
<tr>
<th>Related List</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Groups</td>
<td>Vulnerability groups associated with this vulnerable item.</td>
</tr>
<tr>
<td>Affecting Tasks</td>
<td>Tasks associated with this vulnerable item.</td>
</tr>
<tr>
<td>Associated IP Addresses</td>
<td>Available if the Qualys Vulnerability Integration application is installed.</td>
</tr>
<tr>
<td></td>
<td>IP addresses that are found during de-duplication.</td>
</tr>
<tr>
<td>Impacted Services</td>
<td>Business services impacted by this vulnerable item. Shown when this information is available in the cmdb record. This information can be entered manually or using the ServiceNow® Service Mapping application. See Service Mapping for more information.</td>
</tr>
<tr>
<td></td>
<td>If an affected CI associated with the vulnerable item is added or updated, information in this related list is automatically updated when the record is saved.</td>
</tr>
<tr>
<td>Qualys Tickets</td>
<td>Qualys ticket integration information associated with this vulnerable item.</td>
</tr>
</tbody>
</table>

**Bulk edit Vulnerability Response vulnerable items**

You can edit vulnerable items in bulk by selecting fields and running an asynchronous bulk edit job in the background.

**Before you begin**

Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.
About this task

Procedure

1. Navigate to Vulnerability > Vulnerabilities > Vulnerable Items.

2. Select the vulnerable items to edit by checking the box next to each item or creating a filter.

3. Click the **Bulk Edit** button.

4. Select and enter updates in the pop-up window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record Selection</td>
<td>Select which records to update. Choices are:</td>
</tr>
<tr>
<td></td>
<td>• Only Selected Vulnerable Items</td>
</tr>
<tr>
<td></td>
<td>• All Vulnerable Items that match filter</td>
</tr>
<tr>
<td></td>
<td>• Vulnerability Group</td>
</tr>
<tr>
<td></td>
<td>• Vulnerability entry</td>
</tr>
<tr>
<td>State</td>
<td>Select the change for the State in the vulnerable item. Choices are:</td>
</tr>
<tr>
<td></td>
<td>• Do Not Update</td>
</tr>
<tr>
<td></td>
<td>• Open</td>
</tr>
<tr>
<td></td>
<td>• Under Investigation</td>
</tr>
<tr>
<td></td>
<td>• Awaiting Implementation</td>
</tr>
<tr>
<td></td>
<td>• Deferred</td>
</tr>
<tr>
<td></td>
<td>• Closed</td>
</tr>
<tr>
<td></td>
<td>• Resolved</td>
</tr>
</tbody>
</table>
Table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 10.0: Preferred Solution</td>
<td>The solution targeted for remediating all the vulnerable items selected for bulk edit. Select the change for the Preferred Solution field in the vulnerable item. Choices are from a lookup list of available preferred solutions for the VIs selected.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>• The Preferred Solution field must be correctly set on all VIs selected for bulk edit.</td>
</tr>
<tr>
<td></td>
<td>• The set of available preferred solutions is an intersection of all potential solutions of the vulnerabilities across all selected VIs.</td>
</tr>
<tr>
<td></td>
<td>• When selecting Record selection &gt; Vulnerability Entry for bulk edit, all VIs for the vulnerability should be set to the selected preferred solution; however, this operation does not set the Preferred solution at the vulnerability entry level. Setting the Preferred solution at the vulnerability entry level would set the Preferred solution for all new VIs going forward. Bulk edit only modifies the current set of VIs.</td>
</tr>
<tr>
<td></td>
<td>• Distinct vulnerabilities across the selection criteria is limited to 500. If there are more than 500, a warning message is displayed asking you to select VIs with different criteria for setting the Preferred solution.</td>
</tr>
<tr>
<td></td>
<td>• The total number of solutions that can be shown in the lookup list is limited to 170. If there are more than 170, a warning message is shown.</td>
</tr>
<tr>
<td></td>
<td>The updated value is shown in the Vulnerable item list view.</td>
</tr>
<tr>
<td>Version 10.3: Assignment group</td>
<td>Assignment group for the VI. Select manually, or using Assignment Recommendations if it is enabled.</td>
</tr>
<tr>
<td>Work notes</td>
<td>Enter text describing the changes.</td>
</tr>
</tbody>
</table>

**5. Click OK.**
A bulk edit asynchronous job updates the selected records. The job number with a link is displayed on the Vulnerable Items page where you can view its status.

If you select Close, the **Reason** field is included. If you select Defer, once approved, the **Close/defer reason** and the **Defer expiration** fields are shown.

**Defer a vulnerable item**

If you determine that the issue associated with a vulnerable item is of low risk and can be immediately deferred without further analysis, you can use the **Defer** feature.

**Before you begin**

Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see [Assign the Vulnerability Response persona roles using Setup Assistant](#). For more information about managing granular roles, see [Manage persona and granular roles for Vulnerability Response](#).

**About this task**

A scheduled job runs every day checking for deferred vulnerable items that have reached their reopen date. On the day, the group is reopened.

**Procedure**

1. Navigate to **Vulnerability > Vulnerabilities > Vulnerable Items**.
2. Open a vulnerable item.
3. Click the **Close/Defer** button.
4. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select a state.</td>
</tr>
<tr>
<td></td>
<td>Choices are:</td>
</tr>
<tr>
<td></td>
<td>• Deferred</td>
</tr>
<tr>
<td></td>
<td>• Closed</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Until</td>
<td>Select the date when the <strong>Defer</strong> state expires and the vulnerability group is reactivated. After the record is submitted, if email notifications are defined, members of the Vulnerability Response group receive an email when the expiration date is within one week. When the defer date expires, the vulnerable item is set back to <strong>Open</strong> and a second email notification is sent out.</td>
</tr>
</tbody>
</table>
| Reason           | Enter the reason for deferring the issue. Choices include:  
  • Awaiting maintenance window  
  • False positive  
  • Fix unavailable  
  • Risk accepted  
  • Mitigating control in place  
  • Other |
| Additional information | Enter any other relevant information. |

5. Click **Submit**. The group is marked **Deferred**. A **Reopen** related link appears. The reopen date and reason appear in work notes under the **Defer/Closed** tab.

**Refresh Vulnerability Response vulnerable items**

The **Refresh associated vulnerable items** related link is used to have vulnerable items inspected to see if there are any additional vulnerable items that belong to this group. Use it if an update is warranted outside the scheduled job.

**Before you begin**

Role required: `sn_vul.vulnerability_write` or, v10.3 `sn_vul.vulnerability.admin` or `sn_vul.admin` (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see **Assign the Vulnerability Response persona roles using Setup Assistant**. For more
information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

**About this task**
The **Refresh associated vulnerable items** related link is only editable on the vulnerable group form in the Open or Under Investigation state, using a filter group or where the filter type is condition. This inspection is done regardless of the status of the **Automatically refresh vulnerable items** check box.

**Procedure**
1. Navigate to Vulnerability > Vulnerabilities > Vulnerability Groups.
2. Open any vulnerable group in the Open or Under Investigation state.
3. Click the **Refresh associated vulnerable items** link.
   New vulnerable items appear under the **Associated Vulnerable Items** tab.

**Identify and escalate security issues in third-party software**
You can view software vulnerabilities returned from third-party entries to determine remediation. Use this information to match the vulnerable software entries to a Software Asset Management discovery model.

**Before you begin**
Role required: sn_vul.vulnerability_write

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see **Assign the Vulnerability Response persona roles using Setup Assistant**. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

**Procedure**
1. Navigate to Vulnerability > Libraries > Third Party.
   A list of vulnerable software downloaded is shown.
2. Click a software record to view vulnerability information.
3. Click the following related lists to get more information for identifying vulnerabilities.

<table>
<thead>
<tr>
<th>Related list</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerable Items</td>
<td>Lists any vulnerable items, which consist of pairings of a potentially vulnera-</td>
</tr>
</tbody>
</table>
### Identify and escalate security issues using NVD

When Common Vulnerability and Exposures identifier (CVE-ID) records are downloaded from the National Vulnerability Database (NVD), they are compared to the software in your company network as identified by the Software Asset discovery model. When a CVE-ID matches vulnerable software or configuration item in your network, a vulnerable item is created. You use the information in the CVE-ID record to decide whether to escalate the vulnerable item for remediation.

**Before you begin**

**Role required:** `sn_vul.vulnerability_write`

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see [Assign the Vulnerability Response persona roles using Setup Assistant](#). For more information about managing granular roles, see [Manage persona and granular roles for Vulnerability Response](#).

**Procedure**

1. Navigate to **Vulnerability > Libraries > NVD**.
   
   A list of CVE-IDs that were downloaded from the NVD is shown. Updates from the NVD can be performed on-demand or using a scheduled job.

2. Click a CVE record to view the following information:

<table>
<thead>
<tr>
<th>Related list</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Entries</td>
<td>Lists vulnerability entries for the selected software record. Click a record to view its details.</td>
</tr>
</tbody>
</table>

**Note:** If software is removed, any associated vulnerable items are closed and removed from the **Vulnerable Items** related list.
• a summary for the CVE-ID.
• a reference to a Common Weakness Enumeration (CWE) entry, if applicable.
• the vulnerability score of the CVE-ID on the Common Vulnerability Scoring System (CVSS). For more information on the CVSS, see the National Vulnerability Database website.

3. Click the following related lists to get more information for identifying vulnerabilities.

<table>
<thead>
<tr>
<th>Related list</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerable Items</td>
<td>Lists any vulnerable items, which consist of pairings of a potentially vulnerable configuration item and software. To get more information about a pairing, click the information icon (1).</td>
</tr>
<tr>
<td>Note: If software is removed, any associated vulnerable items are closed and removed from the Vulnerable Items related list.</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Entries</td>
<td>Lists vulnerability entries for the selected software record. Click a record to view its details.</td>
</tr>
</tbody>
</table>

If vulnerabilities were identified and vulnerable items were created, you can Remediate Vulnerability Response groups, as needed.

**Identify and escalate security issues using CWE**

View the library of Common Weakness Enumeration (CWE) records from the National Vulnerability Database (NVD) to understand how they relate to the Common Vulnerability and Exposure (CVE) records. Then use this information to match the vulnerable software entries to a Software Asset Management discovery model.

**Before you begin**

Role required: sn_vul.vulnerability_write

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more
information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure
1. Navigate to Vulnerability > Libraries > CWE.
   A list of vulnerable software downloaded is shown.
2. Click a CWE software record to view vulnerability information.
3. Click the following related lists to get more information for identifying vulnerabilities.

<table>
<thead>
<tr>
<th>Related list</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerable Items</td>
<td>Lists any vulnerable items, which consist of pairings of a potentially vulnerable configuration item and software. To get more information about a pairing, click the information icon (i).</td>
</tr>
<tr>
<td>Note: If software is removed, any associated vulnerable items are closed and removed from the Vulnerable Items related list.</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Entries</td>
<td>Lists vulnerability entries for the selected software record. Click a record to view its details.</td>
</tr>
</tbody>
</table>

If vulnerabilities were identified and vulnerable items were created, you can Remediate Vulnerability Response groups, as needed.

Configure Exception Management for a vulnerability response
Limit the duration of an exception requested using the Vulnerability Response module. By default, an exception is requested using the ServiceNow® Vulnerability Response module. You can also request an exception using the GRC: Policy and Compliance Management integration.

Before you begin
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.
Role required: sn_vul.vulnerability_admin

About this task
If Vulnerability Response is enabled, you can limit the duration for which an exception can be requested. Similarly, if the GRC: Policy and Compliance Management module is installed, you can select GRC: Policy and Compliance Management on the configuration screen. Enabling this option lets you request an exception that specifies the Policy and Control objective from GRC.

Procedure
1. Navigate to Vulnerability Response > Administration > Exception Management.
2. On the Exception Management Configuration form, select how you want to manage an exception by selecting an option from the Manage exception using list. You can select either Vulnerability Response or GRC: Policy and Compliance Management.
3. If you selected the Vulnerability Response option, enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration</td>
<td>Period for which an exception can be requested.</td>
</tr>
<tr>
<td>Unit</td>
<td>Unit of time for the specified period.</td>
</tr>
</tbody>
</table>

Note:
You must install the GRC plugin to use GRC: Policy and Compliance Management to request an exception. Changing the configuration does not impact the existing data.

4. Click Save.

Add an exception approver
Add users to the approver groups so that you can request an exception.

Before you begin
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more
information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Role required: sn_vul.exception_approver

About this task
An exception request for a vulnerable item or vulnerability group is approved using the default two-level approval workflow. The request can be approved by two levels of approvers. Adding users to the first-level group is mandatory. If there are no users in the second level, the request is approved after the first-level approval.

Note: If there's no first-level approver, an exception can't be requested.

Procedure
1. Navigate to User Administration > Groups.
2. In the Name column, search for Exception, and click Exception Approver - Level 1.
3. On the Group Exception Approver - Level 1 form, click the Group Members related list.
4. Click New to create a list.
5. On the form, fill in the fields.

User form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>Unique identifier for the user.</td>
</tr>
<tr>
<td>First name</td>
<td>User's first name.</td>
</tr>
<tr>
<td>Last name</td>
<td>User's last name.</td>
</tr>
<tr>
<td>Title</td>
<td>User's job title. Enter a title or job description, or select one from the list.</td>
</tr>
<tr>
<td>Department</td>
<td>User's department.</td>
</tr>
<tr>
<td>Password</td>
<td>Password assigned to the user. This password can be permanent or temporary.</td>
</tr>
<tr>
<td>Password needs reset</td>
<td>Option to enable the user to reset the password to ensure security.</td>
</tr>
<tr>
<td>Locked out</td>
<td>Option to lock the user out of the instance and terminate all the user's</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>active sessions. The system</td>
<td>prevents users with the admin role from locking themselves out.</td>
</tr>
<tr>
<td>Active</td>
<td>Option to make this user active. Only you can see an inactive user in these areas:</td>
</tr>
<tr>
<td></td>
<td>• Lists of users</td>
</tr>
<tr>
<td></td>
<td>• Selection list on reference fields (magnifying glass icon)</td>
</tr>
<tr>
<td></td>
<td>• Auto-complete list that appears when you type into a reference field</td>
</tr>
<tr>
<td>Web service access only</td>
<td>Option to designate this user as a non-interactive user.</td>
</tr>
<tr>
<td>Internal Integration User</td>
<td>Option to designate this user as an internal integration user.</td>
</tr>
<tr>
<td>Email</td>
<td>User's email address.</td>
</tr>
<tr>
<td>Language</td>
<td>User's preferred language.</td>
</tr>
<tr>
<td>Calendar integration</td>
<td>Calendar used to manage the work schedule. For example, Outlook.</td>
</tr>
<tr>
<td>Time zone</td>
<td>Time zone for this user's location.</td>
</tr>
<tr>
<td>Date format</td>
<td>User's preferred format for dates.</td>
</tr>
<tr>
<td>Business phone</td>
<td>User's business phone.</td>
</tr>
<tr>
<td>Mobile phone</td>
<td>User's mobile phone.</td>
</tr>
<tr>
<td>Photo</td>
<td>Photo that you can upload by clicking on <strong>Click to add</strong>....</td>
</tr>
</tbody>
</table>

6. Click **Submit**.

7. **Optional:** Repeat steps 1–5 to create an Exception Approver - Level 2. The approver must navigate to **Vulnerability Response > My Approvals** and approve requests.

**Note:** To approve an exception for GRC: Policy and Compliance Management, see **Policy Exception Integration with Vulnerability Response**.
Add a false positive approver

Only users added to the False Positive Approver group can approve false positives for vulnerable items (VIs) and vulnerability groups (VGs). Granting a false positive is a single-level approval process.

Before you begin
Role required: admin
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure

1. Navigate to User Administration > Groups.
2. In the Name column, search for False Positive and click the option.
3. On the Group form, navigate to Group members > New (or Edit).
4. On the User form, create a record by entering the user details, and click Submit.
   All roles are granted to the user. The selected users are added to the Group Members list. These members can approve requests to mark VIs or VGs as false positive. Once approved, the state of the record is updated to Closed and it is reopened only on the specified date.

Optional Vulnerability Response setup tasks

In case they are needed, manual tasks for vulnerability groups, group rules, calculator groups, calculators, severity maps, and remediation target rules are available outside of Setup Assistant. You can configure vulnerability scanners and vulnerability integrations, as well.

Many of these tasks are available within the Setup Assistant in a new and more user-friendly user interface (UI). Manual versions of the tasks are provided for the convenience of existing users who may find them more familiar.

Instructions for configuring vulnerability scanners and creating custom integrations remain from prior releases.

Configure the vulnerable item key

Configure the granularity of the vulnerable item (VI) key in the Vulnerability Response application to define what makes a vulnerable item (VI) in your organization.
Before you begin
Role required: admin
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Key terms

**Configuration item (CI)**
An existing asset listed on your CMDB.

**Vulnerability**
A record of a known vulnerability imported from the National Institute of Standards and Technology (NIST), National Vulnerability Database (NVD), Common Vulnerabilities and Exposures (CWE), or third-party integrations with Vulnerability Response.

**Vulnerable item**
A vulnerable item is created when an imported vulnerability matches a configuration item in your CMDB.

**Detection**
A single, distinct occurrence of a vulnerability as reported by the scanners of your third-party integrations. Detections are imported and displayed on both the detection and the vulnerable item records in your instance. Also referred to as a Vulnerable Item Detection.

By default, a vulnerable item is a unique combination of a configuration item (CI), a vulnerability, and an integration instance. To create vulnerable items with more granularity, add unique ports from vulnerable item detections to help you manage remediation of vulnerabilities at the level you feel is most effective for your organization.

If you want to create vulnerable items with more granularity, configure the vulnerable item key so that it includes port. When Include port is enabled, vulnerable items are created by unique ports from vulnerable item detections.

Choose an option from the following table to enable the Include port option.
Three scenarios for enabling the Include port option with the VI key for the first time

<table>
<thead>
<tr>
<th>If...</th>
<th>Description</th>
</tr>
</thead>
</table>
| One or more of the following conditions is true:  
• You are upgrading from a version of Vulnerability Response prior to v10.0 that did not support vulnerable item detections.  
• You are a new customer and you have no Vulnerability Response data (vulnerable items or vulnerable item detections) in your Now Platform® instance.  
• You have already deleted all your vulnerable item records and related data in your instance and you are ready to build all your Vulnerability Response data starting with a fresh import to include VIs distinguished by unique port. | Enable Include Port.  
After Include port is enabled, imported detections create vulnerable items that include VIs distinguished by unique port starting with the next import. |
| Both conditions are true:  
• You have v10.0 or later of Vulnerability Response and you have existing Vulnerability Response data (vulnerable items or vulnerable item detections) in your instance that you want to preserve.  
• You want to start creating new vulnerable items to include VIs distinguished by unique port. | Enable Include port. Your existing detections and their associated vulnerable items will be preserved.  
After Include port is enabled, new detections create new vulnerable items that include VIs distinguished by unique port starting with the next import. |
| Both conditions are true:  
• You have v10.0 or later of Vulnerability Response.  
• You have existing Vulnerability Response data (vulnerable items or vulnerable item detections), but you do not want to preserve your | 1. Delete all your vulnerable item records and related data from your instance.  
2. Enable Include port.  
After Include port is enabled, new detections create new vulnerable |
Three scenarios for enabling the Include port option with the VI key for the first time (continued)

<table>
<thead>
<tr>
<th>If...</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>existing data, because you prefer to build your vulnerability data starting from a fresh import and you want to include VIs distinguished by unique port.</td>
<td>items that include VIs distinguished by unique port starting with the next import.</td>
</tr>
</tbody>
</table>

⚠️ **Note:**

If the Include port option is enabled, more than one vulnerable item may be created for a configuration item. For example, if a vulnerability exists for two ports on a configuration item, ports 80 and 443, two unique VIs are created, one for each port starting with the next import.

⚠️ **Note:** Be sure you want to create VIs to include VIs by unique ports before you enable this feature. Once you enable the VI key to include port, you must first delete your Vulnerability Response data before you can disable Include port and return to importing vulnerability data using the default VI key granularity, that is, where VIs are created for port but not distinguished by a unique port. For more information about deleting your vulnerability data, see Delete all your vulnerable item records and related data in Vulnerability Response.

**Procedure**

1. Navigate to **Vulnerability Response > Administration > Configure VI granularity**.
   
The Last Updated field displays the date the VI key was last configured.
2. Click the Include Port check box to enable it.
3. **Click Save**.
   
The Confirmation dialog is displayed.

   If you have no vulnerable item detection records in your instance, both vulnerable item detections and vulnerable items are created by unique port starting with your next import.

   If you have existing vulnerable item detections and vulnerable items in your instance, existing detections and associated vulnerable items will be preserved. New detections create new vulnerable that include VIs distinguished by unique port starting with the next import.
What to do next
Verify vulnerable items by port are displayed on the vulnerable item detection and vulnerable item records. For more information, see View Vulnerability Response vulnerable item detection data.

Delete all your vulnerable item records and related data in Vulnerability Response
Permanently remove all Vulnerability Response data (vulnerable items or vulnerable item detections) and related data and records from the Vulnerability Response application in your Now Platform® instance.

Before you begin
Delete vulnerable item detection records, vulnerable items, vulnerability groups, and any related records in the Vulnerability Response application from your instance. Use this process to clean out your instance to import data with a fresh start from your third-party integrations, or, as a prerequisite to returning the vulnerable item (VI) key configuration to its default setting. For more information on configuring the VI key, see Configure the vulnerable item key.

Note: This action deletes all the vulnerable item records and any related data from your instance. This data once deleted cannot be retrieved. It also requires you to suspend data import and disable your active third-party integrations with Vulnerability Response.

Deleting your vulnerable item data with this process prior to changing the VI key configuration is required. Removing all data ensures that all your vulnerable items and vulnerable item detections are mapped and updated with the most current data starting with the next Import.

Verify the following conditions apply prior to deleting your data:
• You have v10.0 or later of Vulnerability Response installed. Version 10.0 supports vulnerable item detections from third-party scanners. For more information, see Vulnerability Response vulnerable item detections from third-party integrations.
• You want to disable Include port and return the VI key configuration to its default setting.
• You have existing vulnerable items and vulnerable item detections but do not want, or need to update and keep them.
• You have determined you want to remove all existing Vulnerability Response data and related records to clean up your instance.

Role required: vuln.admin
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

**Procedure**

1. Navigate to Vulnerability Response > Vulnerability Integrations.
2. Record all of the active integrations that are displayed.
   
   All of the active integrations listed with scheduled jobs are disabled prior to deleting all of your vulnerable items and related data so that no new data is imported during the data removal. Recording this list helps you activate your integrations after the delete is completed.

3. Navigate to KB0820838 How to delete existing Vulnerability Response Data for reimport.
4. If a warning message is displayed that prevents you from writing to the Active column, to disable active integrations, follow these steps.
   
   a. In the Name column click an item to open the record.
   
   b. If you cannot edit the Active check box, click the here link to edit the record.
   
   c. Click the Active check box to disable the integration and the cancel the next scheduled job.
   
   d. Click Update to save your changes and return to the list.

   e. Verify you have disabled any active integrations from the Integrations list. After you disable an integration, it is no longer displayed on the active integrations list. To view a list inactive integrations, and locate all the integrations you disabled after you delete all your vulnerability data, in the Active column at the top, enter =false.

5. Continue with the steps in the KB article for deleting your existing vulnerability data.

6. After you have confirmed that all data is successfully deleted, navigate to Vulnerability Response > Administration > Configure VI granularity.

7. On the form:
• If you deleted data because you prefer to build your vulnerability data to include port from a fresh import, enable Include port and click Save.

• If you deleted data because you want to return the VI key to its default setting, disable Include port and click Save.

For more information, see Configure the vulnerable item key.

**Manually create a Vulnerability Response group**

Creating a vulnerability group manually is done when you want to group vulnerable items by something other than the Vulnerability Group Rules criteria. For example, you can create groups for a particular manager, or for active, new exploits, such as ransomware, that include different vulnerabilities. You can also use it to group ungrouped vulnerable items.

**Before you begin**

Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

**Procedure**

1. Navigate to Vulnerability > Vulnerabilities > Vulnerability Groups.
2. Click New.
3. Fill in the fields on the form, as appropriate. For information on specific fields, see Vulnerability Response group form fields.
4. Click Submit.

When the group is created, using the Condition or Filter Group filter type the Vulnerable Item related list searches for and displays all matching vulnerable items.

You can use the Related Link, Re-scan for Vulnerabilities to manually trigger a ServiceNow®-initiated scan. For information on how to configure a vulnerability scanner, see Configure and manage Qualys vulnerability scanners and scans.

For a Qualys Vulnerability Integration, a default scanner is pre-installed in the Vulnerability Scanners module. This scanner is disabled by default. Select the Active and Default check boxes to enable the Qualys scanner to work using the Scan for Vulnerabilities related link on the vulnerability group and vulnerable item forms.
The **Update status** related link displays the date and time of the last update. It rolls up information from the VIs in the group. See **Vulnerability Response group form fields** for more information. When a group is formed based on a specific vulnerability, that vulnerability is listed on the VG form.

If you open an associated vulnerable item, any associated vulnerability group entries appear under the **Vulnerable Group** related list tab.

**Vulnerability Response group form fields**

Using vulnerability groups, the analyst can monitor progress and drive the mediation process more efficiently.

The imported fields in this table are read-only.

### Vulnerability group (VG) fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>The automatically generated vulnerable item (VI) number for this record.</td>
</tr>
<tr>
<td>Risk rating</td>
<td>Rollup of vulnerable item risk scores separated into ranges: Critical, High, Medium, Low and None. For more information on risk ratings see, Vulnerability Response calculators and vulnerability calculator rules.</td>
</tr>
<tr>
<td></td>
<td>️ <strong>Note:</strong> This base <strong>Risk rating</strong> is not the same as the Solution record <strong>Risk rating</strong>.</td>
</tr>
<tr>
<td>Risk score</td>
<td>Rollup of the risk scores of all of the vulnerable items associated with this vulnerability group. Amount of risk the vulnerable items, collectively, pose to your environment.</td>
</tr>
<tr>
<td></td>
<td>️ <strong>Note:</strong> This base <strong>Risk score</strong> is not the same as the Solution record <strong>Risk score</strong>.</td>
</tr>
<tr>
<td>Remediation target</td>
<td>Date by which the vulnerable items should be remediated, since first identified.</td>
</tr>
<tr>
<td></td>
<td>For more information on remediation targets see Vulnerability Response remediation target rules.</td>
</tr>
<tr>
<td>Remediation status</td>
<td>Status of the remediation for the group. It is determined by the vulnerable item with the nearest due date.</td>
</tr>
<tr>
<td></td>
<td>For open groups states include:</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
### Vulnerability group (VG) fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• In-flight</td>
<td></td>
</tr>
<tr>
<td>• Approaching Target</td>
<td></td>
</tr>
<tr>
<td>• Target Missed</td>
<td></td>
</tr>
<tr>
<td>For closed groups states include:</td>
<td></td>
</tr>
<tr>
<td>• No Target</td>
<td></td>
</tr>
<tr>
<td>• Target Met</td>
<td></td>
</tr>
<tr>
<td>• Target Missed</td>
<td></td>
</tr>
</tbody>
</table>

For calculated remediation target dates, if the VG is closed, the overall remediation status of all of the closed vulnerable items is shown in the VG. Those determine whether the VG met its date or not. A closed VG remediation Status is **No Target** if none of its closed items had a remediation target date. It is **Target Missed** if any of its closed items missed their target date. It is **Target Met** if at least one closed VI met its target and none of the others missed it.

<table>
<thead>
<tr>
<th>State</th>
<th>Progress status of the group. States include:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Open</td>
<td>• Open</td>
</tr>
<tr>
<td>• Under Investigation</td>
<td>• Under Investigation</td>
</tr>
<tr>
<td>• Awaiting Implementation</td>
<td>• Awaiting Implementation</td>
</tr>
<tr>
<td>• Deferred</td>
<td>• Deferred</td>
</tr>
<tr>
<td>• In Review</td>
<td>• In Review</td>
</tr>
<tr>
<td>• Resolved</td>
<td>• Resolved</td>
</tr>
<tr>
<td>• Closed</td>
<td>• Closed</td>
</tr>
</tbody>
</table>

For more information on states, see Vulnerability Response group and vulnerable item states.

| Assignment group           | Group selected to work on this vulnerability group.                         |
### Vulnerability group (VG) fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigned to</td>
<td>Individual from the selected assignment group that works on this vulnerability.</td>
</tr>
<tr>
<td>Created</td>
<td>Date this vulnerability group was created.</td>
</tr>
<tr>
<td>Updated</td>
<td>Date this vulnerability group was last updated.</td>
</tr>
<tr>
<td><strong>Version 10.0: Vulnerability</strong></td>
<td>Vulnerability applicable to the group. (Visible when the group is formed based on a single vulnerability.)</td>
</tr>
<tr>
<td>Short description</td>
<td>Brief description of this vulnerability group.</td>
</tr>
<tr>
<td><strong>In Review</strong> (visible when the VG is in the In Review state)</td>
<td></td>
</tr>
<tr>
<td>Requested by</td>
<td>Individual who requested the deferral.</td>
</tr>
<tr>
<td>Desired reason</td>
<td>Reason for deferral.</td>
</tr>
<tr>
<td>Desired state</td>
<td>The state requested from the approver.</td>
</tr>
<tr>
<td>Desired substate</td>
<td>The reason requested from the approver.</td>
</tr>
<tr>
<td><strong>Deferral</strong> (visible when the VG is in the Deferred state)</td>
<td></td>
</tr>
<tr>
<td>Deferred by</td>
<td>Individual who deferred the vulnerability group.</td>
</tr>
<tr>
<td>Defer expiration</td>
<td>Date the deferral expires.</td>
</tr>
<tr>
<td>Reason to defer</td>
<td>Reason for the deferral.</td>
</tr>
<tr>
<td><strong>Resolution</strong> (visible when the VG is in the Resolved state)</td>
<td></td>
</tr>
<tr>
<td>Resolved by</td>
<td>Individual who resolved the vulnerability group.</td>
</tr>
<tr>
<td>Resolution date</td>
<td>Date the vulnerability group was resolved.</td>
</tr>
<tr>
<td>Resolution notes</td>
<td>Additional information.</td>
</tr>
<tr>
<td><strong>Close</strong> (visible when the VG is in the Closed state)</td>
<td></td>
</tr>
<tr>
<td>Closed by</td>
<td>Individual who resolved the vulnerability group.</td>
</tr>
<tr>
<td>Closed</td>
<td>Date the vulnerability group was closed.</td>
</tr>
<tr>
<td>Close notes</td>
<td>Additional information.</td>
</tr>
</tbody>
</table>
## Vulnerability group (VG) fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group Configuration</strong> (visible in all states)</td>
<td></td>
</tr>
<tr>
<td>Filter type</td>
<td>Type of filtering used to select vulnerabilities for the group:</td>
</tr>
<tr>
<td></td>
<td><strong>Condition</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Diagram" /></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Refreshes once an hour.</td>
</tr>
<tr>
<td>Filter group</td>
<td></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Diagram" /></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Refreshes once an hour.</td>
</tr>
<tr>
<td>Manual</td>
<td></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Diagram" /></td>
</tr>
</tbody>
</table>

## Remediation Status

### Excludes Deferred

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerable items</td>
<td>Number of active vulnerable items within this group. This count excludes deferred vulnerable items.</td>
</tr>
<tr>
<td>Total VIs</td>
<td>Total number of vulnerable items within this group. This count excludes deferred vulnerable items.</td>
</tr>
<tr>
<td>%VIs remediated</td>
<td>Percent complete for remediation of vulnerable items within this group. This count excludes deferred vulnerable items.</td>
</tr>
</tbody>
</table>

### Includes Deferred

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerable items</td>
<td>Number of active vulnerable items within this group.</td>
</tr>
</tbody>
</table>
### Vulnerability group (VG) fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total VIs</td>
<td>Total number of vulnerable items within this group.</td>
</tr>
<tr>
<td>%VIs remediated</td>
<td>Percent complete for remediation of vulnerable items within this group.</td>
</tr>
</tbody>
</table>

**Notes** (visible in all states)

<table>
<thead>
<tr>
<th>Description</th>
<th>Description of the group or remediation actions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional comments</td>
<td>Additional information.</td>
</tr>
<tr>
<td>Activities</td>
<td>System notes.</td>
</tr>
</tbody>
</table>

**Related Links**

<table>
<thead>
<tr>
<th>Re-scan vulnerable items</th>
<th>Triggers a re-scan of the vulnerable items to determine if they are fixed.</th>
</tr>
</thead>
</table>
| Version 10.0: Update Status | Displays date and time of the last update.  \  
Rolls up the following from the VIs in the group:  \  
- Vulnerability group state  \  
- Risk scores and risk ratings  \  
- Remediation target date and status (if applicable)  \  
- Metrics such as Active VIs, Total VIs from the Remediation Status section |

**Related Lists**

<table>
<thead>
<tr>
<th>Vulnerable items</th>
<th>Vulnerable items in this group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task SLAs</td>
<td>Platform SLAs associated with this group.</td>
</tr>
<tr>
<td>Preferred Solutions</td>
<td>Preferred solutions of the vulnerable items in this group.</td>
</tr>
<tr>
<td>Change Requests</td>
<td>Change requests associated with this group.</td>
</tr>
<tr>
<td>Requested Approvals</td>
<td>(Visible when the group is in the In Review state.) List of approvers. Once the deferral is approved, the vulnerability group moves to the Deferred state.</td>
</tr>
</tbody>
</table>
Add users to the Vulnerability Response group

When the Close/Defer feature is used to defer or close a vulnerable item without requiring a scan, the Vulnerability Response group is notified to approve or reject the request. You can assign the appropriate users.

Before you begin
Role required: admin

Procedure
1. Navigate to User Administration > Groups.
2. Open the Vulnerability Response group.
3. Click the Group Members related list and click Edit.
4. Select one or more name in the Collection list.
5. Click Add.
6. Click Save.

Related information
Create a user

Create or edit Vulnerability Response assignment rules

You can create rules to automatically assign vulnerable items based on filter conditions. These rules assign vulnerable items as they are imported or manually created.

Before you begin
Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task
The base system ships with one vulnerability assignment rule, Assign to CI support group, which assigns vulnerable items to the same assignment group as the CI support group. This rule can be modified using filter conditions or you can create a new rule. With assignment rules, you define the condition(s) of assignment and the order of execution. Once a VI matches a rule condition, the assignment lookup stops.
Procedure

1. Navigate to Vulnerabilities > Administration > Assignment Rules.
2. Open the Assign to CI support group rule or click New.
3. If New, fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the group rule.</td>
</tr>
<tr>
<td>Active</td>
<td>Indicates whether the assignment rule is active.</td>
</tr>
<tr>
<td>Execution order</td>
<td>Order in which the rules are evaluated. High priority rules, items that need special handling, where risk is critical, or a VI should be handled by regulatory compliance, to be run first. Next, run your general rules, where no special handling is required, and you know who should be responsible for them. Finally, create a default rule to assign VIs to the group that will figure out what assignment group it should belong to. This group could add another rule to cover their decisions. This default rule would run last.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the assignment rule.</td>
</tr>
<tr>
<td>Condition</td>
<td>Conditions that must be met.</td>
</tr>
<tr>
<td>Preview</td>
<td>Shows how many results this query will return.</td>
</tr>
<tr>
<td>Condition fields</td>
<td>Adds more condition filter fields to choose from.</td>
</tr>
<tr>
<td>New Criteria</td>
<td>Adds more condition filter fields to choose from.</td>
</tr>
<tr>
<td>Assign using</td>
<td>To automate the assignment of groups created based on this rule, choose one of the options available.</td>
</tr>
</tbody>
</table>

Note: To make Rapid7 InsightVM asset tags available for use in the Condition filter for Assignment Rules, you must run the Rapid7 InsightVM Asset List integration before the other Rapid7 InsightVM integrations.

Starting with v13.0, case sensitivity for the search text you enter in the condition builder is not supported on this record or form. Prior to v13.0, case sensitivity is supported for the search text you enter in the condition builder.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• User group</td>
<td>Select a user group from the lookup table.</td>
</tr>
<tr>
<td>• User group field</td>
<td>Select a user group field from the drop-down menu.</td>
</tr>
<tr>
<td>• Script</td>
<td>Create or edit a script.</td>
</tr>
</tbody>
</table>

Note: Creating or edit a script requires ServiceNow expertise.

4. Click **Submit**.
   New or updated rules are evaluated on the next import.

Note:
The reapply feature requires a baseline application of the rules. Once your rules are created, if you haven’t already done so, activate the **Reapply all vulnerability assignment rules** scheduled job to execute, at your convenience. It applies all the rules to all Open VIs except those manually assigned. Depending on how many active VIs you have in your environment, remember to set the **Run** field appropriately following the initial run to prevent performance impacts.

If you haven’t run this scheduled job, when you try to use the **Apply Changes** button on the Assignment Rules form, you will have to do it then. Reapplying assignment rules does not regroup the vulnerable items.

Create or edit Vulnerability Response group rules
Create rules to automatically group vulnerable items based on filter conditions. These rules automatically group vulnerable items as they are imported or manually created. Use the filter to limit the vulnerable items grouped by this rule, such as selecting all vulnerable items with exploits.

Before you begin
Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see **Assign the Vulnerability Response persona roles using Setup Assistant**. For more information about managing granular roles, see **Manage persona and granular roles for Vulnerability Response**.

About this task
The base system ships with one vulnerability group rule, **Vulnerability**, which groups vulnerable items by vulnerability and assignment group (from **Assignment** rule).
Rules). You can reapply the rules from the form or list view. For some sample entries, Vulnerability Response group rules examples.

This rule can be modified as follows:

By using filter conditions and Group by choices.

By default, VGRs use Assignment Rules, when available, as part of their filter criteria.

⚠️ Note: If no assignment rules exist, you can select a group using the User group field.

Procedure

1. Navigate to Vulnerabilities > Administration > Vulnerability Group Rules.
2. Open the Vulnerability rule or click New.
3. If New, fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Vulnerability Group Rule</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the group rule.</td>
</tr>
<tr>
<td>Active</td>
<td>Indicates whether the group is active.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the rule.</td>
</tr>
<tr>
<td>Case sensitive</td>
<td>Determines whether a condition is case sensitive or not.</td>
</tr>
</tbody>
</table>

⚠️ Note: The default value is case insensitive.

Condition | Optional filter conditions for the rule.

⚠️ Note: To make Rapid7 InsightVM asset tags available for use in the Condition filter for Vulnerability Group Rules, you must run the Rapid7 InsightVM Asset List integration before the other Rapid7 InsightVM integrations.

Starting with v13.0, by default, (Case sensitive check box disabled), the search text you enter in the condition builder on group rules records and forms is not case-sensitive. Select the check box to enable case-sensitive searches on group records and forms.

Group by (up to six condition sets are available)
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group vulnerable items from</strong></td>
<td>The table the rule uses to group VIs. You can have up to six filters. Choices are:</td>
</tr>
<tr>
<td></td>
<td>• Vulnerable Item [sn_vul_vulnerable_item]</td>
</tr>
<tr>
<td></td>
<td>• Vulnerable Item → Configuration Item [cmdb_ci]</td>
</tr>
<tr>
<td></td>
<td>• Vulnerable Item → Vulnerability [sn_vul_third_party_entry]</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you choose an extended table, the <strong>Using field</strong> is applied only for vulnerable items that use that extended table.</td>
</tr>
<tr>
<td><strong>Using field</strong></td>
<td>Field on the table that the rule uses to group VIs.</td>
</tr>
</tbody>
</table>

**Assignment**

**Assign vulnerability groups by**

When automatically assigning vulnerability groups, the Assignment choice is used in addition to the **Group By** choices to group the vulnerable items. New groups are created, as needed, to ensure that each vulnerable item is placed in a group with a matching assignment group set.

To automate the assignment of groups created based on this rule, choose one of the options available.

- Group by field
  - Group by field: If you selected any user group field from the Using field values in the Group by section, they appear in the drop-down menu.
- User group
  - User Group: Use the lookup list to select a static user group.

**Note:** If you change your mind about any of the Group by settings, the Clear group by fields related link resets the Group by fields on the form.

When a group rule is deleted, from the form or list view, you have the option to delete all Open groups created by that rule. Groups not in the Open state are excluded.

For some sample entries, see Vulnerability Response group rules examples.

**Vulnerability Response group rules examples**

Examples of vulnerability group rules using vulnerability and risk, or impact, or configuration item (CI).
Vulnerability group rule to group high risk Java and Oracle vulnerable items

This example shows a walk-through of the rule that groups Java and Oracle vulnerable items by vulnerability and assigns them to their respective support groups.

Right-click in the header to **Save**.

**Vulnerability group rule to group all high impact vulnerable items by Vulnerability and CI support group**

This example shows the form field settings for a group rule for high impact vulnerable items that assigns them to the CI support group.
Vulnerability group rule to group all the high risk vulnerabilities on an external-facing CI in a German data center

This example shows the form field settings for a group rule for high risk vulnerabilities on external facing CIs in a German data center. They are assigned to the German data center assignment group.
Create, enable, or modify Vulnerability Response auto delete rules

You can create, enable, or modify the delete vulnerability item (VI) and vulnerability group (VG) delete rules. Use auto delete to remove older records from the VI and VG tables.

Before you begin
Roles required:

- admin: modify the auto delete rules
- v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated): view the auto-delete module

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.
About this task
Over time, a large amount of closed records are likely to accumulate in the VI and VG tables in your instance. Many of these records may have been closed for more than 365 days but have not been removed. Use auto delete rules to remove many of these older, closed records. Removing these records not only significantly reduces the number of records in the VI and VG tables, deleting them also helps you maintain high performance.

Although auto delete targets records by default that have been closed for 365 days, the very first run may attempt to purge too many records in a single transaction. Depending on the size of your environment, you may prefer to stagger the deletion process to limit the scope of the query. For example, you might start your first run for closed records that are older than 450 days. After that run is completed, you might work your way down by smaller increments (425, 400, 375) until you have reduced the number of records that are older than 365 days.

There are two rules supplied with your Now Platform® that automatically delete closed records that meet specified conditions along with any records that refer to them. One rule deletes vulnerable items, and the other rule deletes vulnerability groups. By default, these auto delete rules are disabled so that you are required to enable them manually prior to deleting any records. You can choose the two pre-configured rules that are provided with your instance, or, you can create your own.

Procedure
1. Navigate to Vulnerability Response > Administration > Auto-Delete Rules. The list view is displayed.

2. To edit: Select the delete rule for vulnerable items (sn_vul_vulnerable_item) or the rule for vulnerability groups (sn_vul_vulnerability).

3. To create: Click New.

4. Fill in or edit the fields on the form, as appropriate.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Name of the application in which records are being deleted. The default value is Vulnerability Response.</td>
</tr>
<tr>
<td>Tablename</td>
<td>Name of the table for which the rule is being applied.</td>
</tr>
<tr>
<td>Matchfield</td>
<td>Field for which the system monitors the duration.</td>
</tr>
<tr>
<td>Active</td>
<td>Option for activating the rule. Once activated, the record can be deleted.</td>
</tr>
<tr>
<td>Cascade</td>
<td>Option to delete all matching records, plus any records referring to them. If this option is not selected, only matching records are deleted, but not the records that refer to them.</td>
</tr>
<tr>
<td>Age in seconds</td>
<td>Age of the vulnerability record to be deleted. For both VI and VG rules, the age is 365 days. This age is displayed in seconds.</td>
</tr>
<tr>
<td>Conditions</td>
<td>Filter conditions defining the records in the VI and VG tables to which the rules apply.</td>
</tr>
</tbody>
</table>

5. Select the **Active** option to activate a rule.

Once the rule is activated, the hourly platform function, **Auto flush**, deletes those records from the table for which the rule is activated.

If your environment has millions, or ten of millions of records that match your delete criteria, you may want to consult with ServiceNow customer support prior to enabling the auto delete rules to help you delete records using a phased process.
Create or edit Vulnerability Response remediation target rules

Vulnerability managers set up a remediation target rule at the vulnerable item level to drive the remediation of high-risk vulnerabilities in a timely manner. When the remediation date for a vulnerable item nears, a notification is sent to the users or groups specified in the rule.

Before you begin
Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure
1. Navigate to Vulnerability > Administration > Remediation Target Rules.
2. Click New.
3. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the rule.</td>
</tr>
<tr>
<td>Target (days)</td>
<td>Specify the number of days within which the vulnerable items should be remediated, since first identified.</td>
</tr>
<tr>
<td>Active</td>
<td>By default the Active check box is selected, which means the remediation target rule is active. If this check box is cleared, this rule does not apply to new vulnerable items created in the system.</td>
</tr>
<tr>
<td>Notify (days before due)</td>
<td>Number of days prior to the targeted remediation time for a notification to be sent. The notification date calculated using this value is used to show the remediation status and color coding. If the date is before the notification date, the remediation status is “In flight.” If it is past the notification date and before the remediation target date, the status is shown as approaching target.</td>
</tr>
</tbody>
</table>

Note: If this field is set to 0, only a Target Missed notification is sent.
# Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule applies to</td>
<td>Using the condition filter, select the criteria for applying the rule to the vulnerable items. To prevent performance impact, test your conditions at full production scale. Testing enables you to determine how long the Evaluate remediation targets job takes to execute, given the conditions and the size of your Configuration Management Database (CMDB).</td>
</tr>
</tbody>
</table>

**Notifications**

**Note:** The count shown in the notification email does not include vulnerable items in the Deferred, Resolved, or Closed state.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>The people to notify when the selected vulnerable item is approaching or passes its targeted remediation target time.</td>
</tr>
<tr>
<td>Group</td>
<td>The group to notify when the selected vulnerable item is approaching or passes its targeted remediation target time.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

This rule goes into effect during the next run of the scheduled job, Evaluate remediation targets or, starting with v12.0, when using the Change Apply button on the Remediation Target Rules list view. The same is true when an
existing rule is updated. For more information on the scheduled job, see Vulnerability Response remediation target rules.

Create a Vulnerability Response CI lookup rule

The CI Lookup Rules module contains rules that define what fields have matching data in the Configuration Management Database (CMDB). These rules are used to identify configuration items (CIs) and add them to the vulnerable item record to aid in remediation.
Before you begin
Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)
Starting with v10.3, persona and granular roles are available to help you
manage what users and groups can see and do in the Vulnerability Response
application. For initial assignment of the persona roles in Setup Assistant, see
Assign the Vulnerability Response persona roles using Setup Assistant. For more
information about managing granular roles, see Manage persona and granular
roles for Vulnerability Response.

About this task
Creating CI lookup rules requires advanced ServiceNow and Vulnerability
Response expertise. Rather than modifying one of the existing lookup rules,
consider copying it and modifying the copy. When you are satisfied that the
new rule does what you want, deactivate the original.

Note: Rules, once removed, cannot be recovered. Rather than removing
existing rules, deactivate them when creating new ones.

Procedure
2. Click New.
3. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the rule.</td>
</tr>
<tr>
<td>Lookup method</td>
<td>Method used for matching. Choices are:</td>
</tr>
<tr>
<td></td>
<td>• Script: Pre-built (IP address, DNS name, and so on) or custom script.</td>
</tr>
<tr>
<td></td>
<td>• Field matching: Search on table or field in the CMDB.</td>
</tr>
<tr>
<td>Type</td>
<td>Type used with the Script Lookup method.</td>
</tr>
<tr>
<td>Order</td>
<td>Order of precedence for the rule. Rules with the lowest order are evaluated first.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box for whether the rule is active or disabled.</td>
</tr>
<tr>
<td>Source</td>
<td>Source used as input to this rule.</td>
</tr>
<tr>
<td>Source field</td>
<td>Source field used as input to this rule. Select any field, but it is treated as a string value.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Version 12.0: Condition</td>
<td>Condition based on which the CI lookup rule is applied. This condition depends on the attribute from the third-party scanner.</td>
</tr>
<tr>
<td></td>
<td>Note: The asset attribute is a part of the payload. It is received from the third-party scanner. See the Discovered Items table for payload examples.</td>
</tr>
<tr>
<td>Script</td>
<td>Editable sample script, based on the Type, is shown. Implement the custom script following the comments included in the template of the default function.</td>
</tr>
<tr>
<td></td>
<td>Note: The process function has three parameters: rule, sourceValue, and sourcePayload</td>
</tr>
<tr>
<td>Search on table</td>
<td>Table to search within the CMDB. Used with field matching Lookup Method.</td>
</tr>
<tr>
<td>Search on field</td>
<td>Field that contains information that can be used to locate a CI. Used with the field matching Lookup method. This field may be on the CI record, or on a related record, such as a network adapter.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

For more information implementation information for CI Lookup Rules see, Prevent duplicate or orphaned records after running Vulnerability Response CI lookup rules.
Example of a CI lookup rule using a condition builder for V12.0

Example of a CI lookup rule using a script prior to V12.0
Related reference
  Vulnerability Response vulnerable item form fields

Ignore CI classes
To ignore some configuration item (CI) classes, for example Load Balancer [cmdb_ci_lb], when running CI Lookup Rules, set the `ignoreCIClass [sn_sec_cmn.ignoreCIClass]` system property.

Before you begin
Role required: admin

ℹ️ Note:
The `ignoreCIClass` system property is available the property functionality is not available upon upgrade from any previous version.

If you have upgraded from any Security Operations application, prior to version 9.0, see KB0788209 for instructions on how to enable this functionality.

Procedure
1. Enter `sys_properties.list` in the left navigation bar. Click Enter.
2. In the Search menu, under Name enter `sn_sec_cmn.ignoreCIClass`.
3. In the Value text box, enter the CI classes to exclude in a comma-separated list.
4. Click **Update**.

   This list is used by CI Lookup Rules during the next import. Vulnerable items created during import are not associated to a CI of any type listed in the **Value** field of the `sn_sec_cmn.ignoreCIClass` system property.

**Filter decommissioned CIs**

Filter decommissioned CIs while running the CI lookup rules. Starting with v12.0, to filter decommissioned CIs when running the Security Operations CMDB CI lookup rules, set the `filterOutDecommissionedCI` system property. The default value is true.

**Before you begin**

You can also run lookup rules to auto-promote all the CIs by setting the `autoPromoteFields` system property. For example:

```json
{
    "cmdb_ci_network_adapter": "cmdb_ci",
    "cmdb_ci_nic": "cmdb_ci",
```
Role required: sn_vul.vulnerability_admin

Procedure
1. Enter sys_properties.list in the left navigation bar. Click Enter.
2. In the Search menu, under Name enter sn_sec_cmn.filterOutDecommissionedCI to filter the decommissioned CIs.
3. In the Value text box, enter the CIs to filter in a comma-separated list.
4. Click Update.
   This list is used by CI Lookup Rules during the next import. The sn_sec_cmn.filterOutDecommissionedCI system property filters out the decommissioned CIs while running these lookup rules.

Manually reclassify unmatched configuration items from Discovered Items
Use this process to manually reclassify configuration items (CIs) in the Discovered Items list when the Reclassify button is unavailable.

Before you begin
Role required: admin

About this task
If a configuration item (CI) has already been reclassified once, the Reclassify button on the Discovered Items list cannot be used again. Also, the Reclassify button is not available for unmatched CIs imported from Kingston or earlier versions of third-party integrations.

Procedure
2. To reclassify the configuration item:
   a. In the Class column, double-click inside the first Class field box (not the link).

   The Class list appears.
b. To reclassify, select a different class from the **Class** list.

c. Click the green check mark icon (✓).

Any data added to or left in these fields is transferred to the resulting **Configuration Item** when it is reclassified.

**3. Optional:** To update the record for this CI in the CMBD directly, click the information icon (ℹ️) next to **Configuration Item** within the **Discovered Items** record.

a. Click **Open record**.

b. Make your changes and click **Update**.

**Create a Vulnerability Response calculator**

A vulnerability calculator is a pre-defined formula to calculate a target field when certain criteria are met. Calculators, which calculate the vulnerable item **Risk Score**, can contain **Risk Rules**.

**Before you begin**

Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see **Assign the Vulnerability Response persona roles using Setup Assistant**. For more information about managing granular roles, see **Manage persona and granular roles for Vulnerability Response**.

⚠️ **Note:** You may notice performance degradation when running vulnerability calculators that contain scripts.

Order your rules to run the simplest rules first and only run scripts on the items that cannot be handled with a condition and template value or a risk rule.
Procedure
1. Navigate to Vulnerability > Administration > Vulnerability Calculators.
2. Click New.
3. Fill in the fields on the form, as appropriate.

Vulnerability calculator form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the vulnerability calculator.</td>
</tr>
<tr>
<td>Table</td>
<td>Auto-filled with the name of the vulnerable item table.</td>
</tr>
<tr>
<td>Application</td>
<td>Auto-filled with Vulnerability Response.</td>
</tr>
<tr>
<td>Target field</td>
<td>Field to calculate.</td>
</tr>
<tr>
<td>Description</td>
<td>Text description of the calculator.</td>
</tr>
<tr>
<td>Active</td>
<td>Turn the calculator on or off.</td>
</tr>
</tbody>
</table>

4. Right-click in the header to Save.
The Vulnerability Calculator Rules section appears.
5. Create a rule for the calculator by clicking New.

Note: For the New Risk Rules form (only available when the Target field is Risk Score) see step 10.
6. Fill in the fields, as appropriate.

Vulnerability Calculator Rule form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the calculator rule.</td>
</tr>
<tr>
<td>Order</td>
<td>The order in which to run the vulnerability calculator.</td>
</tr>
<tr>
<td></td>
<td>A calculator with an order entry of 100 runs before a calculator with an order entry of 200.</td>
</tr>
<tr>
<td>Calculator</td>
<td>Auto-filled with the calculator parent.</td>
</tr>
<tr>
<td>Active</td>
<td>By default the Active check box is selected, which means the calculator rule is active. If you clear this check box, this rule does not apply to new vulnerable items created in the system.</td>
</tr>
</tbody>
</table>
7. Fill in the fields in the **When this condition is met** tab, as appropriate.

### When this condition is met tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the calculator rule.</td>
</tr>
<tr>
<td>Order</td>
<td>The order in which to run the vulnerability calculator. A calculator with an order entry of 100 runs before a calculator with an order entry of 200.</td>
</tr>
<tr>
<td>Calculator</td>
<td>Auto-filled with the calculator parent.</td>
</tr>
<tr>
<td>Active</td>
<td>By default the <strong>Active</strong> check box is selected, which means the calculator rule is active. If you clear this check box, this rule does not apply to new vulnerable items created in the system.</td>
</tr>
<tr>
<td>Advanced view</td>
<td>When selected, select scripted conditions and scripted values from <strong>Condition type</strong> and <strong>Value type</strong>.</td>
</tr>
<tr>
<td>Condition type</td>
<td>Available when you select the <strong>Advanced view</strong>. Choices include:</td>
</tr>
<tr>
<td></td>
<td>• Filter: Uses filter conditions.</td>
</tr>
<tr>
<td></td>
<td>• Filter group: See <a href="#">create a new filter group</a> to define the calculator criteria.</td>
</tr>
<tr>
<td></td>
<td>• Script: Script condition used to determine when to apply this calculator.</td>
</tr>
<tr>
<td>Note:</td>
<td>Before you write scripts for determining when to apply the calculators, return to the <strong>Vulnerability Calculators</strong> list. Explore the vulnerability calculator records shipped with the base system.</td>
</tr>
<tr>
<td>Condition</td>
<td>Defines basic filter conditions for determining whether to use the calculator or not.</td>
</tr>
</tbody>
</table>

Selecting either the **Filter group** or **Script** condition types, hides this field.

Starting with v13.0, case sensitivity for the search text you enter in the condition builder is not supported on this record.
or form. Prior to v 13.0, case sensitivity is supported for the search text you enter in the condition builder.

8. Click the Set these values tab and fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value type</td>
<td>Available when you select the Advanced view. Choices include:</td>
</tr>
<tr>
<td></td>
<td>• Template: Define the values to set on each field.</td>
</tr>
<tr>
<td></td>
<td>• Script: Used to set the values on each field.</td>
</tr>
<tr>
<td>Script values</td>
<td>Available if you selected the Script value type.</td>
</tr>
<tr>
<td></td>
<td>Defines what values to apply the calculations to.</td>
</tr>
<tr>
<td>Template</td>
<td>Select the fields and values you want to use for the calculator.</td>
</tr>
<tr>
<td></td>
<td>Selecting either the Script value type, hides this field.</td>
</tr>
</tbody>
</table>

9. When you have completed all entries, click Submit.

Note: When you edit an existing calculator, and you want to update all existing scores, you can use the Reapply Calculator button. It runs through all active vulnerable items (VIs), and if that calculator would be used to set its value, recalculates the value for those VIs. Since reapplying a calculator can take a long time, a scheduled job handles it.

10. For the **New Risk Rules** form, fill in the fields as appropriate.

    Set each weight according to the percentage of the result that should come from that value. For any data that your scanner does not provide, or for data that should not be part of the risk score, set the weight to zero.
    
    Starting with v14.0 of Vulnerability Response, you can add, delete, or update the fields. You can also configure the weightage percentage for the field values. For more information, see .
    
    As you update the weights, scenarios display the weights remaining, as well as anticipated **Risk Score** results.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the calculator rule.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Order</td>
<td>The order in which to run the vulnerability calculator. A calculator with an order entry of 100 runs before a calculator with an order entry of 200.</td>
</tr>
<tr>
<td>Calculator</td>
<td>Auto-filled with the calculator parent.</td>
</tr>
<tr>
<td>Active</td>
<td>By default the <strong>Active</strong> check box is selected, which means the calculator rule is active. If you clear this check box, this rule does not apply to new vulnerable items created in the system.</td>
</tr>
<tr>
<td>Condition</td>
<td>Defines basic filter conditions for determining whether to use the calculator. Selecting either the <strong>Filter group</strong> or <strong>Script</strong> condition types, hides this field.</td>
</tr>
<tr>
<td><strong>Weights</strong></td>
<td></td>
</tr>
<tr>
<td>Vulnerability Severity</td>
<td>Percentage of the result that comes from severity.</td>
</tr>
<tr>
<td>Exploit exists</td>
<td>Percentage of the result that comes from the existence of an exploit. If this information is not present in your vulnerabilities, set the weight to zero.</td>
</tr>
<tr>
<td>Exploit skill level</td>
<td>Percentage of the result that comes from the skill level required by the exploit. If this information is not present in your vulnerabilities, set the weight to zero.</td>
</tr>
<tr>
<td>Exploit attack vector</td>
<td>Percentage of the result that comes from where the attack is targeted. If this information is not present in your vulnerabilities, the set weight to zero.</td>
</tr>
<tr>
<td>Business criticality</td>
<td>Percentage of the result that comes from business criticality. If you have not linked your CIs to business services, the set weight to zero.</td>
</tr>
<tr>
<td>CI Exposure</td>
<td>Percentage of the result that comes from whether the CI is internet-facing. If the weight is non-zero, a condition filter appears to define which CI are internet-facing. Set the filter to select your Internet-facing configuration items. You can preview which records match the condition.</td>
</tr>
<tr>
<td>Running total</td>
<td>Auto-computed percentage totals. When this value reaches 100, the Scenario preview shows you sample risk scores in different scenarios.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Risk score</td>
<td>When all weights total 100%, risk score scenarios display, providing a preview of the risk score in some of the possible scenarios.</td>
</tr>
<tr>
<td>scenarios</td>
<td></td>
</tr>
</tbody>
</table>

Starting with v14.0 of Vulnerability Response, you can add or remove criteria, and adjust the weight of each criteria using the Embedded list.

**Risk Rule CI for VR v14.0**

11. Click **Submit**.

**Filtering within Vulnerability Response**

Vulnerability Group Rules, Calculators, and Assignment Rules use conditions during import, created using the **Condition builder**. Changes to their criteria can affect performance since each record is evaluated using these filters.

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
The rules and calculators shipped with the base system are optimized for performance. Editing or creating rules or calculators takes care and may require both ServiceNow and Vulnerability Response expertise. That said, some guidance is available.

Avoid filtering based on subclass fields
Some tables support extension. An example of that is the CMDB CI [cmdb_ci] table. Tables like cmdb_ci_hardware and cmdb_ci_computer extend this table. If you filter based on a field that is not on the parent table, that filter can be expensive to construct and evaluate.

For example, filtering on Configuration Item > Cost would not adversely affect performance because Cost is a class field, and not a subclass field, of Configuration Item.

Configuration Item > Computer, however, is a subclass requiring a dot-walk to another field, in this case, Operating System. This process can take many milliseconds which adds up quickly, when millions of vulnerable items are being imported, and affect performance.

Note: Using the [contains] condition is like a wild card search and can cause performance impact. Using [is], wherever possible, is more efficient.

Create a Vulnerability Response severity map
Vulnerability Response severity mapping transforms third-party source severity fields to recognizable fields in Vulnerability Response.
Before you begin
Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task
Vulnerability Response ships with National Vulnerability Database (NVD) to normalized ServiceNow severity mapping. ServiceNow third-party integrations such as the Qualys Vulnerability Integration provide severity mappings upon installation. These maps can be adjusted by changing the fields in existing maps. Creating or editing a severity map is intended only for customized or non-standard third-party mappings in your environment.

Procedure
2. Click New.
3. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>The name of the source for the severity mapping.</td>
</tr>
<tr>
<td>Source value</td>
<td>The source severity value.</td>
</tr>
<tr>
<td>Target value</td>
<td>The target severity value. Choices are:</td>
</tr>
<tr>
<td></td>
<td>• 1 - Critical</td>
</tr>
<tr>
<td></td>
<td>• 2 - High</td>
</tr>
<tr>
<td></td>
<td>• 3 - Medium</td>
</tr>
<tr>
<td></td>
<td>• 4 - Low</td>
</tr>
<tr>
<td></td>
<td>• 5 - None</td>
</tr>
</tbody>
</table>

4. Repeat Step 3 for each source severity level.
5. Click Submit.
Create a vulnerability solution

Create a vulnerability solution so that you can track vulnerability solutions that are not covered by third-party solution content.

Before you begin
Role required: admin, v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated), or vulnerability.write
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task
You can create a solution from any of the solution lists.

Procedure
1. Navigate to Vulnerability Response > Solutions.
2. Choose a solution list: All, Highest Supersedence or With Vulnerable Items.
3. Click New.
4. Fill in the editable fields on the form, as appropriate. You can leave any unused fields blank.
5. Right-click Save in the header.
   The solution record is added and appears in the All and Highest Supersedence lists, by default.
6. The Related Lists appear. You can associate this solution to the following related lists: Vulnerable Items, Third-Party Vulnerabilities, CVEs, Superseding
**Solutions** and **Preceding Solutions**. Choose a vulnerability or solution and click **Submit**.

1. **Note:**

   Vulnerability Solution Management automatically associates vulnerable items and vulnerability groups with solutions when vulnerability records are associated manually with solutions.

   Vulnerable items manually re-assigned to another solution are not automatically updated with solution changes at the vulnerability level.

   If you want to exclude the relationship between a third-party vulnerability and a solution because it is not relevant to the CI you are remediating, or it is not a concern in your environment, see **Manually exclude solutions from third-party records or vice versa**.

**Solution form fields**

Solutions are created automatically when records are downloaded from third-party solution integrations and stored under **Solutions** in Vulnerability Response.

**Solution integration entry fields**

The imported fields in this table are read-only.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Identifier assigned to the solution.</td>
</tr>
<tr>
<td>Source</td>
<td>Origin of the solution.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Source identifier for this solution.</td>
</tr>
<tr>
<td>Risk rating</td>
<td>Separates Solution record <strong>Risk score</strong> into ranges from Critical to None. For more information on solution <strong>Risk rating</strong>, see Vulnerability Solution Management.</td>
</tr>
</tbody>
</table>

1. **Note:** Solution **Risk rating** is not the same as the **Vulnerable Item**, **Third-party Vulnerability Entry**, and **Vulnerability Group** records **Risk rating**.

| Risk score | Weighted calculation based on the **Risk score** and count of vulnerable items with this solution as their **Preferred solution**. For more information on solution risk score, see Vulnerability Solution Management. |
### Field | Description
--- | ---
| **Note:** Solution record **Risk score** is not the same as the **Vulnerable Item**, **Third-party Vulnerability Entry**, and **Vulnerability Group** records **Risk score**. Available when SAM NVD is enabled, but if there are no active vulnerable items (VI) associated with a vulnerability the solution **Risk score** is set to zero.
| Highest-supersedence | Indicates that no solution supersedes it.
| Solution type | What kind of solution it is. Choices are:
- Workaround
- Mitigation
- Vendor Fix
- Patch
- Rollup
- Entitlement
- Will Not Fix
- None available
| Requires restart | Restart needed. Choices are:
- Yes
- No
- Maybe
| Date published | Date the vulnerability was published by source.
| Last modified | Date the vulnerability was last modified by source.
| Summary | Remediation summary of the solution.
| Product Categories | Product categories to which the solution applies.
| Products | Products to which the solution applies.
| **Solution Details** | **Solution Details**
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>If no content is available from the solution source, you are directed to another relevant section or solution for more information.</td>
</tr>
<tr>
<td>Links</td>
<td>Imported internet resources associated with the solution.</td>
</tr>
</tbody>
</table>

#### Vulnerability Details

| Vulnerability Notes     | Summary of vulnerabilities remediated by the solution.                                                                                       |

#### Remediation Status

**Preferred Solution Targets**

Remediation status for vulnerable items and their unique configuration items (CIs), for which this is the preferred solution.

**Note:** A unique CI is one that is counted only once, regardless of how many VIs it is associated with.

<table>
<thead>
<tr>
<th>Vulnerable Items</th>
<th>Number of active (non-closed) vulnerable items for which this solution is preferred for remediation. This count excludes deferred vulnerable items.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total VIs</td>
<td>Number of active and closed vulnerable items for which this solution is preferred for remediation. This count excludes deferred vulnerable items.</td>
</tr>
<tr>
<td>% VIs remediated</td>
<td>Percent complete for vulnerable item (VI) remediation. Applies to VIs for which this solution is preferred. This count excludes deferred VIs.</td>
</tr>
<tr>
<td>Remaining CIs</td>
<td>Number of unique CIs associated with one or more active vulnerable items for which this solution is preferred for remediation. This count excludes the CIs of deferred vulnerable items.</td>
</tr>
<tr>
<td>Total CIs</td>
<td>Number of unique CIs associated with one or more active and closed vulnerable items for which this solution is preferred for remediation. This count excludes the CIs of deferred vulnerable items.</td>
</tr>
<tr>
<td>% CIs remediated</td>
<td>Percent complete of unique CIs remediated (meaning all VIs for that CI and this solution are remediated). Determined by the number of remediated CIs over the total unique CIs associated to vulnerable items with the preferred solution. This count excludes the CIs of deferred vulnerable items.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Preferred Solution Targets (Includes Deferred)</strong></td>
<td>Remediation status for vulnerable items and their unique CIs, including deferred, for which this is the preferred solution.</td>
</tr>
<tr>
<td>Vulnerable Items</td>
<td>Number of active (non-closed) vulnerable items for which this solution is preferred for remediation.</td>
</tr>
<tr>
<td>Total VIs</td>
<td>Number of active and closed vulnerable items for which this solution is preferred for remediation.</td>
</tr>
<tr>
<td>% VIs remediated</td>
<td>Percent complete for vulnerable item (VI) remediation. Applies to VIs for which this solution is preferred.</td>
</tr>
<tr>
<td>Remaining CIs</td>
<td>Number of unique CIs associated with one or more active vulnerable items for which this solution is preferred for remediation.</td>
</tr>
<tr>
<td>Total CIs</td>
<td>Number of unique CIs associated with one or more active and closed vulnerable items for which this solution is preferred for remediation.</td>
</tr>
<tr>
<td>% CIs remediated</td>
<td>Percent complete of unique CIs remediated (meaning all VIs for that CI and this solution are remediated). Determined by the number of remediated CIs over the total unique CIs associated to vulnerable items with the preferred solution. This count excludes the CIs of deferred vulnerable items.</td>
</tr>
<tr>
<td><strong>Potential Solution Targets</strong></td>
<td>Remediation status for vulnerable items and their unique CIs, with a vulnerability related to this solution.</td>
</tr>
<tr>
<td>Vulnerable items</td>
<td>Number of active (non-closed) vulnerable items for which this solution is a potential solution for remediation. This count excludes deferred vulnerable items.</td>
</tr>
<tr>
<td>Remaining CIs</td>
<td>Number of unique CIs associated with one or more active vulnerable items for which this solution is a potential solution for remediation. This count excludes deferred vulnerable items.</td>
</tr>
<tr>
<td><strong>Potential Solution Targets (Includes Deferred)</strong></td>
<td>Remediation status for vulnerable items and their unique CIs, including deferred, with a vulnerability that can be remediated by this solution, including preferred solution counts.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Vulnerable items</td>
<td>Number of active (non-closed) vulnerable items for which this solution is a potential solution for remediation.</td>
</tr>
<tr>
<td>Remaining CIs</td>
<td>Number of unique CIs associated with one or more active vulnerable items for which this solution is a potential solution for remediation.</td>
</tr>
</tbody>
</table>

**Notes**

| Internal notes               | Editable field provided for the remediation specialist.                                                                                                                                                     |

**Related Links**

| Version 10.0: Update status  | Date and time when the Remediation status was last updated.                                                                                                                                                |
|                              | Updates the following:                                                                                                                                                                                     |
|                              | • Vulnerability group state                                                                                                                                                                               |
|                              | • Risk score and rating                                                                                                                                                                                    |
|                              | • Metrics from the Remediation Status section                                                                                                                                                             |

**Related Lists**

| Vulnerable Items             | Vulnerable items associated with this solution as the preferred solution for remediation.                                                                                                                  |
| Third-Party Vulnerabilities  | Third-party vulnerabilities associated with this solution.                                                                                                                                                |
| CVEs                         | Common Vulnerability and Exposure (CVE) vulnerabilities associated with this solution.                                                                                                                     |
| Vulnerability Groups         | Vulnerability groups that contain related vulnerable items with this solution preferred for remediation.                                                                                                  |
| Preceding Solutions          | Earlier solutions which resolve one or more of this solution’s vulnerabilities.                                                                                                                              |
| Superseding Solutions        | Later solutions that resolve all of this solution’s vulnerabilities. This list is empty when the `highest-supersedence` box is checked.                                                                   |

**Manually exclude solutions from third-party records or vice versa**

Exclude the relationship between a third-party vulnerability and a solution because it is not relevant to the CI you are remediating, or it is not a concern.
in your environment. Manually exclude solutions using either a third-party vulnerability or solution record.

**Before you begin**

Role required: sn_vul.write
sn_vul.remediation_owner

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see **Assign the Vulnerability Response persona roles using Setup Assistant**. For more information about managing granular roles, see **Manage persona and granular roles for Vulnerability Response**.

**Procedure**

1. Navigate to **Vulnerability Response > Libraries > Third-Party** or **Vulnerability Response > All Solutions**
2. Open a third-party vulnerability or solution record.
   a. For a third-party record: Select the **Solutions** related tab.
   b. For a solution record: Select the **Third-Party Vulnerabilities** related tab.
3. Check the box next to each vulnerability or solution record you want to exclude.
4. From the **Actions on selected rows** drop-down menu, choose **Exclude**.

The third-party or solution record no longer appears in the related tab. Third-party vulnerability relationships to solutions are excluded during the nightly scheduled job. Excluding third-party vulnerabilities means that the solution is no longer a factor for any preferred solution evaluation. Exclusion impacts:
• All counts for solutions since the third-party vulnerability, vulnerable items (VIs), and, configuration items (CIs) attached to the third-party vulnerability do not count toward the solution anymore.

• Determining the preferred solution for the third-party vulnerability and by extension the preferred solution of any attached VIs and vulnerability groups containing the VI.

Define service classifications for Vulnerability Response reporting and related lists

Bring more focus to reporting and related lists in Vulnerability Response by defining service classifications. In addition, reducing the number of requested service classifications can improve the performance of Vulnerability Response data gathering.

Before you begin
Role required: admin

Note:
Editing system properties requires both ServiceNow and Vulnerability Response expertise.

Procedure

1. Enter `sys_properties_list.do` in the left navigation bar. Click Enter.
2. In the Search menu, under Name enter `sn_vul.service_classifications`.
3. Open the `sn_vul.service_classifications` system property.
4. In the Value text box, enter the comma-separated list of the service classifications you want.

   Note: When this setting is empty, all services are listed.

   Examples:

   To see Business Services, Technical Services and Application Services and exclude Service Offerings, Shared Services, and unclassified services, set the value to: Business Service, Technical Service, Application Service.

   To see Application Services, set the value to: Application Service.

5. Click Update.

   The data in each report and vulnerable item related list is filtered by service classification during the next run of the nightly performance analytics job.
Audit selected fields in the vulnerable items table

Enable auditing for fields you specify in the Vulnerable Item [sn_vul_vulnerable_item] table. This method of auditing is useful when you want to audit fields that you cannot audit by default.

Before you begin
Role required: admin

About this task
The sn_vul_vulnerable_item table is auditable by default. Starting with v10.0, fields that have the no_audit attribute set to true are not auditable. For more information about auditing tables, see Enable auditing for a table.

Procedure
1. Navigate to Vulnerability Response > System Definition > Tables and search for the sn_vul_vulnerable_item table. The list of dictionary entries for the table is displayed.
2. To enable auditing for a field, click the name of the entry. The Dictionary Entry page for that entry is displayed.
3. Navigate to Attributes > No audit. The Dictionary Attribute page is displayed.
4. To remove the no audit=true attribute, click Delete. Auditing for this field is enabled.
View Vulnerability Response SLAs for vulnerability groups

To ensure that vulnerable items are processed correctly, you can define a Service Level Agreement (SLA) for Vulnerability Response vulnerability groups.

Before you begin
Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task
The SLA definitions in this list are a subset of the platform SLA list, specific to Vulnerability Response.

For detailed instructions, see Create an SLA definition.

Procedure

1. Navigate to Vulnerability > Administration > SLA Definitions.
2. Click on a definition.
   Task SLAs are shown in the related lists of Vulnerability Groups.

Quick start tests for Vulnerability Response

Validate that Vulnerability Response still works after you make any configuration change such as apply an upgrade or develop an application. Copy and customize these quick start tests to pass when using your instance-specific data.

Vulnerability Response quick start tests require activating the Vulnerability Response application (sn_vul) and loading the demo data.

<table>
<thead>
<tr>
<th>Test</th>
<th>Description</th>
<th>Release version</th>
</tr>
</thead>
<tbody>
<tr>
<td>VR: Create Remediation Target Rule</td>
<td>Create a Remediation Target Rule.</td>
<td>Madrid</td>
</tr>
<tr>
<td>VR: Create Vulnerability Group Rule</td>
<td>Create a Vulnerability Group Rule.</td>
<td>Madrid</td>
</tr>
<tr>
<td>VR: Create Vulnerable Item via Form</td>
<td>Determine whether a user can successfully create a vulnerable item</td>
<td>Madrid</td>
</tr>
<tr>
<td>Test</td>
<td>Description</td>
<td>Release version</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>VR: Vulnerability Group Life Cycle</td>
<td>Determine whether a user can successfully resolve a vulnerability group.</td>
<td>Madrid</td>
</tr>
<tr>
<td>VR: Vulnerable Item life cycle</td>
<td>Determine whether a user can successfully move a vulnerable item through its life cycle, and also determine whether a closed vulnerable item can be reopened.</td>
<td>Madrid</td>
</tr>
<tr>
<td>VR: Rollup Calculator</td>
<td>Determine whether the rollup risk calculator can provide an overall risk score for an entire group of vulnerable items using the scores for all the vulnerable items in a vulnerability group.</td>
<td>New York</td>
</tr>
<tr>
<td>VR: Vulnerability Response Assignment Rules</td>
<td>Determine whether a sample set of assignment rules can successfully auto-assign vulnerable items to an assignment group for remediation.</td>
<td>New York</td>
</tr>
<tr>
<td>VR: Vulnerability Calculators</td>
<td>Test the vulnerability calculators.</td>
<td>New York</td>
</tr>
<tr>
<td>VR: CI Lookup - Qualys</td>
<td>Create a new lookup rule with method &quot;field_matching&quot; called &quot;Lookup By Network Adapter&quot; for Qualys. Determine whether a configuration item is successfully matched in the Discovered Item table by network.</td>
<td>Orlando</td>
</tr>
<tr>
<td>Test</td>
<td>Description</td>
<td>Release version</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>VR: Create Normal and Emergency Change Request</td>
<td>Determine whether the user can successfully create normal and emergency change requests from a vulnerability group.</td>
<td>Orlando</td>
</tr>
<tr>
<td>VR: Split Vulnerability Group</td>
<td>Determine whether the user can successfully split a vulnerability group.</td>
<td>Orlando</td>
</tr>
<tr>
<td>VR: Update VG state when a CHG is cancelled.</td>
<td>Determine whether the State field on a vulnerability group successfully transitions when a change request that is associated with the vulnerability group is cancelled.</td>
<td>Orlando</td>
</tr>
<tr>
<td>VR: Update VG state when a CHG transitions to Review.</td>
<td>Determine whether the State field on a vulnerability group successfully transitions when a change request that is associated with it moves to the Review state.</td>
<td>Orlando</td>
</tr>
<tr>
<td>VR: CI Lookup -Rapid7</td>
<td>Test CI lookup using the existing Rapid7 Vulnerability Integration lookup rule, <strong>IP Address</strong>.</td>
<td>Orlando</td>
</tr>
<tr>
<td>VR: CI lookup - Qualys</td>
<td>Test CI lookup by creating a new lookup rule for the Qualys Vulnerability Integration</td>
<td>Orlando</td>
</tr>
<tr>
<td>VR: Exception Approval Workflow for VI</td>
<td>Create an exception request and verify that</td>
<td>Orlando</td>
</tr>
<tr>
<td>Test</td>
<td>Description</td>
<td>Release version</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>VR: False Positive Approval Workflow for VI</td>
<td>Create a false positive exception request and verify that the approval process is working.</td>
<td>Orlando</td>
</tr>
<tr>
<td>VR: Application Vulnerability Response (AVR)</td>
<td>Determine whether your rules and calculators are working correctly. Verify that updates are working.</td>
<td>Orlando</td>
</tr>
<tr>
<td>Remediation target rules: VI import test</td>
<td>Tests VR remediation target rules during import</td>
<td>Paris</td>
</tr>
</tbody>
</table>

**Related information**

**Quick start tests**

**Run the Automated Test Framework (ATF) test suite for Vulnerability Response**

Run the Automated Test Framework (ATF) test suite after you install or upgrade the Vulnerability Response application.

**Before you begin**

Confirm a successful installation and that your instance works as designed.

The test execution property is disabled by default to prevent running tests on a production system. Run tests only on development, test, and other non-production instances. If demo data or demo accounts are created, all demo data should be removed prior to using the instance in non-production or production.

- Verify you installed demo data when you installed Vulnerability Response. Demo data is required to run the Vulnerability Response test suite.
- To enable the test, follow these steps:
  2. If not selected, select the Enable test/test suite execution check box.
  3. Click Save.
  4. If the scope is not set to Vulnerability Response in the header, or the scope is not displayed in the header, click the settings icon at the top of the page in the browser window.

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
5. In the System Settings window, click Developer.

6. If not selected, click Show application picker in header and close the window.

7. In the list that is displayed next to System Administrator, click Vulnerability Response for the field. The field is displayed as shown in the following image.

Role required: admin or atf_test_admin

Procedure

1. Navigate to Automated Test Framework (ATF) > Suites.
2. From the Test Suites list, locate Vulnerability Response Quick Start Tests.
3. Click it to open the record.
4. In the open record, select the Active check box.
5. Click Update.
6. If the Run Test Suite button is not displayed, refresh your screen, open the record again and click Run Test Suite to start the test. After a few moments, the Run Test Suite dialog indicates a successful test. Click Go to Result for more information.

What to do next

Congratulations! You can continue with your configuration of Vulnerability Response.
For more information about automated tests for Vulnerability Response and automated tests, tests suites, and creating automated tests, see Automated Test Framework (ATF).

**Vulnerability Response remediation overview**

Vulnerability Response remediation is a phased process consisting of verifying import completion, triaging new vulnerabilities, and monitoring progress to completion. Approached in this way, remediation becomes manageable, timely, and in many ways, automated.

Understanding your security posture across company assets helps you identify the most critical vulnerabilities for remediation. This remediation process requires that Vulnerability Response and a third-party integration such as the Qualys Vulnerability Integration are installed and configured.

Verify the successful completion of third-party integration imports

The first phase in this process is to ensure that everything is working correctly. Vulnerability Response is preset to download National Vulnerability Database (NVD) and Common Enumeration Weakness (CWE) vulnerabilities. Third-party imports provide you with the data you need to create vulnerable items and vulnerability groups. Successful remediation depends on the consistent and successful import of vulnerabilities and vulnerable items.

During import CI Lookup Rules match third-party assets to assets in the Configuration Management Database (CMDB). All assets are stored in the Discovered Items module. CI information is critical to solution implementation.
Note: Once a third-party integration has been installed and configured, there are few instances where an import can fail, for example, if the third-party vendor throttles their API calls. When imports do fail, they require prompt attention.

Integration status run reports for the Qualys Vulnerability Integration, Rapid7 Vulnerability Integration, and, starting with v12.1 of Vulnerability Response, the Tenable Vulnerability Integration, are shipped with the applications to give you a graphical overview of your imports. Use this report, or create your own, to easily determine whether your latest import has succeeded.

Review and triage vulnerabilities and vulnerable items

The next phase of remediation calls for the review of new vulnerabilities and vulnerable items. A vulnerable item (VI) is a detected combination of vulnerability and configuration item (CI). As vulnerable items are formed, various rules are run that assign VIs, determine the risk they pose and set remediation targets. Adjust any rules, as necessary, to ensure that the vulnerable items have been triaged successfully.

Most vulnerable items are automatically grouped upon import, based on vulnerability group rules (VGRs). In this phase, focus on vulnerable items that were not grouped and on configuration items that were not matched to items in the CMDB. Matching Discovered Item record information to the CMDB gives you more granular control of your assets and resolving threats to them. Vulnerability groups allow you to remediate large numbers of vulnerable items efficiently. Vulnerable items that are not in a group must be managed individually, costing you time and effort. This is where strong vulnerability group rules are helpful.

Monitor the progress of existing vulnerability remediation

The final phase of remediation consists of monitoring your progress.

• Review the status of imports for patch implementations that have not shown up and follow up with IT Operations.
• Track the progress of regulatory compliance obligations and ensure their completion.
• Review deferred item status and revise or implement fixes.
• Monitor Vulnerability Management dashboards. To review trends, view reports in real-time, and use metrics that track your remediation target attainment rates, you may prefer to monitor your processes with the Performance Analytics for Vulnerability Response application.
• not recently detected by your third-party integrations.
Successful completion of Vulnerability Response integration imports verification

The easiest way to determine whether your imports have succeeded is to use an Integration Run Status dashboard. The Integration Run Status dashboard provides an example of a graphical view of the status of third-party integration runs.

The Qualys and Rapid7 vulnerability integrations have an integration run status dashboard. See Qualys integration run status chart or Rapid7 Vulnerability Integration run status chart for detailed information on the chart contents.

Note: Charts, for integrations not provided by ServiceNow®, can be created from reports in a dashboard but may require ServiceNow expertise. For more information on creating reports and dashboards, see Getting started with reports and Dashboards.

View Vulnerability Response vulnerable item detection data

Starting with v10.0, the complete data gathered by your third-party scanner integrations with Vulnerability Response are displayed on the Detections and Initial Detections tabs on the vulnerable item records (VIT). It is also displayed on Detection records on the Vulnerable Item Detection list in your Now Platform® instance.

Before you begin

Starting with v10.0, third-party Integrations retrieve vulnerable item detection data. Detections are distinct occurrences of vulnerabilities as reported by the scanners. Detection data are paired with vulnerable items and VI state is updated based on the state of the detections. If a VI is not found, a new one is created. Detections are only opened or closed by data found directly by a scanner.

Role required:

sn_vuln.admin initiates integration runs and views vulnerable item detection data

sn_vuln.remediation_owner is assigned vulnerable items created from vulnerable item detections and views data on VI records

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.
Procedure

1. To view the vulnerable item detection data, navigate to a vulnerable item record and open it. Starting with v10.0, the record is displayed with the Initial Detections and Detections tabs.

   **Note:** Data previously displayed on the Configuration Details tab is displayed along with other detection data on the Initial Detection and Detections tabs.

2. Select the Detections tab.

   When a vulnerable item is created from the results of a third-party scan, the data from the scan are displayed on the detection record, as shown in the following figure.
Each row in the Vulnerable Item Detections section represents data from a distinct detection. In the First found column, the date the vulnerable item is first detected by the scanner is displayed. In the Last found column, the date of the most current detection is displayed. The Source field displays the scanner that retrieved the data.

Note: For Qualys, with vulnerable item detections starting with v10.0, the following fields are deprecated on the VI record and are no longer populated:

- Qualys severity
- Last updated by source

Also for Qualys, as shown in the preceding figure, when a VI is created from a scan, the value from the scan for Results is displayed in the Proof column on the detection record. However, this value is not displayed on the upper portion of the VI record.

For Rapid7, when a VI is created from a scan, the value for Proof from the scan can be displayed in both the Proof column on the detection record and on the upper portion of the VI record, but not by default. To display this value on the upper portion of the VI record, select the Proof field from the form layout.

3. Optional: To configure the layout of the Detections tab on the record, follow these steps.
a. The following columns are displayed on the Detections tab by default.
   • Status
   • First found (data)
   • Last found (date)
   • DNS name
   • Net BIOSName
   • IP address
   • Times found
   • Port
   • Protocol
   • Proof
   • SSL

   Note:
   Note: if there is no value in a column, data for that field was not detected by the scanner.

b. Click the gear icon (⚙️) to personalize your view.

c. Select the columns from the slushbucket to display specific data and click OK.

4. With the Detections tab selected, in the Status column, click an item to open the detection record and view the details associated with that vulnerable item, including a Solution summary (Rapid7 InsightVM integration only).
## Qualys detection record

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>DET0000010001</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>QID-24687</td>
</tr>
<tr>
<td>Configuration</td>
<td>WIN-OGBUTNAGR11</td>
</tr>
<tr>
<td>Vulnerable Item</td>
<td>VIT000003</td>
</tr>
<tr>
<td>Discovered Item</td>
<td>SD00000000010001</td>
</tr>
<tr>
<td>Integration run</td>
<td>WINTRUN0001001</td>
</tr>
<tr>
<td>Source</td>
<td>Qualys</td>
</tr>
<tr>
<td>Status</td>
<td>Open</td>
</tr>
<tr>
<td>Source status</td>
<td>Active</td>
</tr>
<tr>
<td>First found</td>
<td>2017-07-18 12:12:05</td>
</tr>
<tr>
<td>Last found</td>
<td>2017-10-03 12:46:25</td>
</tr>
<tr>
<td>Times found</td>
<td>2</td>
</tr>
</tbody>
</table>

### Details

- **IP address**: 172.33.4.290
- **Port**: 3,389
- **Protocol**: TCP
- **SSL**: checked

### Proof

CIPHER KEY EXCHANGE AUTHENTICATION MAC ENCRYPTION (KEY-STRENGTH) GRADE TLSv1 WITH DES/3DES CIPHER IS SUPPORTED DES-CBC3-SHA RSA SHA1 3DES(168) MEDIUM TLSv1.2 WITH DES/3DES CIPHER IS SUPPORTED DES-CBC3-SHA RSA SHA1 3DES(168) MEDIUM TLSv1.2 WITH DES/3DES CIPHER IS SUPPORTED DES-CBC3-SHA RSA SHA1 3DES(168)

## Rapid7 detection record

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>DET0000061451</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>RTP-off-semb-signing-disabled</td>
</tr>
<tr>
<td>Configuration</td>
<td>wckliyg2-3-usvuln.lax.rapid7.com</td>
</tr>
<tr>
<td>Vulnerable Item</td>
<td>VIT0003380</td>
</tr>
<tr>
<td>Discovered Item</td>
<td>SD0000000002658</td>
</tr>
<tr>
<td>Integration run</td>
<td>WINTRUN0001001</td>
</tr>
<tr>
<td>Source</td>
<td>Rapid7</td>
</tr>
<tr>
<td>Status</td>
<td>Open</td>
</tr>
<tr>
<td>Source status</td>
<td>open</td>
</tr>
<tr>
<td>First found</td>
<td>2018-09-04 16:35:18</td>
</tr>
<tr>
<td>Last found</td>
<td>2019-02-13 13:15:30</td>
</tr>
<tr>
<td>Times found</td>
<td>0</td>
</tr>
</tbody>
</table>

### Details

- **IP address**: 10.4.26.79
- **Port**: 139
- **Protocol**: TCP
- **SSL**: unchecked

### Proof

SMB signing is disabled

### Solution summary

Configure SMB signing for Windows

© 2021 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
5. Return to the record and select the Initial Detection tab.

The Initial Detections tab displays the data imported from the third-party scanner on the first occurrence of the detection. This information on the initial detection tab does not change as detection data are updated.

6. **Optional:** Navigate to Vulnerable Item Detections to view the Vulnerable Item Detection List.

(Optional) The Vulnerable Item Detection list is displayed. Each row on the Vulnerable Items Detections list represents a distinct detection. The columns display the same data as the VI record.
Detections are only opened or closed by data that is found by a scanner, they do not roll down from VIs. As Detections are imported, they are used to create VIs and update the states of VIs. If all detections are closed for a vulnerable item, that vulnerable item will be closed. On the VI record, the state is closed, and the substate is fixed.

When all VIs are closed for a VG, the VG is closed.

Starting with v10.3, vulnerable items set to 'Resolved' in your instance but not transitioned to 'Closed/Fixed' by the subsequent integration runs are reopened if they are detected during rescans.

For Rapid7 detections, an option is now available on the Rapid7 configuration page in your instance to reopen resolved VIs by age. If enabled, VIs set to 'Resolved' but then not transitioned to 'Closed/Fixed' by subsequent scans transition back to 'Open' after the number of days you enter.

For Qualys detections, if the scanner continues to find VIs that were set to 'Resolved' but then not transitioned to 'Closed/Fixed' by subsequent scans, these VIs move back to 'Open' when the last found date is later than the Resolved date.

What to do next
To view more data, including item and detection counts, you can Verify Vulnerability Response vulnerable item detection data on integration run (VINTRUN) records.

Verify Vulnerability Response vulnerable item detection data on integration run (VINTRUN) records
Starting with v10.0, from integration run records in your Now Platform® instance, you can locate third-party integration vulnerable item detection data based
on the date and time of scans. Verify the scan successfully completed, view the number (counts) of individual detections, as well as any vulnerable items (VIs) that are created or updated directly as a result of the scans.

**Before you begin**
Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

You may prefer to have the integration run information, either date and time of the scan, or the integration run record number (VINTRUN#) from the vulnerable item or detection records to help you locate specific records from the following lists.

**Procedure**
1. Choose one to continue.

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to Rapid7 Vulnerability Integration &gt; Administration &gt; Integrations</td>
<td>From the Rapid7 Integrations list, choose the integration you want to view the detection scan results for.</td>
</tr>
<tr>
<td>a. Rapid7 Data Warehouse:</td>
<td></td>
</tr>
<tr>
<td>• Vulnerable Item Integration</td>
<td></td>
</tr>
<tr>
<td>• Vulnerable Item Resolution Integration</td>
<td></td>
</tr>
<tr>
<td>b. Rapid7# Vulnerable Item Resolution Integration (InsightVM)</td>
<td></td>
</tr>
<tr>
<td>• Vulnerability integration</td>
<td></td>
</tr>
<tr>
<td>• Vulnerable Item Integration - API</td>
<td></td>
</tr>
</tbody>
</table>

| Navigate to Qualys > Qualys Vulnerability Integration > Primary Integrations | |
| From the Qualys Integrations list, choose Qualys Host Detection Integration. | |

2. On the bottom of the page that is displayed, select the Vulnerability Integration Runs tab.

3. Click an item in either the Number or Import Source columns to open a record.
The integration run record is displayed.

Rapid7 Integration run record

Qualys Integration run record

The integration run record is displayed. You can verify in the State field that the integration ran successfully. Starting with v10.0, new tabs, Items and Detections, are displayed. Information that was previously displayed on the top of the record is displayed on these tabs. Select the Items tab.
The Items tab displays the following information:

- Prior to v10, imported items on the integration record referred to total detections imported. Starting with v10.0, this Items tab displays the total number of VIs that are imported. You can see the total detections imported by adding the numbers listed on the Detections tab.

- The New items field displays the number of vulnerable items that are created from this integration run.

- The Imported items field displays the sum of all the fields in this section.

- Starting with v10.0, the Duplicate items field is no longer populated.

- The Updated items field displays the number of times vulnerable items are updated during this integration run. This value is not the number of unique vulnerable items that are updated. If, for example, a vulnerable item is updated two times during the integration run, it is counted two times and displayed as 2 updated items.

- The Unchanged items field displays vulnerable items found during the integration run that already exist in the database but were not updated, because none of the relevant field values had changed.

4. Select the Detections tab.

This tab is only displayed if the integration run has any detections. You can verify the total detections imported by adding the numbers listed.
The Detections tab displays the following information:

- The New detections field displays new detections that are created during this integration run.
- The Unchanged detections field displays detections found during the integration run that already exist in the database but were not updated, because none of the relevant field values had changed.
- The Updated detections field displays the number of times detections are updated during this integration run. This value is not the number of unique detections updated. If for example, a detection is updated twice as part of the integration run, it is counted two times and displayed as 2 updated detections.

**Note:** Detections that are not displayed in these counts are detections that are in a closed state (Fixed), because fixed records are used to update existing VIs. If you want more visibility to these detection records, you can display the closed VIs that are created when there is not an existing, matching VI in an open state. For more information about Vulnerabilities in the fixed state that you can enable in Setup Assistant for the Qualys integration, see Configuring Vulnerability Response using the Setup Assistant.

5. Click an item in either the Number or Import Source columns to open a record.

**View a solution**

View all solutions, solutions with highest-supersedence and solutions associated with vulnerable items to inform your remediation activities.
Before you begin
Role required:
- sn_vul.read, v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated), or
- sn_vul.remediation_owner

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task
As a Vulnerability Analyst or Remediation Owner, you can view different solution sets related to vulnerable items.

Note: Solution records are read-only except under Notes in the Internal notes section or user-created solutions.

Procedure
1. Navigate to Vulnerability Response > Solutions.
2. Choose a solution list.
   - Note: You can filter a solution list using wildcards for the Product name.
3. To review, click each item.
4. [Optional] Enter notes under the Notes tab and right-click Save to remain on the page or click Update to save and return to the Vulnerability Solutions list.
   - Note: If you only have the sn_vul.read role, you would not be able to perform this step.

Refresh Vulnerability Response vulnerable items
The Refresh associated vulnerable items related link is used to have vulnerable items inspected to see if there are any additional vulnerable items that belong to this group. Use it if an update is warranted outside the scheduled job.

Before you begin
Role required: sn_vul.vulnerability_write or, v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more
About this task
The Refresh associated vulnerable items related link is only editable on the vulnerable group form in the Open or Under Investigation state, using a filter group or where the filter type is condition. This inspection is done regardless of the status of the Automatically refresh vulnerable items check box.

Procedure
1. Navigate to Vulnerability > Vulnerabilities > Vulnerability Groups.
2. Open any vulnerable group in the Open or Under Investigation state.
3. Click the Refresh associated vulnerable items link.
   New vulnerable items appear under the Associated Vulnerable Items tab.

View the remediation target status of a Vulnerability Response vulnerable item
When a vulnerable item has nearly reached (or passed) its remediation target date, as defined by a remediation target rule, the vulnerable item record is updated with a status. This information can help the analyst proactively monitor upcoming remediation activities.

Before you begin
Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task
A scheduled job called Evaluate remediation targets runs once per day to compare the current date against the vulnerable item remediation date specified in the associated remediation target rule. When the current date falls within the number of days before the remediation is past due, a remediation status is added to the vulnerable item record.

Procedure
1. Navigate to Vulnerability > Vulnerable Items.
2. Click on the vulnerable item you want to review.
If the remediation date for the vulnerable item is within range of the conditions set in the remediation target rule, the **Remediation Target Status** tab is visible.

3. Click on the **Remediation Target Status** tab.
4. Click on the remediation target status record to review it.

**Note:** To view the number of Vulnerable Items that are Approaching Target, In-flight and Past Target, see Using the default Vulnerability Response dashboards.

**Related information**

Create or edit Vulnerability Response remediation target rules

**Triage vulnerabilities automatically**

Reviewing and triaging new vulnerabilities is necessary to ensure successful remediation. Transform vulnerability imports into remediation tasks with automated vulnerable item (VI) assignment, risk calculation, remediation targets, and VI grouping.

Starting with imported vulnerabilities, reconcile the assets not found in the CMDB, prioritize the results, translate that to remediation activities that are automatically assigned, orchestrate the remediation process, and confirm completion with a validation scan.

New vulnerable items are usually sorted into vulnerability groups upon import, based on vulnerability group rules. Sometimes, vulnerable items cannot be grouped or do not contain a recognized configuration item.

An overview of the vulnerability triage process:

- Log in to your Vulnerability Response instance.

- Validate that your rules (CI Lookup, Assignment) for vulnerable item are working as expected. For information on revising CI Lookup Rules, see CI Lookup Rules for identifying configuration items from Vulnerability Response third-party vulnerability integrations. For information on Assignment rules, see Vulnerability Response assignment rules overview.

  **Note:** Due to the large volume in data imports, care should be taken with automated vulnerable item assignment.

- Validate that your remediation targets are correct. See Vulnerability Response remediation target rules for information on how remediation target rules work and how to revise them.

- View ungrouped vulnerable items.
Looking at the ungrouped vulnerable items, consider revising your group rules and performing a rescan. See Create or edit Vulnerability Response group rules for more information.

Manually group the vulnerable items. Manually create a Vulnerability Response group for more information.

Revise risk scores for the vulnerable items in your groups. See Vulnerability Response calculators and vulnerability calculator rules for more information.

Close older vulnerable items not recently detected by your third-party integrations. See for more information.

- View and reclassify unmatched configuration items.
- Research what needs to be done for remediation.

This step can include:

- Determine what to deal with now and what you can defer. This determination is often based on risk score, affected systems, and patches with change windows.

  **Note:** Remediation target rules belong to vulnerable items. These rules are run when the vulnerable item is imported. These rules were created previously in the Setup Assistant.

- Refresh vulnerable items, if necessary, and View the remediation target status of a Vulnerability Response vulnerable item.

- Create a Change Request and assign the vulnerability group to an assignment group (IT Operations) for remediation.

  **Note:** If the vulnerability constitutes a security incident and the Security Incident Response plugin (com.snc.security_incident) is activated, you can create security incident records from the vulnerability group instead.

- After submitting one or more change requests, move the group state to Under Investigation.

**Bulk edit Vulnerability Response vulnerable items**

You can edit vulnerable items in bulk by selecting fields and running an asynchronous bulk edit job in the background.

**Before you begin**

Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response
application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task

Procedure

1. Navigate to **Vulnerability > Vulnerabilities > Vulnerable Items**.
2. Select the vulnerable items to edit by checking the box next to each item or creating a filter.
3. Click the **Bulk Edit** button.
4. Select and enter updates in the pop-up window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record Selection</td>
<td>Select which records to update. Choices are:</td>
</tr>
<tr>
<td></td>
<td>• Only Selected Vulnerable Items</td>
</tr>
<tr>
<td></td>
<td>• All Vulnerable Items that match filter</td>
</tr>
<tr>
<td></td>
<td>• Vulnerability Group</td>
</tr>
<tr>
<td></td>
<td>• Vulnerability entry</td>
</tr>
<tr>
<td>State</td>
<td>Select the change for the <strong>State</strong> in the vulnerable item. Choices are:</td>
</tr>
<tr>
<td></td>
<td>• Do Not Update</td>
</tr>
<tr>
<td></td>
<td>• Open</td>
</tr>
<tr>
<td></td>
<td>• Under Investigation</td>
</tr>
<tr>
<td></td>
<td>• Awaiting Implementation</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
|                       | • Deferred  
|                       | • Closed  
|                       | • Resolved  |
| Version 10.0:         | The solution targeted for remediating all the vulnerable items selected for bulk edit. Select the change for the Preferred Solution field in the vulnerable item. Choices are from a lookup list of available preferred solutions for the VIs selected. |
| Preferred Solution    |                                                                                                                                              |
| Note:                | • The Preferred Solution field must be correctly set on all VIs selected for bulk edit.  
|                       | • The set of available preferred solutions is an intersection of all potential solutions of the vulnerabilities across all selected VIs.  
|                       | • When selecting Record selection > Vulnerability Entry for bulk edit, all VIs for the vulnerability should be set to the selected preferred solution; however, this operation does not set the Preferred solution at the vulnerability entry level. Setting the Preferred solution at the vulnerability entry level would set the Preferred solution for all new VIs going forward. Bulk edit only modifies the current set of VIs.  
|                       | • Distinct vulnerabilities across the selection criteria is limited to 500. If there are more than 500, a warning message is displayed asking you to select VIs with different criteria for setting the Preferred solution.  
|                       | • The total number of solutions that can be shown in the lookup list is limited to 170. If there are more than 170, a warning message is shown. |
|                       |                                                                                                                                              |
| Version 10.3:         | Assignment group for the VI. Select manually, or using Assignment Recommendations if it is enabled.                                         |
| Assignment group      |                                                                                                                                              |
| Work notes            | Enter text describing the changes.                                                                                                          |

5. Click OK.
A bulk edit asynchronous job updates the selected records. The job number with a link is displayed on the Vulnerable Items page where you can view its status.

If you select Close, the Reason field is included. If you select Defer, once approved, the Close/defer reason and the Defer expiration fields are shown.

**Ungrouped Vulnerability Response vulnerable items**

Vulnerable items are automatically assigned to a group when they are imported. However, sometimes, if a vulnerable item (VI) is created manually, for example, the VI can become an orphan. The Ungrouped Vulnerable Items module lists those vulnerable items without a group.

ℹ️ **Note:** Integration automated processes do not create orphans, so this use case is expected to be small.

Being ungrouped occurs if a vulnerable item was created without a vulnerability, or there is no vulnerability group rule that assigns the VI to a group. In that case, review the list of ungrouped vulnerable items by navigating to **Vulnerability > Vulnerabilities > Ungrouped Vulnerable Items**.

After review, your choices are as follows:

- You can create a vulnerability group rule to catch any items that appear on this list.
- You can create a Vulnerability Response group and manually add items from this list to the group or define a condition that matches these items.
- You can open an existing group and add any relevant vulnerable items to the group as long as it is in the Open or Under Investigation state.

ℹ️ **Note:** Manually added vulnerable items are not automatically removed from vulnerability groups by vulnerability group rules or group conditions.

For more information on how vulnerability groups and group rules behave, see **Vulnerability Response groups and group rules overview**.

**View ungrouped Vulnerability Response vulnerable items**

Vulnerable items that are not assigned to a group are placed in a viewable list.

**Before you begin**

Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see
Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure
1. Navigate to Vulnerability > Vulnerabilities > Ungrouped Vulnerable Items.
2. Review the vulnerable items in the list.
3. Click each vulnerable item to view and determine how to include in a group.

Manually add a Vulnerability Response vulnerable item to a vulnerability group
If a vulnerable item is left ungrouped, you can add it to a vulnerability group for remediation.

Before you begin
Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure
1. Record the vulnerable number.
3. Choose a vulnerability group for your vulnerable item.
4. Click Edit in the Associated Vulnerable Item related list.
5. Enter the vulnerable item number in the search box for the collection.
6. Select the vulnerable item from the collection and add to the list.
7. Click Save.

Unmatched CIs
Configuration items (CIs) are automatically matched to CIs in the Configuration Management Database (CMDB) when they are imported. By default, the Security Operations > CMDB > Discovered Items module lists those configuration items without a match.

If you think an unmatched CI belongs to an existing class in the CMDB, review your CI lookup rules. Otherwise, consider reclassifying the configuration item.
Note: The default filter for this list is set to Unmatched. You can view all discovered items from an import by removing the filter.

View and reclassify unmatched configuration items

Configuration items (CIs) that are not found in the Configuration Management Database (CMDB) are placed in a viewable list of discovered items. This list offers a convenient way to reclassify unmatched CIs.

Before you begin
Role required:
- `sn_vul.read` (minimum to view Unmatched CIs)
- itil or asset (to reclassify)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task
As a Vulnerability Analyst you can view unmatched CIs.

The reclassify action is available only on `sn_sec_cmn_unmatched_ci` class CIs, when you have either the itil or asset roles. Once a CI has been reclassified, it cannot be reclassified using the UI. You can reclassify, from the CI form or the CI list view, by changing the class value.

Procedure

2. To review, click each item.
3. To make corrections to the information in the Discovered Item form fields, edit in this page, and right-click Save. Any data added to or left in these fields is transferred to the resulting Configuration Item when it is reclassified.
4. If everything looks correct, click Reclassify.
5. From the choice list, select a Class Name and click Submit. The Discovered Item Class is updated, the State field is changed to Reclassified, and all data is in the CMDB.
Change Management tasks for Vulnerability Response

From vulnerability groups (VG), create change requests, associate VGs to existing change requests, or split vulnerability groups into new groups with subsets of vulnerable items (VI).

Create and manage change requests directly from a vulnerability group if a manual and controlled process of any kind is required for modification or removal of supported configuration items (CIs) in your CMDB. Creating and managing change requests directly from a vulnerability group record helps you investigate and resolve vulnerabilities quickly.

See Change management for Vulnerability Response for an overview of how change management works with the Vulnerability Response application and the system requirements.

Refer to the following topics for how to create change requests, associate vulnerability groups to existing change requests, and split vulnerability groups. See State synchronization between change requests and vulnerability groups for information about how state fields on change requests (CHG) automatically resolve vulnerability groups.

Create a change request from a vulnerability group

As an IT remediation owner, create a change request (CHG) directly from a vulnerability group (VG) for all the vulnerable items in the group. Create a change request with pre-populated information that includes the preferred solution to expedite your investigation for vulnerabilities that require manual intervention.

Before you begin

You can create, approve, implement, review, and close change requests directly from a vulnerability group. You can create three types of change requests with pre-populated information from a vulnerability group:

- **Standard.** A pre-authorized change that is low risk, relatively common and follows a specified procedure or work instruction.
- **Normal.** Normal change requests follow a prescriptive process which requires two levels of approval before being implemented, reviewed, and closed.
- **Emergency.** A change to resolve a major incident.

The following image illustrates the basic flow for creating a change request from a VG. The detailed steps for this flow follow the image.
**Note:** Key points about creating new change requests:

- You can create new change requests for any vulnerability group in a state other than **Closed**.
- Verify that you have an approver for change requests other than Standard (pre-approved) that you create or associate to a VG. This expedites moving the VG to resolution. For more information on adding users, see Add users to the Vulnerability Response group.
- Before a vulnerability group can be resolved, all tasks on at least one CHG that is associated with the VG must be completed so that the change request can be implemented and moved to the **Review** state.
Role required for creating a change request: Any user with the itil role. The sn_vul.remediation_owner role is also automatically assigned when the itil role is assigned to a user.

Role required for approval of change requests: users with itil, admin, sn_change_write, change_manager roles.

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure

1. To create a complete change request from an existing vulnerability group record, navigate to Vulnerability Response > Vulnerabilities > Assigned to My Groups. The list of Vulnerability Groups assigned to your assignment group is displayed.

2. Optional: Navigate to Vulnerability Response > Remediation Overview to view the Remediation Overview dashboard and locate a VG assigned to you or your assignment group. Alternatively, skip to step 4.

3. In the Number column, click a vulnerability group to open the record and view the details.
The vulnerability group record is displayed.

4. With the VG record displayed that you want to create the change request for, in the upper right of the record, click **Create Change**.

The Create change request form is displayed as shown in the following figure.

5. Fill in the fields.

   a. From the choice list of the Applies to field, choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All active vulnerable items in</td>
<td>If selected, all active vulnerable items from this vulnerability group with a state other than closed are added to the change request.</td>
</tr>
<tr>
<td>this group</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>added automatically to the change request after you click <strong>Create Change</strong>.</td>
<td></td>
</tr>
<tr>
<td>All vulnerable items in this group matching a set of conditions</td>
<td>If selected, the Condition builder is displayed as shown in the second figure below. Enter filter criteria to identify the vulnerable items that you want for the new change request. An example of a filter might include only vulnerable items that match specific search criteria: <strong>State is Open</strong> and <strong>Risk score greater than 75</strong>. After you enter your conditions, a message is displayed with the number of VIs that match your criteria (10). A link (<a href="#">Preview matching items</a>) to preview the matching items is displayed. If no items match your filter conditions, a message is displayed below the Condition builder that instructs you to adjust your filter. After you click <strong>Create Change</strong>, all vulnerable items that match this condition filter are moved a new vulnerability group. This change request is associated with the new vulnerability group.</td>
</tr>
</tbody>
</table>
b. **Optional:** If displayed on the form, click the **Preview matching items** link for a list of the VIs that match your filter criteria. The Vulnerability Group List preview is displayed. You can select items on this preview list and perform UI actions on them, however, these actions are also performed on the VG.
delete a VI from the preview list, that VI is also deleted from the VG.

c. After you complete your preview, close the browser window to return the change request form.

d. For the Add CIs to CR check box, choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check box selected</td>
<td>Default is selected. If the check box is selected, any configuration items (CI) that belong to active vulnerable items in this vulnerability group are added to this change request. The VG automatically moves to the Awaiting Implementation state.</td>
</tr>
<tr>
<td>Check box cleared</td>
<td>Clear the check box if you do not want the CIs from the active vulnerable items from this vulnerability group added to the new change request. When disabled, the state of the change request is not synched to the VG, and the VG remains in its current state.</td>
</tr>
</tbody>
</table>
e. From the choice list for the Change type field, choose one to continue.

<table>
<thead>
<tr>
<th>Change type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency</td>
<td>A change to resolve a major incident.</td>
</tr>
<tr>
<td>Normal</td>
<td>A change type that is used to implement any change to a service that is not a standard or emergency change.</td>
</tr>
<tr>
<td>Standard</td>
<td>A pre-authorized, low-risk change request that is frequently implemented. Approved standard change requests can be predefined in a catalog of templates to make accessing and requesting a standard change more efficient. If selected, two fields are displayed as shown in the following figure. Select one from each choice list to fill in these fields:</td>
</tr>
</tbody>
</table>

- **Change category**: Select a category for the change from your existing catalog, for example, Hardware, Server Standard Changes, Software. In this example, Patching Standard Changes is selected.

- **Change template**: Select one available template for change requests with pre-defined supporting tasks from your catalog. In this example, the Microsoft Monthly Patching Cycle template is selected.

For more information on ITSM change request categories, templates, and change types, see Change types.

The feature automatically reads the types of change requests that you set up in your catalog in ITSM Change Management. For example, if you change the name for your Standard change requests in ITSM from
Standard to Pre-approved, your new name is automatically displayed in the Change type choice list on the Create change request form as shown in the following figure.

The fields in the Change Request Preview section of the form are pre-populated with information from the VG. If required, these field values can be edited. For example, review the values in the fields in the following figure:

- **Planned end date**: This date (2019-10-10) is the same value that is displayed in the Remediation target date field of the VG. This value is derived from the earliest remediation target date from the vulnerable items that belong to the VG. If you are creating a change request for a critical issue that requires an earlier remediation date, you may prefer to edit this value and the value in the Priority field.

- **Justification**: This field displays the number of CIs that are added to the CHG. If you want to add additional information, you may prefer to edit this text. For example, you may prefer to add a note in this field about the filter you used to create the new VG, for example, Risk score greater than 75. This text can help you locate your new change request and vulnerability group.

- **Implementation plan**: This field displays the preferred solution for the vulnerability.

- **Assignment group** and **Assigned to**: Edit these fields to change the assignment group or reassign this change request to a user in one of your assignment groups.
6. Continue to preview and edit the fields as required.

7. To save your changes and remain on this page, in the gray banner at the top of the form, right-click and select Insert and Stay.

8. After you complete your edits, choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Change</td>
<td>Your change request is created and the new change request is displayed in the New state. At the top, mes-</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Cancel</td>
<td>The change request is not created and the VG is displayed.</td>
</tr>
</tbody>
</table>

Option

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sages are displayed that indicate the change request is successfully created with the number of vulnerable items that were added as shown in the following figure.</td>
</tr>
</tbody>
</table>

If state synchronization is enabled and the VG is not already in Under Investigation, the VG is automatically moved to Under Investigation and a work note is posted.

Note:

For a vulnerability group in the Open state with the Assignment group and Assigned to fields unassigned (empty), the current logged-on user is automatically assigned to the VG after you click Create Change. In addition, the Add CIs to CR check box must be selected. At the top of the VG, a blue confirmation message is displayed that indicates this assignment as shown in the following figure.

What to do next

Monitor the change request and the change tasks to verify that they are completed and the change request is implemented. After this CHG is implemented and moved to the Review state, if state synchronization is enabled, the VG automatically moves to Resolved. For more information on state synchronization, see State synchronization between change requests and vulnerability groups.
Associate a vulnerability group to an existing change request

As an IT remediation owner, avoid creating duplicate change requests (CHG) as you work to resolve your vulnerability groups by associating a vulnerability group (VG) to a change request that is already available in your instance.

Before you begin
As a remediation owner, you can associate vulnerability groups that are assigned to you or your assignment group to existing change requests directly from the vulnerability group records. The following image illustrates the basic flow for associating a change request to an existing VG. The detailed steps for this flow follow the image.

1. Associate (Add) the vulnerability group to an existing change request.

2. Optionally add all the configuration items from active vulnerable items from the vulnerability group to the change request.

3. Monitor the life cycle of the change request.

4. When the change request is implemented and in review, the vulnerability group is automatically resolved.
Note: You can associate an existing change request to a VG in any state (Open, Under Investigation, Awaiting Implementation, Closed, and Deferred). When you associate a change request to an existing VG, only the active VIs are added to the change request.

Before you begin, to avoid creating duplicate change requests, you might prefer to view any existing change requests already associated with a VG. To easily track the number of change requests that are related to a specific VG, refer to the CR count column on the Vulnerability Groups list. If not displayed, click the settings icon (⚙️). Move the CR count column from Available to Selected and click OK.

To automatically populate the new column, for customers with existing data in this table, run the scheduled job: Populate new CR Count Column.

Role required: Any user with the itil role. The sn_vul.remediation_owner role is also assigned automatically to a user when the itil role is assigned.

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure

1. To associate a vulnerability group to an existing change request, navigate to Vulnerabilities > Assigned to My Groups.

2. Locate the vulnerability group you are working with.

3. Optional: Navigate to Vulnerability Response > Remediation Overview to view the Remediation Overview dashboard and locate a VG assigned to you or your assignment group.
4. In the Number column, click a VG record to open it. The VG record is displayed.

5. With the open record displayed, if not already displayed, scroll to the Change Requests related list and select it. Any change requests associated with the VG are displayed along with the Add button. In the following figure, there are no change requests already associated with this VG.

6. To associate the VG with an existing CHG, click Add. The Add Existing Change Request to Vulnerability Group form is displayed.
7. In the form, click the search icon. A list view of existing change requests is displayed in a new window as shown in the following figure.

8. Select an item from the displayed list, or, alternatively, click the filter (🔍) and enter conditions to limit your search results.

9. For the Add CIs to CR check box, choose one to continue.

**Note:** This check box is displayed only for existing change requests in the **New** state.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check box selected</td>
<td>Default is selected. If the check box is selected, any configuration items (CI) that belong to active vulnerable items in this vulnerability group are added to this change request. When selected, the state of the change request is synched to the VG. For more information, see <em>State synchronization between change requests and vulnerability groups</em>.</td>
</tr>
<tr>
<td>Check box cleared</td>
<td>Clear the check box if you do not want the CIs from the active vulnerable items from this vulnerability group added to the new change request. When disabled, the state of the change request is not synched to the VG.</td>
</tr>
</tbody>
</table>
10. With the change request number you want displayed in the Search for Change Request field, click **Submit**.

The VG is displayed. At the top of the record, the blue confirmation message is displayed indicating that the change request you selected is successfully associated to the VG.
For a VG in the open state with the Assignment group and Assigned to fields unassigned (empty), the current logged-on user is automatically assigned to the VG after you click Add. In addition, the Add CIs to CR check box must be selected. At the top of the VG, a blue confirmation message is displayed that indicates this assignment, as shown in the following figure.

What to do next
Review the VG record. In the Change Request column on the Change Requests related list, click link for the new CHG to view CR record. On the open CHG record, you can monitor the state of the change request. The affected configuration items (CIs) and the vulnerability groups are displayed on the Affected CIs and Vulnerability Groups related lists.

Split a vulnerability group
As an IT remediation owner, from an existing vulnerability group (VG), identify a subset of vulnerable items (VI) that you want to move to a new vulnerability group.

Before you begin
You can split existing vulnerability groups with more than one vulnerable item that are in the Open, Under Investigation, or Awaiting Implementation states. By creating a new VG with vulnerable items that match specific criteria, you can work with a specific group of vulnerable items without impacting the original vulnerability group.

When you specify the conditions for the vulnerable items that you want to move to a new vulnerability group with the condition builder, only the active VIs that match your criteria are moved to the new group.

You are not required to create change requests (CHG) when you split a VG. You have the option to split a VG at the same time you create a change request, or, you can split a VG without creating a change request. The following image illustrates the basic flow for splitting a vulnerability group. The detailed steps for this flow follow the image.
For a vulnerability group in the following states that has more than one vulnerable item:

1. Identify a subset of vulnerable items and create a new vulnerability group for them.

2. Optionally create a new change request for a new group, or associate it with an existing change request.

3. Monitor the life cycle of the change request.

4. When the change request is implemented and in review, the vulnerability group is automatically resolved.

Note:

Use cases for splitting VIs from existing VGs into new groups might include the following examples:

- When you want to create a change request or change requests for a split group.
- When you reassign a split group to another user in your assignment group.
- When you request a deferral or exception for a split group because you know that some vulnerabilities on specific configuration items (CI) cannot be remediated in a given time frame.
Role required for splitting a VG: Any user with the itil role. The sn_vul.remediation_owner role is also automatically assigned when the itil role is assigned to a user.

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure

1. Navigate to **Vulnerabilities > Assigned to My Groups**. The Vulnerability Groups list is displayed.

2. In the Number column, click a vulnerability group. The vulnerability group record is displayed.

3. On the upper right of the VG, click **Split Group**.
Note: If the Split Group button is not displayed in the upper right on the VG record, verify that the VG has more than one vulnerable item.

The Split vulnerability group form is displayed.

4. With the condition filter displayed, specify the conditions for the vulnerable items that you want to move to a new vulnerability group. For example, you may prefer to filter out only vulnerable items that match the following conditions:

- In Open states.
- Risk scores greater than 80.
- Configuration items that contain 'WINSV'.
- Located in San Diego.

As shown in the following figure, if vulnerable items match your filter after you enter the conditions, a message is displayed with the number vulnerable items (5) that match.
Note: If a message is displayed that no vulnerable items match your filter, adjust the conditions so at least one vulnerable item matches your filter criteria.

5. Optional: Adjust the filter as required.

6. Optional: To help you identify the new VG after it is created, you may prefer to update the Short description field. If edited, use the short description field as search criteria for the new VG to help you locate it after it is created. In the preceding image in the short description field, the text **LOCATED IN SAN DIEGO** is displayed.

7. Optional: To preview details about the vulnerable items that match your filter criteria, follow these steps before you click **Split Group** to create the new VG. These details include existing change requests that are already associated with this subset and VGs with these vulnerable items. Viewing this information on the preview may prevent you from creating duplicate VGs.

   a. In the blue confirmation message on the Split vulnerability group form shown in the preceding figure, click **Preview matching items**. The Vulnerability Group Items list is displayed in a new window in your browser with a list of vulnerable items that match your conditions.
b. In the Number column, click an item to open the record.

c. In the record that is displayed, to the right of the vulnerability group or the vulnerability item fields, click the information icon for the vulnerability item(s) to view the records.

d. On the dialog that is displayed, click **Open Record**. Information about the remediation target date is displayed. In the Related Lists section, click a related list to view the information about the VI that includes the following details:

- **Vulnerability Groups**: A list of the VGs that have this VI.
- **Affecting Tasks**: Any existing change requests (**Affecting Tasks**) that are associated with this VI.
- **Impacted Services**: The affected CI services.
- **Remediation Target Status**: The current progress on remediation.

8. When you are ready to create the new VG with the VI(s) that meet your conditions, close the preview window to return to the split vulnerability group form and, at the top of the form, click **Split Group**.
Note:

For under 200 VIs, the split operation is done synchronously.

For over 200 VIs, the split operation is done asynchronously in the background, and it may take a few seconds for the VIs to appear in the new group.

A confirmation message is displayed that shows all the active VIs (5) that are moved to the new group. The new vulnerability group number is also displayed. If not already in Under Investigation, the VG is moved to the Under Investigation state. Check the Short description field for the text you entered for the new VG in the split vulnerability form (LOCATED IN SAN DIEGO).

Roll-up calculations on the new group are performed to calculate its new Risk Score, Remediation Target Date, and other field values.

The vulnerable items, preferred solutions, and change requests are displayed on the Related Lists on the bottom of the record. Process and monitor this new vulnerability group as you would with any vulnerability group record.

9. Optional: Scroll to the Notes related list and click to select it.
Confirm that the number of vulnerable items from the original vulnerability group (VUL0004437) have been moved to the new group.
10. Optional: On the new VG, to select and split the VIs from the Vulnerable items related list once again, scroll to the bottom of the vulnerability group record, and, with the VIs you want to move selected in the Vulnerable item column of the Vulnerable Items related list, from the Actions on selected rows choice list, select **Split Group**.

The Split Vulnerability group form is displayed.

11. To split the group again and move the selected items to a new group, click **Split Group**.
The selected VIs are moved to another vulnerability group, the confirmation message is displayed, and the new group is displayed. You can perform this UI split action from the Actions on selected rows choice list on any vulnerability group record. This UI action is useful if you know exactly which vulnerable item(s) you want to move into a new vulnerability group.

12. Choose one to continue your investigation or remediation.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Security Incident</td>
<td>Create a security incident.</td>
</tr>
<tr>
<td>Create Change</td>
<td>Create a change request for this vulnerability group.</td>
</tr>
<tr>
<td>Split Group</td>
<td>If the new group has more than one VI, split this vulnerability group again to create another subset of vulnerable items.</td>
</tr>
<tr>
<td>Awaiting Implementation</td>
<td>If displayed, move the group from Under Investigation to the Awaiting Implementation state.</td>
</tr>
</tbody>
</table>
| Close/Defer            | Close or defer the vulnerability group. A confirmation dialog is displayed with the following required fields:  
  • State  
  • Reason  
  • Additional information  
  Fill in the fields to close or defer the group and click Submit. |
<p>| Delete                 | Delete this vulnerability group.                                            |
| State                  | Move the record to another state displayed in the choice list and click Update to save your changes to the record. |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong></td>
<td>You can manually move the new VG through the states of its life cycle. However, if state synchronization is enabled, and the system registers that a change request associated with the VG has changed its state, or you add a CHG or remove it from the VG, state synchronization potentially can override your manual intervention. For more information, see State synchronization between change requests and vulnerability groups.</td>
</tr>
<tr>
<td>Assignment group</td>
<td>Reassign the VG to an assignment group and click <strong>Update</strong> to save your changes to the record.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>Assign the VG to yourself or to a specific user in another assignment group and click <strong>Update</strong> to save your changes to the record.</td>
</tr>
</tbody>
</table>

**What to do next**

Monitor the state of the new VG to expedite its resolution.

**State synchronization between change requests and vulnerability groups**

There is a synchronized relationship between the State fields of vulnerability groups (VG) and the State fields of change requests (CHG) in the Vulnerability Response product. As a change request moves through its life cycle, it also moves the state of any related vulnerability groups automatically.

**Overview**

State synchronization is enabled by a system property (sn_vul.cr_state_synch) by default in your instance when you download the Vulnerability Response product from the ServiceNow Store.

When state synchronization is enabled, the CHG State field changes the VG State field automatically in the following cases:
• When a new CHG is created for a VG, if it is not in Awaiting Implementation, the VG state moves forward to Awaiting Implementation.

• When an existing CHG is associated to a VG, if it is not in Awaiting Implementation, the VG state moves forward to Awaiting Implementation.

• After the tasks on a CHG are completed (Implemented), and the CHG is moved to the Review state, the VG moves forward to Resolved.

For more information and examples of state synchronization, see the following sections.

⚠️ Note: You can still manually move CHGs and VGs through the states of their life cycles on their respective records with state synchronization enabled, but when the system registers that a CHG has changed its state, or you add a CHG or remove it from a VG, state synchronization potentially can override your manual intervention. However, change requests states do not automatically move the VG from the Closed or Deferred states.

**Forward state synchronization**

The following image illustrates how CHG states automatically move VG states in a forward life cycle, that is, from Open to Resolved.
You can create new change requests for any vulnerability group in a state other than Closed. State synchronization automatically moves the VG bi-directionally through the Open, Under Investigation, Awaiting Implementation, and Resolved states. This movement is based on certain values of the state field on the change request. State synchronization between the change request and the vulnerability group is invoked automatically unless the check box (Add CIs to CR) is displayed on a form and you choose to clear the check box.

The VG does not move forward to Resolved when a CHG is in its open states. Any CHG in states prior to Review in its life cycle such as, New, Assess, Authorize, Scheduled or Implement as shown in the preceding figure are considered open states for the CHG. Open states do not move the state field on the VG, because investigations or tasks on the CHG are not completed. State synchronization is invoked when a CHG is created for, or associated to, the VG, or the state of an existing relationship changes on the CHG. The completed CHG states are Review and successfully Closed. When a CHG is closed successfully, its closed codes are: Successful, or Successful with issues, in which case the VG moves forward to Resolved.
Backward state synchronization

As a CHG is processed during its life cycle, it may be canceled at some point. In this case, if the CHG is Cancelled, or Closed (with a close code of Unsuccessful), the VG automatically moves back to Under Investigation. The VG moves back to Under Investigation, because there is no active plan to remediate the vulnerability.

If a VG is in a Resolved state, and you create a new CHG or associate it to an existing CHG in one of the initial open states, the VG automatically transitions back to Awaiting Implementation. The VG moves back to this state, because more work is now assigned to the CHG.

VGs with more than one CHG

If a VG in Awaiting Implementation has more than one CHG associated with it, state synchronization is based on the status of the CHG in the earliest state of its life cycle. For example, a VG has four CHGs associated with it, CHG1, CHG2, CHG3, and CHG4 as shown in the following table.

<table>
<thead>
<tr>
<th>CHG number</th>
<th>CHG state</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Implement</td>
</tr>
<tr>
<td>2</td>
<td>Canceled</td>
</tr>
<tr>
<td>3</td>
<td>Closed (close code of Unsuccessful)</td>
</tr>
<tr>
<td>4</td>
<td>Closed (close code Successful)</td>
</tr>
</tbody>
</table>

State synchronization between the CHG and the VG in this case is based on CHG1, which is in the earliest state of the four CHGs, (Implement). In this case, the VG remains in Awaiting Implementation.

In another example, if a VG is in the Resolved state and has an existing CHG that has been implemented and is in the Review state, and a new CHG is created, the VG moves back from Resolved to Awaiting Implementation. State synchronization is based on the CHG in the New state, which is the CHG in the earliest state.

<table>
<thead>
<tr>
<th>CHG number</th>
<th>CHG state</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Review</td>
</tr>
<tr>
<td>2</td>
<td>New</td>
</tr>
</tbody>
</table>

Additionally, when VGs have more than one CHG, the state of the VG transitions automatically in the following cases:
• When a CHG moves forward to Review, if all other CHGs associated with the VG are in Review or Closed states (with a successful close code), the VG automatically transitions to Resolved. Any other related CHGs that are canceled or closed unsuccessfully are ignored.

• When a CHG moves to Cancelled or Closed (close code of Unsuccessful), if all other CHGs associated with the VG are in the same state, then the VG automatically transitions back to Under Investigation.

For more information about vulnerability group states and what you can do in each state, see Vulnerability Response group and vulnerable item states.

Software exposure assessment using Software Asset Management (SAM)

Use the ServiceNow® Exposure Assessment application to determine your total installed software count for a specific software package on your assets. When used with the ServiceNow® ITSM Software Asset Management application, evaluate your exposure, create vulnerable items, and manage remediation for the vulnerable software you discover.

Overview

Determine your exposure to vulnerable software by providing the vulnerable software information (publisher, product, edition and version) without using the Common Vulnerabilities and Exposures (CVE) database. Assess cases of a zero-day (current day) vulnerabilities to software for the following cases:

• When products do not yet have CVE data.

• When there is a lag between the time a vulnerability becomes publicly known and the CVE data with the vulnerability is updated in the NVD.

• When you learn about the vulnerability in-between the scheduled scans of your vulnerability scanner.

With the Exposure Assessment application, if you know the publisher and product for the vulnerable software, using the records that list the installed software in your network created by the SAM application, you can assess your exposure to potentially malicious software packages on-demand.

Knowing the scale of your exposure to this type of vulnerability permits you to proactively respond by implementing a red alert and uninstalling the software, or informing your security operations center (SOC) to look for a specific patch. You can create vulnerable items and assign tasks to the remediation specialist for further investigation remediation. View a vulnerability group (VG) list to verify that the vulnerable items you want are created and associated correctly to the VG.
The Exposure Assessment application for the Vulnerability Response application is compatible with the New York v10.0 and Orlando family releases.

**Related information**

Configure Exposure Assessment
Assess your exposure to vulnerable software

**Assess your exposure to vulnerable software**

You can provide the publisher and product information in the Exposure Assessment module to assess your zero-day (current day) exposure of your assets to vulnerable software using the ITSM Software Asset Management application.

**Before you begin**

For more information on system requirements, see Configure Exposure Assessment.

**Use case**

View the software exposure assessment module and create and edit exposure assessment records on-demand for vulnerable software in your Now Platform® instance.

You manage the vulnerability response activities for a large operation responsible for many assets. The Security Operations Center (SOC) in your operation contacts you about a version of software that they have learned is vulnerable. You discover that a scan of your assets just recently completed and did not find this vulnerability. The SOC team learned about this vulnerability from a reliable source outside of the National Vulnerability Database (NVD), Common Weakness Enumeration (CWE), or the other third-party libraries in your instance, and you are concerned that your vulnerability scanner has not yet added the plugin for it.

You are confident that the data for this vulnerability will be updated in the NVD and imported soon so that your scanner can catch this vulnerability in the next scan, but because you are concerned about the scope of your potential exposure, you want to determine today if you have assets in your network that have this software installed.

Role required: vulnerability admin (sn_vulnerability_write)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.
Have the following information available about the vulnerable software you want to assess:

- Publisher
- Version
- Product
- Edition

**Procedure**

1. To create a new exposure assessment, navigate to **Vulnerability Scanning > Exposure Assessment**. The Exposure Assessments list is displayed.

2. Click **New**. The Exposure Assessment form is displayed.

3. Fill out the form.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publisher</td>
<td>Name of the software publisher.</td>
</tr>
<tr>
<td>(Optional) Version</td>
<td>Enter the version number to help you narrow the search on your assets.</td>
</tr>
<tr>
<td>Product</td>
<td>Name of the software product.</td>
</tr>
<tr>
<td>(Optional) Edition</td>
<td>Enter the edition to help you narrow the search on your assets.</td>
</tr>
<tr>
<td>CI filter</td>
<td>Use the choice lists for the Configuration Item (CI) filter to limit your search to specific configuration items (assets). For example, you can submit a query for only active assets that may have this software installed: Operational status is Operational</td>
</tr>
</tbody>
</table>

4. Click **Show Exposure**.

The Exposure Assessment record with your discovery model and the software installation count on your assets as of the specific date is displayed.
5. Choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Exposure</td>
<td>Add additional CI filter conditions and click <strong>Show Exposure</strong> to further refine your search results.</td>
</tr>
<tr>
<td>Create Vulnerable Items</td>
<td>Create vulnerable items for the configuration items from your search results. If vulnerable items are successfully created, a vulnerability group is created for all the vulnerable items and displayed on the exposure assessment record.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete this record and return to the Exposure Assessments list. A confirmation dialog is displayed.</td>
</tr>
</tbody>
</table>

6. **Optional:** Create vulnerable item for your search result. Alternatively, revise your filter conditions and further refine your search results.

*Note:* After you create vulnerable items, you cannot alter the search criteria for this exposure record.

7. To create vulnerable items, follow these steps:

a. **Click Create Vulnerable Items.**
   The Create Vulnerable Items dialog is displayed.

b. **Fill in the fields.**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using</td>
<td>Form the choice list, choose one to continue.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Existing vulnerability.</strong> To the right of the Vulnerability field, click the search icon. In the list that is displayed, select the CVE-ID, or enter search criteria to locate the existing CVE-ID, for example, CVE 2018-9120.</td>
</tr>
<tr>
<td></td>
<td><em>Note:</em> This can be a CVE-ID from a vulnerability database other than the NVD.</td>
</tr>
<tr>
<td></td>
<td>• <strong>New vulnerability.</strong> Enter the CVE-ID for your new vulnerability in xxxx-xxxx, xxxx-xxxxx, or xxxx-xxxxxxx format.</td>
</tr>
<tr>
<td>Vulnerability summary (for new vulnerability only)</td>
<td>Enter a summary for the new vulnerability, for example, An attacker can execute script on an unsuspecting user's browser.</td>
</tr>
</tbody>
</table>

The following images show examples of the completed form for an existing vulnerability and a new vulnerability.
c. Click **Create Vulnerable items**.
The Exposure Assessment record is displayed with a status message that indicates vulnerable items are being created.

d. After a few seconds, at the top of the form, right-click in the gray banner to reload the page.
The new vulnerable items are displayed as shown in the following figure on the Assessed Vulnerable Items tab (531). The new vulnerability group created for these vulnerable items is displayed on the Vulnerability Groups tab (1).
Note: For this example, a vulnerability group is created according to the group rules and conditions from the vulnerability group rule called, Vulnerability. This group rule is the default vulnerability group rule that is installed with the Vulnerability Response product in your Now Platform® instance. In this example, the conditions of this group rule placed all the vulnerable items into a single vulnerability group. If you prefer to create more than one vulnerability group for the vulnerable items that match your exposure assessment search results, you may prefer to set up additional vulnerability group rules. Creating more vulnerability groups may help you prevent creating vulnerability groups with large numbers of vulnerable items. For more information about vulnerability group rules, see Vulnerability Response groups and group rules overview and Create or edit Vulnerability Response group rules.

8. Choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Groups</td>
<td>With the Vulnerability Groups tab selected, in the number column, click to open the record and review and assign the vulnerability group for</td>
</tr>
</tbody>
</table>
**Option** | **Description**
--- | ---
remediation. For more information on assignment groups, see .

**Assessed Vulnerability Items** | With the Assessed Vulnerable Items tab selected, in the Vulnerable item column, click to open the records and review and assign individual vulnerable items.

**Delete** | Delete the exposure assessment record. A confirmation dialog is displayed.

**Note:** If you delete the exposure record after you create vulnerability items, any vulnerable items that you create for this record that are not related to another exposure record are automatically moved to the Closed state. The reason for closure is Cancelled.

---

**Confirmation**

Deleting this record results in the following actions:

- Related exposed discovery models are deleted.
- All assessed vulnerable items are closed.

Are you sure you want to delete this record?

- [Cancel](#)
- [Delete](#)

---

**What to do next**

Respond to any zero-day (current day) threats based on your exposure assessment. For more information about vulnerability groups and change management for Vulnerability Response, see [Vulnerability Response groups and group rules overview](#) and [Change management for Vulnerability Response](#).

---

**Vulnerability Response remediation progress monitoring**

Monitoring vulnerability remediation involves viewing trends, managing risk, and monitoring assignment groups. You can review high risk issues, assignment group workloads, deferrals and, reoccurring vulnerabilities. Vulnerability Response offers tools, reports, and procedures to make that process more productive and efficient.
**Vulnerability Response remediation process**

Most remediation is done from the **Vulnerability Group** (VG). From the groups in the Under Investigation state, you can perform several tasks.

- Create change requests.
- Add work notes and descriptions of vulnerabilities within the group.
- Defer the group and the vulnerable items in it until a later date.
- Close the group.
- Track new regulatory compliance obligations, which are usually time sensitive.

An overview of the process:

- Log in to your Vulnerability Response instance.
- Review your dashboards and reports to locate problem areas. For example, view dashboards that show **Vulnerability Group** aging by states or high risk vulnerable items (VIs) past their remediation target date.

⚠️ **Note:**

Vulnerability Response, the Qualys Vulnerability Integration, and, starting with v12.1, the Tenable Vulnerability Integration, ship with overviews and dashboards. These overviews and dashboards include the Vulnerability Management dashboard which can help you monitor areas of concern. See **Using the default Vulnerability Response dashboards** for more information.

When the Performance Analytics for Vulnerability Response plugin (com.snc.vulnerability.analytics) is activated, users with certain roles can view data of interest to the Chief Information Security Officer (CISO).

A large number of vulnerable items within your deployment can affect the performance of your dashboards. Consider using filter conditions to limit the number of vulnerable items reported.

Version 13.0: To limit the amount of data gathered for reports or related lists, see **Define service classifications for Vulnerability Response reporting and related lists**.

- Review the state of **Vulnerability Groups**, in order of risk.
- Revise the prioritization for the groups by adjusting your risk score calculators if the risk score is not being calculated correctly or deferring VIs or VGs, as needed. See **Vulnerability Response calculators and vulnerability calculator rules** or **Defer a vulnerability group** for more information on these options.
- Review deferred vulnerable items about to reopen for further action.
- Review feedback from IT Operations.
Once you are notified that a change request is resolved, wait for the next scan. Scans are triggered automatically by the third-party import schedule configured in the Setup Assistant.

- After a scan, if the state is Fixed, vulnerable items are automatically closed during import. The group closes when all vulnerable items in the group are fixed.
- After the scan, if the state is not Fixed, the VI is automatically moved back to Under Investigation.
- Vulnerable items set to 'Resolved' in your instance but not transitioned to 'Closed/Fixed' by the third party integration runs are reopened if they are detected during rescans.
  
  For Qualys detections, if the scanner continues to find VIs that were set to 'Resolved' but then not transitioned to 'Closed/Fixed' by subsequent scans, these VIs move back to 'Open' when the last found date is later than the Resolved date.

  For Rapid7 detections, an option is now available on the Rapid7 configuration page in your instance to reopen resolved VIs by age. If enabled, VIs set to 'Resolved' but then not transitioned to 'Closed/Fixed' by subsequent scans transition back to 'Open' after the number of days that you enter.

**Vulnerability Solution Management Deployment Progress**

Comprehensive deployment metrics for vulnerability groups and vulnerability entries are included in Vulnerability Solution Management under Remediaion Status in vulnerabilities, vulnerable items. Easily identify which vulnerability group or vulnerability is slowing remediation progress. Drill down into how the vulnerability is identified, or what aspects of the affected assets may be causing the remediation issue. Update the status of your metrics using the Update status related link in the vulnerability, solutions, and vulnerability group forms.

**Using the default Vulnerability Response dashboards**

The Vulnerability Response overview dashboard (Vulnerability Management) provides an executive view into vulnerabilities and vulnerable items, helping the Vulnerability Admin pinpoint areas of concern quickly. The Vulnerability Response remediation dashboard (Vulnerability Remediation) allows a remediation specialist to focus on the vulnerability groups and vulnerable items they own.

All Vulnerability Response dashboards available from the dashboard menu. These reports are included as part of the Performance Analytics for Vulnerability Response application and do not require a separate subscription.
When the Performance Analytics Content Pack for Vulnerability Response application is installed and activated, the Vulnerability Management (PA) dashboard, is displayed automatically in the Overview module. This dashboard contains reports covering all stages of the vulnerability management lifecycle.

For information on the reports included in the Performance Analytics Content Pack for Vulnerability Response, see Using Performance Analytics for Vulnerability Response.

For information about the CISO dashboard and Scan Coverage reports, see CISO dashboard overview.

Vulnerability Management dashboard
In each chart, you can point to any part of a chart (bar, pie, data point, and so on) to view general data specific to that part. If you click any part of a report, a list opens to provide detailed information.

Note:
If customized dashboards are needed, see Create and use dashboards for more information.
Open Vulnerable Items by CI

Vulnerable Items by Remediation Target Status

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Vulnerable Items by CI</td>
<td>Bar</td>
<td>Displays the number of open vulnerable items recorded for each configuration item (CI), from most to least.</td>
</tr>
<tr>
<td>Vulnerable Items by Remediation Target Status</td>
<td>Bar</td>
<td>Displays the number of Vulnerable Items that are Approaching Target, In-flight, and Past Target. Note: Items in the Deferred, Resolved, or Closed state are not included.</td>
</tr>
</tbody>
</table>
## Vulnerability Overview reports (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deferred Vulnerable Items Expiring this Week</td>
<td>Graph</td>
<td>Displays the number of deferred vulnerable items scheduled to be reactivated within seven days.</td>
</tr>
<tr>
<td>Open Vulnerable Items by Vulnerability</td>
<td>Bar</td>
<td>Displays the number of open vulnerable items for each vulnerability, from most to least.</td>
</tr>
<tr>
<td>Vulnerabilities by Model</td>
<td>Bar</td>
<td>Displays the number of vulnerable items recorded for each model (CI class), from most to least.</td>
</tr>
<tr>
<td>Vulnerabilities by Week</td>
<td>Trend</td>
<td>Displays the number of vulnerability entries recorded each week.</td>
</tr>
<tr>
<td>Most Vulnerable Models</td>
<td>Donut</td>
<td>Displays models (CI classes) with the most vulnerable items.</td>
</tr>
<tr>
<td>Vulnerabilities by Publisher</td>
<td>Bar</td>
<td>Displays the number of vulnerable items recorded for each publisher, from most to least.</td>
</tr>
<tr>
<td>Vulnerabilities by Impact</td>
<td>Bar</td>
<td>Displays the number of vulnerability entries for impacted network types.</td>
</tr>
<tr>
<td>Most Vulnerable Publishers</td>
<td>Donut</td>
<td>Displays publishers with the most vulnerable items.</td>
</tr>
<tr>
<td>Most Vulnerable CIs</td>
<td>Donut</td>
<td>Displays CIs with the most vulnerable items.</td>
</tr>
<tr>
<td>Vulnerabilities by Score</td>
<td>Bar</td>
<td>Displays the number of vulnerability entries by vulnerability scores.</td>
</tr>
<tr>
<td>Reopened Vulnerable Items</td>
<td>List</td>
<td>Lists the reopened vulnerable items and their age.</td>
</tr>
<tr>
<td>Most Vulnerable CIs by Class</td>
<td>Donut</td>
<td>Displays CIs with the most vulnerable items.</td>
</tr>
<tr>
<td>Vulnerable Item Age</td>
<td>List</td>
<td>Lists the number of days since vulnerable items were last opened.</td>
</tr>
<tr>
<td>CIs with Vulnerability by Date</td>
<td>List</td>
<td>Lists configuration items that have been scanned within the last 30 days.</td>
</tr>
<tr>
<td>CIs not Scanned</td>
<td>List</td>
<td>Lists configuration items that have never been scanned for vulnerabilities.</td>
</tr>
</tbody>
</table>
Vulnerability Remediation dashboard

The Vulnerability Remediation dashboard contains the following tabs: **Assigned to My Groups**, **Assigned to Me**, and **Requested by Me**. The Assigned to My Groups and Assigned to Me tabs show the same reports. The former tab reports by the assignment groups you belong to, and the latter by vulnerable items or vulnerability groups that are assigned to you. Starting with v10.3, the Requested by Me tab reports the false positives and exceptions you requested.
## Assigned to My Groups and Assigned to Me

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerable Items by Risk Rating</td>
<td>Bar</td>
<td>Number of active vulnerable items grouped by risk rating over the selected time span.</td>
</tr>
<tr>
<td>Closed Vulnerable Items by Remediation Target Status</td>
<td>Bar</td>
<td>Number of Closed vulnerable items grouped by remediation target status over the selected time span.</td>
</tr>
<tr>
<td>Vulnerability Groups by State</td>
<td>Bar</td>
<td>Number of active vulnerability groups (VGs) grouped by state.</td>
</tr>
<tr>
<td>Vulnerability Groups by Remediation Target Status</td>
<td>Bar</td>
<td>Number of active VGs grouped by remediation target status. This report excludes deferred vulnerable items.</td>
</tr>
<tr>
<td>Vulnerability Group Details</td>
<td></td>
<td>Vulnerability Group record details in a list.</td>
</tr>
</tbody>
</table>

## Requested by Me

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status of my Requests</td>
<td>Bar</td>
<td>Number of active requests from you.</td>
</tr>
<tr>
<td>Deferred and False Positive Vulnerability Groups about to Expire</td>
<td>Bar</td>
<td>Number of Deferred and False Positive Vulnerability Groups (VGs), grouped by Until date.</td>
</tr>
</tbody>
</table>
Vulnerability Approvals dashboard

Starting with v10.3, the Vulnerability Approvals dashboard contains the following reports for exception and false positive approvers.

Reports

Approval reports

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>My Approval Requests by Age</td>
<td>Bar</td>
<td>Number of approvals pending for you, grouped by created date.</td>
</tr>
<tr>
<td>My Approval Requests by Approved and Rejected Status</td>
<td>Bar</td>
<td>Number of approval requests approved or rejected, grouped by approval state.</td>
</tr>
<tr>
<td>All Vulnerability Groups filtered by Risk Rating with Approval Request</td>
<td>Bar</td>
<td>Number of Vulnerability Groups pending approval, grouped by risk rating.</td>
</tr>
</tbody>
</table>
Approval reports (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Approval Requests filtered by Required Substate</td>
<td>Bar</td>
<td>Number of pending approval requests grouped by substate.</td>
</tr>
</tbody>
</table>

Using Performance Analytics for Vulnerability Response

Performance Analytics content packs contain preconfigured best practice dashboards. These dashboards present important metrics for analyzing your Vulnerability Response process, such as viewing remediation target attainment rates. The Performance Analytics for Vulnerability Response content pack is not automatically installed with the Vulnerability Response application. It is available on the ServiceNow Store as a separate subscription.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Enable your Performance Analytics Solutions for Vulnerability Response

For more information about setting up, installing, and configuring your Performance Analytics for Vulnerability Response application, see Install and configure the Performance Analytics for Vulnerability Response [PA] application.

For more information about the standard reports on the Vulnerability Management dashboard that come installed as part of the Vulnerability Response application, see Using the default Vulnerability Response dashboards.

For information about the CISO dashboard and Scan Coverage reports, see CISO dashboard overview.

Key terms

Performance analytics (PA)

Solution that creates management dashboards, reports on KPIs and metrics, and answers key business questions to help increase quality and reduce costs.

Vulnerable item (VI)
A security vulnerability reported by a third-party vulnerability scanner that is present on a configuration item (CI).

**Vulnerability group (VG)**

A group of vulnerable items that represents a task to be assigned to an owner for remediation.

**PA indicator**

Defines a performance measurement taken at regular intervals of a business service, activity, or organizational behavior, for example, Non-Deferred Overdue Critical Vulnerable Items.

**PA indicator source**

Data sets that filter records from one table or database view, for example, VI Active.

**Overview**

The dashboards of the Performance Analytics for Vulnerability Response application provide you with important tools for your Vulnerability Response process. To view the dashboard, navigate to Vulnerability Response > Overview.

Use the Performance Analytics widgets on the dashboard to visualize data over time, analyze your business processes, and identify areas of improvement. With Analytics and Reporting Solutions, you can get value from Performance Analytics for your application with minimal setup. You can always create your own objects as well.

**Important:** Set up and test Analytics and Reporting Solutions on a non-production instance before enabling them in production.

**Note:** Analytics and Reporting Solutions provide all the configuration records required to analyze default applications. Customize these records for use in your production environment. For more information, see Configure Analytics and Reporting Solutions.

**Note:** To evaluate the functionality, you can activate Performance Analytics solutions and in-form analytics on instances that have not licensed Performance Analytics. However, you have the following limitations:

- You cannot create new indicators.
- You cannot collect data older than 180 days.

For full functionality, license Performance Analytics. For more information, see Activate your Performance Analytics subscription.
View reports in real-time
To see what is happening today with the most critical items in your Vulnerability Response application, starting with v10.0, you can view certain reports on the Vulnerability Management (PA) dashboard in real-time. Viewing these reports on-the-fly helps you manage your most important vulnerable items (VIs) and remediate them quickly. You can view the following reports in real time:

- Overview tab - Vulnerable Items by Assignment Group
- Vulnerable CIs tab
  - Vulnerable Configuration Items (CIs) without Owners
  - Retired or Stolen CIs with Active VIs
- Exceptions tab
  - Deferred Vulnerable Items by Reason
  - Deferral Requests About to Expire
  - Deferred Vulnerable Items by CIO Manager
- Remediation tab - Unassigned Vulnerable Items

For more information on each report, including real-time reports and using the Vulnerability Management (PA) dashboard, see View the Performance Analytics for Vulnerability Response [PA] dashboard.

View the Performance Analytics for Vulnerability Response [PA] dashboard
With the Performance Analytics for Vulnerability Response (PA) dashboard, vulnerability management can track the volume, performance and progress of vulnerabilities from initial analysis/detection to containment, or remediation. You can filter reports by assignment group, exploits, risk rating, state and so on. Quickly gain insight into your vulnerability exposure and which business services are affected.

Using the dashboard
Organization are dealing with increasing security incidents due to exploited vulnerabilities. Efficiently determine which vulnerable items present the most risk to your organization. These dashboards provide a graphical view into vulnerable item activity to help determine remediation plans and status progress. You can focus on the KPIs associated with critical affected assets and high-visibility vulnerabilities.

To view the Vulnerability Management (PA) dashboard, navigate to Vulnerability Response > Overview. See reports that show trending data over time and, starting with v10.0, view certain reports with real-time data. View
trends of important metrics on a regular schedule to analyze your overall business processes and identify areas of improvement.

For more information about how to view your PA reports with real-time scores, see, View Performance Analytics for Vulnerability Response [PA] reports in real-time (v10.0).
The Vulnerability Management (PA) dashboard tabs

Overview tab

This dashboard communicates KPIs for vulnerability risk and prevalence, affected assets, remediation target adherence, and remediation progress.

Starting with v10.3, on the Overview tab, you can view the Critical Vulnerable Items by Assignment Group report that is run based on the scheduled job.

v10.0: On the Overview tab, you can view the Critical Vulnerable Items by Assignment Group report in real-time.
Services tab

This dashboard exposes vulnerability risk at the business service level. Sharing this information across the organization can assist service managers to remediate vulnerabilities promptly and proactively, and drive the organization toward a shared responsibility model of information security.

Starting with version 13.0, you can change the service class to technical or application services using the system property sn_vul.service_classifications.
Service Owners tab

This dashboard aggregates the vulnerability risk from the business service level to the service owners — the executives responsible for those business services. It shows which executives are assuming the most vulnerability risk and which may require the most help encouraging prompt remediation activities.
Vulnerable CIs tab

This dashboard shows the scope and composition of CIs with active vulnerabilities, and which categories of CIs need the most attention. Identify decommissioned assets with active vulnerable items and confirm that the assets have been decommissioned. View the number of vulnerable CIs that lack ownership information, so that you can proactively identify owners for these assets before a critical vulnerability affects those systems.

Starting with v10.0, on the Vulnerable CIs tab, you can view the Vulnerable CIs Without Owners and Retired or Stolen CIs with Active VIs reports in real-time.
Exceptions tab

This dashboard help you understand where your organization is taking risk due to potentially excessive deferrals and reconsider remediation options.

Starting with v10.3, you can view Deferred Vulnerable Items by Reason, Expiring Deferral Requests, Exceptions for Critical Vulnerable Items by Assignment Group, and Exception Requests by Requester reports.

Version 10.0: On the Exceptions tab, you can view Deferred Vulnerable Items by Reason, Deferral Requests About to Expire, and Deferred Vulnerable Items by CI Manager reports in real-time.
False Positives tab
This dashboard helps you understand where your organization is taking risk due to potentially excessive false positives and reconsider remediation options. Starting with v10.3, on the False positives tab, you can view False Positive Vulnerable Items by Risk Rating, Expiring False Positive Vulnerability Groups, False Positives for Critical Vulnerable Items by Assignment Group, and False Positive Requests by Requester reports.
Remediation tab

This dashboard helps you understand the progress of your remediation actions, and which support teams need the most assistance with their completion.

On the Remediation tab, you can view Unassigned Vulnerable Items report in real-time.

---

Report details

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerabilities</td>
<td>Single Score</td>
<td>Number of vulnerabilities associated with one or more active vulnerable items.</td>
</tr>
<tr>
<td>Vulnerable Items (VIs)</td>
<td>Single Score</td>
<td>Number of active (non-closed) vulnerable items.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-----------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Vulnerable Configuration Items (CIs)</td>
<td>Single Score</td>
<td>Number of configuration items (CIs) associated with one or more active vulnerable items.</td>
</tr>
<tr>
<td>Vulnerability Groups (VGs)</td>
<td>Single Score</td>
<td>Number of active (non-closed) vulnerability groups.</td>
</tr>
<tr>
<td>Vulnerable Items by Risk Rating</td>
<td>Bar</td>
<td>Number of active vulnerable items grouped by risk rating over the selected time span.</td>
</tr>
<tr>
<td>Vulnerable Items by Age and Risk Rating</td>
<td>Heatmap</td>
<td>Number of active vulnerable items grouped by risk rating and age (in days).</td>
</tr>
<tr>
<td>VIs Met Remediation Target</td>
<td>Single Score</td>
<td>Percentage of closed vulnerable items that have met their remediation target dates in the current and previous quarters.</td>
</tr>
<tr>
<td>VIs Mean Time to Remediation (MTTR)</td>
<td>Single Score</td>
<td>The mean time to remediate (close) a vulnerable item, displayed as a 30-day running average.</td>
</tr>
<tr>
<td>Critical Vulnerability Groups Near Due</td>
<td>Single Score</td>
<td>Number of active vulnerability groups approaching their remediation target date.</td>
</tr>
</tbody>
</table>

Note: The value for Age Closed is calculated when data is collected. The value is the difference between the last_opened date and the date and time of the collection job.
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remediation targets are calculated from the Last Opened date plus the number of days (measured as 24-hour increments). This report excludes deferred vulnerability groups.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New and Closed Vulnerable Items</td>
<td>Bar</td>
<td>Number of New and Closed vulnerable items over the selected time span.</td>
</tr>
<tr>
<td>Note: The value for Age Closed is calculated when data is collected. The value is the difference between the last_opened date and the date and time of the collection job.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Closed Vulnerable Items by Remediation Target Status</td>
<td>Bar</td>
<td>Number of Closed vulnerable items grouped by remediation target status over the selected time span.</td>
</tr>
<tr>
<td>Note: The value for Age Closed is calculated when data is collected. The value is the difference between the last_opened date and the date and time of the collection job.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Critical Vulnerable Items by Assignment Group</td>
<td>List and Line</td>
<td>Number of active vulnerable items with a critical risk rating grouped by assignment group.</td>
</tr>
<tr>
<td>Overdue Critical Vulnerable Items by Assignment Group</td>
<td>List and Line</td>
<td>Number of active vulnerable items with a critical risk rating and past their remediation target dates, grouped by assignment group.</td>
</tr>
<tr>
<td>Remediation targets are calculated from the Last Opened date plus the number of days (measured as 24-hour increments). This report excludes deferred vulnerable items.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Business Services

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical Vulnerable Items</td>
<td>List, Line, and Distribution Bar</td>
<td>Number of active vulnerable items with a critical risk rating, grouped by business service. Displays a weekly average from the current and prior week, the difference between the two weeks (in count and percent), and a trend. The distribution bar displays the difference between all values on the current page of the scorecard.</td>
</tr>
<tr>
<td>Overdue Critical Vulnerable Items</td>
<td>List, Line, and Distribution Bar</td>
<td>Number of active vulnerable items with a critical risk rating and past their remediation target dates, grouped by business service. Displays a weekly average from the current and prior week, the difference between the two weeks (in count and percent), and a trend. The distribution bar displays the difference between all values on the current page of the scorecard. This report excludes deferred vulnerable items.</td>
</tr>
<tr>
<td>High Vulnerable Items</td>
<td>List, Line, and Distribution Bar</td>
<td>Number of active vulnerable items with a high risk rating, grouped by business service. Displays a weekly average from the current and prior week, the difference between the two weeks (in count and percent), and a trend. The distribution bar displays the difference between all values on the current page of the scorecard.</td>
</tr>
<tr>
<td>Overdue High Vulnerable Items</td>
<td>List, Line, and Distribution Bar</td>
<td>Number of active vulnerable items with a high risk rating and past their remediation target dates, grouped by business service.</td>
</tr>
</tbody>
</table>
### Business Services (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Bar</td>
<td>Displays a weekly average from the current and prior week, the difference between the two weeks (in count and percent), and a trend. The distribution bar displays the difference between all values on the current page of the scorecard. This report excludes deferred vulnerable items.</td>
</tr>
</tbody>
</table>

### Service Owners

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical Vulnerable Items</td>
<td>List, Line, and Distribution</td>
<td>Number of active vulnerable items with a critical risk rating, grouped by business service owner. Displays a weekly average from the current and prior week, the difference between the two weeks (in count and percent), and a trend. The distribution bar displays the difference between all values on the current page of the scorecard.</td>
</tr>
<tr>
<td></td>
<td>Bar</td>
<td></td>
</tr>
<tr>
<td>Overdue Critical Vulnerable Items</td>
<td>List, Line, and Distribution</td>
<td>Number of active vulnerable items with a critical risk rating and past their remediation target dates, grouped by business service owner. Displays a weekly average from the current and prior week, the difference between the two weeks (in count and percent), and a trend. The distribution bar displays the difference between all values on the current page of the scorecard. This report excludes deferred vulnerable items.</td>
</tr>
<tr>
<td></td>
<td>Bar</td>
<td></td>
</tr>
</tbody>
</table>
### Service Owners (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High Vulnerable Items</strong></td>
<td>List, Line, and Distribution</td>
<td>Number of active vulnerable items with a high risk rating, grouped by business service owner.</td>
</tr>
<tr>
<td></td>
<td>Bar</td>
<td>Displays a weekly average from the current and prior week, the difference between the two weeks (in count and percent), and a trend.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The distribution bar displays the difference between all values on the current page of the scorecard.</td>
</tr>
<tr>
<td><strong>Overdue High Vulnerable Items</strong></td>
<td>List, Line, and Distribution</td>
<td>Number of active vulnerable items with a high risk rating and past their remediation target dates, grouped by business service owner.</td>
</tr>
<tr>
<td></td>
<td>Bar</td>
<td>Displays a weekly average from the current and prior week, the difference between the two weeks (in count and percent), and a trend.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The distribution bar displays the difference between all values on the current page of the scorecard.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This report excludes deferred vulnerable items.</td>
</tr>
</tbody>
</table>

### Vulnerable CIs

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerable Configuration Items (CIs) by CI Class</strong></td>
<td>Bar</td>
<td>Numbers of configuration items with active vulnerabilities, grouped by CI class in the CMDB.</td>
</tr>
<tr>
<td><strong>Vulnerable Items (VIs) by CI Class</strong></td>
<td>Treemap</td>
<td>Number of active VIs broken down by CI class.</td>
</tr>
</tbody>
</table>
### Vulnerable CIs (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Vulnerable Items per CI</td>
<td>Bar</td>
<td>Average number of vulnerable items belonging to a configuration item, grouped by risk rating.</td>
</tr>
<tr>
<td>Unmatched CIs</td>
<td>Single Score</td>
<td>Number of imported configuration items that do not match any existing CI in the CMDB.</td>
</tr>
<tr>
<td>Vulnerable CIs Without Owners</td>
<td>Single Score</td>
<td>Number of vulnerable configuration items that do not have an assigned support group.</td>
</tr>
<tr>
<td>Retired or Stolen CIs with Active VIs</td>
<td>Single Score</td>
<td>Number of configuration items marked Retired or Stolen in the CMDB that have active vulnerable items.</td>
</tr>
</tbody>
</table>

### Exceptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deferred Vulnerable Items by Reason</td>
<td>Bar</td>
<td>Number of deferred vulnerable items grouped by deferral reason.</td>
</tr>
</tbody>
</table>
| Deferral Requests About to Expire   | Bar         | Number of deferral requests associated with vulnerability groups or vulnerable items that are about to be reopened for review. They are grouped by the number of days left until they reopen.  
If email notifications are defined, an email is sent. |
### Exceptions (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deferred Vulnerable Items by Configuration Item (CI) Manager</td>
<td>Bar</td>
<td>Number of deferred vulnerable items grouped by the manager for the associated configuration item.</td>
</tr>
</tbody>
</table>

### False Positives

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>False Positive Vulnerable Items by Risk Rating</td>
<td>Bar</td>
<td>Number of false positive vulnerable items grouped by risk rating.</td>
</tr>
<tr>
<td>Expiring False Positive Vulnerability Groups</td>
<td>Bar</td>
<td>Number of false positive vulnerability groups that are about to be reopened, grouped by the number of days left until they are reopened.</td>
</tr>
<tr>
<td>False Positives for Critical Vulnerable Items by Assignment Group</td>
<td>List and Line</td>
<td>Number of false positive, critical vulnerable items in a month, grouped by their assignment group. The breakdown filter is not available for this widget.</td>
</tr>
<tr>
<td>False Positive Requests by Requester</td>
<td>List and Line</td>
<td>Number of false positive requests in a month, grouped by their requester. The breakdown filter is not available for this widget.</td>
</tr>
</tbody>
</table>
## Remediation

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Groups by Risk Rating and State</td>
<td>Heatmap</td>
<td>Number of active vulnerability groups (VGs) grouped by risk rating and state.</td>
</tr>
<tr>
<td>Vulnerability Groups by Risk Rating and Remediation Target Status</td>
<td>Heatmap</td>
<td>Number of active VGs grouped by risk rating and remediation target status. This report excludes deferred vulnerable items.</td>
</tr>
<tr>
<td>Critical Vulnerability Groups by Assignment Group</td>
<td>List and Line</td>
<td>Number of active vulnerability groups with a critical risk rating grouped by assignment group. This report excludes deferred vulnerability groups.</td>
</tr>
<tr>
<td>Overdue Critical Vulnerability Groups by Assignment Group</td>
<td>List and Line</td>
<td>Number of active vulnerability groups with a critical risk rating and past their remediation target dates, grouped by assignment group. This report excludes deferred vulnerability groups.</td>
</tr>
<tr>
<td>Unassigned Vulnerability Groups</td>
<td>Single Score</td>
<td>Number of active vulnerability groups without an assignee or assignment group.</td>
</tr>
<tr>
<td>Unassigned Vulnerable Items</td>
<td>Single Score</td>
<td>Number of active vulnerable items without an assignee or assignment group.</td>
</tr>
</tbody>
</table>
Vulnerability Management indicators

The Vulnerability Management (PA) dashboard contains over 30 indicators.

For more information on indicators, see Performance Analytics Indicators. See View the Performance Analytics indicators for Vulnerability Response[PA] to view the Vulnerability Response-specific indicators.

To view the indicators for Performance Analytics for Vulnerability Response, see View the Performance Analytics indicators for Vulnerability Response[PA].

Vulnerability Management breakdowns

The following breakdowns apply to the indicators on the dashboard:

• Assignment Group: Applies to VI or and VG reports
• Exploit Exists: Applies to VI reports.
• Exploit Attack Vector: Applies to VI reports.
• Exploit Skill Level: Applies to VI reports.
• Remediation Target Status: Applies to VI and VG reports.
• Risk Rating: Applies to VI and VG reports.
• State: Applies to VI and VG reports.

For information on how breakdowns work see,

View Performance Analytics for Vulnerability Response [PA] reports in real-time (v10.0)

To manage your most important vulnerable items (VIs) and help you remediate them quickly, starting with v10.0, view reports on-demand, in real-time on the Vulnerability Management (PA) dashboard. The Performance Analytics for Vulnerability Response application is available with a separate subscription from the ServiceNow Store.

Before you begin

Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

For more information about the reports for Performance Analytics for Vulnerability Response, see View the Performance Analytics for Vulnerability Response [PA] dashboard.
For more information about the setup and installation of the Performance Analytics for Vulnerability Response application, see Install and configure the Performance Analytics for Vulnerability Response [PA] application.

If not displayed, to view the dashboard, navigate to **Vulnerability Response > Overview**. At the top of the dashboard the report tabs are displayed.

View the following reports on the tabs of the Vulnerability Management (PA) dashboard in real-time.

- **Overview tab**
  - Critical Vulnerable Items by Assignment Group

- **Vulnerable CIs tab:**
  - Vulnerable CIs Without Owners
  - Retired or Stolen CIs with Active VIs

- **Exceptions tab:**
Deferred Vulnerable Items by Reason
- Deferral Requests About to Expire
- Deferred Vulnerable Items by CIO Manager

- Remediation tab:
  - Unassigned Vulnerable Items

To view real-time scores, with one of the tabs selected that contains real-time reports, follow these steps:

**Procedure**

1. In the report, for example, Critical Vulnerable Items by Assignment Group, click one of the links that is displayed.

2. In the record that is displayed, click the date.
3. In the calendar that is displayed, click Real-time.

If a report does not support a real-time score, the Real-time button is not displayed on the calendar.

It may take a few moments for the value to update. The current date, the records, the number of new records since the last report, and the percent change from the last report are also displayed.
4. **Optional:** To view the records that make up the report, with the real-time report displayed, in the upper right, click **Show records.**
A list of records that make up the score is displayed.

**CISO dashboard overview**

Executive users, like the Chief Information Security Officers (CISOs) in your organization, can view the CISO dashboard for Vulnerability Response to understand how effective their vulnerability management program is. They can view the Key Performance Metrics (KPIs) for vulnerability remediation, see the highest risks, verify what the scan coverage is, and learn how to lower these risks.

**Required roles**

- `sn_vul.vulnerability_ciso`, needed to view the dashboard.
- `sn_vul.ciso_write`, needed to edit the dashboard.

**Activating the CISO dashboard**

As an administrator, to activate the CISO dashboard, you must install Performance Analytics for Vulnerability Response v12.0 and activate the corresponding Performance Analytics job. For more information, see [Using Performance Analytics for Vulnerability Response](#).

**Using the CISO dashboard**

As an executive user, you can view the CISO dashboard by navigating to **Vulnerability Response > CISO Dashboard.** Use the top-level filters to filter reports by Risk Rating, Age Range, or Internet Facing. Some reports display trending
data over a period of time. You can view how the important metrics are trending on a regular basis, analyze the overall business security risk, and identify the areas that need improvement.

Running the scheduled jobs
Run the scheduled jobs in this order to update the data in the reports:

1. Update CISO dashboard tables
2. [PA VR] CISO Dashboard

### Scheduled jobs for CISO dashboard

<table>
<thead>
<tr>
<th>Scheduled job name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update CISO dashboard tables</td>
<td>Daily scheduled job that you must run before the [PA VR] CISO Dashboard job so that you can collect the CISO data. By running this scheduled job, you update the Scan Coverage reports. The information updated includes the operational configuration items (CIs) that are scanned in the last 90 days, their classes, and the total number of operational CIs that correspond to these classes. Running this scheduled job updates the reports in the <strong>Recommended Actions</strong> tab as well. Note: Operational CIs refer to the CIs that have an operational status as <strong>Operational</strong>.</td>
</tr>
<tr>
<td>[PA VR] CISO Dashboard</td>
<td>After the Update CISO dashboard tables scheduled job is complete, run this scheduled job to populate all the reports in the <strong>CISO Overview</strong> tab.</td>
</tr>
</tbody>
</table>

### CISO dashboard tabs

This dashboard lets users see the risks that are present in Vulnerability Management. They can view the vulnerabilities and their related data by region, age, services, and other breakdowns.
Overview tab

The **Overview** tab contains reports that let users see the security posture of your organization at a glance.

**Note:** The top-level filter can only be used for some reports.
Recommended Actions tab

The **Recommended Actions** tab contains reports that let users get insights into exploitable, aging, and prevalent vulnerabilities. It also contains recommended actions to reduce the risks. Run the Update CISO dashboard tables scheduled job to update the reports in this tab.

Scan Coverage reports

Scan coverage reports display the number of CIs that are scanned by the scanners in the last 90 days, compared to the number of CIs that are considered scannable in the CMDB. Devices that are scanned by Tenable, Qualys, and Rapid7 are supported in the scan coverage reports. The scan coverage reports are:

- **Scan coverage**: Number of scanned assets that is compared to the total number of scannable assets, shown over time. The CI Classes included in the widget are specified in the Scan Coverage Configuration module.

- **Monthly Scan Coverage**: Percentage of the number of scanned assets that is divided by the total number of scannable assets for the current month.

**Note**: The top-level filter is not available for these reports.
Note: In the Analytics Hub, users can view the class-wise scan coverage reports. You can further break down the reports by CI class to see the extent of the coverage.

![Analytics Hub screenshot](image)

### Report details

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Vulnerabilities per Asset</td>
<td>Single Score</td>
<td>Average number of active vulnerable items for each configuration item.</td>
</tr>
<tr>
<td>Mean Time to Remediate (MTTR)</td>
<td>Single Score</td>
<td>Mean time to remediate (close) a vulnerable item. This score is displayed as a 30-day running average.</td>
</tr>
</tbody>
</table>

Note: The value for Age Closed is calculated when data is collected. The value is the difference between the last opened date and the date and time of the collection job.
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Age of Vulnerabilities</td>
<td>Single Score</td>
<td>Average age of active vulnerable items in days.</td>
</tr>
<tr>
<td>Services with Most Vulnerabilities</td>
<td>List and Line</td>
<td>Monthly average of active vulnerable items for services in the organization.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◀ Note: For information on defining the service classifications that you want to display in Vulnerability Response reporting and related lists, see the Services tab in View the Performance Analytics for Vulnerability Response [PA] dashboard.</td>
</tr>
<tr>
<td>Countries with Most Vulnerabilities</td>
<td>Donut</td>
<td>Top 10 countries with the highest number of vulnerable items.</td>
</tr>
<tr>
<td>Monthly Remediation Efficiency</td>
<td>Single Score</td>
<td>Percentage of closed vulnerable items that is divided by new vulnerable items in the current month.</td>
</tr>
<tr>
<td>New and Closed Vulnerable Items</td>
<td>Bar</td>
<td>Number of new vulnerable items that were imported and the number of vulnerable items that were closed in a month.</td>
</tr>
<tr>
<td>Scan Coverage</td>
<td>Line</td>
<td>Number of scanned assets that are compared to the total number of scannable assets, shown over time. The CI Classes included in the widget are specified in the Scan Coverage Configuration module. For information on configuring the Scan Coverage module, see Configure the Scan Coverage reports.</td>
</tr>
<tr>
<td>Monthly Scan Coverage</td>
<td>Single Score</td>
<td>Percentage of scanned assets that is divided by the total number of scannable assets for the current month.</td>
</tr>
</tbody>
</table>
### Recommended Actions

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 10 Vulnerabilities with Exploits Available</td>
<td>List</td>
<td>Active vulnerabilities with exploits available for all the threat intelligence vendors that use the Vulnerability Response (VR) exploit framework.</td>
</tr>
<tr>
<td>Top 10 Highest Impact Solutions</td>
<td>List</td>
<td>Preferred solutions or patches with the highest risk scores for active vulnerable items. This report uses the capabilities of Vulnerability Solution Management (VSM), which correlates patches from Microsoft and Red Hat to vulnerabilities in the environment. VSM helps identify the preferred solution for vulnerabilities.</td>
</tr>
<tr>
<td>Top 10 Oldest Vulnerable Items</td>
<td>List</td>
<td>Active vulnerable items with the highest age. Resolve these items to lower the average vulnerability age on the Overview tab.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Top 10 Vulnerabilities Most</td>
<td></td>
<td>Active vulnerable items available for the highest number of assets.</td>
</tr>
<tr>
<td>Prevalent on Assets</td>
<td>List</td>
<td></td>
</tr>
</tbody>
</table>

**PA indicators for the CISO dashboard**

The Performance Analytics indicators define a performance measurement that is taken at regular intervals of a business service, activity, or organizational behavior. The CISO dashboard contains over 10 indicators.

For more information on indicators, see Performance Analytics Indicators.

**CISO dashboard breakdowns**

The following breakdowns apply to the indicators on the dashboard:

- **Assignment Group**: Applies to some vulnerable item (VI) reports.
- **Risk Rating**: Applies to VI reports.
- **Age Range**: Applies to VI reports.
- **Age Closed**: Applies to reports for closed VIs.
- **Internet Facing**: Indicates whether the CI belongs to the hardware class and is internet facing.
- **Region**: The CMDB CI parameter used is Location. This location indicates the country of origin of the configuration item.

For information on how breakdowns work, see .

**Configure the Scan Coverage reports**

Enable your users to run scan coverage reports from the CISO dashboard. With these reports, your users can see what the organization's scan coverage is over a period of time.

**Before you begin**

Role required:

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

**About this task**

The scan coverage shows the number of assets that are being scanned by the vulnerability scanners for the various classes over the last 90 days.
These assets are compared to the number of scannable assets in the Configuration Management Database (CMDB). By default, the Scan Coverage Configuration module includes CMDB CI classes, to which at least one scanned asset has been matched. You can add a CI class from the CMDB to the Scan Coverage report that is displayed on the CISO dashboard. You can include or exclude CMDB CI classes that appear on the Scan Coverage reports.

Procedure

1. Navigate to **Vulnerability Response > Administration > Scan Coverage Configuration**.
2. Click **New**.
3. On the form, fill in the fields.

### Scan Coverage Configuration form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMDB CI Class</td>
<td>CI class that must be added to the Scan Coverage Report on the CISO dashboard.</td>
</tr>
<tr>
<td>Consider Scannable</td>
<td>Option to define if the CI class must be included or not. Include a CI class if you want its data to be added.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>to the scan coverage reports. If excluded, the data for that CI class is not added.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**Configure the PA indicators for the CISO Dashboard**

Monitor the automated and formulated CISO indicators so that you can manage the vulnerability data in your instance.

**Before you begin**

Role required: sn_vul.vulnerability.admin

**About this task**

Vulnerability Response has both automated and formulated indicators.

**Key terms**

**Indicator**

Defines a performance measurement taken at regular intervals of a business service, activity, or organizational behavior. An example is an Active Vulnerable Item.

**Indicator source**

Data sets that consist of records filtered from one table or database view for increased efficiency. An example is VI.Active (Internet facing).

**Breakdowns**

Breakdowns filter and group indicator scores using qualitative attributes such as Priority, Category, and Assignment Group.

**Scheduled jobs**

Scheduled jobs are run to populate the indicator source data. The [PA VR] CISO Dashboard daily scheduled job is disabled by default. You must activate it to collect indicator scores for the CISO dashboard.
Procedure

1. Navigate to **Performance Analytics > Indicators** and choose one of the following:
   - Automated Indicators
   - Formula Indicators

   For more information on indicators, see [Performance Analytics Indicators](#).

2. On the Indicators page, search for the required indicator name in the Name column.

3. Click the indicator name to open the record and view its details.

   The indicators for the CISO dashboard do not collect records by default. You can choose to collect records by selecting the **Collect records** check box.

   **Note:** Activating collect records in an indicator may cause performance issues such as taking a lot more time and memory that is required to run the data collection job.

   The maximum number of rows that you can fetch for an indicator source is 1,000,000.

---

**View the Performance Analytics indicators for Vulnerability Response[PA]**

View automated and formulated Performance Analytics indicators representing the vulnerability data in your instance.

**Before you begin**

The collect records option for the indicators is disabled by default for the Performance Analytics - Content Pack Vulnerability Response application. This option is disabled so that certain reports can be viewed in real-time. Trending information used by these indicators is still available if you prefer to enable collect records manually and view the records that make up the scores.

**Note:** Activating collect records in an indicator may impact your performance and considerably lengthen the time and memory required to run the data collection job.

**Role required:** v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated), or pa.viewer

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see [Assign the Vulnerability Response persona roles using Setup Assistant](#). For more information about managing granular roles, see [Manage persona and granular roles for Vulnerability Response](#).
About this task
Vulnerability Response has both automated and formulated indicators.

Key terms

**PA indicator**
Defines a performance measurement taken at regular intervals of a business service, activity, or organizational behavior, for example, Non-Deferred Overdue Critical Vulnerable Items.

**PA indicator source**
Data sets that filter records from one table or database view, for example, VI Active.

**Collect records**
When enabled, stores records in memory and provides access to Analytics Hub.

**Breakdowns**
Breakdowns filter and group collected records. Breakdowns may increase memory use, especially as their number and diversity increase.

**Breakdown exclusions**
Exclusions remove certain breakdowns, which may reduce memory consumption.

Procedure
1. For automated indicators, navigate to Performance Analytics > Indicators > Automated Indicators.

2. For formulated indicators, navigate to Performance Analytics > Formula Indicators.

For detailed information on indicators, see Performance Analytics Indicators.

3. In either case, search on Application > Performance Analytics.

   Note: If it is not in your default view, add the Application column using the gear icon (⚙️) in the upper left corner of the page. The Application column is then displayed in your Search drop-down menu.

4. Optional: To enable Collect records on a Performance Analytics for Vulnerability Response indicator, follow these steps:
a. With the list of automated indicators displayed, in the Name column, click the indicator you want to enable collect records for. The indicator record is displayed.

b. In the Indicator properties section with the Source tab selected, select the Collect records check box.

c. Choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Update</strong></td>
<td>Save your edits and return to the Indicators list.</td>
</tr>
<tr>
<td><strong>Manage Breakdowns</strong></td>
<td>Reactivate second-level breakdowns for the listed indicators, or, edit breakdowns for other indicators. (Optional) For more information on Performance Analytics breakdowns, see <a href="#">Performance Analytics Breakdowns</a>.</td>
</tr>
</tbody>
</table>

---

**Note:** If you choose to reactivate second-level breakdowns, you may significantly increase your memory consumption and slow the data collection job.
By default, second-level breakdown exclusions have been applied to the following indicators:

- Vulnerable Configuration Items
- Retired CIs
- Deferred VIs

d. Click Manage Breakdowns.

e. In the form that is displayed, click Configure Breakdown Matrix. The Breakdown Matrix form is displayed. Excluded combinations are selected and displayed with colors, as shown in the following figure.

f. To remove the exclusion and reactive an excluded combination, click a selected cell.
g. In the upper right of the form, click **Close** to return the Manage Breakdown form.

h. Click the back arrow to return to the indicator record.

i. Click **Update** to save your edits and return to the Indicators list.

**Remediate Vulnerability Response groups**

The flexibility inherent in Vulnerability Response allows you to remediate vulnerabilities in whatever way suits your security organization.

**Before you begin**

Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

**About this task**

Once you are notified that a change request is resolved, move the vulnerability group state to Resolved and wait for the next scan. Rescans are triggered automatically by the third-party import schedule configured in the Setup Assistant.

ℹ️ **Note:**

If state synchronization is enabled, vulnerability groups are automatically moved to the **Resolved** state after a change request associated with a **VG** is implemented and in the **Review** state. See Change management for Vulnerability Response.

**Procedure**

1. Navigate to **Vulnerability > Vulnerabilities > Vulnerability Groups**.

2. Click a vulnerable group record that is in the Open state.
   
   The Open state indicates that the record has not yet been worked on. The form displays:
   
   - Vulnerability group information
   - Group Configuration details
• Notes
• Associated vulnerable items
• Task SLAs
• Change Requests

3. Perform your analysis of the group.

4. When you are ready to start working on the record, choose any of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the vulnerable item poses a risk to your IT environment, create a CHG record and escalate the issue to Change Management team.</td>
<td>Assign the group to the appropriate group or individual and click Create Change.</td>
</tr>
<tr>
<td>If the vulnerable item poses a potential security risk to your organization, create a security incident record and escalate the issue to the Security Incident Response team.</td>
<td>Click Create Security Incident. This button is displayed only when Security Incident Response is activated. A business impact calculation is applied, the incident is assigned, and the security incident is created.</td>
</tr>
</tbody>
</table>

After you create a change request, the appropriate record appears in the Change Requests related list on the Vulnerability Group form.

5. If you determine that the issue is of low risk and can be deferred, click Close/Defer.
   For instructions, see Defer a vulnerability group.

6. If you determine that the issue can be immediately closed without further analysis, click Close/Defer.
   For instructions, see Close a vulnerability group.

7. A third-party integration scheduled job automatically updates and scans records at a set interval. The vulnerable items are scanned at the next scheduled date and time. Alternatively, you can manually initiate a vulnerability scan using the Scan for Vulnerabilities related link.

   If the scan again finds the vulnerability on the configuration item and does not mark it Fixed, the vulnerable item returns to the Under Investigation state. Contact IT Operations to reopen the change request.
If the scan does not find the vulnerability and returns that the vulnerable item has been marked Fixed, the vulnerable item transitions to the Closed-Fixed state and is closed during import.

Only when all vulnerable items in a group are in the Closed-Fixed state, does the vulnerability group close automatically. Vulnerability groups with vulnerable items in Closed states other than Fixed must be closed manually.

**Defer a vulnerability group**

If you determine that the issue associated with a vulnerability group is a low priority and can be immediately deferred without further analysis, you can use the **Defer** feature.

**Before you begin**

Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see **Assign the Vulnerability Response persona roles using Setup Assistant**. For more information about managing granular roles, see **Manage persona and granular roles for Vulnerability Response**.

**About this task**

A scheduled job runs every day checking for deferred vulnerability groups that have reached their reopen date. On the day, the group is reopened.

**Note:** You can manually move change requests and vulnerability groups through the states of their life cycles on their respective records with state synchronization enabled, but when the system registers that a CHG has changed its state, or you add a CHG or remove it from a vulnerability group, state synchronization potentially can override your manual intervention. However, change request states do not automatically move vulnerability groups from the **Closed** or **Deferred** states.

**Procedure**

1. Navigate to **Vulnerability > Vulnerabilities > Vulnerability Groups**.
2. Open a vulnerability group.
3. Click the **Close/Defer** button.
4. Fill in the fields on the form, as appropriate.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select a state. Choices are: • Deferred • Closed</td>
</tr>
<tr>
<td>Until</td>
<td>Select the date when the <strong>Defer</strong> state expires and the vulnerability group is reactivated. After the record is submitted, if email notifications are defined, members of the Vulnerability Response group receive an email when the expiration date is within one week. When the defer date expires, the vulnerability group is set back to <strong>Open</strong> and a second email notification is sent out.</td>
</tr>
<tr>
<td>Reason</td>
<td>Enter the reason for deferring the issue. Choices include: • Awaiting maintenance window • False positive • Fix unavailable • Risk accepted • Mitigating control in place • Other</td>
</tr>
<tr>
<td>Additional information</td>
<td>Enter any other relevant information.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.
   The group is marked **Deferred**. A **Reopen** related link appears. The reopen date and reason appear in work notes under the **Defer/Closed** tab.

**Close a vulnerability group**

If you determine that the issue associated with a vulnerability group can be immediately closed without further analysis, you can use the **Close** feature.
Before you begin
Role required: admin
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Important: You can manually move change requests and vulnerability groups through the states of their life cycles on their respective records with state synchronization enabled, but when the system registers that a CHG has changed its state, or you add a CHG or remove it from a vulnerability group, state synchronization potentially can override your manual intervention. However, change request states do not automatically move vulnerability groups from the Closed or Deferred states.

Procedure
1. Open the vulnerable group record for which you want to request a review.
2. Click the Close/Defer button.
3. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select a state. Choices are: • Deferred • Closed</td>
</tr>
<tr>
<td>Until</td>
<td>Only available in the Defer state popup. Select the date when the Defer state expires and the vulnerability group is reactivated. After the record is submitted, if email notifications are defined, members of the Vulnerability Response group receive an email when the expiration date is within one week. When the defer date expires, the vulnerable</td>
</tr>
</tbody>
</table>
### Field Description

- **item is set back to Open and a second email notification is sent out.**
- **Reason** Enter the reason for closing the issue.
- **Additional information** Enter any other relevant information.

4. Click **Submit**. The group is marked **Closed**.

**Viewing assignment recommendations**

An assignment group is usually allocated to a vulnerable item by using assignment rules. These rules are configured by the vulnerability administrator to allocate the correct assignment groups that are based on the data received from third-party scanners such as Qualys and Rapid7.

For more information, see **Vulnerability Response assignment rules overview**. If a matching assignment group is not available or is incorrect, you can use **Vulnerability Assignment Recommendations** to view alternative assignment groups.

Use **Vulnerability Assignment Recommendations** to do the following actions:

- Request assignment group recommendations for a vulnerable item.
- Request assignment group recommendations for multiple vulnerable items.
- Request assignment group recommendations for a vulnerability group.

**Request assignment group recommendations for a vulnerable item**

Request **Vulnerability Assignment Recommendations** so that you can view assignment group recommendations. You can request recommendations if a matching assignment group is not available or is incorrect for a vulnerable item (VI).

**Before you begin**

Role required: sn_vul.remediation_owner

**Procedure**

1. Navigate to **Vulnerability Response > Vulnerable Items** and open a VI. The item must be in the Open, Deferred, Under investigation, or Awaiting implementation state.
2. Click the recommend icon ( ) next to the Assignment group field for assignment suggestions for that VI.

3. From the Assignment Group Recommendations dialog box, select a recommendation that is based on the confidence score. The confidence score predicts how relevant the match is for the VI. For more information, see Machine Learning solutions for Vulnerability Response.

4. Click Assign.

Results
The selected group appears in the Assignment group field and the Assignment type changes to Recommendation.

Request assignment group recommendations for multiple vulnerable items
Use Vulnerability Assignment Recommendations to view the assignment group recommendations for multiple vulnerable items (VIs) using a bulk edit. When multiple VIs are selected, a prediction is performed on a random sample of the selected VIs.

Before you begin
Role required: sn_vul.remediation_owner

About this task
The recommendations and their confidence scores may differ slightly between invocations, based on the samples taken from the selected VIs. The confidence score evaluates whether the system is confident that the recommended assignment group is suited to resolve the vulnerability. Use the assignment_recommendation_batchsize system property to set the batch size when you request Vulnerability Assignment Recommendations for vulnerability groups (VGs) and VIs using the bulk edit option. The default value of this system property is set for optimum prediction performance.

Note: If you increase the default value, the response time for Vulnerability Assignment Recommendations for these cases might change.

Procedure
1. Navigate to Vulnerability Response > Vulnerable Item and select multiple VIs. The items must be in the Open, Under investigation, or Awaiting implementation state.
2. Click **Bulk Edit**.

3. On the form, fill in the fields.

### Bulk Vulnerable Items form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record selection</td>
<td>Records to be selected for bulk edit.</td>
</tr>
<tr>
<td>Assignment group</td>
<td>Assignment group to set for the selected vulnerable items. To view the recommended assignment groups, click the recommend icon (💡) next to the field. Select a recommendation that is based on the confidence score and click <strong>Assign</strong>.</td>
</tr>
<tr>
<td>Work notes</td>
<td>Notes to be added.</td>
</tr>
</tbody>
</table>

4. Click **OK**.

**Results**
The selected group appears in the **Assignment group** field and the Assignment type changes to Recommendation for all the selected VIs.

**Request assignment group recommendations for a vulnerability group**

Use Vulnerability Assignment Recommendations to view assignment group recommendations for a vulnerability group (VG).

**Before you begin**
Role required: sn_vul.remediation_owner

**About this task**

Use the `assignment_recommendation_batchsize` system property to set the batch size when you request Vulnerability Assignment Recommendations for VGs and vulnerable items (VIs) using the bulk edit option. The default value of this system property is set for optimum prediction performance.

**Note:** If you increase the default value, the response time for Vulnerability Assignment Recommendations for these cases might change.
Procedure

1. Navigate to **Vulnerability Response > Vulnerability Groups** and select a VG. The group must be in the Open, Under investigation, or Awaiting implementation state.

2. Click the recommend icon (💡) next to the **Assignment group** field for the assignment group recommendations for the selected VG. The Assignment Group Recommendations dialog box displays the recommended assignment groups with the average confidence score for all the VIs in that group.

3. Select a recommendation from the Assignment group list based on the confidence score. The confidence score predicts how relevant the match is for the selected VG.

4. Click **Assign**. The selected group appears in the **Assignment group** field.

5. Save the vulnerability group with the updated information.

Results

All the VIs with the same assignment group as the VG are assigned to the selected assignment group. The Assignment type changes to Recommendation for the VG, as well as all the modified VIs.

**Requesting and approving an exception**

You can request to defer the remediation of a vulnerable item or vulnerability group for a specified period. For example, as a remediation owner, you can request an exception if a patch is not available for a machine. Approvers who have access can approve requests from other users.

You can request exceptions for the following:

- Request an exception for a vulnerable item
- Request an exception for a vulnerability group
- Request a bulk exception

You can also request policy exceptions using GRC: Policy and Compliance Management:
• Request an exception using GRC: Policy and Compliance Management
• Request a bulk exception using GRC: Policy and Compliance Management

Note:
Email notifications are sent at every stage of exception management, providing the status and other details of a request. For example, when an exception is requested, the requester receives an email confirming that the request is raised. The approver also receives an email stating that an exception has been requested.

Request an exception for a vulnerable item
Request an exception for a vulnerable item that cannot be remediated immediately. For example, as a remediation owner, you can request an exception if a patch is not available for a machine.

Before you begin
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Role required: sn_vul.remediation_owner

Procedure
1. Navigate to Vulnerability Response > Vulnerable Items > All and select the item that you want to request an exception for. The selected item must be in Open, Under Investigation, or Awaiting Implementation state.
2. On the Vulnerable Item form, click Request Exception.
3. On the form, fill in the fields.

Request Exception form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Until</td>
<td>Date on which the exception request expires. This date must be within the exception duration that is defined in the configuration.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Reason</td>
<td>Justification for requesting an exception.</td>
</tr>
<tr>
<td>Additional information</td>
<td>Details that are related to the reason why this request is being made.</td>
</tr>
<tr>
<td></td>
<td>Required field to be updated by the remediation owner.</td>
</tr>
</tbody>
</table>

4. Click **Request Approval**.

**Request an exception for a vulnerability group**

Request an exception to defer the remediation of a vulnerability group for a specified period if it cannot be remediated immediately.

**Before you begin**

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see **Assign the Vulnerability Response persona roles using Setup Assistant**. For more information about managing granular roles, see **Manage persona and granular roles for Vulnerability Response**.

Role required: sn_vul.remediation_owner

**Procedure**

1. Navigate to **Vulnerability Response > Vulnerability Groups > All** and select the group that you want to request an exception for.
   The selected group must be in the Open, Under Investigation, or Awaiting Implementation state.

2. On the Vulnerability Group form, click **Request Exception**.

3. On the form, fill in the fields.

**Request Exception form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Until</td>
<td>Date on which the exception request expires. This date must be within the exception duration that is defined in the configuration.</td>
</tr>
<tr>
<td>Reason</td>
<td>Justification for requesting an exception.</td>
</tr>
</tbody>
</table>
Field | Description
---|---
Additional information | Details that are related to the reason why this request is being made. This required field is to be updated by the remediation owner.

4. Click **Request Approval**.

**Request a bulk exception**

Use the bulk edit option to request an exception for multiple vulnerable items (VIs) instead of manually selecting each item.

**Before you begin**

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Role required: sn_vul.vulnerability_analyst

**About this task**

When multiple VIs are selected, a vulnerability group (VG) is formed with these items. See Bulk edit Vulnerability Response vulnerable items for more information on editing multiple VIs.

**Procedure**

1. Navigate to **Vulnerability Response > Vulnerable Items > All** and select the items that you want to request an exception for. The selected items must be in the Open, Under Investigation, or Awaiting Implementation state.

2. Click **Bulk Edit**.

3. On the form, fill in the fields.

**Vulnerable Item Bulk Edit form**

Field | Description
---|---
Record selection | Records that you selected for a bulk edit.
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>State of the vulnerable item. Select the Deferred state to request an exception for the selected items.</td>
</tr>
<tr>
<td>Reason</td>
<td>Substate for the State that you selected.</td>
</tr>
<tr>
<td>Short description</td>
<td>Name of the vulnerability group that you are creating.</td>
</tr>
<tr>
<td>Until</td>
<td>Ending date that you specify for your exception request.</td>
</tr>
<tr>
<td>Additional information</td>
<td>Further details that you want to mention to inform the approver about the reasons for your request.</td>
</tr>
<tr>
<td>Preferred solution</td>
<td>Solution that is targeted for remediating all the vulnerable items that you selected for a bulk edit.</td>
</tr>
<tr>
<td>Assignment group</td>
<td>Assignment group for the VI. You can select a group manually or use Assignment Recommendations if that feature is enabled.</td>
</tr>
<tr>
<td>Work notes</td>
<td>Notes to be added.</td>
</tr>
</tbody>
</table>

4. Click **OK**.

A VG is created containing the VIs that you selected. This VG is submitted for approval.

**Request an exception using GRC: Policy and Compliance Management**

Starting with Version 10.3, request policy exceptions using the GRC policy exception management capability in Version 10.1 of the Policy and Compliance Management application from within Vulnerability Response.

**Before you begin**

Before you can use the Policy Exception Integration to request policy exceptions, you must download the GRC: Policy and Compliance Management application from the ServiceNow Store.

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see **Assign the Vulnerability Response persona roles using Setup Assistant**. For more
information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Role required: sn_vul.remediation_owner

Procedure

1. Navigate to Vulnerability Response > Vulnerable Items (or Vulnerability Groups) > All, and open the item or group for which you want to request an exception.
   The selected item or group must be in Open, Under investigation, or Awaiting implementation state.

2. On the selected form, click Request Exception.

3. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Request Exception form</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
</tr>
<tr>
<td>Policy</td>
</tr>
<tr>
<td>Control objective</td>
</tr>
<tr>
<td>Valid from</td>
</tr>
<tr>
<td>Valid until</td>
</tr>
<tr>
<td>Reason</td>
</tr>
</tbody>
</table>

Note: The number of days that the policy exception is valid cannot exceed the Maximum exception duration (days) that you set for the policy in Policy and Compliance. For more information, see .

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>Details that are related to the reason why this request is being made. This mandatory field must be filled in by the remediation owner.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

For more information on the Policy Exception Integration and the hand-off between the remediation owner and the compliance manager, see Policy Exception Integration with Vulnerability Response.

**Request a bulk exception using GRC: Policy and Compliance Management**

Select a group of vulnerable items and submit a bulk exception.

**Before you begin**

Before you can use the Policy Exception Integration to request bulk exceptions, you must download the GRC: Policy and Compliance Management application from the ServiceNow Store.

**Note:** To use this feature, you must upgrade GRC: Policy and Compliance Management before upgrading Vulnerability Response. If you have already upgraded Vulnerability Response before GRC: Policy and Compliance Management, and want to use this feature, you must perform the upgrade procedures again in the correct order.

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Role required: sn_vul.remediation_owner

**Procedure**

1. Navigate to **Vulnerability Response > Vulnerable Items > All** and select the items that you want to request an exception for.
   The selected items must be in Open, Under investigation, or Awaiting implementation state.

2. Click **Bulk Edit**.

3. On the form, fill in the fields.
**Vulnerable Item Bulk Edit form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record selection</td>
<td>Records that you selected for a bulk edit.</td>
</tr>
<tr>
<td>State</td>
<td>State of the vulnerable item. Select the Deferred state to request an exception for the selected items.</td>
</tr>
<tr>
<td>Short description</td>
<td>Name of the vulnerability group that you are creating.</td>
</tr>
<tr>
<td>Preferred solution</td>
<td>Solution that you are targeting for remediating all the vulnerable items that you selected for bulk edit.</td>
</tr>
<tr>
<td>Assignment group</td>
<td>Assignment group for the VI. You can select a group manually or use Assignment Recommendations if that feature is enabled.</td>
</tr>
<tr>
<td>Work notes</td>
<td>Notes to be added.</td>
</tr>
</tbody>
</table>

4. Click **OK**.
   A vulnerability group is created with the selected vulnerable items.

5. On the form, fill in the fields.

**Request Exception form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>Vulnerability Management policy that you are requesting an exception for.</td>
</tr>
<tr>
<td>Control objective</td>
<td>Control objectives that are associated with the policy that you selected. If a policy is not selected, all the control objectives are listed.</td>
</tr>
<tr>
<td>Valid from</td>
<td>Date when the exception will start. The default value is the current date. This date cannot be in the past.</td>
</tr>
<tr>
<td>Valid until</td>
<td>Date that the policy exception expires and the state of the</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vulnerable item or group changes from Deferred to Open.</td>
</tr>
</tbody>
</table>

**Note:** The number of days that the policy exception is valid cannot exceed the **Maximum exception duration (days)** that you set for the policy in GRC: Policy and Compliance Management. For more information, see .

<table>
<thead>
<tr>
<th>Reason</th>
<th>Reason for requesting an exception.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>Details that are related to the reason why this request is being made. This mandatory field must be filled in by the remediation owner.</td>
</tr>
</tbody>
</table>

6. Click **Submit**.

   For more information on the Policy Exception Integration and the hand-off between the remediation owner and the compliance manager, see Policy Exception Integration with Vulnerability Response.

### Approve an exception request

Approve exception requests for vulnerable items or vulnerability groups that can't be remediated immediately. You must assess these requests for risk and then approve them for deferral until they can be remediated.

### Before you begin

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Role required: sn_vul.exception Approver

### Procedure

1. Navigate to **Vulnerability Response > Vulnerabilities > My Approvals**.
2. Select a request from your queue.
3. Approve or reject the request with appropriate comments.
Working with an exception rule

Version 12.0: You can request an exception for vulnerabilities, vulnerable items (VIs), or configuration items (CIs) that can’t be remediated or deferred immediately. By automating the VI deferral process, you can defer the matching VIs based on the rule when the system identifies them.

You can perform the following tasks for an exception rule:

- Create an exception rule
- Approve an exception rule request
- Activating an exception rule
- Reopen an exception rule
- Update an approved exception rule
- Delete an exception rule

Create an exception rule

Version 12.0: Create a rule to automatically request an exception for a specific condition for a group of vulnerable items (VIs), such as a rule with a condition that is based on the vulnerability severity of these VIs. With this rule, you can defer new and existing VIs automatically if they match the approved rule condition.

Before you begin
Role required: sn_vul.vulnerability_admin

About this task
The rule is applied from the "Valid from" until the "Valid to" date. The vulnerable group (VG) is created when the rule is approved. The grouping method for this VG is known as exception rules. The VG is created in the Deferred state. You can’t close, reopen, or delete this VG. New and reopened VIs are deferred and added to this VG from the "Valid from" date until the group expires on the "Valid to" date.

⚠️ Note:
Email notifications are sent at every stage of the exception rule work flow. These emails provide the status and other details of a request. For example, when an exception rule is requested, the requester receives an email that confirms that the request is submitted.

⚠️ Note: If the rule is rejected, you can reopen it in the Draft state, update it, and then resubmit it for approval.
Procedure
1. Navigate to **Vulnerability Response > Administration > Exception Rules**.
2. On the Exception Rule new record page, click **New** to create a rule.
3. On the form, fill in the fields.

**Exception Rule form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the exception rule.</td>
</tr>
<tr>
<td>Valid from</td>
<td>Date from which this rule is active to defer the VIs.</td>
</tr>
<tr>
<td>Valid to</td>
<td>Date from which the vulnerability group (VG) stops accepting new VIs.</td>
</tr>
<tr>
<td>Reason</td>
<td>Reason to create this exception rule.</td>
</tr>
<tr>
<td>Assignment group</td>
<td>Group that the VG that was created for tracking the deferred VIs is assigned to.</td>
</tr>
<tr>
<td>Additional information</td>
<td>Additional information that the requester wants to provide to the approver. This information is populated in the description field of the VG.</td>
</tr>
<tr>
<td>Condition</td>
<td>Filter condition for the VIs that can be defined while processing the VIs.</td>
</tr>
<tr>
<td>Execute on existing data</td>
<td>Option that enables you to run this rule on existing data the first time that this rule is run.</td>
</tr>
<tr>
<td>Workflow stage</td>
<td>Current approval status of the exception rule.</td>
</tr>
<tr>
<td>State</td>
<td>State of the exception rule.</td>
</tr>
<tr>
<td>Execution order</td>
<td>Unique order for each exception rule.</td>
</tr>
<tr>
<td>Deferred until</td>
<td>Date until when the VGs and VIs are deferred. On this date, the created VG is closed, all the VIs move out of the group, and group rules are reapplied.</td>
</tr>
</tbody>
</table>
4. Add the assignment group when you are creating the rule.

5. Submit the form for approval.
   The status of the request changes to In review. Until you submit the exception rule, it remains in the Draft state.

**Approve an exception rule request**

Version 12.0: Assess exception rule requests from users so that you can approve or reject these requests.

**Before you begin**

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Role required: sn_vul.exception_approver

**About this task**

Exception approver level 1 user group members can approve the level 1 exception rule requests. Similarly, exception approver level 2 user group members can approve the level 2 exception rule requests. Both the user groups inherit the exception approver role by default.

**Procedure**

1. Navigate to Vulnerability Response > Vulnerabilities > My Approvals.
2. Select a request from your queue.
3. Approve or reject the request with and explain why you approved or rejected the request.

After an exception rule is approved, a vulnerability group (VG) is created in the Deferred state by default. Starting from the "Valid from" date, this rule runs on all the VIs that are created and also on the ones that are moved from the Closed to the Open state. VIs that match the defined conditions are added to the VG and deferred for the specified period.

**Note:** If the rule is rejected, you can reopen it in the Draft state, update it, and then resubmit it for approval.

**Activating an exception rule**

Version 12.0: A rule is activated on its "Valid from" date. After activation, it automates the exception process for vulnerable items (VIs).
The exception rule follows this life cycle:

1. The new vulnerable items (VIs) that you create or reopen, and that meet the specified condition, are deferred. If you enable the Execute on existing data option when you run the exception rule for the first time, all the active and non-deferred VIs that match the exception rule condition are moved to the newly created vulnerability group (VG) and its state is changed to Deferred.

2. If a newly created VI matches the exception rule condition, it is moved to the deferred VG that is associated with the rule and the group rule is not run on it.

3. On the "Valid from" date, existing VIs are added if you enable the Execute on existing data option.

4. The VG stops accepting new VIs when the rule expires on the "Valid to" date. The VG remains in existence until the "Deferred until" date.

5. The exception rule expires on the "Valid to" date.

**Reopen an exception rule**

Version 12.0: Reopen an exception rule that has been rejected, but you want to resubmit. Reopening the rule moves it to the Draft state.

**Before you begin**
Role required: sn_vul.vulnerability_admin

**About this task**
You can then update and resubmit the rule for approval.

**Procedure**
1. Navigate to **Vulnerability Response > Administration > Exception Rules**.
2. Find the rule that you want to reopen and click **Reopen**.
3. Update the form and resubmit it for approval.

**Update an approved exception rule**

Version 12.0: Cancel an approved rule to be able to update it. For example, before you can modify any dates or add a condition to an approved rule, you must cancel it so that the vulnerability group (VG) is deleted, and the vulnerable items (VIs) move to the Open state.

**Before you begin**
Role required: sn_vul.vulnerability_admin
About this task
Group rules are reapplied to these VIs. Submit the rule after making the changes so that it goes through the approval process once again.

Procedure
1. Navigate to Vulnerability Response > Administration > Exception Rules.
2. Open the exception rule that you want to cancel and click Cancel.
3. In the Cancel Rule dialog box, click Cancel rule.
   The rule moves back to the Draft state and the associated VG is deleted. The related VIs are reopened, and group rules are applied to the individual VIs.

Delete an exception rule
Version 12.0: Delete an exception rule that is not required anymore. For example, you can delete a rule if you don't want to defer a vulnerable item (VI) during ingestion.

Before you begin
Role required: sn_vul.vulnerability_admin

About this task
Deleting a rule cancels the associated vulnerability group (VG). The related VIs are reopened, and group rules are applied to the individual VIs.

Procedure
1. Navigate to Vulnerability Response > Administration > Exception Rules.
2. Open the exception rule that you want to delete and click Delete.
3. In the Delete Rule dialog box, click Delete rule to delete the selected rule.
   The associated VG is also deleted. The related VIs are reopened, and group rules are applied to the individual VIs.

Marking and approving a false positive
Vulnerable items (VIs) and vulnerability groups (VGs) can be marked as false positives. Approvers with write access can approve such requests from other users.

- Mark as a false positive
- Bulk edit for false positive
- Approve a false positive
Note:

Email notifications are sent at every stage of the false positive workflow, providing the status and other details of a request. For example, when a VI or VG is marked as a false positive, the requester receives a confirmation email. Simultaneously, the approver receives an email stating that a VI or VG has been marked as a false positive.

Mark as a false positive

Mark a vulnerable item (VI) or vulnerability group (VG) as a false positive if the warning given by the scanner is not actually an issue. For example, if a configuration item has been decommissioned but the scanner is still raising an issue related to it, mark it as a false positive.

Before you begin
Role required: remediation owner
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure

1. Navigate to Vulnerability Response > Vulnerable Items (or Vulnerability Groups) > All.
2. Open the VI or VG you want to mark as a false positive and click Mark as False Positive. The VI or VG must be in an Open state.
3. On the False Positive form, enter details in Additional information and click Request Approval.
   The request is sent for approval and the State of the VI or VG changes to In Review.

Bulk edit for false positive

Use bulk edit to mark multiple vulnerable items (VIs) as false positive. If multiple VIs are selected, a vulnerability group is formed with these items. See Bulk edit Vulnerability Response vulnerable items for more information on editing VIs.

Before you begin
Role required: remediation owner
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response
application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure
1. Navigate to Vulnerability Response > Vulnerable Items > All and select the items you want to mark as false positive. The selected items must be in Open, Under investigation, or Awaiting implementation state.
2. Click Bulk Edit.
3. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record selection</td>
<td>Records to be selected for bulk edit.</td>
</tr>
<tr>
<td>State</td>
<td>State of the vulnerable items. Select Closed to mark as false positive.</td>
</tr>
<tr>
<td>Reason</td>
<td>Substate for the State that was selected. If you selected Closed as the State, select False Positive here to mark as false positive.</td>
</tr>
<tr>
<td>Short description</td>
<td>Name of the vulnerability group being created.</td>
</tr>
<tr>
<td>Additional information</td>
<td>Any further details you want to mention to inform the approver about the reasons for your request.</td>
</tr>
<tr>
<td>Preferred solution</td>
<td>Solution targeted for remediating all the vulnerable items selected for bulk edit.</td>
</tr>
<tr>
<td>Assignment group</td>
<td>Assignment group for the VI. Select manually, or using Assignment Recommendations if it is enabled.</td>
</tr>
<tr>
<td>Work notes</td>
<td>Notes to be added.</td>
</tr>
</tbody>
</table>

4. Click OK.
A new vulnerability group is created containing the selected VIs, and this group is sent for approval.
Approve a false positive

As a false positive approver, you can approve false positive requests from other users.

Before you begin

Role required: false_positive_approver

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure

1. Navigate to Vulnerability Response > Vulnerabilities > My Approvals.
2. Select a request from your queue.
3. Approve or reject the request with appropriate comments.

⚠️ Note: A false positive can be time bound. Only the approver can set the end date.

Vulnerability Response integrations

Vulnerability Response includes support for third-party integrations. Included in this section are some basic guidelines for developing your own integrations.

Third-party integrations

Vulnerability integrations help enrich the vulnerability data on your instance by retrieving data from external systems and vendors.
Your enterprise environment

1. Third-party detection vulnerability scanners
   - Scanner searches for known vulnerable assets, activities, and traffic on your network.
   - Data found by scanner is imported into Now Platform Vulnerability Response.

2. Servicenow environment
   - Asset (1)
   - Vulnerability Response
Third-party integrations are treated separately. If more than one third-party integration application is in use in your environment there is no vulnerable item (VI) deduplication across integrations. For example, VI deduplication between Rapid7 and Qualys is not available.

However, mismatches in detection count between a third-party scanner (for example, Qualys) to VIs in your ServiceNow instance are expected, since we dedupe across IPs, ports and so on.

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Vulnerability Response supports the following third-party integrations:

- **Microsoft Threat and Vulnerability Management Integration**
  For information on the installation and configuration of the Microsoft Threat and Vulnerability Management Integration, see Install and configure the Vulnerability Response Integration with the MS TVM application using Setup Assistant.

- **Qualys Vulnerability Integration**
  For information on the installation and configuration of the Qualys Vulnerability Integration, see Install the Qualys Vulnerability Integration.

- **Rapid7 Vulnerability Integration**
  For information on the installation and configuration of the Rapid7 Vulnerability Integration, see Install and configure the Rapid7 Vulnerability Integration.

**Note:** During import, CVE records, not already present, are created as NVD records and referenced in third-party entries for Qualys and Rapid7, by default.

The template integration for either Qualys or Rapid7 cannot be deleted. Disable it instead.

- **Starting with v12.1 of Vulnerability Response, the The Tenable Vulnerability Integration developed by ServiceNow is available. See Install and configure the Vulnerability Response Integration with Tenable application using Setup Assistant and Configure the Tenable Vulnerability Integration using Setup Assistant for more information.**

- **Tenable for Vulnerability Response**
Note: The Tenable for Vulnerability Response application is created and maintained by Tenable. See Tenable for Vulnerability Response to view their documentation.

- **Shodan Exploit Integration**
  For information on the installation and configuration of the Shodan Exploit Integration, see Install and configure the Shodan Exploit Integration for Security Operations.

- **Microsoft Security Response Center Solution Integration**
  The Microsoft Security Response Center Solution Integration is available with Vulnerability Solution Management. For information on the installation and configuration of the Microsoft Security Response Center Solution Integration, see Install the Solution Management for Vulnerability Response application. You can configure the Microsoft Security Response Center Solution Integration from within Setup Assistant.

- **Red Hat Solution Integration**
  Starting with v10.3 of Vulnerability Response, the Red Hat Solution Integration is available with Vulnerability Solution Management. See Install the Solution Management for Vulnerability Response application. You can configure the Red Hat Solution Integration from within Setup Assistant.

- **Starting with Vulnerability Response v13.0, National Vulnerability Database (NVD) integrations are available separately from the ServiceNow Store. See Understanding the NVD integrations for more information on this application.**

- **Prior to Vulnerability Response v13.0, Vulnerability Response and Application Vulnerability Response included the National Vulnerability Database (NVD) integrations. See Managing NVD, CWE, and third-party data libraries for more information.**

**Manually created integrations**
You can add other integrations that are not available as ServiceNow Store applications, as needed. See Manually create a vulnerability integration for more information.

**Understanding the NVD integrations**
The NVD integrations use data imported from the NIST National Vulnerability Database (NVD) product to help you determine the impact and priority of flaws in your code.
Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

The NIST NVD collects both Common Vulnerabilities and Exposures (CVE) and Common Platform Enumeration (CPE) data and makes that data available to the Now Platform®. It easily integrates with Vulnerability Response to map CVE and CPE vulnerabilities enriching the data in your instance.

There is a configured run-as user for each integration record. The default value for this user is VR.System. Do not change this value.

Every day, the NIST National Vulnerability Database Integration - API (CVE only) integration is invoked automatically as a scheduled job. You can also execute individual scheduled jobs manually. Scheduled jobs simplify the vulnerability remediation life cycle by keeping the instance synchronized with other vulnerability management systems.

Available versions

<table>
<thead>
<tr>
<th>Release version</th>
<th>Release Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Response Integration with NVD v1.0</td>
<td>Vulnerability Response Integrations Release Notes</td>
</tr>
</tbody>
</table>

NVD integrations

To view the NVD integrations, navigate to Vulnerability Response or Application Vulnerability Response > Administration > Integrations.

The following integrations are included in the base system.

⚠ Note: Only the NIST National Vulnerability Database Integration - API (CVE only) integration is active, by default.

NVD integrations

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST National Vulnerability Database</td>
<td>Retrieves NIST NVD vulnerability data (CVE) and enriches your Vulnerability Response or Application Vulnerability Response data. This integration is set to run daily automatically.</td>
</tr>
</tbody>
</table>
NVD integrations (continued)

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration - API (CVE only)</td>
<td>Retrieves CVE and CPE data from NIST NVD. This integration is set to run weekly and is inactive by default. To activate this integration, see Activate the NIST National Vulnerability Database - API CVE CPE Integration.</td>
</tr>
<tr>
<td>NIST National Vulnerability Database Integration - API (CVE and CPE)</td>
<td></td>
</tr>
</tbody>
</table>

For integration run statuses see, View the NVD integration import run status.

To view data in third-party vulnerabilities, see View Vulnerability Response vulnerability libraries.

Preparing for the NVD integrations

A successful integration requires planning and careful execution of pre-integration tasks. Prepare for the integration by performing these tasks. The NVD integrations assume that you are familiar with the NIST National Vulnerability Database (NVD).

Before you begin
Role required: admin

About this task

Note: Before running the NVD integrations, make any necessary configuration changes based on your requirements.

- There is a configured run-as user for each integration record. The default value for this user is VR.System. Do not change this value.

Install the ServiceNow® Vulnerability Response Integration with NVD application

Before you run the integration on your instance, the installation and configuration steps must be completed so the NIST National Vulnerability Database (NVD) product properly integrates with Vulnerability Response. This application is available as a separate subscription.

Before you begin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.
Note: This process applies only to applications downloaded to production instances. If you’re downloading applications to sub-production or development instances, it’s not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

<table>
<thead>
<tr>
<th>Setup tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that the Vulnerability Response application is installed and activated.</td>
<td>To verify that this application is activated, navigate to Subscription Management &gt; Subscriptions in your instance. The list displays the subscriptions your organization has purchased. If the application is not installed and activated see, Install and configure Vulnerability Response.</td>
</tr>
<tr>
<td>Verify that you have the required ServiceNow roles for your instance.</td>
<td>The following roles are required for installation, configuration, and verification of expected results:</td>
</tr>
<tr>
<td></td>
<td>• If not already assigned, the System Administrator [admin] installs the application and assigns users to the Vulnerability Manager in Vulnerability Response or the App-Sec Manager group in Application Vulnerability Response. For information on Group roles in Vulnerability Responsesee, Manage persona and granular roles for Vulnerability Response. For information on group roles in Application Vulnerability Response see Manage Application Vulnerability Response user groups and roles.</td>
</tr>
<tr>
<td></td>
<td>• The Vulnerability Manager or App-Sec Manager oversees configuration and verifies expected results.</td>
</tr>
</tbody>
</table>

Role required: admin
Procedure

1. Log in to the instance you want to install the NVD integrations on.
2. Navigate to the ServiceNow Store.
3. In the ServiceNow Store, search for the Vulnerability Response Integration with NVD application.
4. Click the application tile. Detailed information about the application you are installing is displayed.
   
   Note: Consider reading the Other Requirements and Dependencies sections, as applicable.
5. Click Request App and enter your Now Support login credentials.
6. Click Get.
7. Enter the Instance Name and Reason for the Instance, and click Validate Instance.
8. Click Request. You will receive an email with detailed installation instructions.
10. Locate the application, select it, and click Install. Your application is automatically installed on your instance.

What to do next

Note: No configuration is required for the NVD integrations.

After initial installation, for modifications refer to Optional NVD integration modification and activities.

Optional NVD integration modification and activities

Configure optional modifications specifically for the NVD integrations.

Note: Changing other NVD integration settings, other than the ones listed here, requires advanced ServiceNow and Vulnerability Response expertise and is beyond the scope of the product documentation.

Perform a manual NVD integration import

If your initial import failed, or you do not want to wait for the scheduled initial import, you can perform a full data import independent of the daily or weekly scheduled job.
Before you begin
Role required: sn_vul.vulnerability.admin

Note: The NIST National Vulnerability Database Integration - API (CVE and CPE) Integration is inactive by default. See Activate the NIST National Vulnerability Database - API CVE CPE Integration for more information.

Procedure
1. Navigate to Vulnerability Response or Application Vulnerability Response > Administration > Integrations.
2. Choose and integration, for example, the NIST National Vulnerability Database Integration - API (CVE only) integration.
3. Click Execute Now.

Note: If the NIST National Vulnerability Database Integration - API (CVE and CPE) Integration is activated, CPE data is stored in the Vulnerable Software related list of the NVD vulnerability entry. See Vulnerability Response vulnerability form fields.

4. For integration run statuses see, View the NVD integration import run status.

View the NVD integration import run status
Use the Vulnerability Integration Runs related list to verify the success of your integration runs, locate any issues, and inform your remediation decisions.

Before you begin
To view the NVD integration import run status:

- Vulnerability Response and the Vulnerability Response integration with NVD integration application must be installed and configured.
- The NVD integration imports must be running. The NIST National Vulnerability Database Integration - API (CVE only) integration runs by default.

Note: The NIST National Vulnerability Database Integration - API (CVE and CPE) integration is inactive by default. See Activate the NIST National Vulnerability Database - API CVE CPE Integration for more information.

Role required: sn_vul.vulnerability.admin or App-Sec Manager
Procedure

1. Navigate to Vulnerability Response or Application Vulnerability Response > Administration > Integrations.
2. Select an integration.
3. Click the Vulnerability Integration Runs related list.
4. Verify that all imports have succeeded.

Trouble?
The most common causes for a failed run include:

- Network interruption.
- An issue in the data transfer resulting in corrupted data during the transform.

If you encounter any of these conditions, click Execute Now, and rerun the integration.

Activate the NIST National Vulnerability Database - API CVE CPE Integration

If you want to ingest Common Platform Enumeration (CPE) data in addition to Common Vulnerabilities and Exposures (CVE) data, you can perform a full data import with a weekly scheduled job.

Before you begin
Role required: sn_vul.vulnerability.admin or App-Sec Manager
The NIST National Vulnerability Database Integration - API (CVE and CPE) Integration captures (CPE) data that includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name. This information is stored in an NVD vulnerability entry record related list.

Procedure

1. Navigate to Vulnerability Response or Application Vulnerability Response > NVD > Integrations.
2. Choose the NIST National Vulnerability Database Integration - API (CVE and CPE) Integration.
3. Select the Active checkbox.

Note: The integration is pre-configured to run weekly. Changing any other integration parameter requires both ServiceNow and Vulnerability Response expertise and could result in incomplete data.
The **Import since** date field in the NIST National Vulnerability Database Integration - API (CVE and CPE) Integration is set to January 1, 2020, by default.

To retrieve historical data during your initial import from the NVD scan, set a start date in the NIST National Vulnerability Database Integration - API (CVE and CPE) Integration record.

**a.** Navigate to **Vulnerability Response > Administration > Integrations**

**b.** Select NIST National Vulnerability Database Integration - API (CVE and CPE) Integration.

**c.** Set the **Import since** field to the earliest date you want to retrieve. Each successful import resets this date to that day's date and time.

**4.** Click **Execute Now** to perform an initial full import integration run. Once the initial import is complete, scheduled imports of delta data resume.

**5.** For integration run statuses see, **View the NVD integration import run status**.

### Understanding the Qualys Vulnerability Integration

Qualys Cloud Platform sensors collect the data and automatically send it to the Qualys Cloud Platform application, which continuously analyzes and correlates the information. It easily integrates with Vulnerability Response as the Qualys Vulnerability Integration to map vulnerabilities to CIs and business services to determine impact and priority of potentially malicious threats.

Configure your Qualys Vulnerability Integration using **Vulnerability > Administration > Setup Assistant** to make data retrieval more flexible and scalable.

If you have multiple deployments of the Qualys Cloud Platform application, you can add an integration for each deployment. Assets, identified by multiple third-party deployments and their vulnerabilities, are consolidated and reconciled with your CMDB. This consolidation happens even when scan processes overlap between the multiple deployments. Data sourced from each deployment is identified and available in a single instance of Vulnerability Response. Qualys vulnerability integration Knowledge Base records are normalized across deployments, ensuring that instances of the same vulnerability across deployments are treated as the same vulnerability.

**Note:** You cannot delete the original vulnerability integration but you can disable it. Integrations created from disabled templates are disabled by default.
There is a configured run-as user for each integration record. The default value for this user is `VR.System`. Do not change this value.

**Note:** While the Qualys Vulnerability Integration creates integrations for Appliance List, Asset Group, Dynamic Search List, and Static Search List, they are not required for normal operation.

### Available versions for Paris

<table>
<thead>
<tr>
<th>Release versions with Paris</th>
<th>Release Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualys Vulnerability Integration v12.1</td>
<td>Vulnerability Response integrations release notes</td>
</tr>
<tr>
<td>Qualys Vulnerability Integration v12.0</td>
<td>For compatibility information, see KB0856498</td>
</tr>
<tr>
<td>Qualys Vulnerability Integration v11.1</td>
<td>Vulnerability Response Compatibility Matrix</td>
</tr>
<tr>
<td>Qualys Vulnerability Integration v11.0</td>
<td>and Release Schema Changes</td>
</tr>
<tr>
<td>Qualys Vulnerability Integration v10.3</td>
<td></td>
</tr>
<tr>
<td>Qualys Vulnerability Integration v10.0</td>
<td></td>
</tr>
</tbody>
</table>

### Primary and Supporting Integrations

Qualys primary and supporting integrations enrich the vulnerability data on your instance by retrieving data from the Qualys Vulnerability Integration. A series of scheduled jobs invoke the integrations automatically. You can also execute them manually. Scheduled jobs simplify the vulnerability remediation lifecycle by keeping the instance synchronized with other vulnerability management systems. Primary and supporting integrations can be modified.

The Qualys integrations are executed as scheduled jobs. There is a configured run-as user for each integration record. The default value for this user is `VR.System`. This value should not be changed.

**Note:** Failing to set a valid run-as user results in multiple, often duplicate, data retrieval attachments on the data source records, every time the integration runs. Multiple attachments on the data source increase processing time, resulting in inconsistent transform results.

Qualys Cloud Platform integration tasks involve the following roles.
• sn_vul_qualys.admin — can read, write, and delete records
• sn_vul_qualys.user — can read and write records
• sn_vul_qualys.read — can read records

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Primary integrations
A primary integration is an entry point to the Qualys Cloud Platform interacting with the Qualys API invoked on a schedule.

View the primary integrations by navigating to Qualys Vulnerability Integration > Administration > Primary Integrations.

The following primary integrations are included in the base system.

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualys Appliance List Integration</td>
<td>Retrieves scanner appliance information from Qualys.</td>
</tr>
<tr>
<td>Qualys Asset Group Integration</td>
<td>Retrieves asset group information from Qualys. Asset groups are used to identify which scanner appliances to use for scanning matching configuration items.</td>
</tr>
<tr>
<td>Qualys Dynamic Search List</td>
<td>Synchronizes Qualys search lists for finding vulnerable entries, and retrieves dynamic list type records.</td>
</tr>
<tr>
<td>Integration</td>
<td></td>
</tr>
<tr>
<td>Qualys Host Detection Integration</td>
<td>Retrieves host and vulnerability data from Qualys and processes it in your instance. It coordinates the REST message calls to the Host List Detection API. The outputs of this integration are vulnerable items. Version 10.0: Qualys host tags are imported in this integration.</td>
</tr>
</tbody>
</table>
### Primary integrations (continued)

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualys Host List Integration</td>
<td>Retrieves authenticated and unauthenticated host scan data, and starting with v10.3, host tags from Qualys once a week and stores it in the Discovered Items module in your instance. Helps identify assets that haven't been scanned recently.</td>
</tr>
<tr>
<td>Qualys Knowledge Base</td>
<td>Retrieves Qualys knowledge base entries. The retrieved data is based on the date the vulnerabilities were updated by Qualys and since the last time the integration ran. This data is useful for populating historical data into your instance as well as ensuring the Qualys Identifiers (QIDs) are up to date.</td>
</tr>
<tr>
<td>Qualys Knowledge Base (Backfill)</td>
<td>Retrieves Qualys knowledge base entries. Scheduled to run after the Qualys Host Detection Integration. Updates your instance with any QIDs that were referenced in the Host Detection integration but did not exist in the system.</td>
</tr>
<tr>
<td>Qualys Static Search List Integration</td>
<td>Synchronizes Qualys search lists for finding vulnerable entries. Retrieves only static list type records.</td>
</tr>
<tr>
<td>Qualys Option Profile List Integration</td>
<td>Version 12.0: Retrieves option profiles from the Qualys product. Option profiles include scan settings which are required when you initiate scans from your Now Platform® instance.</td>
</tr>
<tr>
<td>Qualys Ticket Integration</td>
<td>Retrieves Qualys tickets and adds them to your instance. It coordinates the REST message calls to the ticket list API. There are often fewer tickets than Host Detections since Qualys settings can constrain the detections that result in a ticket.</td>
</tr>
</tbody>
</table>

### Supporting integrations

A supporting integration is a process that is not intended to run on a schedule nor without invocation by a primary integration.

View the supporting integrations by navigating to Qualys Vulnerability Integration > Administration > Supporting Integrations.

The following supporting integrations are included in the base system.
Supporting integrations

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Group Pagination Handler</td>
<td>Directs the pagination of the Asset Group Integration.</td>
</tr>
<tr>
<td>Host Detection Import Set Reprocess Integration</td>
<td>Handles reprocessing of the Host List import set created by the Host Detection Integration. Processes detections found for each host and results in vulnerable items being inserted or updated in your instance.</td>
</tr>
<tr>
<td>Host Detection Pagination Handler</td>
<td>Directs the pagination of the Host Detection Integration. The Host List Detection API coordinates REST calls for each page request to the server.</td>
</tr>
</tbody>
</table>

Search lists

Search lists are used in Qualys to create custom groups of vulnerabilities. You can save them and use for ticket creation and to customize vulnerability scans and reports. The Search Lists module allows you to download search list data from Qualys to your instance on a scheduled basis.

Search lists are pulled from Qualys using the Dynamic Search List Import and/or Static Search List Import data transformation maps. In each of these transforms, you can define schedules for performing the import.

Option profiles (v 12.0)

Starting with v12.0, Option profiles are available with Qualys scan settings. An option profile is required when you initiate a scan from your Now Platform.

Option profiles are imported from the Qualys product by the Option Profile List Integration. You might prefer to run the Option Profile List Integration after an import from the Search Lists Integrations, the Qualys Dynamic Search List and Qualys Static Search List Integrations so that you can see which search lists are associated with option profiles.

Asset groups

Asset groups are setup in the Qualys platform. Asset groups identify which scanner appliances are used for scanning matching IP addresses when a scan is initiated from the Now Platform.
Asset groups that have associated appliances are pulled from Qualys by the Asset Group List Integration.

Initiate the Appliance List Integration after you import asset groups to populate the Appliance name and Appliance status fields on the Qualys Default Applications records in your Now Platform.

Host tags

Version 10.3: All host tags are imported as part of the Qualys Host List integration. Host tags are used primarily for filtering in Vulnerability Response Assignment and Vulnerability Group Rules. They are displayed in the Discovered Item form.

Note: The Qualys Host List integration should be run prior to creating Assignment or Vulnerability Group Rules in Vulnerability Response so that all tags can be present in the rules and before vulnerable items are imported and grouped.

- Tag storage is not case sensitive. If a San Diego tag is created, then a SAN DIEGO tag cannot be stored in the Host tag table. “San Diego” and “SAN DIEGO” are considered to be the same host tag. Whichever tag was imported first wins.
- Using host tags as a Group Key in a Vulnerability Group Rule can have unexpected results. Host tags are intended for use only in the Condition builder.
- Host tags are controlled by the global system property sn_vul.import_host_tags. This property is set to true by default. Turning tags off turns them off across all instances.

Host tags (also called asset tags) are used for organizing and tracking the assets in your organization. You can assign tags to your host assets. Then, when launching scans, you can select tags associated with the hosts you want to scan. The Host Tags module allows you to download host tag data from Qualys to your instance on a scheduled basis.

Reopen resolved vulnerable items not closed by scans

Starting with v10.3, vulnerable items set to 'Resolved' in your Now Platform instance but not transitioned to 'Closed/Fixed' by the third-party integration runs are reopened if they are detected during rescans.

For Qualys detections, if the scanner continues to find VIs that were set to 'Resolved' but then not transitioned to 'Closed/Fixed' by subsequent scans, these VIs move back to 'Open' when the last found date is later than the Resolved date.
Data retrieval limitations

By default, there are no restrictions on how data is retrieved from Qualys. Many records can be related to low severity vulnerabilities that a customer is not willing to remediate using their vulnerability response process. Updating the corresponding REST message/method parameters can modify this behavior.

The REST message/method responsible for this update is **Qualys Host Detection – Standard/post**. To update the values, add a new HTTP Query Parameter to the post method with the following values:

- **Name**: severities
- **Value**: 3-5 (or whatever appropriate severities are desired)

Request apps on the Store

Visit the [ServiceNow Store](https://www.servicenow.com) website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the [ServiceNow Store version history release notes](https://www.servicenow.com).

Related information

Qualys REST messages

Preparing for the Qualys Vulnerability Integration

A successful integration requires planning and careful execution of pre-integration tasks. It is essential that you prepare for the integration by performing these procedures. The Qualys Vulnerability Integration assumes that you are familiar with and run Qualys Cloud Platform scans in your environment.

**Note:** Make any necessary configuration changes based on your requirements before running the integrations.

Important prerequisites

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see [Assign the Vulnerability Response persona roles using Setup Assistant](https://www.servicenow.com). For more information about managing granular roles, see [Manage persona and granular roles for Vulnerability Response](https://www.servicenow.com).

Validate your instance sizing based on the number of vulnerable items you expect to import. An undersized instance can lead to long load times. If you do not know the size of your instance, contact Customer Service and Support.
Use filtering to limit the number of items for initial import and phase your deployment by adjusting filters in subsequent imports.

**Actions to take**

- **Determine an initial start date** for Host Detection List Import integrations. Consider setting the **Start time** field to a few hours or days in the past. Ideally, choose the date of the last Qualys scan. The start date can include vulnerabilities discovered prior to using the vulnerability management solution. Set the earliest start time used to the start of your scanning cycle. So, if it takes a week before all hosts are scanned, set this value to a week prior to that time.

- **Add users to the roles** for admin, sn_vuln.admin, and sn_vul_qualys.admin. For more information see, [Assign a role to a user](Assign a role to a user).

- **There is a configured run-as user** for each integration record. The default value for this user is **VR.System**. Do not change this value.

- **If you do not use vulnerability calculators**, disable the default calculator, in addition to any others you have defined. Vulnerability calculators run every time a vulnerable item record is created or updated, and can impact initial import performance.

- **During the initial import of records**, certain notification-related business rules can cause many notifications to be generated, impacting performance. Prior to your initial import, **disable the business rules**.

- **If you wish to use a different scanner than the Qualys default**, see [set up scanner appliances](set up scanner appliances).

- **Have your Qualys server URL and authentication credentials ready.** The credentials must provide adequate permissions for retrieving knowledge, scan, and detection information for a Qualys subscription.

- **Version 10.3**: If you plan to use host tags in Vulnerability Response Assignment or Vulnerability Group Rules, ensure the Qualys Host List integration was run prior to creating rules.

**Install the Qualys Vulnerability Integration**

Before you run the Qualys Vulnerability Integration in your instance, you must install and configure the Qualys Vulnerability Integration application. This application is available as a separate subscription.

**Before you begin**

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.
Note: This process applies only to applications downloaded to production instances. If you’re downloading applications to sub-production or development instances, it’s not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Role required: admin to download and install the application

<table>
<thead>
<tr>
<th>Setup tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that the Vulnerability Response application is installed and activated.</td>
<td>To verify that it is activated, navigate to Subscription Management &gt; Subscriptions in your instance. The list displays the subscriptions your organization has purchased. If the application is not installed and activated see, Install and configure Vulnerability Response.</td>
</tr>
<tr>
<td>Get entitlements for the Qualys Vulnerability Integration application and download it to your Now Platform® instance.</td>
<td>If the application is not already downloaded on your instance, see Download an application from the ServiceNow Store for the first time.</td>
</tr>
<tr>
<td>Prepare for the integration.</td>
<td>See Preparing for the Qualys Vulnerability Integration.</td>
</tr>
</tbody>
</table>

Procedure

1. Navigate to **Vulnerability Response > Administration > Setup Assistant**.

   After a few moments, the applications that are available for installation on your instance are displayed.

2. Locate the **Qualys Vulnerability Integration** tile and click **Install**.

3. Follow the prompts in the Setup Assistant.

4. For more information about installing applications using Setup Assistant, see Install Vulnerability Response third-party applications using Setup Assistant.

What to do next

After you complete the installation in Setup Assistant, navigate to **Integration Configuration>Scanner Integrations** in Setup Assistant to continue with the configuration. If you want more information to supplement the prompts provided in Setup Assistant, see Configure the Qualys Vulnerability Integration using Setup Assistant.

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Optional Qualys modifications

Configure optional modifications and streamline some of the data specifically for the Qualys integration.

Create domain-separated imports for the Qualys Host Detection Integration

If you require imported host detection data to be in a specific domain, the user assigned to run the integrations must belong to that domain.

Before you begin
Role required: sn_qualys.admin and import_admin
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task
This set of tasks require coding or advanced ServiceNow expertise.

The import queues contain data attachments that the scheduled jobs (integrations) process. In a domain-separated environment, you must match the scheduled job with the correct import queue.

Procedure

1. Create a domain.

2. For every domain you create, create a user and assign the user to that domain.
   Think of this user as a run_as placeholder for the domain in, for example, the Qualys Host Detection Integration. It is the equivalent to the VR.System user in the global domain. This user needs access to data sources, transform maps, and vulnerability data.

   Note: Do not use this user for any other purpose.

3. In each domain, create a scheduled job by copying Scheduled Vulnerability Data Source Processor found under System Definition > Scheduled Jobs. Append the domain to the name to identify the scheduled job. Change the run_as user to the user you created in the previous step.
4. **Note:** Edit the following UI action so that the integration runs in the *run_as* user domain.

Edit the **Execute Now** UI action in the **Qualys Host Detection Integration** to add this code block to the top of the file.

**Example**

```java
//sys id below is of host detection integration
if(current.sys_id == "5d9cf0daff540300c68c9f783894fa4d") {
    current.run_as = gs.getUserID()
    ()
}
```

5. **Note:** Edit the following script includes so that integration run in the *run_as* user domain.

Edit the **VulnerabilityIntegrationUtils** script include method **addIntegrationRun** to add the highlighted code
6. Edit the `VulnerabilityIntegrationUtils` script include method `addProcessRun` to add the highlighted code.

   ```javascript
   addProcessRun: function(runGr, parameters) {
     var gr = new GlideRecord("sn_vul_integration_run");
     gr.initialize();
     varSysDomain = runGr.getValue("sys_domain");
     if (parameters) {
       var json = new global.JSON();
       var encodedParams = json.encode(parameters);
       gr.setValue("parameters", encodedParams);
     }
   }
   ```

7. Edit the `VulnerabilityIntegrationUtils` script include method `copyProcess` to add the highlighted code.

   ```javascript
   _copyProcess: function(intProcGr, isProcessErrored) {
     var copy = new GlideRecord("sn_vul_integration_process");
     copy.initialize();
     copy.setValue("sys_domain", intProcGr.getValue("sys_domain"));
     copy.setValue("integration_run", intProcGr.getValue("integration_run"));
     copy.setValue("parameters", intProcGr.getValue("parameters");
     copy.setValue("state", "new");
     var nextRetryDueOn = new GlideDate(time); 
     if (isProcessErrored) {
       copy.setValue("errors_retries", parseInt(intProcGr.getValue("errors_retries"))); 
       var nextRetryDueOn = 0; 
       if (intProcGr.getValue("next_retry_due_on") != "") 
         nextRetryDueOn = new GlideDate(intProcGr.getValue("next_retry_due_on"); 
       } else 
         nextRetryDueOn = new GlideDate(time); 
     var instance = new sn_vul.VulnerabilityIntegrationUtils().getScriptInstance(intProcGr); 
     var nextRetryDelay = intProcGr.getValue("nextRetryDelay") + 60; 
     if (parseInt(intProcGr.getValue("errors_retries"))) + 1 < intProcGr.getValue("maxRetries") 
       copy.setValue("next_retry_due_on", nextRetryDueOn.getValue()); 
     else 
       copy.setValue("retries", intProcGr.retries + 1); 
     copy.insert(); 
     return copy;
   }
   ```
8. Edit the **DataSourceVulnReportRefreshProcessor** script include method `_processFromDataSourceGroups` to change this original code:

   Original `_processFromDataSourceGroups` code

   ```javascript
   _processFromDataSourceGroups: function(payload, fileName) {
       var gr = new GlideRecord("sn_vul_int_data_src");
       gr.addQuery("sn_vul_integration", this.integrationGr.sys_id + "");
       gr.orderBy("ds_group_number");
       gr.query();
       var lastGroup;
       if (gr.getNextCount() == 0) {
           throw new Error("There are no data sources to provide data to.");
       }
       while (gr.next()) {
           var thisGroup = gr.getValue("ds_group_number");
           if (lastGroup == thisGroup & lastGroup !== undefined) {
               continue;
           } else {
               var ds = new GlideRecord("sys_data_source");
               if (ds.get(sys_data_source + ""))
                   continue;
               var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
               mgr.queueItem(ds, getUniqueValue(), fileName, payload, this.integrationProcessor, getUniqueValue(), this.integrationProcessor, getValue("sys_domain");
               gr.setValue("last_used", new GlideDateTime().getValue());
               gr.update();
               lastGroup = thisGroup;
           }
       }
   }
   ```

   To:

   **Edited `_processFromDataSourceGroups` code**

   ```javascript
   _processFromDataSourceGroups: function(payload, fileName) {
       var gr = new GlideRecord("sn_vul_int_data_src");
       gr.addQuery("sn_vul_integration", this.integrationGr.sys_id + "");
       gr.orderBy("ds_group_number");
       gr.query();
       var lastGroup;
       if (gr.getNextCount() == 0) {
           throw new Error("There are no data sources to provide data to.");
       }
       while (gr.next()) {
           var thisGroup = gr.getValue("ds_group_number");
           if (lastGroup == thisGroup & lastGroup !== undefined) {
               continue;
           } else {
               var ds = new GlideRecord("sys_data_source");
               if (ds.get(sys_data_source + ""))
                   continue;
               var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
               mgr.queueItem(ds, getUniqueValue(), fileName, payload, this.integrationProcessor, getUniqueValue(), this.integrationProcessor, getValue("sys_domain");
               gr.setValue("last_used", new GlideDateTime().getValue());
               gr.update();
               lastGroup = thisGroup;
           }
       }
   }
   ```

9. Edit the **VulnerabilityDSAttachmentManager** script include method, **queueItem**
to add the following highlighted code blocks

   ```javascript
   queueItem: function(dataSource, attachmentName, reportData, optIntegrationProcess, optDomain) {
       var gr = new GlideRecord(this._QUELE_TABLE);
       gr.initialize();
       gr.setValue("status", "NEW");
       gr.setValue("dataSource");
       gr.setValue("dataSource");
       if (optIntegrationProcess)
           gr.setValue("integration process", optIntegrationProcess);
       if (optDomain)
           gr.setValue("sys_domain", optDomain);
       var sysId = gr.insert();
   }
   ```
_processQueueEntry function

At this point, you are ready for domain-separated host detection imports.

**Note:** If you have multiple deployments of the Qualys Vulnerability Integration, repeat this process for each deployment.

**Disable the default vulnerability calculator if not used**

If you do not use vulnerability calculators, it is best to disable the default calculators in addition to any others you have defined. Vulnerability calculators run every time a vulnerable item record is accessed, and can impact instance performance.

**Before you begin**

Role required: admin
Procedure
1. Navigate to Vulnerability > Administration > Vulnerability Calculators.
2. Open the Vulnerability Impact group.
3. Open the Score and Service Based Impact calculator.
4. Deselect the Active field to deactivate the calculator.
5. Click Update.

Disable notification-related business rules prior to initial record import
During the initial import of records, certain notification-related business rules can generate many notifications, impacting performance. These business rules should be modified to disable them during the import.

Before you begin
Role required: admin

Procedure
1. Navigate to System Definition > Business Rules.
2. Search for Affected ci notifications.
3. Open the business rule and insert this condition: current.sys_class_name != "sn_vul_vulnerable_item".
4. Click Update.
5. Repeat this procedure for the following business rules:
   - Affected cost center notifications
   - Affected group notifications
   - Affected location notifications

Note: After the completion of the initial record import, you have the option of re-enabling these business rules. However, consider leaving them disabled. They can generate large numbers of notifications and impact the performance of your instance.

Modify an initial start date
During installation using Setup Assistant, you set an initial start date for the Qualys integrations. You can reset that start date in Setup Assistant or from the primary integration as shown below.
Before you begin
Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure
1. Navigate to Qualys Vulnerability Integration > Administration > Primary Integrations.
2. Click Qualys Host Detection Integration.
3. Click Integration Details.
4. Set the Start time field to a value in the past, so all scanned and detected vulnerabilities since that time are detected.
   If you configured Qualys using Setup Assistant, the Start time field is pre-filled, initially to three months prior today’s date, and subsequently to today’s date.
   
   Note: Consider setting the value to a maximum of a month in the past. This keeps large amount of data from exceeding the Qualys API rate limitations, as well as triggering execution timeouts.
5. Click Submit or Update.
6. Optional: Click Execute Now to run immediately.

Advanced Qualys configurations and modifications
Configure advanced optional modifications and streamline some of the data specifically for the Qualys integration. Most of these modifications require coding or advanced ServiceNow or Qualys Cloud Platform expertise.

Modify the Qualys to ServiceNow priority and state mapping values
Modify mapping values for priority and state for your requirements.

Before you begin
Role required: admin
About this task
This is an advanced customization option.

Procedure
1. Navigate to System Definition > Business Rules.
2. Search for Map Qualys Values and open it.
3. Click the Advanced tab.
4. Modify per your requirements. The most common modifications include adding new state values or revising criticality or priority.
5. Click Update.

Restrict the ability to write to a record based on an assignment group
You can restrict write/read rights on records based on membership to an assigned group. Modify conditions and script based on specific requirements.

Before you begin
Role required: security_admin (elevated role from admin)
⚠️ Note: This action is performed in the Vulnerability scope.

Procedure
1. Navigate to System Security > Access Control (ACL).
2. Search for ACLs that start with sn_vul.
3. Choose an Access Control record, for example, sn_vul_vulnerable_item, Operation write.
4. Check the Advanced box in the record, if necessary, to display the Role entries.
5. Modify the Role script for your requirements.
Script Example of modifying access by group.

```javascript
answer = (current.assigned_to == gs.getUserID() ||
           isMemberOfForScopedApp(current.assignment_group));
// Note: standard 'isMemberOf' does not work within Scoped App
// gs.getUser().isMemberOf(current.assignment_group);
function isMemberOfForScopedApp(groupID){
  var result = false;
  if (groupID != ''){
    var userID = gs.getUserID();
    var now_GR = new GlideRecord("sys_user_grmember");
    now_GR.addQuery("group", groupID);
    now_GR.queryActive();
    var member = now_GR retrieves(
```
6. Click **Update**.

**Set up scanner appliances**

If you are initiating scans from ServiceNow®, instead of directly from Qualys, you can set up scans for IP address ranges.

**Before you begin**

The data comes from the Qualys integration based on Qualys asset groups and their related default appliances (scanners).

If no appliances are configured for the targeted IP address ranges, the appliance that is set as the default for the integration instance is used for the scan.

Role required: sn_vul_qualys.admin

**Procedure**

1. Navigate to **Qualys Vulnerability Integration > Scanner Appliances**.
2. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance name</td>
<td>Enter the name for the Qualys scanner appliance to be used for invoking scans for matching configuration items. If you have manually created records that do have an Appliance ID provided, the appliance name is used. Use the External value when you want the scan to be launched with an external scanner.</td>
</tr>
<tr>
<td>Appliance ID</td>
<td>Enter the appliance identifier for the Qualys scanner appliance to be used for invoking scans for matching configuration items. If you entered both an Appliance name and an Appliance ID, the identifier is used.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use the 0 value</td>
<td>Use the 0 value when you want the scan to be launched with an external scanner.</td>
</tr>
<tr>
<td>Appliance status</td>
<td>Displays the last status of the scanner appliance on the data returned by the Qualys integration. For manually created records, the status is updated only if a valid Appliance ID is specified.</td>
</tr>
<tr>
<td>Asset group ID</td>
<td>Displays the Qualys asset group identifier that created this record. This field displays a value only for records created by the Qualys integration.</td>
</tr>
<tr>
<td>Asset group name</td>
<td>Displays the Qualys asset group name that created this record. This field displays a value only for records created by the Qualys integration.</td>
</tr>
<tr>
<td>Order</td>
<td>Enter a value to be used for determining scanning priority. For appliance that have conflicting criteria, an appliance with a lower order value is given a higher priority.</td>
</tr>
<tr>
<td>Manually created</td>
<td>Indicates whether this record was created manually by the user.</td>
</tr>
<tr>
<td>Use filter group</td>
<td>Select this check box to specify a filter group for finding matching configuration items for scanning.</td>
</tr>
<tr>
<td>Filter group</td>
<td>Select the filter group you want to use for finding matching configuration items for scanning. This field appears only if you selected Use filter group.</td>
</tr>
<tr>
<td>IPs</td>
<td>A comma-separated list of IP addresses or ranges of IP addresses to be used by this appliance when invoking scans.</td>
</tr>
<tr>
<td>Integration instance</td>
<td>Starting with v12.0, the Qualys integration instance associated with this appliance.</td>
</tr>
<tr>
<td>Option profile</td>
<td>Starting with v12.0, select the option profile you want to use for scans for matching configuration items.</td>
</tr>
</tbody>
</table>

3. Click Update.

**Configure and manage Qualys vulnerability scanners and scans**

Qualys vulnerability scans can be performed to find software vulnerabilities that affect your CIs. You can initiate scans from a vulnerable item record or by creating a scan record directly for configuration items (CIs) and IP addresses.
If you scan Qualys vulnerable items directly from the Vulnerable Items screen, you also have the option of scanning multiple vulnerable items at the same time.

If Security Incident Response is activated, you can also initiate a scan from the security incident catalog, a security incident record, or a security scan request.

Scans submitted from Qualys vulnerable items, the Security Incident Catalog, security incidents, or security scan requests are performed by the default Qualys scanner.

Starting with v12.0 of the Qualys Vulnerability Integration, you can select the option profile you want to use for scans for matching configuration items.

- Option profiles contain Qualys scan settings.
- An option profile is required when you initiate a Qualys scan from your Now Platform®.

Configure the ServiceNow-initiated Qualys IP scan

The Qualys scanner included with the base system provides a baseline integration to initiate scans based on IP addresses.

Before you begin
Starting with v12.0 of the Qualys Vulnerability Integration, you can select the option profile you want to use for scans for matching configuration items.

- Option profiles contain Qualys scan settings.
- An option profile is required when you initiate a Qualys scan from your Now Platform®.

Role required: web_service_admin

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure
1. Navigate to Vulnerability Response > Vulnerability Scanning > Scanners.
2. Open the Qualys record.
3. Select the Active and Default check boxes.
Starting with v12.0, selecting **Active** is required to use the Qualys scanner to scan Qualys VIs automatically. You also don’t need to select **Default** to have it run automatically.

Prior to v12.0, **Active** is required to use the scanner. If **Default** is also selected, the scanner is automatically used without having to be selected during scanning.

4. Starting with v12.0, for the Source integration field, click the search icon and select the option for **Qualys**, for example, **Qualys Cloud Platform**.

5. Click **Update**.

6. Navigate to **Qualys Vulnerability Integration > Administration > Primary Integrations**.

7. Open the **Qualys Asset Group List Integration**.
   a. Select the **Active** check box.
   b. Click **Execute Now**.

8. Starting with v12.0, follow these steps to populate your scanner appliances.
   
   ![Note:](image)
   You might prefer to run the **Option Profile List Integration** after an import from the **Search Lists Integrations**, the **Qualys Dynamic Search List**, and **Qualys Static Search List Integrations**, so that you can see which search lists are associated with option profiles.

   a. Open the **Qualys Option Profile List Integration**.
   
   b. Select the **Active** check box.
   
   c. Click **Execute Now**.
   
   d. Follow the steps listed in **Set up scanner appliances** to configure your scanner appliances. Return here after you complete those steps to continue with the configuration.
   
   e. Navigate to **Qualys Vulnerability Integration > Administration > Primary Integrations**.
   
   f. Open the **Qualys Appliance List Integration**.
   
   g. Select the **Active** check box.
h. Click Execute Now.
   Your Qualys scanner appliances are now correctly populated.

Related information
   Understanding the Qualys Vulnerability Integration

Scan multiple Qualys vulnerabilities or vulnerable items
You can simultaneously scan multiple Qualys vulnerabilities or vulnerable items
that contain at least one affected configuration item (CI) or an IP address
populated on the form.

Before you begin
Role required: sn_vul.vulnerability_write

Starting with v10.3, persona and granular roles are available to help you
manage what users and groups can see and do in the Vulnerability Response
application. For initial assignment of the persona roles in Setup Assistant, see
Assign the Vulnerability Response persona roles using Setup Assistant. For more
information about managing granular roles, see Manage persona and granular
roles for Vulnerability Response.

Procedure
1. Do one of the following:
   • Navigate to Vulnerability Response > Vulnerabilities > Vulnerability Groups.
   • Navigate to Vulnerability Response > Vulnerabilities > All Vulnerable Items.
2. Select the check boxes for the records you want to scan.
3. Click the Actions on selected rows list, and click Scan for Vulnerabilities.
   A message appears with a link to the scan and the work notes are updated.
4. Click the link to see the progress or results of the scan.
Prior to v13.0 of Vulnerability Response and v12.0 of the Qualys Vulnerability Integration, the Scan screen includes a Source related list that shows the individual vulnerabilities or vulnerable items scanned.

### Scan results prior to v13.0 of Vulnerability Response and v12.0 of the Qualys Vulnerability Integration

<table>
<thead>
<tr>
<th>Number</th>
<th>VISCAN0001002</th>
<th>Time requested</th>
<th>2016-05-03 15:05:04</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Qualys</td>
<td>Requested by</td>
<td>System Administrator</td>
</tr>
<tr>
<td>IP Addresses</td>
<td></td>
<td>State</td>
<td>Error</td>
</tr>
</tbody>
</table>

Scan reference: 
Status message: Error: No ip addresses were provided to scan.

### Configure the Qualys auto scan for resolved vulnerability groups (v 12.0)

Starting with v12.0 of the Qualys Vulnerability Integration, you can schedule the scan that runs automatically to update your Qualys vulnerable items.

#### Before you begin

After a vulnerability group (VG) is transitioned to **Resolved**, a scan is initiated automatically to update the state of the associated vulnerable items.

- The scan is disabled by default.
- Enable the scan with the `scan_on_resolved` integration instance parameter in the Qualys record located at **Qualys Vulnerability Integration > Integration Instances > Qualys**. See the following steps for more information.
This scan is instance-specific. If you have multiple instances and you want to enable or disable this scan, you must disable the `scan_on_resolved` parameter in the integration instance parameters in each instance you want changed.

When the scan is enabled, you can initiate the scan on-demand, or you can schedule the scan to run only within a specified time window. See Configure Qualys rescans to run only within scheduled intervals (v 12.0) for how to set the start and end times for the time window.

Role required: sn_vul_qualys.admin

Procedure
1. Navigate to Qualys Vulnerability Integration > Integration Instances > Qualys.
2. Click Qualys to open the record.
   The integration instance parameters for Qualys are displayed.
3. To enable the auto scan, locate the `scan_on_resolved` parameter.
4. In the Value column for the property, enter `true`.
5. Click Update.

Configure Qualys rescans to run only within scheduled intervals (v 12.0)

Starting with v12.0 of the Qualys Vulnerability Integration, set the scan start and end time parameters so that rescans run, or are available, only during the hours that you want.

Before you begin
This configuration applies to both scheduled rescans and the rescans you initiate manually in the Qualys product from your Now Platform® instance.

Setting the scan start and end time parameters for integration instances permits you to specify time windows when rescans in the Qualys product are available. For example, you might prefer to specify that rescans are only available during off-hours, for example, midnight to 10 AM.

This setting is instance-specific. If you have multiple instances, you must configure the `scan_start_time` and `scan_end_time` values in the integration instance parameters in each instance you want to change.

Role required: sn_vul_qualys.admin

Procedure
1. Navigate to Qualys Vulnerability Integration > Integration Instances > Qualys.
2. Click Qualys to open the record.
The integration instance parameters for Qualys are displayed.

3. For the scan_start_time parameter, in the Value column, enter the time in the UTC time zone in 24 hour format (00:00 through 24:00) for the start time of the window that you want rescans available.

4. For the scan_end_time, in the Value column, enter times in the same format (00:00 through 24:00) for the end time of the available window. For example, if you enter a start time of 00:00 for the scan_start_time parameter, and an scan_end_time of 10:00 AM that same morning, scans scheduled or manually launched outside of the midnight to 10 AM time window are queued and launched at the start time of the following day’s time window, 00:00.

In the same example, if a remediation owner manually initiates a rescan at 11:00 AM, the rescan is not immediately launched, because it lies outside of the available configured scan times. The scan request remains queued until the start of the following day’s time window, in this example, (00:00).

5. Click Update to save your settings.

View the Qualys vulnerability scan queue
Vulnerability scan requests submitted to Qualys vulnerability scanning integration are queued so as not to overload system resources. You can view the status of queued requests, as needed.

Before you begin
Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task
In the list of queued scans, each scan includes an automatically generated scan name that identifies the CI that was scanned.

Procedure
1. Navigate to Vulnerability Response > Vulnerability Scanning > Scan Queue. All Qualys scan requests that have been submitted are shown in a list. The State column shows the current state of each queued entry. A state of Complete indicates that the scan has left the queue. It does not necessarily
indicate that the scan has completed processing. When the scans have been completed or if they failed, the **Processing** column shows the appropriate work notes text.

**Note:** If a hash value was submitted for scanning and the scanner fails to find a result, the **State** shows **Complete** and the work note in the **Processing** column indicates **Unknown**.

2. After a scan has finished processing, click a queued record to view details for the scan request.

**Initiate rescan for the Qualys Vulnerability Integration (v 12.0)**

Starting with version 12.0 of the Qualys Vulnerability Integration, verify your vulnerable items have been remediated between scheduled scanning cycles by initiating rescans in the Qualys product from your Now Platform.

**Before you begin**

You can initiate a rescan on-demand for vulnerable items for the Qualys product from your Now Platform® instance.

To help reduce the overhead and volume involved with scheduled, full scans, remediation owners, IT specialists, vulnerability analysts, or vulnerability managers can initiate targeted rescans on-demand for specific vulnerabilities on assets (configuration items) in their environments. You can initiate rescans in the Qualys product from vulnerable item (VI), vulnerability groups (VG), third-party entry (TPE), or discovered item records from your Now Platform instance.

Rescans permit you to verify that your remediation activities, patches, and other actions have successfully fixed specific vulnerabilities on your configuration items (CIs).

**Use case**

As an example, say your entire environment is scanned once every three weeks. The most recent full scan was completed a week ago, but you applied a patch yesterday to fix a critical vulnerability. Due to the nature of this vulnerability, you cannot wait two weeks for the next scheduled scan to verify that it has been remediated. To verify that your patch successfully fixed a critical vulnerability discovered during an earlier scan, you can initiate a targeted rescan from your Now Platform for Qualys vulnerable items.

**Required setup for rescans in the Qualys product initiated from your Now Platform**

Verify you have completed the following setup required for rescans. See the steps starting with **Configure and manage Qualys vulnerability scanners and scans** listed in the previous sections for more information.
Role required: sn_vul_manually_initiate_rescan

Procedure

1. Navigate to Vulnerability Response > Vulnerable items.

2. Locate the vulnerable item record that you want to trigger a rescan from and open it.

   **Note:** You can only initiate rescans for VIs with Qualys as the source. Verify Qualys is displayed in the Source column on the VI List views, or in the Source fields on individual records. You can use the condition builder to group VIs by Source. Or, if the Source column is not displayed on the VI List view, in the upper left of the list, click the Personalize List icon (Gear icon) and use the Slushbucket to move Source from Available to Selected.

3. Alternatively, navigate to Vulnerability Response > Vulnerability Groups, Vulnerability Response > Libraries > Third-Party, or to Discovered items for the vulnerability group, third-party entry, or discovered items records, respectively, that you want to use for the rescan.

   Depending on your choice, the Rescan button is available on the following records:

   - On a single VI record, the VI must be from the Qualys product and in any state other than Closed. For multiple VI records, all the VIs must have Qualys as the source and in any state other than Closed.
   - On a VG record, the VG can be in any state other than Closed, and all the associated VIs must have Qualys as the source.
   - On a third-party entry (TPE) record, the record must have at least one associated VI record in any state other than Closed with Qualys as the source.
   - On a discovered item record, the configuration item has at least one associated VI with Qualys as the source in any state other than Closed.

4. In the upper right of the record you chose, click Rescan.

   In the dialog that is displayed, choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the Specify option profiles check box.</td>
<td>From the list, choose the option profile for the Qualys scanner you want to use for the rescan. These are the appliances (scanners) you have available.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Clear the <strong>Specify option profiles</strong> check box (not selected).</td>
<td>The Qualys option profile for the scanner you have set as your default scanner on the Scanner Appliances list is used for the scan. For more information about setting the default scanners you initiate from your Now Platform, <a href="#">Setup scanner appliances</a> listed in the previous section for more information.</td>
</tr>
</tbody>
</table>

5. **Click Request Scan.**

A message is displayed that indicates your scan is being processed. Status for all rescans can be found at any time under the Scan related lists on the VI, VG, TPE, and discovered item records you used to launch the rescans. In the message, click **View details** to view the status of the rescan and view any other rescans launched from a given record.

Your instance tracks the rescan status until it successfully completes, or until the set tracking period times out, whichever happens first. The time-out does not stop the scan. The time-out refers to when the Now Platform stopped tracking your rescan status, not when the actual rescan stopped.

After the rescan is successfully completed, the Qualys Host Detection Integration is automatically initiated to update your vulnerable items. Depending on how many VIs you have, your detections, VIs and VGs are updated after the completion of the Qualys Host Detection Integration scan. Navigate to these records to view the updates after the Host Detection Integration is completed.

This scan is instance-specific and can be disabled. For more information about the Qualys integrations and how to view the integrations, see [Understanding the Qualys Vulnerability Integration](#).

**What to do next**

You can view a .csv attachment on the scan record to see details about the rescans.
As shown in the previous image, during the rescan, if hosts (configuration items) in your environment are not accessible, any detections and VIs associated with these assets are not updated when the rescan is completed. To help you understand why they are not included, after the rescan is completed, the asset IP addresses for these CIs are listed on Vulnerability records in the Hosts not scanned field.

**Scan a new or existing Qualys vulnerable item (Prior to v 12.0)**

You can scan a new or existing Qualys vulnerable item that contains at least one affected configuration item (CI) or has an IP address populated on the form.

**Before you begin**
The vulnerable item that you want to scan must contain an affected CI or IP address.
Role required: sn_vul.vulnerability_write

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response
application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

**Procedure**

1. Navigate to **Vulnerability Response > Vulnerabilities > Vulnerable Items**.
2. Create a new vulnerable item or open an existing one.
3. Click the **Scan for Vulnerabilities** related link.
   A message appears with a link to the scan and the work notes are updated.
4. Click the link to see the progress or results of the scan.

   **Note:** It is a good practice is to rescan vulnerabilities or vulnerable items after they have been remediated and a vulnerability patch has been applied to the affected records. The rescan can be performed using the preceding procedure, but you can also automate the rescans.

**Qualys vulnerability scan rate limits**

You can define the rate that different types of scans are performed to limit the number of requests that are sent to an external scanner. After you have defined rate limits, you can apply them to the Qualys scanners.

**Define Qualys scan rate limits**

You can define the rate that different types of scans are performed to balance the load in your scan queue. Conditions defined in the rate limit determine whether the rate limits are applied to queued entries.

**Before you begin**

Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.
Procedure

1. Navigate to **Vulnerability Response > Vulnerability Scanning > Rate Limit Definitions**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

### Rate limit definition

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Provide a descriptive name that identifies the conditions the queue entry must meet. For example, scans per minute</td>
</tr>
<tr>
<td>Queue conditions</td>
<td>Enter conditions used to determine whether a queued scan entry is subject to this rate limit. The conditions should not be specific to a particular scanner.</td>
</tr>
<tr>
<td>Evaluation script</td>
<td>Write a script with the logic to evaluate the queued entry. It is important that the script return true/false to define whether the entry is processed. Also, base the evaluation script on the queued entry being evaluated.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**Apply scan rate limits to Qualys scanners**

After you have defined scan rate limits using **Rate Limit Definitions**, you can apply rate limits to specific Qualys scanners.

**Before you begin**

Role required: sn.vul_admin

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see **Assign the Vulnerability Response persona roles using Setup Assistant**. For more information about managing granular roles, see **Manage persona and granular roles for Vulnerability Response**.

Procedure

1. Navigate to **Vulnerability Response > Vulnerability Scanning > Scanner Rate Limits**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

### Scanner rate limit

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scanner</td>
<td>Select the scanner to which you want to apply a rate limit.</td>
</tr>
<tr>
<td>Rate limit</td>
<td>Select the rate limit you want to apply to this scanner.</td>
</tr>
<tr>
<td>Threshold</td>
<td>Enter the threshold that you want to subject the selected scanner to for the selected rate limit. For example, if the scanner allows 4 scans per minute, and the rate limit is defined as requests per minute, the threshold would be 4.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**Resolving Qualys Vulnerability Integration issues**

Some commonly encountered issues, along with workarounds are discussed.

**Attachments not appearing after import**

If attachments are not appearing as expected for data sources or on a security incident after third-party integration imports, check your IP restrictions.

IP access restrictions can prevent attachments from being seen unless you are logged in from a safe IP. Since a new attachment is added with each import, this can result in duplicates you have to remove.

For example, when you run a third-party host import integration, if you do not see any attachments on your data sources, check your IP restrictions and add users to the safe list prior to import.

**CVE data is missing from the vulnerability entry**

If Common Vulnerability Enumeration (CVE) data is missing from your Qualys third-party vulnerability entries, this means the NIST National Vulnerability Database (NVD) database is not populated in Vulnerability Response. Set the `insert_nvd` parameter to `true`, perform an NVD on-demand update and rerun the Qualys Knowledge Base integration.

**Before you begin**

Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see...
Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure

1. Navigate to Qualys Vulnerability Integration > Administration > Integration Instances.
2. Change `insert_nvd` to `true`.
3. Navigate to Vulnerability > Administration > On-Demand Update.
4. Update the NVD vulnerability records. See the instructions in Update NVD on-demand (Prior to v13.0).
5. Set the Start date to an earlier date and rerun the Qualys Knowledge Base integration.

Modify transform maps

Transform maps are provided with base configurations and are sufficient usually. You can modify transform mappings depending on the needs of your organization.

Before you begin

Role required: sn_vul_qualys.admin + import_admin

Procedure

1. Navigate to System Import Sets > Administration > Transform Maps to view the REST messages.
2. Filter the resulting list by application, and limit the list to the Qualys Vulnerability Integration application.
3. Modify the transform maps per the customer requirements.
   For details on the data provided by the Qualys API, see the Qualys API documentation (https://www.qualys.com/docs/qualys-api-v2-user-guide.pdf).

Check XML attachment property size

Verifies that the XML attachment property is sufficient for large files.

Before you begin

Role required: admin
Procedure
1. Navigate to **System Properties > Import Export**.
2. Scroll down to **Import Properties > XML Format** at the bottom of the page.

3. If necessary, change the value to 250 and click **Save**.

Related information

Data retrieval limitations
By default, there are no restrictions on how data is retrieved from Qualys. Many records can be related to low severity vulnerabilities that a customer is not willing to remediate using their vulnerability response process. Updating the corresponding REST message/method parameters can modify this behavior.

The REST message/method responsible for this update is **Qualys Host Detection – Standard/post**. To update the values, add a new HTTP Query Parameter to the post method with the following values:

- **Name**: severities
- **Value**: 3-5 (or whatever appropriate severities are desired)

Qualys Vulnerability Integration reporting
The Qualys Cloud Platform overview is an executive view into vulnerability activity. By providing trends, reports, and drill-downs into specific data, an administrator or analyst can quickly pinpoint areas of concern. The charts are populated with data after vulnerable items and Qualys knowledge base data has been retrieved.

**Note:** Using the Qualys Cloud Platform Vulnerability integration assumes that tuning, testing and deployment have occurred in your instance. These functions are areas beyond the scope of product documentation. For assistance, contact Customer Service and Support.
In each chart, you can point to any part of a chart (bar, pie, data point, and so on) to view general data specific to that part. If you click any part of a report, a list opens to provide detailed information.

The following reports are available on the Qualys Cloud Platform homepage.

### Qualys Vulnerability Integration Overview reports

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIs Synchronized With Qualys</td>
<td>Bar</td>
<td>Displays the number of open vulnerable items recorded for each CI, from most to least.</td>
</tr>
<tr>
<td>Open Qualys Vulnerable Items</td>
<td>Bar</td>
<td>Displays the number of open vulnerable items associated with vulnerabilities (CVE records), from most to least.</td>
</tr>
<tr>
<td>Total Qualys Vulnerable Items</td>
<td>Bar</td>
<td>Displays the number of ignored vulnerable items scheduled to be expired within 7 days.</td>
</tr>
</tbody>
</table>
Qualys Vulnerability Integration Overview reports (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerable Items by Priority</td>
<td>Trend</td>
<td>Displays the number of vulnerability entries recorded each week.</td>
</tr>
<tr>
<td>QID Prevalence</td>
<td>Bar</td>
<td>Displays the number of vulnerable items recorded for each model, from most to least.</td>
</tr>
<tr>
<td>Open Qualys Vulnerable Items</td>
<td>List</td>
<td>Displays the number of vulnerable items recorded for each publisher, from most to least.</td>
</tr>
</tbody>
</table>

Qualys integration run status chart

The Qualys Integration Run Status module is a graphical view of the status of Qualys integration runs.

In the chart, point to any part (bar, pie, data point, and so on) to view general data specific to that part. If you click any part of a report, a list opens to provide detailed information.

Multiple factors can impact the performance of the integration run, like the amount of data and time taken to process this data. Starting with v10.3, two new graphs have been added to compare the performance metrics:

- Qualys Vulnerable Item Ingestion Performance Metrics: Compare daily performance metrics for assignment rules, group rules, risk rules, queue wait time, queue processing time, and other statistics for vulnerable items for the last 30 days, to identify the cause for any deviations in performance.
Qualys Vulnerable Item Ingestion Performance Throughput: Compare daily vulnerable item ingestion throughput for the Qualys Host Detection integration. Throughput is measured in items per hour.
Sample Qualys Integration Run Status chart (v10.0)

Starting with v10.0:

- The values in the Imported Items column represents the total number of vulnerable items that are created from an integration run.

- The New items column displays the number of vulnerable items that are created from an integration run.

- The Duplicate items column is no longer populated. You may prefer to remove this column from the display.

- The Updated items column displays the number of times vulnerable items are updated during an integration run. This value is not the number of unique vulnerable items that are updated. If for example, a vulnerable item is updated two times during the integration run, it is counted two times and displayed as 2 updated items.

- The Unchanged items column displays vulnerable items found during the integration run that already exist in the database but were not updated, because none of the relevant field values had changed.

Note: Integration runs with zero results for all four of the following values: New CIs, Existing CIs, New Items, and Updated Items are filtered out of the Qualys Integration Runs list.

Qualys integration run status chart reports

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last 30 Days Qualys Results</td>
<td>The number of integration runs completed for each integration. Shows both successful and failed runs. Run in a bar visual.</td>
</tr>
</tbody>
</table>
### Qualys integration run status chart reports (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last 30 Days Qualys New VIs</td>
<td>The number of new vulnerable items imported in the last 30 days. Shown as an integer.</td>
</tr>
<tr>
<td>Last 30 Days Qualys Updated VIs</td>
<td>The number of updated vulnerable items imported in the last 30 days. Shown as an integer.</td>
</tr>
<tr>
<td>Last 30 Days Qualys Duplicates</td>
<td>The number of duplicate vulnerable items imported in the last 30 days. Shown as an integer.</td>
</tr>
<tr>
<td>Qualys Integration Runs</td>
<td>The integration run records in a list.</td>
</tr>
<tr>
<td>Version 10.3: Last 30 Days Qualys Vulnerable Item Ingestion Performance Metrics</td>
<td>Daily performance metrics for vulnerable items compared for the last 30 days.</td>
</tr>
<tr>
<td>Version 10.3: Last 30 Days Qualys Vulnerable Item Ingestion Performance Throughput</td>
<td>Daily vulnerable item ingestion throughput measured for the Qualys Host Detection integration for the last 30 days.</td>
</tr>
</tbody>
</table>

### Qualys data transformation

The data retrieved from Qualys is processed through a set of data sources and transforms.

Most transforms for the Qualys Vulnerability Integration are performed using transform scripts. These scripts are for internal use deleting is not recommended. Modifications require coding or advanced ServiceNow or Qualys Vulnerability Integration expertise. The remaining maps are listed in this section and use field maps.

**Note:** During installation, normalized severity maps, that transform imported Qualys Cloud Platform severity levels to standard ServiceNow severity levels, are installed in the Vulnerability Response Normalized Severity Mapping module. See Create a Vulnerability Response severity map for more information.
**Dynamic Search List Import**

The Qualys dynamic search list transform map is used to transform and import Qualys Dynamic Search Lists. Changes to this transform alter how Dynamic Search Lists are processed and inserted into the system.

To access this transform map, navigate to Qualys Vulnerability Integration > Import Set Tables > Dynamic Search List Import.

The table shows the fields currently being transformed.

<table>
<thead>
<tr>
<th>Source Field</th>
<th>Target Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>u_id</td>
<td>id</td>
<td>Used as the identifier for the Qualys Dynamic Search List.</td>
</tr>
<tr>
<td>[Script]</td>
<td>list_type</td>
<td>The type of search list. Dynamic is the default for the Dynamic Search List transform.</td>
</tr>
<tr>
<td>u_title</td>
<td>title</td>
<td>The name in Qualys for this search list.</td>
</tr>
</tbody>
</table>

In addition to field mappings, there is also a transform script that is executed during the transformation process.

The following table shows when this script runs and what it is used for.

<table>
<thead>
<tr>
<th>When the script is run</th>
<th>Purpose of the script</th>
</tr>
</thead>
<tbody>
<tr>
<td>onAfter (after an import set has completed transformation).</td>
<td>Creates the relationships between Search Lists and their related vulnerabilities. For internal use. Modifying or deleting is not recommended.</td>
</tr>
</tbody>
</table>

**Static Search List Import**

The Qualys static search list transform map is used to transform and import Qualys Static Search Lists. Changes to this transform alter how Static Search Lists are processed and inserted into the system.

To access this transform map, navigate to Qualys Vulnerability Integration > Import Set Tables > Static Search List Import.

The table shows the fields currently being transformed.
Qualys static search list transform map fields

<table>
<thead>
<tr>
<th>Source Field</th>
<th>Target field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>u_id</td>
<td>id</td>
<td>Used as the identifier for the Qualys Static Search List.</td>
</tr>
<tr>
<td>u_title</td>
<td>title</td>
<td>The name in Qualys for this search list.</td>
</tr>
<tr>
<td>[Script]</td>
<td>list_type</td>
<td>The type of search list. Static is the default for the Static Search List transform.</td>
</tr>
</tbody>
</table>

In addition to field mappings, there is also a transform script that is executed during the transformation process.

The following table shows when this script runs and what it is used for.

Qualys static search list transform map script timing and purpose

<table>
<thead>
<tr>
<th>When the script is run</th>
<th>Purpose of the script</th>
</tr>
</thead>
<tbody>
<tr>
<td>onAfter (after an import set has completed transformation).</td>
<td>Creates the relationships between Search Lists and their related vulnerabilities. For internal use. Modifying or deleting is not recommended.</td>
</tr>
</tbody>
</table>

Asset Group Import

The Qualys Asset Group Appliance Transform map is used to transform Qualys Asset Group data to create scanner appliance records. Changes to this transform alter how scanner appliances are created and modified.

To access this transform map, navigate to Qualys Vulnerability Integration > Import Set Tables > Asset Group Import.

The table shows the fields currently being transformed.

Qualys asset group transform map fields

<table>
<thead>
<tr>
<th>Source Field</th>
<th>Target field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>u_id</td>
<td>id</td>
<td>Used as identifier for the Qualys Asset Group.</td>
</tr>
<tr>
<td>[Script]</td>
<td>manual</td>
<td>Scripted value to determine how the target record was created. When created through</td>
</tr>
</tbody>
</table>
Qualys asset group transform map fields (continued)

<table>
<thead>
<tr>
<th>Source Field</th>
<th>Target field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Script]</td>
<td>ips</td>
<td>The IP addresses that are associated with the asset group being transformed.</td>
</tr>
<tr>
<td>u_default_appliance_id</td>
<td>appliance_id</td>
<td>The Qualys appliance identifier for the default appliance in this asset group.</td>
</tr>
<tr>
<td>u_title</td>
<td>asset_group_name</td>
<td>The name of the Qualys asset group.</td>
</tr>
</tbody>
</table>

In addition to field mappings, there is also a transform script that is executed during the transformation process.

The following table shows when this script runs and what it is used for.

Qualys asset group transform map script timing and purpose

<table>
<thead>
<tr>
<th>When the script is run</th>
<th>Purpose of the script</th>
</tr>
</thead>
<tbody>
<tr>
<td>onBefore (before an import set has completed transformation)</td>
<td>The script that constrains the asset group imports to only asset groups with a default appliance and a set of mapped IP addresses. For internal use. Modifying or deleting is not recommended.</td>
</tr>
</tbody>
</table>

Appliance Import

The Qualys Appliance Transform map is used to transform Qualys Appliance data into appliance records. This is used to update the appliance records that would initially be created from the Asset Group Import. Changes to this transform alter how appliance records are updated with appliance details.

To access this transform map, navigate to Qualys Vulnerability Integration > Import Set Tables > Appliance Import.

The table shows the fields currently being transformed.
Qualys appliance transform map fields

<table>
<thead>
<tr>
<th>Source Field</th>
<th>Target field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>u_name</td>
<td>appliance_name</td>
<td>The name of the Qualys scanner appliance.</td>
</tr>
<tr>
<td>u_status</td>
<td>appliance_status</td>
<td>The last reported status of the Qualys scanner appliance.</td>
</tr>
<tr>
<td>u_id</td>
<td>appliance_id</td>
<td>The Qualys appliance identifier.</td>
</tr>
</tbody>
</table>

In addition to field mappings, there is also a transform script that is executed during the transformation process.

The following table shows when this script runs and what it is used for.

<table>
<thead>
<tr>
<th>When the script is run</th>
<th>Purpose of the script</th>
</tr>
</thead>
<tbody>
<tr>
<td>onBefore (before an import set has completed transformation)</td>
<td>Used to update appliance names and statuses for the given ID. For internal use. Modifying or deleting is not recommended.</td>
</tr>
</tbody>
</table>

Qualys REST messages

Qualys REST messages are used to make calls to the Qualys API.

Qualys Host Detection REST message

The Qualys Host Detection REST message makes the initial call to the Host List Detection API for the Qualys Host Detection Integration.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>list</td>
<td>Indicates the type of operation requested. Required parameter. Changes are not required.</td>
</tr>
<tr>
<td>output_format</td>
<td>XML</td>
<td>Sets the format of the report returned by Qualys.</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The various scripts and transforms assume XML, so changes to the value are not recommended.</td>
</tr>
<tr>
<td>detection_updated_since</td>
<td>${lastScanDate}</td>
<td>Shows only detections whose detection status changed after a certain date and time. For detections that have never changed the date is applied to the last detection date.</td>
</tr>
<tr>
<td>truncation_limit</td>
<td>500</td>
<td>The number of hosts to retrieve data from, per request. This parameter is used for pagination purposes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default value is 500, but larger or smaller values can be used. Do not set at less than 100 since it significantly increases system load.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Smaller values require more calls to the Qualys API and larger values result in larger result sets to process and potential data retrieval/processing timeouts.</td>
</tr>
<tr>
<td>status</td>
<td>New, Fixed, Active, Re-opened</td>
<td>Detection statuses to retrieve from Qualys.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default is to retrieve all statuses. For large data pulls (often the initial pull of data), it can be beneficial to exclude Fixed statuses from this list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>It is important to include the Fixed status when updating vulnerabilities already in the system.</td>
</tr>
</tbody>
</table>
Qualys host detection pagination REST message
The Host Detection Pagination REST message handles pagination requests to the Host Detection API.

When the primary host detection runs, if the Qualys API provides a URL to fetch the next page of data, this REST message retrieves that additional data. This data is used by Host Detection Pagination Handler.

Host detection pagination REST is a specialized REST message and is not intended to be modified.

Qualys knowledge base (backfill) REST message
The Qualys Knowledge Base (Backfill) REST message retrieves Qualys knowledge base data based on the last modified timestamp of the vulnerability data for the Qualys Knowledge Base integration.

Changes to the REST message method record impact the request made to Qualys to retrieve knowledge base information.

The following table shows the request parameters that are sent.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>list</td>
<td>Indicates the type of operation being requested. Required parameter. Changes are not recommended.</td>
</tr>
<tr>
<td>details</td>
<td>All</td>
<td>Indicates the level of detail shown for vulnerabilities retrieved. Safe to modify as needed.</td>
</tr>
<tr>
<td>ids</td>
<td>${qids}</td>
<td>Specifies which QIDs to retrieve from Qualys. Referenced in code. Modifications are not recommended.</td>
</tr>
</tbody>
</table>

Qualys knowledge base (date-based) REST message
The Qualys Knowledge Base (Date-Based) REST message is used to retrieve Qualys knowledge base data based on the last modified timestamp of the vulnerability data. This message is used by the Qualys Knowledge Base integration.

Changes to the REST message method record impact the request made to Qualys to retrieve knowledge base information.

The following table shows the request parameters that are sent.
### Qualys knowledge base (date-based) REST message parameters

<table>
<thead>
<tr>
<th>Source Field</th>
<th>Target Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>list</td>
<td>Indicates the type of operation requested. Required parameter. Changes are not recommended.</td>
</tr>
<tr>
<td>details</td>
<td>All</td>
<td>Indicates the level of detail shown for vulnerabilities retrieved. Safe to modify as needed.</td>
</tr>
<tr>
<td>last_modified_after</td>
<td>${dateStart}</td>
<td>Indicates when to start retrieving historical data. Used by code to determine both the start time and to assist with pagination. Modifications or removal is not recommended.</td>
</tr>
<tr>
<td>last_modifiedbefore</td>
<td>${dateEnd}</td>
<td>Indicates when to end retrieving historical data. Used by code to determine both the end time and to assist with pagination. Modifications or removal is not recommended.</td>
</tr>
</tbody>
</table>

### Qualys tickets REST message

The Qualys tickets REST message retrieves Qualys ticket information for the Qualys Ticket Integration. Changes to the REST message method record impact the requests made to Qualys to retrieve ticket information.

The table shows the request parameters that are sent.

### Qualys tickets REST message parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>modified_since_datetime</td>
<td>${lastRunDatetime}</td>
<td>Indicates the last run date of the integration and the date after which to pull data. Used by code. Changes are not recommended.</td>
</tr>
<tr>
<td>since_ticket_number</td>
<td>${lastTicketNumber}</td>
<td>Indicates which ticket was last retrieved from Qualys.</td>
</tr>
</tbody>
</table>
Qualys tickets REST message parameters (continued)

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Used for pagination. Changes are not recommended.</td>
</tr>
<tr>
<td>show_vuln_details</td>
<td>1</td>
<td>Indicates whether the vulnerability details are retrieved.</td>
</tr>
</tbody>
</table>

Understanding the Rapid7 Vulnerability Integration

The Rapid7 Vulnerability Integration by ServiceNow® uses data imported from the Rapid7 Nexpose data warehouse or the Rapid7 InsightVM product to help you determine the impact and priority of potentially malicious threats.

Rapid7 Nexpose sensors collect data and automatically send it to the Rapid7 Nexpose or Rapid7 InsightVM product, which continuously analyzes and correlates the information. It easily integrates with ServiceNow® Vulnerability Response to map vulnerabilities to CIs and services. The Rapid7 Vulnerability Integration enriches the vulnerability data on your instance.

Rapid7 integrations are entry points interacting with the Rapid7 Nexpose data warehouse or Rapid7 InsightVM product, invoked as scheduled jobs. Scheduled jobs simplify the vulnerability remediation lifecycle by keeping the instance synchronized with other vulnerability management systems. The scheduled jobs are run automatically and in the order specified. You can also execute individual scheduled jobs manually.

⚠️ Note:
If you use both Rapid7 data warehouse and Rapid7 InsightVM as sources for your data, you run the risk of duplicate vulnerability records.

⚠️ Note:
When migrating from the Data Warehouse integration type to the InsightVM type, you can deduplicate your existing data warehouse records. See Deduplicate Rapid7 Vulnerability Integration data warehouse records for more information.

If you have multiple deployments of the Rapid7 InsightVM vulnerability integration, you can add an integration for each deployment. Assets, identified by multiple third-party deployments and their vulnerabilities, are consolidated and reconciled with your CMDB. This consolidation happens even when scan processes overlap between the multiple deployments. Data sourced from
each deployment is identified and available in a single instance of Vulnerability Response.

Note: You cannot delete the original vulnerability integration but you can disable it. Integrations created from disabled templates are disabled by default.

There is a configured run-as user for each integration record. The default value for this user is VR.System. Do not change this value.

Available versions for Paris

<table>
<thead>
<tr>
<th>Release version with Paris</th>
<th>Release Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rapid7 Vulnerability Integration v13.0</td>
<td>Vulnerability Response integrations release notes</td>
</tr>
<tr>
<td>Rapid7 Vulnerability Integration v12.0</td>
<td>For compatibility information, see KB0856498</td>
</tr>
<tr>
<td>Rapid7 Vulnerability Integration v11.2</td>
<td>Vulnerability Response Compatibility Matrix and Release Schema Changes</td>
</tr>
<tr>
<td>Rapid7 Vulnerability Integration v11.1</td>
<td></td>
</tr>
<tr>
<td>Rapid7 Vulnerability Integration v11.0</td>
<td></td>
</tr>
<tr>
<td>Rapid7 Vulnerability Integration v10.3</td>
<td></td>
</tr>
<tr>
<td>Rapid7 Vulnerability Integration v10.0</td>
<td></td>
</tr>
</tbody>
</table>

Roles

Rapid7 vulnerability integration tasks involve the following roles.

- sn_vul_r7.admin: Can read, write, and delete records.
- sn_vul_r7.user: Can read and write records.
- sn_vul_r7.read: Can read records.

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Rapid7 Vulnerability Integration integrations

To view the Rapid7 Vulnerability Integration, navigate to Rapid7 > Administration > Integrations.
The following integrations are included in the base system.

### Rapid7 Nexpose data warehouse integrations

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rapid7 Vulnerability Integration</td>
<td>Retrieves vulnerability data from Rapid7 Nexpose and processes it in your instance.</td>
</tr>
<tr>
<td>Version 10.0: Rapid7 Asset List Integration</td>
<td>Retrieves scan data once a week from Rapid7 Nexpose data warehouse and stores it in the Discovered Items module in your instance. Helps identify assets that haven’t been scanned recently using <strong>Last Scan</strong> date. View the <strong>Last Scan</strong> time in the Discovered Items list in Vulnerability Response.</td>
</tr>
<tr>
<td>Rapid7 Category Integration</td>
<td>Retrieves category information from Rapid7 Nexpose. Categories provide high-level classification for vulnerabilities.</td>
</tr>
<tr>
<td>Rapid7 Exploit Integration</td>
<td>Retrieves exploit information from Rapid7 Nexpose.</td>
</tr>
<tr>
<td>Rapid7 Malware Kit Integration</td>
<td>Retrieves malware kit information from Rapid7 Nexpose.</td>
</tr>
<tr>
<td>Rapid7 Reference Integration</td>
<td>Retrieves references to external authority documents such as CVEs or vendor-specific vulnerability references.</td>
</tr>
<tr>
<td>Rapid7 Solution Integration</td>
<td>Retrieves solution data from Rapid7 Nexpose which provides recommended solutions to specific vulnerabilities.</td>
</tr>
<tr>
<td>Rapid7 Superseding Solution Integration</td>
<td>Retrieves information about which solutions are superseded by other solutions.</td>
</tr>
<tr>
<td>Rapid7 Vulnerability Solution Map Integration</td>
<td>Retrieves the mapping to associate solutions with vulnerabilities.</td>
</tr>
<tr>
<td>Rapid7 Vulnerable Item Integration</td>
<td>Retrieves vulnerable item data from Rapid7 Nexpose and processes it in your instance. The outputs of this integration are vulnerable items.</td>
</tr>
</tbody>
</table>
### Rapid7 Nexpose data warehouse integrations (continued)

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rapid7 Vulnerable Item Resolution Integration</td>
<td>Retrieves information about which vulnerable items are marked closed in Rapid7 Nexpose and closes the corresponding vulnerable items in Vulnerability Response.</td>
</tr>
<tr>
<td>Rapid7 Site Integration</td>
<td>Retrieves site data from Rapid7 Nexpose. A site is a collection of assets that are targeted for a scan.</td>
</tr>
<tr>
<td>Rapid7 Asset List Integration</td>
<td>Retrieves scan data once a week from the Rapid7 data warehouse and stores it in the Discovered Items module in your instance. Helps identify assets that haven’t been scanned recently using Last Scan date. View the Last Scan time in the Discovered Items list in Vulnerability Response.</td>
</tr>
<tr>
<td>Version 10.3: Rapid7 Comprehensive Vulnerable Item Integration</td>
<td>Imports all the Rapid7 detections for all configuration items scanned since the last successful integration run. Based on the most current imported data, vulnerable items not recently found during scans are automatically transitioned to ‘Closed’ when the Auto-Close Stale Vulnerable Items module is enabled.</td>
</tr>
</tbody>
</table>

### Rapid7 InsightVM integrations

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rapid7 Vulnerable Item Integration — API</td>
<td>Retrieves vulnerable item data from Rapid7 Nexpose InsightVM and processes it in your instance.</td>
</tr>
<tr>
<td>Rapid7 Vulnerability Integration — API</td>
<td>Retrieves reference, category, exploit, malware kit, and vulnerability data from Rapid7 Nexpose InsightVM and processes it in your instance.</td>
</tr>
<tr>
<td>Rapid7 Asset List Integration - API</td>
<td>Retrieves host tags and scan data once a week from Rapid7 InsightVM and stores it in the Discovered Items module in your instance. Helps identify assets that haven’t been scanned recently using Last Scan date. View the Last Scan time in the Discovered Items list in Vulnerability Response.</td>
</tr>
</tbody>
</table>
Rapid7 InsightVM integrations (continued)

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 10.3: Rapid7 Comprehensive Vulnerable Item Integration - API</td>
<td>Imports all the Rapid7 detections for all configuration items scanned since the last successful integration run. Based on the most current imported data, vulnerable items not recently found during scans are automatically transitioned to ‘Closed’ when the Auto-Close Stale Vulnerable Items module is enabled.</td>
</tr>
<tr>
<td>Version 12.0: Rapid7 Site Integration</td>
<td>Retrieves Site data from the Rapid7 InsightVM product. This integration is set to run weekly at 00:00:00.</td>
</tr>
</tbody>
</table>

CI Lookup Rules

CI Lookup Rules determine how to fill in the Configuration item field in a vulnerable item record.

For more information on how CI lookup rules work, see CI Lookup Rules for identifying configuration items from Vulnerability Response third-party vulnerability integrations.

To create or edit lookup rules, see Create a Vulnerability Response CI lookup rule.

ℹ️ Note: Rules, once removed, cannot be recovered. Rather than removing existing rules, deactivate them when creating new ones.

Discovered Items

This module lists configuration items detected during import from the Rapid7 Vulnerable Item Integrations (data warehouse or InsightVM API) and the Rapid7 Asset List Integration - API. The Rapid7 Nexpose data warehouse Asset List Integration is included.

ℹ️ Note: The default filter for this list is set to Unmatched. You can view all discovered items from an import by removing the filter.

See Discovered Items in Vulnerability Response for more information on the Discovered Items module.

Host tags

Host tags are imported as part of the Rapid7 Asset List Integration - API integration for Rapid7 InsightVM. They are used primarily for filtering in
Vulnerability Response Assignment and Vulnerability Group Rules in Rapid7 InsightVM. They are displayed in the Discovered Item form.

Host tags

Note: The Rapid7 Asset List integration - API integration should be run prior to creating Assignment or Vulnerability Group Rules in Vulnerability Response so that all tags can be present in the rules and before vulnerable items are imported and grouped.

- Tag storage is not case sensitive. If a San Diego tag is created, then a SAN DIEGO tag cannot be stored in the Host tag table. “San Diego” and “SAN DIEGO” are considered to be the same host tag. Whichever tag was imported first wins.
- Using host tags as a Group Key in a Vulnerability Group Rule can have unexpected results. Host tags are intended for use only in the Condition builder.
- Host tags are controlled by the global system property sn_vul.import_host_tags. This property is set to true by default. Turning tags off turns them off across all instances.

Sites

A site is a collection of assets targeted for a scan. A site consists of target assets, a scan template, one or more Scan Engines, and other scan-related settings such as schedules or alerts. Sites are managed by Rapid7 applications.

Rapid7 Vulnerability Integration site filtering during configuration allows you to categorize and request assets by site during import. See Filtering by Rapid7 sites for more information on filtering imports using Rapid7 InsightVM sites.

The Rapid7 Nexpose data warehouse Sites Integration imports sites as a scheduled job.

Note: Prior to v12.0, Rapid7 InsightVM did not have a Site integration. To use the site filtering capability, you must create sites manually. See Create sites for Rapid7 InsightVM (Prior to v12.0) for more information.

To view the imported sites in a list, navigate to Rapid7 > Sites.

Solutions

Solutions are known remediations imported into your Rapid7 Vulnerability Integration from either Rapid7 Nexpose data warehouse or Rapid7 InsightVM.

Rapid7 Nexpose data warehouse imports both solutions and superseding
solutions. Rapid7 InsightVM only imports superseding solutions. To view imported solutions in a list, navigate to **Rapid7 > Solutions**.

**Reopen resolved vulnerable items not closed by scans**
Starting with v10.3, vulnerable items set to 'Resolved' in your Now Platform instance but not transitioned to 'Closed/Fixed' by the subsequent integration runs are reopened if they are detected during rescans.

For Rapid7 detections, an option is now available on the Rapid7 configuration page in your instance to reopen resolved VIs by age. If enabled, VIs set to 'Resolved' but then not transitioned to 'Closed/Fixed' by subsequent scans transition back to 'Open' after the number of days you enter.

**Request apps on the Store**
Visit the [ServiceNow Store](https://www.service-now.com/store) website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the [ServiceNow Store version history](https://www.service-now.com/store/). For cumulative release notes information for all released apps, see the [ServiceNow Store version history](https://www.service-now.com/store/).

**Preparing for the Rapid7 Vulnerability Integration**
A successful integration requires planning and careful execution of pre-integration tasks. Prepare for the integration by performing these tasks. The Rapid7 Vulnerability Integration assumes that you are familiar with and run Rapid7 data warehouse or Rapid7 InsightVM product scans in your environment.

**Before you begin**
The Rapid7 Nexpose data warehouse integration type requires the Rapid7 Nexpose data warehouse add-on. See the Rapid7 Nexpose website and documentation to acquire and install this add-on.

The Rapid7 InsightVM integration type requires an API key from within your Rapid7 Insight account.

Role required: admin

**About this task**

ℹ️ **Note:** Before running the integration, make any necessary configuration changes based on your requirements.

- Validate your instance sizing based on the number of vulnerable items you expect to import. An undersized instance can lead to long load times. If you do not know the size of your instance, contact Customer Service and Support.

Use filtering to limit the number of items for initial import and phase your deployment by adjusting filters in subsequent imports.
• There is a configured run-as user for each integration record. The default value for this user is `VR.System`. Do not change this value.

• If you do not use vulnerability calculators, disable the default calculator, in addition to any others you have defined. Vulnerability calculators run every time a vulnerable item record is created or updated, and can impact initial import performance.

• If you plan to use host tags in Vulnerability Response Assignment or Vulnerability Group Rules, run the Rapid7 Asset List integration prior to creating rules.

**Disable the default vulnerability calculator if not used**

If you do not use vulnerability calculators, disable the default calculator, in addition to any others you have defined. Vulnerability calculators run every time a vulnerable item record is created or updated, and can impact initial import performance.

**Before you begin**

Role required: admin

**Procedure**

1. Navigate to **Vulnerability > Administration > Vulnerability Calculators**.
2. Open the relevant calculator.
3. Clear the **Active** check box to deactivate the calculator.
4. Click **Update**.

**Install and configure the Rapid7 Vulnerability Integration**

Before you run the integration on your instance, the installation and configuration steps must be completed so the Rapid7 Nexpose or Rapid7 InsightVM product properly integrates with Vulnerability Response. This application is available as a separate subscription.

**Before you begin**

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

⚠️ **Note:** This process applies only to applications downloaded to production instances. If you’re downloading applications to sub-production or development instances, it’s not necessary to get entitlements. Proceed to **Activate a ServiceNow Store application**.
Roles required: admin to install the application and vulnerability admin (sn_vul.vulnerability_admin or sn_vul.admin) to configure the application after it is installed.

<table>
<thead>
<tr>
<th>Setup tasks</th>
<th>Description</th>
</tr>
</thead>
</table>
| Verify that the Vulnerability Response application is installed and activated. | To verify that this application is activated, navigate to Subscription Management > Subscriptions in your instance. The list displays the subscriptions your organization has purchased.  
If the application is not installed and activated see, Install and configure Vulnerability Response. |
| Verify that you have the required ServiceNow roles for your instance.        | The following roles are required for installation, configuration, and verification of expected results: 
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response. |
<p>|                                                                              | • The System Administrator [admin] installs the app and assigns the vulnerability admin [v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)] role. |
|                                                                              | • The vulnerability admin oversees configuration and verifies expected results.                                                                                                                               |
|                                                                              | Prior to v10.3 of Vulnerability Response:                                                                                                                                                                      |</p>
<table>
<thead>
<tr>
<th>Setup tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The System Administrator [admin] installs the app and assigns the Vulnerability Admin [sn_vul.admin] role.</td>
<td></td>
</tr>
<tr>
<td>• The Vulnerability Admin [sn_vul.admin] oversees configuration and verifies expected results.</td>
<td></td>
</tr>
<tr>
<td>The Rapid7 admin role is inherited when you are assigned an administrative role in the Vulnerability Response (VR) application.</td>
<td></td>
</tr>
</tbody>
</table>

Prepare for Rapid7 Vulnerability Integration installation.  
Read Preparing for the Rapid7 Vulnerability Integration.

For the Rapid7 Nexpose data warehouse integration type, ensure that you have a MID Server with access to the Rapid7 Nexpose data warehouse.  
Note the data warehouse name. The Rapid7 data warehouse integration type only supports standalone MID Servers. Clustered MID Servers are not supported.

For the Rapid7 Nexpose data warehouse integration type, download the latest PostgresSQL driver.  
Go to https://jdbc.postgresql.org/download.html and download the latest driver.

For the Rapid7 Nexpose data warehouse integration type, have your Rapid7 Nexpose data warehouse server URL and authentication credentials ready.  
The credentials must provide adequate permissions for retrieving knowledge, scan, and detection information for a Rapid7 Nexpose subscription.

For the Rapid7 InsightVM integration type, have your region and API key ready.  
Contact Rapid7 to obtain the appropriate region and API key.

Note:  
When migrating from the Data Warehouse integration type to the InsightVM type you can deduplicate your existing data warehouse records. See Deduplicate Rapid7 Vulnerability Integration data warehouse records for more information.
Procedure

1. Log in to the instance you want to install the Rapid7 Vulnerability Integration application on.

2. For the Rapid7 Nexpose data warehouse vulnerability integration, install the PostgreSQL JAR file.
   
a. In your ServiceNow instance, navigate to MID Server > JAR Files.

b. Click New.

c. Enter the name of the PostgreSQL driver that you downloaded earlier. Optionally, enter the Version, Source, and Description information. Leave the Active check box selected.

d. Attach the downloaded JAR file using the paper clip icon in the header.

e. Click Submit.

This process completes the Rapid7 Nexpose data warehouse-specific integration tasks.

3. Navigate to the ServiceNow Store.

4. In the ServiceNow Store, search for the Rapid7 Vulnerability Integration application.

5. Click the application tile.

Detailed information about the application you are installing is displayed.

Note: Consider reading the Other Requirements and Dependencies sections, as applicable.

6. Click Request App and enter your Now Support login credentials.

7. Click Get.

8. Enter the Instance Name and Reason for the Instance, and click Validate Instance.

9. Click Request.

You will receive an email with detailed installation instructions.


11. Locate the application, select it, and click Install.

Your application is automatically installed on your instance.
The vulnerability admin can now configure the application.

12. Once the installation completes, navigate to **Rapid7 Vulnerability Integration > Administration > Configuration**.

13. Select an Integration Type from the drop-down menu.

14. Select an integration instance. The default Rapid7 InsightVM integration instance is selected by default. If that is the one you want, go to step 15. For multiple deployments of the Rapid7 InsightVM integrations:

   a. Open the Lookup list on **Integration Instance** field, select an existing integration instance and go to step 15, or click **New** in the pop-up menu.

   b. For **New**, enter a **Name** for the integration instance and click **Submit**. The integration type appears in the Rapid7 configuration form.

   i **Note:** You can delete any integration instance except the default. Deleting an instance deletes the following (excluding VIs):

      • Integrations
      • Instance Parameters
      • Integration Runs
      • Integration Processes
      • Instance column on the VI is marked empty

   c. Continue to step 15.

15. Click the Integration Setup tab.

16. On the appropriate form, fill in the fields:

   **Integration Setup tab for InsightVM integration type**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InsightVM Region</td>
<td>The server URL you acquired from the Rapid7 site.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>API Key</td>
<td>The API key you acquired from your Rapid7 Insight account.</td>
</tr>
<tr>
<td>Validation Status</td>
<td>Read only: Status of credential validation process.</td>
</tr>
</tbody>
</table>

**Integration Setup tab for Data Warehouse Integration type**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JDBC credential name</td>
<td>Name of your data warehouse credentials.</td>
</tr>
<tr>
<td>User name</td>
<td>Rapid7 data warehouse user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Rapid7 data warehouse password.</td>
</tr>
<tr>
<td>Validation Status</td>
<td>Read only: Status of credential validation process.</td>
</tr>
<tr>
<td>Database server DNS/IP</td>
<td>DNS or IP address for your data warehouse.</td>
</tr>
<tr>
<td>Database port</td>
<td>Port to use for your data warehouse integration.</td>
</tr>
<tr>
<td>Database name</td>
<td>Name of your data warehouse.</td>
</tr>
<tr>
<td>Data delay offset (Days)</td>
<td>The data delay offset factors in the delay between the real-time data in Rapid7 Nexpose and the data in the data warehouse.</td>
</tr>
<tr>
<td>MID Server</td>
<td>MID Server to use. Only standalone MID servers are supported. Clumped MID servers are not supported.</td>
</tr>
<tr>
<td>MID Server timeout (min)</td>
<td>Number of minutes to wait for the MID Server to respond before timing out the integration run.</td>
</tr>
</tbody>
</table>

17. Verify successful configuration by clicking **Test credentials**. Configuration is successfully completed unless an error message is displayed. If an error message is displayed during the configuration, reenter your data.

18. Click **Save**.

19. Click the **Import Configuration** tab.
20. On the appropriate form, fill in the fields.

**Import Configuration tab for InsightVM**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min CVSS score</td>
<td>Minimum vulnerable item CVSS score used to filter vulnerable items during import.</td>
</tr>
<tr>
<td>Max CVSS score</td>
<td>Maximum vulnerable item CVSS score used to filter vulnerable items during import.</td>
</tr>
</tbody>
</table>
| Site filter          | Limits the data to the Rapid7 InsightVM sites chosen from the Sites list. You can choose more than one. The default (empty) is all sites. To prepopulate the Sites list, run the Rapid7 Site Integration — API prior to setting this field.  
  **Note:** Prior to v12.0 Sites for Rapid7 InsightVM must be created manually in order to use this feature. See Create sites for Rapid7 InsightVM (Prior to v12.0) for more information.  
  For information on using site filtering, see Filtering by Rapid7 sites. |
| Create CVE entry     | When checked, placeholders for CVEs, not already present, are created as NVD records and referenced in the third-party entry for Rapid7. When unchecked, these CVEs are ignored.  
  **Note:** In version 9.0, CVE records, not already present, are created as NVD records and referenced in the third-party entry for Rapid7, by default. |
| Close by age (Deprecated) | Date after which the scheduled job, Check Close Vul Item By Age, closes the record. When selected, the choices are 30, 60, or 90 days from the Last Found date. |
| v10.3: Reopen resolved by age | When selected, vulnerable items are automatically reopened when the number of days they have been resolved but not closed matches the value displayed in the Reopen resolved after field. |
## Import Configuration tab for Data Warehouse

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create CVE entry check box</td>
<td>When checked, placeholders for CVEs, not already present, are created as NVD records and referenced in the third-party entry for Rapid7. When unchecked, these CVEs are ignored. [Note: In version 9.0, CVE records, not already present, are created as NVD records and referenced in the third-party entry for Rapid7, by default.]</td>
</tr>
<tr>
<td>Min CVSS score</td>
<td>Minimum vulnerable item CVSS score used to filter vulnerable items during import.</td>
</tr>
<tr>
<td>Max CVSS score</td>
<td>Maximum vulnerable item CVSS score used to filter vulnerable items during import.</td>
</tr>
<tr>
<td>Site filter</td>
<td>Limits the imported Sites Integration data to the sites chosen. You can choose more than one. [Note: Since the default setting is to import data from all sites, you do not need to use the filter if you want all sites. Doing so slows down the request.]</td>
</tr>
<tr>
<td>Close by age (Deprecated)</td>
<td>Date after which the scheduled job, Check Close Vul Item By Age, closes the record. When selected, the choices are 30, 60, or 90 days from the Last Found date.</td>
</tr>
<tr>
<td>v10.3: Reopen resolved by age</td>
<td>When selected, vulnerable items are automatically reopened when the number of days they have been resolved but not closed matches the value displayed in the Reopen resolved after field.</td>
</tr>
</tbody>
</table>

21. Click **Save**.

The **Import since** date field in the Rapid7 integrations is blank, by default, except for the Rapid7 Vulnerability Integration - API and the Rapid7 Vulnerable Item Integration - API. For these integrations, these fields are set to 1998-12-31 or 1999-01-01.

To retrieve historical data during your initial import from the Rapid7 scan, set a start date in the appropriate integration records. This process works for any Rapid7 integration with the following exceptions:
• The Rapid7 Exploit and Malware Kit integrations do not show the **Import since** field, because they do not do delta updates and therefore do not use that field.

• The Rapid7 Asset List integration ignores the field since its intent is to retrieve all data.

• For the initial run of the Rapid7 InsightVM Comprehensive Vulnerable Item Integration – API when the Auto-Close Stale Vulnerable Items module is enabled and the **Import since** field is left blank.

Starting with v10.3, when you enable the feature, a successful run from the Rapid7 Comprehensive Vulnerable Item Integration or the Rapid7 Comprehensive Vulnerable Item Integration - API is required. These integrations are disabled by default.

When you enable the Rapid7 InsightVM Comprehensive Vulnerable Item Integration – API, if you leave the **Import since** field blank on the integration configuration page, the value in the **days ago** field of the Auto-Close Stale Vulnerable Items form is also used for the **Import since** date on the first integration run. The default value for Auto-Close Stale Vulnerable Items is (90 days).

For example, if the **days ago** field in the Auto-Close Stale Vulnerable Items form is 90, and the **Import since** field on the Rapid7 Comprehensive Vulnerable Item Integration – API configuration page is blank, the first integration run imports the data for the last 90 days.

This relationship between the **Import since** and **days ago** fields applies only to the first integration run. After that, changing the **days ago** field on the Auto-Close Stale Vulnerable Items form doesn’t affect the **Import since** field on the Rapid7 Comprehensive Vulnerable Item Integration – API configuration page. The field is changed to the first run’s start time so that the subsequent integration runs import only the delta information.

The **Import since** field is editable, and you can enter whatever values you want for each of the integrations. To edit the **Import since** field, follow these steps.

**a. Navigate to Rapid 7 > Administration > Integrations**

**b. Select, for example, Rapid7 Vulnerable Item Integration - API.**

**c. Set the **Import since** field to the earliest date you want to retrieve. Each successful import resets this date to that day’s date and time.**

Your Rapid7 Vulnerability Integration configuration is complete.
What to do next
If your environment requires domain-separated imports, see Create domain-separated imports for the Rapid7 vulnerability integration.

To create or refine your lookup rules prior to import, see Create a Vulnerability Response CI lookup rule.

Create sites for Rapid7 InsightVM (Prior to v12.0)
Rapid7 InsightVM does not have a Site Integration. To use the site filtering capability for Rapid7 InsightVM, you must create sites manually.

Before you begin
Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure
1. Navigate to Rapid7 Vulnerability Integration > Sites.
2. Click New.
3. Enter a name for the Rapid7 InsightVM. The site name needs match exactly what appears in the Rapid7 application.
4. Enter a Rapid7 InsightVM integration instance.
   This site is ready to be used in the Site filter field within the Rapid7 InsightVM Import Configuration tab. See Filtering by Rapid7 sites for more information on using site filtering.
5. Repeat this process for each site you want to add.
   
   Note: The list of sites for Rapid7 InsightVM is static and needs to be maintained over time.

Filtering by Rapid7 sites
Filter by site for Rapid7 InsightVM integration types as well as Rapid7 Nexpose data warehouse integration types.

Before you begin
Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response
application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

⚠️ **Note:** Prior to version 12.0: Before you can filter by site using Rapid7 InsightVM, you must manually create sites. See Create sites for Rapid7 InsightVM (Prior to v12.0) for instructions on creating those sites.

Using site filtering can have a performance impact. For information on performance and other considerations prior to using site filtering, see KB0789221.

About this task

Procedure

1. Navigate to **Rapid7 Vulnerability Integration > Configuration**.
2. Select an integration instance.
3. Click on the **Import Configuration** tab.

⚠️ **Note:** If you want all sites, leave the site filter field empty. No site filter is equivalent to adding all sites.

Sites are integration instance specific. The lookup list for site filtering displays both Rapid7 InsightVM and Rapid7 Nexpose data warehouse integration instance sites. Make sure the site you choose matches the integration instance you selected. For example, if you choose a data warehouse site, by mistake, that site will not work for site filtering by Rapid7 InsightVM.

4. Click on the lookup list to view the site records for the current integration instance.
5. Add a site from the list to add to the site filter.
6. Repeat selection to add additional sites.

7. Click **Save**.
   These sites are used to filter by site during the next import. See [for information on adding the prefix SITE to your site data](#).

**Create domain-separated imports for the Rapid7 vulnerability integration**

If you require vulnerability integration data to be imported to a specific domain, you must assign a user in that domain to run the integrations.

**Before you begin**

Role required: sn_vul_r7.admin and import_admin

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see [Assign the Vulnerability Response persona roles using Setup Assistant](#). For more information about managing granular roles, see [Manage persona and granular roles for Vulnerability Response](#).
About this task
This set of tasks require coding or advanced ServiceNow expertise.

The import queues contain data attachments that the scheduled jobs (integrations) process. In a domain-separated environment, you must match the scheduled job with the correct import queue.

Procedure
1. Create a domain.
2. For every domain you create, create a user and assign the user to that domain.
   Think of this user as a run_as placeholder for the domain in one of your Rapid7 vulnerability integrations. It is the equivalent to the VR.System user in the global domain. This user needs access to data sources, and vulnerability data.

   Note: Do not use this user for any other purpose.
3. In each domain, create a scheduled job.
   a. Navigate to System Definition > Scheduled Jobs.
   b. Copy Scheduled Vulnerability Data Source Processor into the domain.
   c. To identify the scheduled job, append the domain to the name.
   d. In the Run as field change the run_as user to the user you created in the Step 2.
4. Ensure the integration runs in the run_as user domain.
a. Edit the **Execute Now** UI action to add this code to the top of the file.

**Example**

```javascript
// sys id below is of host detection integration
if (current.sys_id == "5d9cf0daff540300c68c9f783894fa4d") {
  current.run_as = gs.getUserID()
}
```

b. Edit the **VulnerabilityIntegrationUtils** script include method **addIntegrationRun** to add the highlighted code.

```javascript
addIntegrationRun: function(integrationGr, optInitialState) {
  if (!optInitialState)
    optInitialState = "ready";
  var importSource = "";
  if (integrationGr.getValue("name").indexOf("Qualys") !== -1)
    importSource = "Qualys";
  var gr = new GlideRecord("sn_vul_integration_run");
  gr.initialize();
  gr.setValue("integration", integrationGr.getUniqueValue());
  gr.setValue("state", optInitialState);
  gr.setValue("source", importSource);
  var qUser = new GlideRecord("sys_user");
  qUser.get(gs.getUserID());
  gr.setValue("sys_domain", qUser.getValue("sys_domain"));
  return gr.insert();
},
```

c. Add the highlighted code to the **VulnerabilityIntegrationUtils** script include method **addProcessRun**.

```javascript
addProcessRun: function(runGr, parameters) {
  var gr = new GlideRecord("sn_vul_integration_process");
  gr.initialize();
  gr.setValue("sys_domain", runGr.getValue("sys_domain"));
  gr.setValue("integration_run", runGr.getUniqueValue());
  if (parameters) {
    var json = new global.JSON();
    var encodedParams = json.encode(parameters);
    gr.setValue("parameters", encodedParams);
  }
```

d. Add the highlighted code to the **VulnerabilityIntegrationUtils** script include method **copyProcess**.

```javascript
copyProcess code
```
e. Edit the `DataSourceVulnReportRefreshProcessor` script include method `_processFromDataSourceGroups`.

**Example**

Change the original line of code:

```
this.integrationProcessGr.getUniqueValues());
```

to

```
this.integrationProcessGr.getUniqueValue(),this.integrationProcessGr.getValue("sys_domain")
```

Edited `_processFromDataSourcesGroups code`

```java
var mStr = new sn_vul.VulnerabilityDSAttachmentManager();
var queueItem = uds.getUniqueValue(), filename, payload;
`this.IntegrationProcessGr.getUniqueValue(), this.IntegrationProcessGr.getValue("sys_domain")`;
var g = new GlideRecord("this.QUEUE_TABLE");
g.initialize();
g.setValue("status", "MDM");
g.setValue("dataSource", dataSource);
if (optIntegrationProcess)
g.setValue("integrationProcess", optIntegrationProcess);
if (optDomain) {
    g.setValue("sys_domain", optDomain);
}
var sysId = g.insert();
```
h. Add the following highlighted code blocks to the `VulnerabilityDSAttachmentManager` script include function, `_processQueueEntry`.

```javascript
// processQueueEntry function
function processQueueEntry(entry) {
  if (this._getImportStatus(entry.data_source)) {
    var dataSourceGr = new GlideRecord('sys_data_source');
    if (dataSourceGr.get(entry.data_source)) {
      dataSourceGr.setValue('status', 'COMPLETE');
      dataSourceGr.setValue('processing_result', 'Data source does not exist, could not process.');
      dataSourceGr.updateDynamic();
      return;
    }
    try {
      var deletedDataSourceAttachments = new GlideRecord('sys_data_source_attachments_deleted');
      if (deletedDataSourceAttachments.get(entry.data_source)) {
        var error = 'VulnerabilityDSAttachmentManager.processQueueEntry: Attachments not deleted for queue entry ' + entry.sys_id;
        throw error;
      }
      var attachmentAso = new GlideAttachment();
      attachmentAso.copy(dataSourceGr, entry.sys_id + '' + sys_id + '');
      var schd = new GlideRecord('scheduled_import_set');
      schd.set('check_id', check_id);
      schd.set('check_name', 'Data source: ' + entry.data_source);
      schd.set('check_status', 'in_progress');
      schd.set('check_host', entry.instance_name);
      schd.set('check_host', entry.instance_name);
      schd.save(true);
    }
  } else {
    var gr = new GlideRecord('sys_queue_table');
    gr.addQuery('status', 'COMPLETE');
    gr.query();
    if (gr.next()) {
      return gr;
    }
  }
  // Then handle the regular queued items
  gr = new GlideRecord('sys_queue_table');
  gr.addQuery('status', 'COMPLETE');
  gr.query();
  if (gr.next()) {
    return gr;
  }
```

At this point, you are ready for domain-separated host detection imports.

**Note:** If you have multiple deployments of the Rapid7 InsightVM vulnerability integration, repeat this process for each deployment.

**Deduplicate Rapid7 Vulnerability Integration data warehouse records**

When migrating to the InsightVM integration type from the Data Warehouse integration type, you can deduplicate existing data warehouse vulnerable items as long as they belong to the same source data as your Rapid7 InsightVM data.
Before you begin
Role required: sn_vul_r7.admin or, v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task
This deduplication only works from the Rapid7 InsightVM vulnerable item integration to the Rapid7 Nexpose data warehouse records and not the other way around.

Procedure
1. Navigate to Rapid 7 > Integrations.
2. Set all Rapid7 Nexpose data warehouse integrations Active column settings to False, disabling the integrations.
3. Enter sys_properties.list in the left navigation panel.
4. Search for the Name: sn_vul_r7.deduplicate_DW_vulnerable_item.
5. Change the Value field to True.
6. Click the green checkmark icon.
   During the next Rapid7 InsightVM vulnerable item integration import, any match with existing data warehouse records prevents a duplicate vulnerable item from being created.

Rapid7 Vulnerability Integration run status chart
Rapid7 Nexpose sensors collect the data and automatically send it to the Rapid7 Nexpose or Rapid7 InsightVM products, which continuously analyze and correlates the information. It easily integrates with Vulnerability Response to map vulnerabilities to CIs and business services to determine impact and priority of potentially malicious threats. The Rapid7 Vulnerability Integration Run Status module is a graphical view of the status of Rapid7 Vulnerability Integration runs.
In the chart, point to any part (bar, pie, data point, and so on) to view general data specific to that part. If you click any part of a report, a list opens to provide detailed information.

Multiple factors can impact the performance of the integration run, like the amount of data and time taken to process this data. Starting with v10.3, two new graphs have been added to compare the performance metrics:

- **Rapid7 Vulnerable Item Ingestion Performance Metrics**: Compare daily performance metrics for assignment rules, group rules, risk rules, queue wait time, queue processing time, and other statistics for vulnerable items for the last 30 days, to identify the cause for any deviations in performance.

- **Rapid7 Vulnerable Item Ingestion Performance Throughput**: Compare daily vulnerable item ingestion throughput for the Rapid7 Vulnerable Item Integration - API. Throughput is measured in items per hour.

**Note**: In Rapid7, these graphs are supported only for the Insight VM integration.

---

© 2021 ServiceNow, Inc. All rights reserved.  
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Starting with v10.0:

- The value in the Imported Items column represents the total number of vulnerable items that are created from an integration run.
- The New items column displays the number of vulnerable items that are created from an integration run.
- The Duplicate items column is no longer populated. You may prefer to remove this column from the display.
- The Updated items column displays the number of times vulnerable items are updated during an integration run. This value is not the number of unique vulnerable items that are updated. If for example, a vulnerable item is updated two times during the integration run, it is counted two times and displayed as 2 updated items.
- The Unchanged items column displays vulnerable items found during the integration run that already exist in the database but were not updated, because none of the relevant field values had changed.

Note: Integration runs with zero results for all four of the following values: New CIs, Existing CIs, New Items, and Updated Items are filtered out of the Rapid7 Integration Runs list.

### Rapid7 Vulnerability Integration run status chart reports

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last 30 Days Rapid7 Results</td>
<td>The number of integration runs completed for each integration. Shows both successful and failed runs. Run in a bar visual.</td>
</tr>
<tr>
<td>Last 30 Days Rapid7 New VIs</td>
<td>The number of new vulnerable items imported in the last 30 days. Shown as an integer.</td>
</tr>
</tbody>
</table>
Rapid7 Vulnerability Integration run status chart reports (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last 30 Days Rapid7 Updated VIs</td>
<td>The number of updated vulnerable items imported in the last 30 days. Shown as an integer.</td>
</tr>
<tr>
<td>Last 30 Days Rapid7 Duplicates</td>
<td>The number of duplicate vulnerable items imported in the last 30 days. Shown as an integer.</td>
</tr>
<tr>
<td>Rapid7 Integration Runs</td>
<td>The integration run records in a list.</td>
</tr>
<tr>
<td>Version 10.3: Last 30 Days Rapid7 Vulnerable Item Ingestion Performance Metrics</td>
<td>Daily performance metrics for vulnerable items compared for the last 30 days.</td>
</tr>
<tr>
<td>Version 10.3: Last 30 Days Rapid7 Vulnerable Item Ingestion Performance Throughput</td>
<td>Daily vulnerable item ingestion throughput for the Rapid7 Vulnerable Item Integration - API measured for the last 30 days.</td>
</tr>
</tbody>
</table>

View the Rapid7 Vulnerability Integration import runs status dashboard

Use the Rapid7 vulnerability import run status dashboard to verify the success of your integration runs, locate any issues and inform your remediation decisions.

Before you begin
Roles required: sn_vuln.admin

About this task
This procedure makes the following assumptions.

- You have Vulnerability Response and the Rapid7 Vulnerability Integration installed and configured.
- Rapid7 Vulnerability Integration imports are scheduled and running.
- Rapid7 integration run status charts are in use.

Procedure
1. Navigate to Rapid7 > Integration Run Status.
2. If you are not using the Rapid7 integration run status chart, navigate to Rapid7 > Integrations.
Choose an integration.

Click the Vulnerability Integration Runs related list.

Verify that all imports have succeeded.

**Trouble?**

The most common causes for a failed run:

- Network interruption
- Bit decay in the data transfer resulting in corrupted data during the transform

For all these conditions, click **Execute now** and rerun the integration.

**Understanding the Shodan Exploit Integration**

The ServiceNow® Shodan Exploit Integration application uses data imported from the Shodan search engine to help you determine the impact and priority of potentially malicious exploits.

**Request apps on the Store**

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

**Shodan Exploit Integration**

The Shodan search engine collects exploit data and the Shodan API makes that database available to the Now Platform®. It easily integrates with the ServiceNow® Vulnerability Response application to map exploits to third-party vulnerabilities enriching the exploit data in your instance.

There is a configured run-as user for each integration record. The default value for this user is **VR.System**. Do not change this value.

Every day, scheduled jobs invoke the integrations automatically in the order they are listed. You can also execute individual scheduled jobs manually. Scheduled jobs simplify the vulnerability remediation lifecycle by keeping the instance synchronized with other vulnerability management systems.
Available versions

<table>
<thead>
<tr>
<th>Release version with Paris</th>
<th>Release Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shodan Exploit Integration v10.5</td>
<td></td>
</tr>
<tr>
<td>Shodan Exploit Integration v10.4</td>
<td></td>
</tr>
<tr>
<td>Shodan Exploit Integration v10.3</td>
<td></td>
</tr>
<tr>
<td>Shodan Exploit Integration v10.0</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Response integrations release notes</td>
<td></td>
</tr>
<tr>
<td>For compatibility information, see KB0856498</td>
<td>Vulnerability Response Compatibility Matrix and Release Schema Changes</td>
</tr>
</tbody>
</table>

Roles
Shodan Exploit Integration tasks involve the following roles.

- **sn_vul_shodan.admin**: Users with this role can read, write, and delete records.
- **sn_vul_shodan.user**: Users with this role can read and write records.
- **sn_vul_shodan.read**: Users with this role can read records.

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Shodan exploit integrations
To view the Shodan exploit integrations, navigate to **Shodan Exploit Integration > Integrations**.

The following integrations are included in the base system. These integrations are active by default.

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shodan ExploitDB Integration</td>
<td>Retrieves ExploitDB data from Shodan and enriches your third-party vulnerability data. This integration is set to run daily at 03:15:00.</td>
</tr>
</tbody>
</table>
Shodan exploit integrations (continued)

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shodan Metasploit Integration</td>
<td>Retrieves Metasploit information from Shodan and enriches your third-party vulnerability data. This integration is set to run daily at 01:15:00.</td>
</tr>
</tbody>
</table>

To change the default start time for the scheduled integration imports, see Set Shodan Exploit Integration import time.

To view exploit data in third-party vulnerabilities, see View Vulnerability Response vulnerability libraries.

Changing other Shodan Exploit Integration settings requires advanced ServiceNow and Vulnerability Response expertise and is beyond the scope of the product documentation.

Preparing for the Shodan Exploit Integration

A successful Shodan Exploit Integration requires planning and careful execution of pre-integration tasks. Prepare for the integration by performing these tasks. The Shodan Exploit Integration assumes that you are familiar with the Shodan search engine and API.

Before you begin

The Shodan Exploit Integration requires an API key. Register with the Shodan website for a free subscription to acquire this key.

Role required: admin

About this task

Note: Before running the integration, make any necessary configuration changes based on your requirements.

- If you have not imported NIST Vulnerability Database (NVD) data into Vulnerability Response, do so before installing the Shodan Exploit Integration. Importing the NVD data ensures that your Common Vulnerability and Exposure (CVE) data auto-populates the exploit records.

  Without NVD data, a placeholder is created in the exploit record and not entered until the next NVD update. For more information on NVD, see Managing NVD, CWE, and third-party data libraries.

- There is a configured run-as user for each integration record. The default value for this user is VR.System. Do not change this value.
Install and configure the Shodan Exploit Integration for Security Operations

Before you can run the Shodan Exploit Integration in your instance, download and install it from the ServiceNow Store. This application is available as a separate subscription.

**Before you begin**

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

ℹ️ **Note:** This process applies only to applications downloaded to production instances. If you're downloading applications to sub-production or development instances, it's not necessary to get entitlements. Proceed to [Activate a ServiceNow Store application](#).

<table>
<thead>
<tr>
<th>Setup tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have valid ServiceNow entitlements for the Vulnerability Response application and the Shodan Exploit Integration for Security Operations application.</td>
<td>To verify entitlements, navigate to <a href="#">Subscription Management &gt; Subscriptions</a> in your instance. The list displays the subscriptions your organization has purchased. For more information about getting entitlements for a Security Operations application from the ServiceNow Store, see <a href="#">Get entitlement for a Security Operations product or application</a>.</td>
</tr>
<tr>
<td>(Optional) If not already installed and activated, you may prefer to install the Vulnerability Response application prior to installing the third-party application.</td>
<td>For more information about installing and activating the Vulnerability Response application, see, <a href="#">Install and configure Vulnerability Response</a>.</td>
</tr>
<tr>
<td>Prepare for the integration.</td>
<td>See <a href="#">Preparing for the Shodan Exploit Integration</a>.</td>
</tr>
</tbody>
</table>

Role required: admin

**Procedure**

1. Log in to the instance you want to install the Shodan Exploit Integration application on.

2. Navigate to [System Applications > All Available Applications > All](#).
3. Locate the Shodan Exploit Integration for Security Operations application, select the version you want, and click **Install**.

![Shodan Exploit Integration for Security Operations](image)

**Note:** If you are entitled to an update for this application, the **Update** button is displayed.

The Application installation dialog displays the application dependency status. Any required dependencies not already installed are automatically installed along with the application.

4. In the dialog, click **Install**.

![Application installation dialog](image)

The Install dialog indicates when the installation is successfully completed.

5. Navigate to **Shodan Exploit Integration > Configuration**.

6. Enter your Shodan API Key.
7. Click **Save**.
   Your Shodan Exploit Integration configuration is complete.

### Set Shodan Exploit Integration import time
For your convenience, you can reset the start time for the Shodan exploit integrations.

**Before you begin**
Role required: admin

**About this task**
After the initial import, Shodan exploit integrations bring in delta data unless a full import is requested. See Perform a manual Shodan exploit import for more information on full imports.

**Procedure**
1. Navigate to **Shodan Exploit Integration > Integrations**.
2. Choose an integration.
3. Set the new **Start time**. Time is calculated as Hours in local time. The default time for the Shodan exploit imports is 03:15:00.
4. Click **Update**.
   The new time is used for the next scheduled import.
**Perform a manual Shodan exploit import**

If your initial import failed, or you do not want to wait for the scheduled initial import, you can perform a full data import independent of the daily scheduled job.

**Before you begin**

Role required: v10.3 sn_vul.vulnerability.admin or sn_vulv.admin (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

**Procedure**

1. Navigate to **Shodan Exploit Integration > Integrations**.
2. Choose an integration.
3. Select the **Full data import** check box.
4. Click **Execute Now**.
   - Once the import is complete, the check box is unchecked and delta imports resume.

**View the Shodan Exploit Integration import run status**

Use the Vulnerability Integration Runs related list to verify the success of your integration runs, locate any issues, and inform your remediation decisions.

**Before you begin**

To view the Shodan import run status:

- The Vulnerability Response application and the Shodan Exploit Integration must be installed and configured.
- The Shodan Exploit Integration imports must be scheduled and running.

Role required: sn_vuln.admin

**Procedure**

1. Navigate to **Shodan Exploit Integration > Integrations**.
2. Select an integration.
3. Click the **Vulnerability Integration Runs** related list.
4. Verify that all imports have succeeded.
Trouble?
The most common causes for a failed run include:

- Network interruption
- Bit decay in the data transfer resulting in corrupted data during the transform

If you encounter any of these conditions, select the Full data import check box, click Execute Now, and rerun the integration.

Understanding the Tenable Vulnerability Integration

The Vulnerability Response Integration with Tenable application developed by ServiceNow engineering for the Tenable Vulnerability Integration uses data imported from the Tenable.io and Tenable.sc products to help you prioritize and remediate vulnerabilities for your assets. The application is available with a separate subscription from the ServiceNow® Store.

Starting with version 12.1 of Vulnerability Response, the Tenable Vulnerability Integration employs two Tenable integrations, Tenable.io and Tenable.sc, to import third-party scanner data about your assets and vulnerabilities. The Vulnerability Response Integration with Tenable application supports the Tenable.sc product starting with version 5.13.

- Tenable.io is a cloud-based enterprise integration.
- Tenable.sc is an on-premises integration that gives you the option to use a MID Server if the Tenable.sc product and your Now Platform instance are in the same environment.
- If the Tenable.sc product and your Now Platform instance are not in the same environment, you are required to use a MID Server.

The Vulnerability Response Integration with Tenable application is available on the ServiceNow Store with a separate subscription.
Available versions for Paris

<table>
<thead>
<tr>
<th>Release version</th>
<th>Release notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Response Integration with Tenable v2.2</td>
<td>Vulnerability Response integrations release notes</td>
</tr>
<tr>
<td>Vulnerability Response Integration with Tenable v2.1</td>
<td>For compatibility information, see KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes</td>
</tr>
<tr>
<td>Vulnerability Response Integration with Tenable v2.0</td>
<td></td>
</tr>
</tbody>
</table>

Terms and Key features of the integrations

**Vulnerable items and vulnerabilities**

A vulnerable item is created in your Now Platform instance when:

- An imported vulnerability from a third-party scanner is matched to an existing asset (a configuration item in your CMDB). The Tenable product refers to these matches as **vulnerabilities**.

- An imported vulnerability from a third-party scanner is not matched to an existing asset in your CMDB. In this case, an unmatched CI is also created along with a vulnerable item.

For unmatched CIs, you can also use the Identification and Reconciliation Engine (IRE) to create CIs in two new classes when an existing CI cannot be matched with a host. Otherwise, unmatched CIs are created in the Unmatched CI classes. For more information, see Creating CIs for Vulnerability Response using the Identification and Reconciliation engine.

Third-party vulnerability entries and plugins
Third-party vulnerability entries are imported from third-party scanners and listed in the Third-Party Vulnerability Entries table in your Now Platform instance. Third-party vulnerability entries from Tenable are ingested and used to search for matches to existing assets listed in your CMDB. Tenable refers to third-party vulnerability entries as Plugins.

**Configuration item (CI)**

Configuration items are the existing assets listed in your CMDB.

**Discovered item**

Assets ingested from the Tenable asset import are matched to existing configuration items in your CMDB. Imported assets are updated.

If a match is not found, a CI is created in the Unmatched CI class of the CMDB. If the CMDB CI Class Models plugin is enabled, the Identification and Reconciliation Engine (IRE) creates new CIs using new classes. For more information, see Creating CIs for Vulnerability Response using the Identification and Reconciliation engine. If the original, unmatched CI is reclassified, discovered item records are updated to reflect the state. Discovered items give you visibility into how assets are identified and mapped to CIs in the CMDB.

**CI lookup rules**

When data is imported from a third-party integration, Vulnerability Response automatically uses host (asset) data to search for matches in the Configuration Management Database (CMDB). CI lookup rules are used to identify CIs and add them to VI records when VIs are created to aid you with remediation.

**Rescan and remediation scan**

You can initiate a targeted rescan command on a specific configuration item, vulnerability group, or third-party entry directly from vulnerable item, vulnerability group, and third-party vulnerability entry records in your Now Platform instance. Tenable refers to this rescan as a remediation scan.

**Automatically close older VIs**

With the Auto-Close Stale Vulnerable Items module in your Now Platform, you can clean up older, stale vulnerable items (VI)s not recently found by your third-party integrations. Moving these VIs to Closed helps you reduce the number of active vulnerable items and vulnerability groups and reconcile assets in your CMDB.
You can use all the integrations with the Vulnerability Response Integration with Tenable to automatically close stale VIs.

The Tenable.io and Tenable.sc integrations also include the following key features:

- Starting with v2.1 of the Tenable Vulnerability Integration, create unique configuration items (CIs) that include different network partition identifiers for assets in your environment that share the same IP address. Identify the distinct assets across your environment and update the CIs on your existing discovered item, vulnerable item, and detection records to give you more details about your vulnerabilities.

- You can schedule when you want the jobs to run for all the Tenable.io and Tenable.sc integrations. You can also execute scheduled jobs manually on-demand.

- For asset imports with Tenable.io, you can enable asset tags to organize and track the assets listed in your CMDB in the Tenable.io environment.

- The Tenable.io and Tenable.sc integrations permit you to configure CI Lookup Rules to define how asset data from third-party sources are used to identify Configuration Items (CIs) in your Now Platform CMDB.

- The Tenable.io and Tenable.sc integrations permit you to set import filters on the vulnerabilities import so that you import only the vulnerabilities from Tenable that you want. For Tenable.io, you have the option to import Fixed vulnerabilities from Tenable with the vulnerabilities import.

- For Tenable.sc, you have the option to initiate rescans on-demand directly from vulnerable item, vulnerability group, and third-party entry records in your Now Platform instance. If VIs have been transitioned to Closed/Fixed but are not yet updated in your instance, you can verify vulnerabilities on specific configuration items have been remediated. See Initiate rescan for the Tenable.sc integration.

The following sections list more details about the Tenable integrations.

**Required Now Platform roles**

The integration tasks require the following roles in your Now Platform instance.

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.
admin

The system admin uses Setup Assistant to install the Vulnerability Response Integration with Tenable application. If not assigned, the admin assigns the vulnerability admin (sn_vul.vulnerability_admin) and other roles in Setup Assistant.

sn_vul.vulnerability_admin

Once assigned, the vulnerability admin completes the configuration of the Tenable integrations in Setup Assistant. This role has complete access to the Vulnerability Response (VR) application and its records. The vulnerability admin configures all VR applications and rules for installed third-party integrations.

sn_vul_tenable.configure_integration

This role contains the sn_vul_tenable.read_integration granular role and users with this role can configure the Vulnerability Response Integration with Tenable application.

sn_vul_tenable.read_integration

Users with this roles can view (read) but not edit records of the Vulnerability Response Integration with Tenable application.

Vulnerability Response group

By default, the Vulnerability Response group is available in Setup Assistant. Users assigned to the Vulnerability Response group inherit the sn_vul.read_all and sn_vul.remediation_owner roles automatically.

Tenable.io and Tenable.sc Integrations

Multi-source is supported for all of the Tenable.io and Tenable.sc integrations. You can add and deploy multiple instances of the following integrations across your environment from Setup Assistant in Vulnerability Response. You also install and configure the Vulnerability Response Integration with Tenable application from Setup Assistant.
<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Tenable.io Assets Integration**   | • Retrieves all asset data, including asset tags, from the Tenable.io product and processes it in your instance.  
• Creates unique CIs for unmatched assets, or updates existing CIs with the network partition identifier attribute for assets across your environment that share the same IP address.  
• Coordinates the REST message calls to the Asset API.  
• The output of this integration is discovered items.  
• Data is imported in chunks and stored in the [sn_vul_tenable_chunk_status] table. Table cleaner automatically removes stored data from this table after 30 days.  
• Starting with v2.2, **Last Scan Time** is imported and updated only for assets that have vulnerabilities. |
| **Tenable.io Plugin Integration**   | • Retrieves the plugin data from the Tenable.io product. Retrieved data are based on the date the plugins were last updated by a Tenable.io integration run.  
• This import ensures that the Tenable.io Identifiers (Ten IDs) are current.  
• Coordinates the REST message calls to the Plugin API.  
• The output of this integration is third-party vulnerabilities. |
| **Tenable.io Fixed Vulnerabilities Integration** | • Retrieves vulnerability data based on severity filters from the Tenable.io product and processes it in your instance.  
• When the flag **Fixed Vulnerabilities** is enabled in Setup Assistant, it creates new VIs in the **Fixed** state.  
• Creates unique CIs for unmatched assets, or updates existing CIs with the network partition |
## Tenable.io integrations (continued)

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration identifier attribute for assets across your environment that share the same IP address. • Coordinates the REST message calls to the Vulnerabilities API. • The output of this integration is <strong>Closed/Fixed</strong> vulnerable items (VIs). It also creates assets and third-party entries if they don’t exist. • Data is imported in chunks and stored in the <code>[sn_vul_tenable_chunk_status]</code> table. Table cleaner automatically removes stored data from this table after 30 days.</td>
<td></td>
</tr>
<tr>
<td>This integration run is scheduled. It is a chained integration, which means after a run is successfully completed, the open vulnerabilities integration described below is triggered.</td>
<td></td>
</tr>
<tr>
<td><strong>Tenable.io Open Vulnerabilities Integration</strong></td>
<td>• This integration is triggered upon successful completion of the Tenable.io Fixed Vulnerabilities Integration. • Retrieves vulnerability data based on the severity filters from the Tenable.io product and processes it in your instance. • Creates corresponding vulnerable items for active vulnerabilities. • Creates unique CIs for unmatched assets, or updates existing CIs with the network partition identifier attribute for assets across your environment that share the same IP address. • Coordinates the REST message calls to the Vulnerabilities API. • The output of this integration is <strong>New/Reopened</strong> vulnerable items (VIs). It also creates configuration items and third-party entries if they don’t exist.</td>
</tr>
</tbody>
</table>
### Tenable.io integrations (continued)

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Data is imported in chunks and stored in the [sn_vul_tenable_chunk_status] table. Table cleaner automatically removes stored data from this table after 30 days.</td>
</tr>
</tbody>
</table>

### Tenable.sc integrations

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
</table>
| Tenable.sc Assets Integration | • Retrieves all asset data from the Tenable.sc product and processes it in your instance.  
• Creates unique CIs for unmatched assets, or updates existing CIs with the network partition identifier attribute for assets across your environment that share the same IP address.  
• Coordinates the REST message calls to the Assets API.  
• The output of this integration is discovered items. |
| Tenable.sc Plugin Integration | • Retrieves the plugin data from the Tenable.sc product. Retrieved data are based on the date the plugins were last updated by a Tenable.sc integration run.  
• This import ensures that the Tenable.sc Identifiers (Ten IDs) are current and only active vulnerabilities are imported.  
• Coordinates the REST message calls to the Plugins API.  
• The output of this integration is third-party vulnerabilities. |
| Tenable.sc Fixed Vulnerabilities Integration | • Retrieves vulnerability data based on the query filters you configure for the Tenable.sc product and selected in Setup Assistant and processes it in your instance. |
## Tenable.sc integrations (continued)

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Tenable.sc Fixed Vulnerabilities** | - When the flag **Fixed Vulnerabilities** is enabled in Setup Assistant, it creates new VIs in the **Fixed** state.  
- Creates unique CIs for unmatched assets, or updates existing CIs with the network partition identifier attribute for assets across your environment that share the same IP address.  
- Coordinates the REST message calls to the Vulnerabilities API.  
- The output of this integration is **Closed/Fixed** vulnerable items (VIs). It also creates assets and third-party entries if they don’t exist. |
| **Tenable.sc Open Vulnerabilities Integration** | - This integration is triggered upon successful completion of the Tenable.sc Fixed Vulnerabilities Integration.  
- Retrieves vulnerability data based on the query filters selected from the Tenable.sc product and processes it in your instance.  
- Creates corresponding vulnerable items for active vulnerabilities.  
- Creates unique CIs for unmatched assets, or updates existing CIs with the network partition identifier attribute for assets across your environment that share the same IP address.  
- Coordinates the REST message calls to the Vulnerabilities API. |
### Tenable.sc integrations (continued)

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tenable.sc Scan Credential Integration</strong></td>
<td>- The output of this integration is <strong>Update/Create new</strong> vulnerable items (VIs) if they do not already exist. It also creates configuration items and third-party entries if they don’t exist.</td>
</tr>
<tr>
<td><strong>Starting with v2.2: Tenable.sc Backfill Vulnerabilities Integration</strong></td>
<td>- This backfill integration imports any open and fixed vulnerabilities that might have been missed during an import.</td>
</tr>
<tr>
<td></td>
<td>- This integration imports both open and fixed vulnerabilities from the last seven days to update your detections and vulnerable items.</td>
</tr>
<tr>
<td></td>
<td>- This integration might impact your performance.</td>
</tr>
<tr>
<td></td>
<td>- This integration is disabled by default.</td>
</tr>
<tr>
<td></td>
<td>- To update your vulnerability data and avoid potential performance problems, you might prefer to schedule the Tenable.sc Fixed Vulnerabilities and Open Vulnerabilities Integrations to run when no other scans are running.</td>
</tr>
<tr>
<td></td>
<td>- The output of this integration is:</td>
</tr>
</tbody>
</table>
### Tenable.sc integrations (continued)

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>◦ Closed/Fixed vulnerable items (VIs). It also creates assets and third-party entries if they don’t exist.</td>
</tr>
<tr>
<td></td>
<td>◦ to <strong>Update/Create new</strong> vulnerable items (VIs) if they do not already exist. It also creates configuration items and third-party entries if they don’t exist.</td>
</tr>
</tbody>
</table>

### Vulnerable items

Vulnerable items are grouped into vulnerability groups according to group rules and assigned for remediation based on your assignment rules. For more information, see [Vulnerability Response groups and group rules overview](#) and [Vulnerability Response assignment rules overview](#).

### Configuration item (CI) lookup rules

CI Lookup Rules identify CIs and determine when to add them to a vulnerable item. For more information on how CI lookup rules work, see [CI Lookup Rules](#) for identifying configuration items from Vulnerability Response third-party vulnerability integrations.

⚠️ **Note:** Rules, once removed, cannot be recovered. Rather than removing existing rules, disable them when creating new ones.

The following Tenable.io lookup rules are shipped with the base system.

- MAC_ADDRESS
- FQDN
- NetBIOS
- HostName
- DNS
- IP

The following Tenable.sc lookup rules are shipped with the base system.

- MAC_ADDRESS
- FQDN
• NetBIOS
• IP

Note: Multiple values for ip_address, mac_address, fqdns and network_interfaces are used for an asset. All values are considered in CI lookup rules for matching. All values are used to create multiple network adapters using IRE.

New properties to ignore IP addresses
In Tenable.io, there are two properties available if you want to ignore multiple IP addresses or multiple Mac addresses as part of your CI lookup rules:

ignoreIPAddress
A list of IP addresses to be ignored for CI lookup and CI creation.

ignoreMacAddress
A list of MAC addresses to be ignored for CI lookup or CI creation.

Discovered items
This module lists configuration items detected during import from the Tenable Vulnerable Item integrations and the Tenable Asset integrations.

Note: The default filter for this list is set to Unmatched. You can view all discovered items from an import by removing the filter.

For more information on the Discovered Items module, see Discovered Items.

Asset tags
Asset tags (also referred to as host tags) are used for organizing and tracking the assets in your organization. You can assign tags to your assets. Then, when launching scans, you can select tags associated with the assets you want to scan. The Asset Tags module allows you to download asset tag data from Tenable.io to your instance on a scheduled basis. Asset data that includes asset tags is pulled from Tenable.io and transformed using the Tenable.io Asset Transform integration transformation maps.

All Asset tags are imported as part of the Tenable.io Asset integration. Asset tags are generally used for filtering in Vulnerability Response assignment rules and Vulnerability Group Rules. The tags are displayed in the Discovered Item form.
Note: Run the Tenable.io Asset Integration prior to creating Vulnerability Response assignment rules or Vulnerability group rules in the Vulnerability Response application so that all tags are available for these rules before vulnerable items are imported and grouped. Also note the following points about tags:

- Tag storage is not case sensitive. For example, if you create a tag to describe assets in your San Diego location, and you create the San Diego tag, you can’t also create a SAN DIEGO tag and store it in the Asset tag table. San Diego and SAN DIEGO are considered to be the same asset tag by the system. Whichever tag is imported first is the tag that is stored and recognized going forward.

- Using asset tags as a Group Key in a Vulnerability Group Rule may have unexpected results. Asset tags are intended for use only in the Condition builder.

- Asset tags are controlled by the global system property sn_vul.import_asset_tags. This property is set to true by default. Disabling tags disables them across all Now Platform® instances.

Data retrieval filters
Data retrieval settings help you determine specifically the type and scope of data you want to import from the Tenable application to your Now Platform® instance. For a list of the most commonly used settings, see Data retrieval settings for the Tenable Vulnerability Integration.

Vulnerability Priority Rating (VPR)
The Vulnerability Priority Rating (VPR) is an attribute from the Tenable product that is imported and used with a new default risk calculator in Vulnerability Response. The Tenable Risk Rule is installed with the Vulnerability Response Integration with Tenable application as part of the Default Risk Calculator in the Vulnerability Calculators from Vulnerability Response.

This risk rule is disabled by default.

By enabling the Tenable risk calculator rule, the imported VPR values are used to calculate the Risk Score for vulnerable items. The default weight distribution for this risk calculator: VPR = 70%, Asset=15%, and Business Criticality=15%. Enabling this Tenable Risk Calculator rule may impact your data ingestion performance. For more information about Vulnerability Response calculators and the Tenable risk calculator rule, see Vulnerability Response calculators and vulnerability calculator rules.
Installation and configuration

After you download the Vulnerability Response Integration with Tenable from the ServiceNow® Store, installation and configuration is supported by the Setup Assistant in Vulnerability Response. See Configuring Vulnerability Response using the Setup Assistant for more information.

Preparing for the Tenable Vulnerability Integration

Prepare for the ServiceNow® Tenable Vulnerability integration by performing the following setup tasks.

Before you begin

A successful integration requires planning and careful execution of pre-integration tasks. For a smooth installation and configuration of the Vulnerability Response Integration with Tenable application, you may prefer to print the following checklist and verify the items listed are completed before you install the application and import vulnerability data into your Now Platform® instance.

⚠️ Note: If you have been importing data with the Tenable-built integration, and you want to start using the ServiceNow® Vulnerability Response Integration with Tenable, see the Required data cleanup for migrating from the Tenable Vulnerability Response integration to the ServiceNow Vulnerability Response Integration with Tenable [KB0863702] article for clearing existing vulnerability data in your instance.

Role required: admin

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>(Optional) If not already installed and activated, you may prefer to install the Vulnerability Response application prior to installing the third-party application. For more information about installing and activating the Vulnerability Response application, see, Install and configure Vulnerability Response. This integration requires version 12.1 of Vulnerability Response or later.</td>
</tr>
<tr>
<td>☐</td>
<td>If you don't already have it on your instance, get entitlements and download the Vulnerability Response Integration with Tenable application to your Now Platform® instance. The Vulnerability Response Integration with Tenable application supports the Tenable.sc product starting with version 5.13.</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>See Download an application from the ServiceNow Store for the first time.</td>
<td></td>
</tr>
</tbody>
</table>

- **Estimate the number of vulnerable items you expect to import.**
  
  Verify your instance can accept the number of vulnerable items you expect to import. An undersized instance can lead to long load times. If you do not know the size of your instance, or, if you need assistance, contact ServiceNow® Technical Support.

- **Verify that you have groups or users to manage the integrations and remediate vulnerable items.**

  **admin**
  
  The system admin uses Setup Assistant to install the Vulnerability Response Integration with Tenable application. If not assigned, the admin assigns the vulnerability admin (sn_vul.vulnerability_admin) and other roles in Setup Assistant.

  **sn_vul.vulnerability_admin**
  
  Once assigned, the vulnerability admin completes the configuration of the Tenable integrations. This role has complete access to the Vulnerability Response (VR) application and its records. Configures all VR applications and rules and configures third-party integrations.

  **sn_vul_tenable.admin**
  
  This role has complete access to the Vulnerability Response Integration with Tenable application and its records.

  **sn_vul_tenable.configure_integration**
  
  Can configure the Tenable Vulnerability Integration. This role contains the sn_vul_tenable.read_integration granular role.

  **sn_vul_tenable.read_integration**
  
  Can view (read) records of the Tenable Vulnerability Integration.
<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerability Response group</strong></td>
<td>By default, the Vulnerability Response group is available in Setup Assistant. Users assigned to the Vulnerability Response group inherit the sn_vul.read_all and sn_vul.remediation_owner roles automatically. The system admin performs the initial assignment of roles to users and groups in Setup Assistant for the integration. By default, the Vulnerability Response group is available. If not already created, you may prefer to create additional groups and add users with the User Administration module in your instance prior to using Setup Assistant. See Create a user group. Persona and granular roles are available to help you manage what users can do and see in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant.</td>
</tr>
<tr>
<td>To promote improved performance for your first import, you may prefer to disable certain features, rules, or jobs in your instance.</td>
<td></td>
</tr>
</tbody>
</table>
• Disable vulnerability calculators if you do not use them. These calculators, plus any you have defined, run every time a vulnerable item record is created or updated. See Disable vulnerability calculators.  
• During the initial import of records, certain notification-related business rules can cause many notifications to be generated, impacting performance. Prior to your initial import, you may prefer to Disable notification-related business rules as described in Optional import modifications for the Tenable Vulnerability Integration. |
| Verify you have enabled any features, rules, dependency plugins, or jobs in your instance required for the integration. |  
• Tenable.sc is an on-premises integration that gives you the option to use a MID Server if the Vulnerability Response Integration with Tenable product and your Now Platform instance are in the same environment. If
<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>the Tenable.sc product and your Now Platform instance are not in the same environment, you are required to use a MID Server. For more information about MID Servers in your instance, see MID Server.</td>
</tr>
<tr>
<td></td>
<td>• Verify the IntegrationHub plugin is installed and activated. This plugin enables base system components to call external systems using integration APIs and activates protocol steps like REST. Navigate to System Applications &gt; All Available Applications &gt; All and locate the plugin. If not installed in your instance, install and activate it.</td>
</tr>
<tr>
<td></td>
<td>Obtain Tenable credentials. Verify you have any account names, passwords, and other service information required by your Tenable products so that you have access to them. Tenable.io requires Administrator access with a permission attribute greater than or equal to 64. Tenable.sc requires Security Analyst or Manager access.</td>
</tr>
</tbody>
</table>

You are ready to Install and configure the Vulnerability Response Integration with Tenable application using Setup Assistant.

Install and configure the Vulnerability Response Integration with Tenable application using Setup Assistant

Before you run the ServiceNow® Tenable Vulnerability Integration, you need to download the Vulnerability Response Integration with Tenable application from the ServiceNow Store and install and configure it using the Setup Assistant in the Vulnerability Response application.

Before you begin

Before you install the Tenable application, verify you have completed all the items in the checklist in Preparing for the Tenable Vulnerability Integration.

Note: This process applies only to applications downloaded to production instances. If you're downloading applications to sub-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Roles required: admin for initial assignment of sn_vul.vulnerability_admin and installing the Tenable application in Setup Assistant. Vulnerability admin
(sn_vul.vulnerability_admin or sn_vul.admin (deprecated) to configure the application in Setup Assistant after it is installed.

Procedure

1. Navigate to Vulnerability Response > Administration > Setup Assistant > Integration application Installation.

After a few moments, the applications that are available for installation on your instance are displayed.

2. Locate the Tenable (Tenable Platform) tile and click Install.

This action installs the Vulnerability Response Integration with Tenable application you downloaded from the ServiceNow Store.

3. Follow the prompts provided in the Setup Assistant to continue with the installation.

4. For more information about installing applications using Setup Assistant, see Install Vulnerability Response third-party applications using Setup Assistant.

What to do next

After you complete the installation in Setup Assistant, navigate to Integration Configuration>Scanner Integrations in Setup Assistant to continue with the configuration. If you want more information to supplement the prompts provided in Setup Assistant, see Configure the Tenable Vulnerability Integration using Setup Assistant.

Data retrieval settings for the Tenable Vulnerability Integration

The following data retrieval settings help you determine specifically the type and scope of data you want to import from the ServiceNow® Tenable Vulnerability Integration to your Now Platform® instance.

The settings described in the following sections help you control the data you want to import. Additionally, you can set the values of these filters in Integration Instances. To view integration instances, navigate to Tenable Vulnerability Integration > Integration Instances and click your integration, Tenable.io or Tenable.sc.

On the Integration Instance page that is displayed, click the Integration Instance Parameters to display a list of parameters, or, the Vulnerability Integrations tabs for a schedule, REST Details, Integration details, Data Sources, and integration run information.
Common severity and retrieval settings and filters for Tenable.io and Tenable.sc in your Now Platform instance

The following settings are available for the Tenable.io and Tenable.sc integrations in your Now Platform instance. These and other configuration settings are displayed on the Integration Instance page of your Now Platform instance. You may prefer to leave these settings in their defaults for the first few integration runs.

Tenable.io

insert_fixed
If you enable the insert_fixed flag in Setup Assistant for the Vulnerabilities Import integration, new VIs are created for detections in the Fixed state that do not already exist in your instance.

severity_critical
This filter is enabled by default (true) to receive critical severity Vulnerabilities from the Tenable.io Open Vulnerabilities and Tenable.io Fixed Vulnerabilities Integrations.

severity_high
This filter is enabled by default (true) to receive high-level severity Vulnerabilities from the Tenable.io Open Vulnerabilities and Tenable.io Fixed Vulnerabilities Integrations.

severity_medium
This filter is disabled by default (false). Enable this filter to receive medium-level severity Vulnerabilities from the Tenable.io Open Vulnerabilities and Tenable.io Fixed Vulnerabilities Integrations.

severity_info
This filter is disabled by default (false). Enable this filter to receive info-level severity Vulnerabilities from the Tenable.io Open Vulnerabilities and Tenable.io Fixed Vulnerabilities Integrations.

severity_low
This filter is disabled by default (false). Enable this filter to receive low-level severity Vulnerabilities from the Tenable.io Open Vulnerabilities and Tenable.io Fixed Vulnerabilities Integrations.

size
This setting defines the number of plugin records to include in the result set from the Tenable.io Plugins Integration. Must be in the int32 format. Default value is 1,000. The maximum size is 10,000.

num_assets
The maximum number of vulnerabilities per exported chunk from the Tenable.io Fixed Vulnerabilities and Tenable.io Open Vulnerabilities Integrations. Default value is 50.

**chunk_size**
Specifies the number of assets per exported chunk by the Tenable.io Assets Integration. Default is 1,000.

**Tenable.sc**

**insert_fixed**
If you enable the `insert_fixed` flag in Setup Assistant for the Vulnerabilities Import integration, new VIs are created for detections in the Fixed state that do not already exist in your instance.

**offset**
Specifies the number of assets, plugins, and vulnerabilities imported in one integration run.

**Query filters**
Query filters are configured from within the Tenable console. These query filters have IDs that can be selected from Setup Assistant or from the Integration Instances page in your Now Platform instance. These filters are applied while retrieving the data from the Tenable.sc integrations.

**REST messages for the Tenable Vulnerability Integration**
The ServiceNow® Tenable Vulnerability Integration REST messages are used to make calls to the Tenable API.

**Tenable.io Assets REST message**
The Tenable.io Assets REST message retrieves Assets information for the Tenable.io Asset Integration. Changes to the REST message method record impact the requests made to Tenable.io to retrieve assets information.

**Tenable.io Plugins REST message**
The Tenable.io Plugins REST message retrieves Plugin information for the Tenable.io Plugin Integration. Changes to the REST message method record impact the requests made to Tenable.io to retrieve plugins information.

**Tenable.io Vulnerabilities REST message**
The Tenable.io Vulnerabilities REST message retrieves vulnerability information for both Open and Closed vulnerabilities from the Tenable.io Vulnerability
Integration. Changes to the REST message method record impact the requests made to Tenable.io to retrieve vulnerabilities information.

**Tenable.sc Assets REST message**

The Tenable.sc Assets REST message retrieves Assets information for the Tenable.sc Asset Integration. Changes to the REST message method record impact the requests made to Tenable.sc to retrieve assets information. The following table lists the request parameters to retrieve assets information.

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceType</td>
<td>cumulative</td>
<td>Indicates the source Tenable pulls data from. Used by code. Changes are not recommended.</td>
</tr>
<tr>
<td>sortDIR</td>
<td>desc</td>
<td>Indicates the sort direction for the data pulled from Tenable. Changes are not recommended.</td>
</tr>
<tr>
<td>sortField</td>
<td>severity</td>
<td>Indicates the field the data sort is based on. Changes are not recommended.</td>
</tr>
<tr>
<td>type</td>
<td>vuln</td>
<td>Indicates the type of data to be fetched from Tenable for the assets integration. Changes are not recommended.</td>
</tr>
</tbody>
</table>

**Tenable.sc Plugins REST message**

The Tenable.sc Plugin REST message retrieves plugin information for the Tenable.sc Plugins Integration. Changes to the REST message Get Plugins method record impact the requests made to Tenable.sc to retrieve plugins information.

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>active</td>
<td>Indicates the source Tenable pulls data from.</td>
</tr>
<tr>
<td>Parameter name</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>fields</td>
<td>id, description, cvssVector, cvssV3Vector, cvssV3TemporalVector, synopsis, cvssVector, baseScore, temporalScore, cvssV3Vector, cvssV3BaseScore, cvssV3TemporalScore, name, vprScore, vprContext, pluginPubDate, pluginModDate, xrefs, family, riskFactor, cpe, seeAlso, solution, exploitAvailable, exploitFrameworks, type, copyright, version, sourceFile, dependencies, requiredPorts, requiredUDPPorts, srcPort, dstPort, protocol, checkType, cvssVectorBF, stigSeverity, patchPubDate, patchModDate, vulnPubDate, modifiedTime, md5</td>
<td>Indicates the list of fields imported from Tenable.</td>
</tr>
</tbody>
</table>

**Tenable.sc Vulnerabilities REST message**

The Tenable.sc vulnerabilities REST message retrieves vulnerability information from the Tenable.sc Integration. Changes to the REST message Fetch Vulnerabilities or Fetch Patched Vulnerabilities method record impact the requests made to Tenable.sc to retrieve vulnerabilities information.
<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceType</td>
<td>cumulative/patched</td>
<td>Indicates the source Tenable pulls data from. For the Tenable.sc Open Vulnerabilities Integration, cumulative is sent as the source type. For the Fixed Vulnerabilities Integration, patched is sent as the source type.</td>
</tr>
<tr>
<td>sortDIR</td>
<td>desc</td>
<td>Indicates the sort direction for the data pulled from Tenable. Changes are not recommended.</td>
</tr>
<tr>
<td>sortField</td>
<td>severity</td>
<td>Indicates the field the data sort is based on. Changes are not recommended.</td>
</tr>
<tr>
<td>type</td>
<td>vuln</td>
<td>Indicates the type of data to be fetched from Tenable for the assets integration. Changes are not recommended.</td>
</tr>
</tbody>
</table>

**Tenable.sc Scan Credentials REST message**

**Tenable.sc Policy REST message**

The Tenable.sc policy POST REST message adds a policy for requested plugins. Generated policy will be used in Tenable.sc scan requests.

**Tenable.sc Scan REST message**

The Tenable.sc scan POST REST message adds a scan that is dependent on the access and permission defined in the request body of the rest message. It uses policy, plugin id, and IP(s) in the request body for the scan request.

**Tenable.sc Scan Result REST message**
The Tenable.sc Scan Result GET REST message provides scan details of the scan generated using the Scan REST message. It uses the scanResultId in the response of the scan REST messages and retrieves scan details for the triggered scan.

**Tenable.sc Scan Credentials**

The Tenable.sc scan credentials REST message retrieves the credentials information from Tenable.sc. Changes to the REST message 'Import' method record impact the requests made to Tenable.sc to retrieve the credentials information.

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fields</td>
<td>id,name,description,type</td>
<td>Indicates the list of fields imported from Tenable.sc</td>
</tr>
<tr>
<td>filter</td>
<td>usable</td>
<td>Indicates that the integration pulls only usable credentials from Tenable.sc</td>
</tr>
</tbody>
</table>

**Data transformation for the Tenable Vulnerability Integration**

After you identify the data to import, it is retrieved from the Tenable product and processed through a set of data sources and transforms in your instance.

During installation, normalized severity maps are installed in the Normalized Severity Mapping module. These maps transform imported Tenable severity levels to standard severity levels for processing in your instance. For information about creating severity maps, see Create a Vulnerability Response severity map on the product documentation website.

**Tenable.io Asset Import**

Imported asset data is first loaded into the Tenable.io Asset Import [sn_vul_tenable_io_asset_import] Table.

The Tenable.io Asset Integration transform map is used to transform the imported assets information. Changes to this transform alter how data from the Tenable Asset import is processed. To access this transform map, navigate to **System Import Sets > Transform Maps**. Search for Tenable.io Asset Transform.
The following tables lists the transform map fields by integration.

**Tenable.io Asset transform map fields**

<table>
<thead>
<tr>
<th>Source field</th>
<th>Target field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>u_id</td>
<td>source_id</td>
<td>Tenable provides a unique id for assets and maps to the discovered item record and is used for CI lookup.</td>
</tr>
<tr>
<td>u_ipv4s</td>
<td>ip_address</td>
<td>Maps the first ip value to the ip_address field on the discovered item record.</td>
</tr>
<tr>
<td>u_mac_addresses</td>
<td>mac_address</td>
<td>Maps the first mac_address value to the mac_address field on the discovered item record.</td>
</tr>
<tr>
<td>u_fqdns</td>
<td>fqdn</td>
<td>Maps the first fqdn value to the fqdn field on the discovered item record.</td>
</tr>
<tr>
<td>u_netbios_names</td>
<td>netbios</td>
<td>Maps the first netbios value to the netbios field on the discovered item record.</td>
</tr>
<tr>
<td>u_operating_systems</td>
<td>os</td>
<td>Maps the first OS value to the os field on the discovered item record.</td>
</tr>
<tr>
<td>u_last_scan_time</td>
<td>last_scan_date</td>
<td>Maps to the last_scan_date field on the discovered item record.</td>
</tr>
<tr>
<td>u_last_authenticated_scan</td>
<td>last_auth_scan_date</td>
<td>Maps to the last_auth_scan_date field on the discovered item record.</td>
</tr>
</tbody>
</table>
Tenable.io Asset transform map fields (continued)

<table>
<thead>
<tr>
<th>Source field</th>
<th>Target field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[script]</td>
<td>name</td>
<td>Maps the host name using the script's logic.</td>
</tr>
<tr>
<td>u_tags</td>
<td></td>
<td>The Tags are saved in sn_sec_cmn_host_tag. The mapping from tags to assets is saved in sn_sec_cmn_m2m_src_ci_tag.</td>
</tr>
</tbody>
</table>

There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

Tenable.io Asset transform map script timing and purpose

<table>
<thead>
<tr>
<th>When the script is run</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>onStart (when an import set has started transformation)</td>
<td>This transform is used to initialize the values in the import_set for the integration process. For internal use. Modifying or deleting is not recommended.</td>
</tr>
<tr>
<td>onBefore (before an import set has completed transformation)</td>
<td>A function used to update values in the host and verify if the host already exists. Based on the results, modifies the values in an import_set. For internal use. Modifying or deleting is not recommended.</td>
</tr>
<tr>
<td>onComplete (when an import set has completed transformation)</td>
<td>This transform is used to set the values of new CIs created, and CIs that have been updated and ignored. For internal use. Modifying or deleting is not recommended.</td>
</tr>
</tbody>
</table>

Tenable.io Plugins Integration

The Tenable.io plugins transform map is used to transform plugins imported from Tenable.io.
Note: Changes to this transform map alters how data received from the Tenable plugins is processed.

To access this transform map, navigate to System Import Sets > Transform Maps. Search for the Tenable.io Plugin Transform.

The tenable.io plugins payload contains all the fields in the `u_attributes` column of the `sn_vul_tenable_io_plugin_import` table. The attributes field is parsed and mapped to the third-party entry table records as listed in the following table.

<table>
<thead>
<tr>
<th>Source field</th>
<th>Target field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>id</td>
<td>Maps id from source and adds the TEN- prefix to it. For example, if the id received is 12345, the id in the target table is TEN-12345.</td>
</tr>
<tr>
<td>[script]</td>
<td>source</td>
<td>The source for imported TPE is Tenable.io.</td>
</tr>
<tr>
<td>[script]</td>
<td>source_instance</td>
<td>Reference to the Tenable deployment that imports this record.</td>
</tr>
<tr>
<td>family</td>
<td>category</td>
<td>Maps the family of plugin to the category column</td>
</tr>
<tr>
<td>plugin_modification_date</td>
<td>last_modified</td>
<td>Maps the <code>plugin_modification_date</code> to the <code>last_modified</code> field.</td>
</tr>
<tr>
<td>plugin_publication_date</td>
<td>date_published</td>
<td>Maps the <code>plugin_publication_date</code> to the <code>published date</code>.</td>
</tr>
<tr>
<td>has_patch</td>
<td>remediation_type</td>
<td>Maps the remediation type from <code>has_patch</code> value.</td>
</tr>
<tr>
<td>synopsis</td>
<td>threat</td>
<td>Maps the threat information about this vulnerability.</td>
</tr>
<tr>
<td>Source field</td>
<td>Target field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>cvss_base__score</td>
<td>score</td>
<td>Maps the cvss base score to the score column in third-party entry table.</td>
</tr>
<tr>
<td>solution</td>
<td>solution</td>
<td>Maps the solution provided by scanner to the solution column in the third-party entry table.</td>
</tr>
<tr>
<td>exploit_available</td>
<td>exploit</td>
<td>Maps the exploit_available provided by scanner to the exploit column in the third-party entry table.</td>
</tr>
<tr>
<td>vpr.score</td>
<td>source_risk_score</td>
<td>Maps the vpr score provided by scanner to the source_risk_score in the third-party entry table.</td>
</tr>
<tr>
<td>[script]</td>
<td>source_risk_rating</td>
<td>Maps the vpr score to the standard risk rating based on the score ranges:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 9 - 10 – Critical</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 7 – 9 – High</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 4 – 7 – Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0-4 - Low</td>
</tr>
<tr>
<td>vpr.drivers.age_of_vuln</td>
<td>age_of_vuln</td>
<td>Maps the age of the vulnerability from the scanner to the age_of_vuln column in the third-party entry table.</td>
</tr>
<tr>
<td>vpr.drivers.exploit_code_maturity</td>
<td>exploit_code_maturity</td>
<td>Maps exploit code maturity from the scanner to exploit_code_maturity</td>
</tr>
<tr>
<td>Source field</td>
<td>Target field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>vpr.drivers.product_coverage</td>
<td>product_coverage</td>
<td>Maps product coverage from the scanner to product_coverage in the third-party entry table.</td>
</tr>
<tr>
<td>vpr.drivers.threat_sources</td>
<td>threat_sources</td>
<td>Maps threat sources in the last 28 days from the scanner to threat_sources in the third-party table.</td>
</tr>
<tr>
<td>vpr.drivers.threat_intensity</td>
<td>threat_intensity</td>
<td>Maps threat intensity in the last 28 days from the scanner to threat_intensity in the third-party entry table.</td>
</tr>
<tr>
<td>vpr.drivers.threat_recency</td>
<td>threat_recency</td>
<td>Maps the threat recency information from scanner to threat_recency in the third-party entry table.</td>
</tr>
<tr>
<td>vpr.drivers.cvss3_impact_score</td>
<td>v3_impact_subscore</td>
<td>Maps cvss3 impact score to v3_impact_subscore column in the third-party entry table.</td>
</tr>
<tr>
<td>cvss_temporal_score</td>
<td>cvss_temporal_score</td>
<td>Maps the temporal score for CVSS v2.</td>
</tr>
<tr>
<td>cvss_v3_temporal_score</td>
<td>v3_temporal_score</td>
<td>Maps the temporal score for CVSS v3.</td>
</tr>
<tr>
<td>risk_factor</td>
<td>source_severity</td>
<td>Maps to the source severity in the third-party entry table.</td>
</tr>
<tr>
<td>name</td>
<td>name</td>
<td>Maps the name of the plugin to name in third-party entry table.</td>
</tr>
<tr>
<td>stig_severity</td>
<td>stig_severity</td>
<td>Maps the vpr score provided by the scanner to the source_risk_score</td>
</tr>
<tr>
<td>Source field</td>
<td>Target field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>plugin_type</td>
<td>check_type</td>
<td>Maps the plugin type to check_type in third-party entry table.</td>
</tr>
<tr>
<td>unsupported_by_vendor</td>
<td>unsupported_by_vendor</td>
<td>Maps the unsupported_by_vendor field to the unsupported_by_vendor column.</td>
</tr>
<tr>
<td>[script]</td>
<td>exploit_attack_vector</td>
<td>The exploit_attack_vector column in the third-party entry table is populated based on exploit_available and v3_attack_vector of columns.</td>
</tr>
</tbody>
</table>

In addition to the direct fields, other information is added as related lists to third-party entries.

<table>
<thead>
<tr>
<th>Source field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cve</td>
<td>Inserts CVE-related data into the reference table (sn_vul_nvd_entry). If the same CVE in the NVD entry table (sn_vul_nvd_entry) is found, it associates the current vulnerability to the NVD entry. The mapping can be found in sn_vul_m2m_entry_cve.</td>
</tr>
<tr>
<td>bid</td>
<td>The list of bug traqs is added as a reference.</td>
</tr>
<tr>
<td>see_also</td>
<td>The list of URLs is added as a reference.</td>
</tr>
<tr>
<td>xrefs</td>
<td>The list of X-REF is added as a reference.</td>
</tr>
</tbody>
</table>
There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

<table>
<thead>
<tr>
<th>When the script is run</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>onStart (when an import set has started transformation)</td>
<td>This transform is used to initialize the values in the import_set for the integration process. For internal use. Modifying or deleting is not recommended.</td>
</tr>
<tr>
<td>onBefore (before an import set has completed transformation)</td>
<td>A function used to update the values in the third-party entry, and verify if the third-party entry already exists. Based on the results, modifies the values in a third-party entry. For internal use. Modifying or deleting is not recommended.</td>
</tr>
<tr>
<td>onComplete (when an import set has completed transformation)</td>
<td>This transform is used to set the values of new CIs created, and CIs that have been updated and ignored. For internal use. Modifying or deleting is not recommended.</td>
</tr>
</tbody>
</table>

The TenableIOPPluginsImportProcessor script include is called from the onBefore transform script. It takes the output from Tenable.io plugins integration and transforms it into Now Platform third-party vulnerability entries. Any changes to this script include may alter the transformation of Tenable.io plugins data in the third-party entry table.

**Tenable.io Vulnerabilities Import**

The Tenable.io Vulnerable Item transform map are used to transform open and fixed vulnerabilities information imported from Tenable.io.

⚠️ **Note:** Changes to this transform map alter how data from the Tenable Vulnerabilities Import is processed.
The same transform map is used for both the Tenable.io Fixed Vulnerabilities Integration and the Tenable.io Open Vulnerabilities Integration. To access this transform map, navigate to **System Import Sets > Transform Maps**. Search for the Tenable.io Vulnerable Item transform map.

<table>
<thead>
<tr>
<th>Source field</th>
<th>Target field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>u_asset.uuid</td>
<td>id</td>
<td>Uuid is mapped to the id field of the cmdb_ci record.</td>
</tr>
<tr>
<td>u_asset.ipv4</td>
<td>ip_address</td>
<td>The ipv4 field is mapped to the ip address field of the cmdb_ci record.</td>
</tr>
<tr>
<td>u_asset.lastAuthenticatedResults.last_auth_scan_date</td>
<td></td>
<td>The last authenticated scan date is mapped to the last auth scan date of the cmdb_ci record.</td>
</tr>
<tr>
<td>u_asset.mac_address</td>
<td>mac_address</td>
<td>Mac address is mapped to the host mac address field of the cmdb_ci record.</td>
</tr>
<tr>
<td>u_asset.netbios_name</td>
<td>netbios</td>
<td>Netbios is mapped to the netbios field of cmdb_ci record.</td>
</tr>
<tr>
<td>u__plugin.cvss3_base_score</td>
<td>v3_temporal_score</td>
<td>CVSS v3 base score is mapped to the v3 base score of the third-party entry record.</td>
</tr>
<tr>
<td>u__plugin.cvss3_temporal_score</td>
<td>publication_date</td>
<td>CVSS v3 temporal score is mapped to the v3 temporal score in the third-party entry record.</td>
</tr>
<tr>
<td>u__plugin.cvss_base_score</td>
<td>score</td>
<td>CVSS base score is mapped to the score</td>
</tr>
<tr>
<td>Source field</td>
<td>Target field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>u_plugin.cvss_temporal_score</td>
<td>temporal_score</td>
<td>Temporal Score is mapped to the temporal score in the third-party entry record.</td>
</tr>
<tr>
<td>u_plugin.description</td>
<td>summary</td>
<td>Description is mapped to the summary field in the third-party entry record.</td>
</tr>
<tr>
<td>u_plugin.family</td>
<td>category</td>
<td>Maps the family of plugin to the category column of the third-party entry record.</td>
</tr>
<tr>
<td>u_plugin.modification_date</td>
<td>last_modified</td>
<td>Last modified date is mapped to the plugin last modified date in the third-party entry record.</td>
</tr>
<tr>
<td>u_plugin.publication_date</td>
<td>date_published</td>
<td>Publication date is mapped to the date published field of the third-party entry record.</td>
</tr>
<tr>
<td>u_plugin.risk_factor</td>
<td>source_severity</td>
<td>Risk factor is mapped to the source_severity field of the third-party entry record.</td>
</tr>
<tr>
<td>u_plugin.solution</td>
<td>solution</td>
<td>Solution is mapped to the solution field of the third-party entry record.</td>
</tr>
<tr>
<td>u_plugin.synopsis</td>
<td>threat</td>
<td>Synopsis is mapped to the threat field of the third-party entry record.</td>
</tr>
<tr>
<td>Source field</td>
<td>Target field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>the third-party entry record.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>u_severity_id</td>
<td>priority</td>
<td>Priority is mapped to the severity id from the payload. The default value is 5.</td>
</tr>
<tr>
<td>u_plugin.exploit_available</td>
<td>exploit</td>
<td>Maps the exploit_available provided by the scanner to the exploit column in the third-party entry table.</td>
</tr>
<tr>
<td>vpr.score</td>
<td>source_risk_score</td>
<td>Maps the vpr score provided by the scanner to the source_risk_score in the third-party entry table.</td>
</tr>
<tr>
<td>[script]</td>
<td>source_risk_rating</td>
<td>Maps the vpr score to the standard risk rating based on the score ranges:</td>
</tr>
<tr>
<td>u_plugin.vpr.drivers.age_of_vuln</td>
<td>age_of_vuln</td>
<td>Maps the age of vulnerability from the scanner to age_of_vuln in the third-party entry table.</td>
</tr>
<tr>
<td>u_plugin.vpr.drivers.exploit_code_maturity</td>
<td>exploit_code_maturity</td>
<td>Maps exploit code maturity from the scanner to exploit_code_maturity</td>
</tr>
<tr>
<td>Source field</td>
<td>Target field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>u_plugin.vpr.drivers.product_coverage</td>
<td>product_coverage</td>
<td>Maps product coverage from the scanner to product_coverage in the third-party entry table.</td>
</tr>
<tr>
<td>u_plugin.vpr.drivers.threat_sources</td>
<td>threat_sources</td>
<td>Maps threat sources in the last 28 days from the scanner to threat_sources in the third-party entry table.</td>
</tr>
<tr>
<td>u_plugin.vpr.drivers.threat_intensity</td>
<td>threat_intensity</td>
<td>Maps threat intensity in the last 28 days from the scanner to threat_intensity in the third-party entry table.</td>
</tr>
<tr>
<td>u_plugin.vpr.drivers.threat_recency</td>
<td>threat_recency</td>
<td>Maps the threat recency information from the scanner to threat_recency in the third-party entry table.</td>
</tr>
<tr>
<td>u_plugin.vpr.drivers.cvss3_impact</td>
<td>v3_impact_subscore</td>
<td>Maps CVSS3 v3 impact score to v3_impact_subscore column in the third-party entry table.</td>
</tr>
<tr>
<td>u_plugin.type</td>
<td>check_type</td>
<td>Maps the plugin type to check_type in third-party entry table.</td>
</tr>
<tr>
<td>u_plugin.unsupported_by_vendor</td>
<td>unsupported_by_vendor</td>
<td>Maps the unsupported_by_vendor field in plugin to the third-party entry table.</td>
</tr>
<tr>
<td>Source field</td>
<td>Target field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>unsupported_by_vendor</td>
<td></td>
<td>unsupported_by_vendor column.</td>
</tr>
<tr>
<td>[script]</td>
<td>exploit_attack_vector</td>
<td>The exploit_attack_vector column in the third-party entry table is populated based on exploit_available and v3_attack_vector of columns.</td>
</tr>
<tr>
<td>u_plugin.family_id</td>
<td>Family_id</td>
<td>Maps the plugin Family id to family_id column in third-party entry table.</td>
</tr>
<tr>
<td>port</td>
<td>port</td>
<td>Port is mapped to the port field of the vulnerable item record.</td>
</tr>
<tr>
<td>protocol</td>
<td>protocol</td>
<td>Protocol is mapped to the protocol field of the vulnerable item record.</td>
</tr>
<tr>
<td>u_first_found</td>
<td>first_found</td>
<td>First found is mapped to the first found field of the vulnerable item record.</td>
</tr>
<tr>
<td>u_last_found</td>
<td>last_found</td>
<td>Last found is mapped to the last found field of the vulnerable item record.</td>
</tr>
<tr>
<td>u_state</td>
<td>state</td>
<td>State is mapped to the State field in the vulnerable item record.</td>
</tr>
<tr>
<td>[script]</td>
<td>source</td>
<td>The source of the integration is populated. The vulnerable items</td>
</tr>
<tr>
<td>Source field</td>
<td>Target field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>[script]</td>
<td>integration_instance</td>
<td>The integration_instance is the name of the instance from which the vulnerable item is imported.</td>
</tr>
<tr>
<td>u_plugin.name</td>
<td>name</td>
<td>Maps the name of the plugin to name in third-party entry table.</td>
</tr>
<tr>
<td>u_plugin.stig_severity</td>
<td>stig_severity</td>
<td>Maps the stig severity of the plugin to stig severity column in Third-Party entry table.</td>
</tr>
</tbody>
</table>

In addition to the direct fields, other information is added as related lists to third-party entries.

<table>
<thead>
<tr>
<th>Source field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cve</td>
<td>Inserts CVE-related data into the reference table (sn_vul_nvd_entry). If the same CVE in the NVD entry table (sn_vul_nvd_entry) is found, it associates the current vulnerability to the NVD entry. The mapping can be found in sn_vul_m2m_entry_cve.</td>
</tr>
<tr>
<td>bid</td>
<td>The list of bug traqs is added as a reference.</td>
</tr>
<tr>
<td>see_also</td>
<td>The list of URLs is added as a reference.</td>
</tr>
<tr>
<td>xrefs</td>
<td>The list of X-REF is added as a reference.</td>
</tr>
</tbody>
</table>
There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

<table>
<thead>
<tr>
<th>When the script is run</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>onStart (when an import set has started transformation)</td>
<td>This transform triggers TenableIOVulnerabilitiesProcessor which imports data from Tenable.io using the import set and loads each record into the CMDB CI table, the Vulnerable Items table, and the Third-party vulnerability table. For internal use. Modifying or deleting is not recommended.</td>
</tr>
<tr>
<td>onBefore (before an import set has completed transformation)</td>
<td>A function to check if the Third-Party Entry and Detections already exist. If not, these records are created in their respective tables. For internal use. Modifying or deleting is not recommended.</td>
</tr>
<tr>
<td>onComplete (when an import set has completed transformation)</td>
<td>This transform is used to update the count of CIs, VIs and Detections as imported from Tenable.io. For internal use. Modifying or deleting is not recommended.</td>
</tr>
</tbody>
</table>

**Tenable.sc Asset Import**

Asset data imported from Tenable.sc is first loaded into the Tenable.sc Asset Import table (sn_vul_tenable_sc_asset_import). The Tenable.sc Asset Integration transform map is used to transform the imported assets information. Changes to this transform alter how data from the Tenable Asset import is Processed. To access this transform map, navigate to **System Import Sets > Transform Maps**. Search for the Tenable.sc Asset Transform.
<table>
<thead>
<tr>
<th>Source field</th>
<th>Target field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>u_uuid</td>
<td>id</td>
<td>The uuid is not populated from the Tenable api, so the 'u_uniqueness' attribute is used to create a unique uuid field for assets and map it to the cmdb_ci record.</td>
</tr>
<tr>
<td>u_ip</td>
<td>ip_address</td>
<td>Maps ip field from API to the ip_address field on a cmdb_ci record.</td>
</tr>
<tr>
<td>u_macaddress</td>
<td>mac_address</td>
<td>Maps the macaddress field from the API to the address field on the cmdb_ci record.</td>
</tr>
<tr>
<td>u_dnsname</td>
<td>fqdn</td>
<td>Maps the dnsname field from the API to the fqdn field on the cmdb_ci record.</td>
</tr>
<tr>
<td>u_netbiosname</td>
<td>netbios</td>
<td>Maps the netbios field from the API to the netbios field on the cmdb_ci record.</td>
</tr>
<tr>
<td>u_oscope</td>
<td>os</td>
<td>The OS information is extracted from the oscpe attribute in the payload and maps it to the os field on the cmdb_ci record.</td>
</tr>
<tr>
<td>u_lastauthrun</td>
<td>last_auth_scan_date</td>
<td>Maps the lastauthrun field from the API to the last_auth_scan_date field on the discovered item record.</td>
</tr>
<tr>
<td>u_lastauthrun and u_lastunauthrun</td>
<td>last_scan_date</td>
<td>The lastauthrun is extracted from the Tenable api or lastunauthrun. Based on</td>
</tr>
</tbody>
</table>
There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

<table>
<thead>
<tr>
<th>When the script is run</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>onStart (when an import set has started transformation)</td>
<td>This transform is used to initialize the values in the import_set for the integration process. For internal use. Modifying or deleting is not recommended.</td>
</tr>
<tr>
<td>onBefore (before an import set has completed transformation)</td>
<td>Function used to update the values in the host and verify if the host already exists. Based on the results, modifies the values in an import_set. For internal use. Modifying or deleting is not recommended.</td>
</tr>
<tr>
<td>onComplete (when an import set has completed transformation)</td>
<td>This transform is used to set the values of new CIs created, and CIs that have been updated and ignored. For internal use. Modifying or deleting is not recommended.</td>
</tr>
</tbody>
</table>

### Tenable.sc Plugins import

Plugins data imported from Tenable.sc is first loaded into the Tenable.sc Plugins Import table (sn_vul_tenable_sc_plugin_import). The Tenable.sc Plugin Transform Map is used to transform the plugins information that has been imported. Changes to this transform alter how data from the Tenable Plugin import is Processed. To access this transform map, navigate to **System Import Sets > Transform Maps**. Search for **Tenable.sc Plugin Transform Map**.
<table>
<thead>
<tr>
<th>Source field</th>
<th>Target field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>For example, if the id received is 12345, the id in the target table is TEN-12345.</td>
<td>u_description summary</td>
<td>Maps the description of the plugin to the summary column.</td>
</tr>
<tr>
<td>Imported TPE from this integration has Tenable.sc as the source.</td>
<td>[script] source</td>
<td>Import TPE from this integration has Tenable.sc as the source.</td>
</tr>
<tr>
<td>Reference to the Tenable deployment that imports this record.</td>
<td>[script] source_instance</td>
<td>Reference to the Tenable deployment that imports this record.</td>
</tr>
<tr>
<td>u_family category</td>
<td>Maps the name field in family object of plugin to the category column.</td>
<td>u_family category category</td>
</tr>
<tr>
<td>Maps the plugin_modification_date to the last modified field.</td>
<td>u_plugin_modification_date last_modified</td>
<td>u_plugin_modification_date last_modified</td>
</tr>
<tr>
<td>Maps the plugin_publication_date to published date.</td>
<td>u_plugin_publication_date date_published</td>
<td>u_plugin_publication_date date_published</td>
</tr>
<tr>
<td>Maps the remediation type from has_patch value.</td>
<td>u_has_patch Remediation_type</td>
<td>u_has_patch Remediation_type</td>
</tr>
<tr>
<td>Maps the threat information about this vulnerability.</td>
<td>u_synopsis threat</td>
<td>u_synopsis threat</td>
</tr>
<tr>
<td>Maps the CVSS base score to the score column in third-party entry table.</td>
<td>u_cvss_base_score score</td>
<td>u_cvss_base_score score</td>
</tr>
<tr>
<td>Maps the solution provided by the scanner to the solution column</td>
<td>u_solution solution</td>
<td>u_solution solution</td>
</tr>
<tr>
<td>Source field</td>
<td>Target field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>u_cvss_temporal_score</td>
<td>cvss_temporal_score</td>
<td>Maps the temporal score for CVSS v2.</td>
</tr>
<tr>
<td>u_cvss_v3_temporal_score</td>
<td>v3_temporal_score</td>
<td>Maps the temporal score for CVSS v3.</td>
</tr>
<tr>
<td>u_risk_factor</td>
<td>source severity</td>
<td>Maps to the source severity in the third-party entry table.</td>
</tr>
<tr>
<td>u_cvss_v3_base_score</td>
<td>v3_base_score</td>
<td>Maps the CVSS base score in the third-party entry table.</td>
</tr>
<tr>
<td>u_exploit_available</td>
<td>exploit</td>
<td>Maps the exploitAvailable provided by the scanner to the exploit column in the third-party entry table.</td>
</tr>
<tr>
<td>u_vpr_score</td>
<td>source_risk_score</td>
<td>Maps VPR score from the scanner to the Source risk score in the third-party entry table.</td>
</tr>
<tr>
<td>[script]</td>
<td>source_risk_rating</td>
<td>Maps the vpr score to the standard risk rating based on the score ranges:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 9 - 10 – Critical</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 7 – 9 – High</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 4 – 7 – Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0-4 - Low</td>
</tr>
<tr>
<td>u_vpr_context[id=age_of_vuln]</td>
<td></td>
<td>Maps the age of the vulnerability from the scanner to age_of_vuln in the third-party entry table.</td>
</tr>
<tr>
<td>Source field</td>
<td>Target field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>u_vpr_context[id=exploit_code_maturity]</td>
<td>exploit_code_maturity</td>
<td>Maps exploit code maturity from the scanner to exploit_code_maturity in the third-party entry table.</td>
</tr>
<tr>
<td>u_vpr_context[id=product_coverage]</td>
<td>product_coverage</td>
<td>Maps product coverage from the scanner to product_coverage in the third-party entry table.</td>
</tr>
<tr>
<td>u_vpr_context[id=&quot;threat_sources_last_28&quot;]</td>
<td>threat_sources</td>
<td>Maps threat sources in the last 28 days from scanner to threat_sources in the third-party table.</td>
</tr>
<tr>
<td>u_vpr_context[id=&quot;threat_intensity_last_28&quot;]</td>
<td>threat_intensity</td>
<td>Maps threat intensity in the last 28 days from the scanner to threat_intensity in the third-party entry table.</td>
</tr>
<tr>
<td>u_vpr_context[id=&quot;threat_recency&quot; ]</td>
<td>threat_recency</td>
<td>Maps the threat recency information from the scanner to threat_recency in the third-party entry table.</td>
</tr>
<tr>
<td>u_vpr_context[id=cvssV3_impactScore]</td>
<td>v3_impact_subscore</td>
<td>Maps CVSS v3 impact score from the scanner to v3_impact_subscore in the third-party entry table.</td>
</tr>
<tr>
<td>u_name</td>
<td>name</td>
<td>Maps the name of the plugin to the name column in the third-party entry table.</td>
</tr>
<tr>
<td>u_stig_severity</td>
<td>stig_severity</td>
<td>Maps the stig_severity field in the plugin to stig_severity in the third-party entry table.</td>
</tr>
<tr>
<td>Source field</td>
<td>Target field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>u_check_type</td>
<td>check_type</td>
<td>Maps the check type to check_type in the third-party entry table.</td>
</tr>
<tr>
<td>u_family.id</td>
<td>family_id</td>
<td>Maps the plugin family_id to family_id in the third-party entry table.</td>
</tr>
<tr>
<td>[script]</td>
<td>exploit_attack_vector</td>
<td>The exploit_attack_vector column in the third-party entry table is populated based on exploit_available and v3_attack_vector of columns.</td>
</tr>
</tbody>
</table>

In addition to the direct fields, other information is added as related lists to third-party entries.

<table>
<thead>
<tr>
<th>Source field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>u_cpe</td>
<td>The list of CPEs is added as a reference.</td>
</tr>
<tr>
<td>u_see_also</td>
<td>The list of URLs is added as a reference.</td>
</tr>
<tr>
<td>u_exploit_frameworks</td>
<td>The list of exploits for that plugin and inserts mapping for applicable exploit framework and plugin to sn_vul_m2m_framework_vul.</td>
</tr>
</tbody>
</table>

There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

<table>
<thead>
<tr>
<th>When the script is run</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>onStart (when an import set has started transformation)</td>
<td>This transform is used to initialize the values in the import_set for the integration process. For internal use. Modifying or deleting is not recommended.</td>
</tr>
</tbody>
</table>
When the script is run | Purpose
---|---
onBefore (before an import set has completed transformation). | Function used to update the values in the third-party entry and verify if the third-party entry already exists. Based on the results, modifies the values in a third-party entry. For internal use. Modifying or deleting is not recommended.
onComplete (when an import set has completed transformation). | This transform is used to set the values of Plugins created and ignored. For internal use. Modifying or deleting is not recommended.

The TenableSCPluginsImportProcessor script include is called from the onBefore transform script. It takes the output from the Tenable.sc plugins integration and transforms it into Servicenow third-party vulnerability entries. Any changes to this script include may alter the transformation of Tenable.sc plugins data in the third-party entry table.

**Tenable.sc Vulnerabilities import**
The Tenable.sc Open Vulnerabilities transform map is used to transform imported data from the Tenable.sc Open Vulnerabilities integration, and the Tenable.sc and Fixed Vulnerabilities transform map is used to transform imported data from the Tenable.sc Fixed Vulnerabilities Integration.

*Note:* Changes to these transform maps alter how data from the Fixed/Open Tenable Vulnerabilities Import is processed.

To access the Tenable.sc Open and Fixed Vulnerabilities transform maps, navigate to Tenable Vulnerability Integration > Administration > Integration Instances > Tenable.sc Fixed/Open Vulnerabilities Integration > Data Sources > Tenable.sc Open/Fixed Vulnerabilities > Transform.

<table>
<thead>
<tr>
<th>Source field</th>
<th>Target field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>u_pluginID</td>
<td>Id</td>
<td>Used as the identifier for the plugin. This field is mapped to the plugin Id in the third-party entry record.</td>
</tr>
<tr>
<td>Source field</td>
<td>Target field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>u_riskfactor</td>
<td>source_severity</td>
<td>This field is mapped to source_severity in the third-party entry record.</td>
</tr>
<tr>
<td>u_severity</td>
<td>priority</td>
<td>The priority field is mapped with the severity. The default value is 5.</td>
</tr>
<tr>
<td>u_hasbeenmitigated</td>
<td>state</td>
<td>Hasbeenmitigated is mapped to the state field of vulnerability record. For the Fixed vulnerabilities integration, all the VIs are in the 'Closed' state.</td>
</tr>
<tr>
<td>u_ip</td>
<td>ip_address</td>
<td>Ip address is mapped to the host ip field of cmdb_ci table.</td>
</tr>
<tr>
<td>u_port</td>
<td>port</td>
<td>Port is mapped to the port field of the vulnerable item record.</td>
</tr>
<tr>
<td>u_protocol</td>
<td>protocol</td>
<td>Protocol is mapped to the port field of the vulnerable item record.</td>
</tr>
<tr>
<td>u_firstSeen</td>
<td>first_found</td>
<td>The first seen value is mapped to the first found field of the VI record.</td>
</tr>
<tr>
<td>u_lastSeen</td>
<td>last_found</td>
<td>The last seen value is mapped to the last found field of the VI record.</td>
</tr>
<tr>
<td>Source field</td>
<td>Target field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>u_exploitAvailable</td>
<td>exploit</td>
<td>ExploitAvailable is mapped to the exploit field in the third-party entry record.</td>
</tr>
<tr>
<td>u_synopsis</td>
<td>threat</td>
<td>Synopsis is mapped to the threat field in the third-party entry record.</td>
</tr>
<tr>
<td>u_description</td>
<td>summary</td>
<td>Description is mapped to the summary field in the third-party entry record.</td>
</tr>
<tr>
<td>u_solution</td>
<td>solution</td>
<td>Solution is mapped to the solution field in the third-party entry record.</td>
</tr>
<tr>
<td>u_basescore</td>
<td>score</td>
<td>BaseScore is mapped to the score field in the third-party entry record.</td>
</tr>
<tr>
<td>u_temporalScore</td>
<td>temporal_score</td>
<td>Temporal Score is mapped to the temporal score in the third-party entry record.</td>
</tr>
<tr>
<td>u_cvssv3basescore</td>
<td>v3_base_score</td>
<td>Cvssv3basescore is mapped to the v3 base score in the third-party entry record.</td>
</tr>
<tr>
<td>u_cvsstemporalscore</td>
<td>v3_temporal_score</td>
<td>Cvssv3temporal score is mapped to the v3 temporal score in the third-party entry record.</td>
</tr>
<tr>
<td>Source field</td>
<td>Target field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>u_pluginpubdate</td>
<td>date_published</td>
<td>Plugin published date is mapped to the plugin published date in the third-party entry record.</td>
</tr>
<tr>
<td>u_pluginmoddate</td>
<td>last_modified</td>
<td>Last modified date is mapped to the plugin last modified date in the third-party entry record.</td>
</tr>
<tr>
<td>u_dnsname</td>
<td>fqdn</td>
<td>DnsName is mapped to the FQDN field of the cmdb_ci record.</td>
</tr>
<tr>
<td>u_macaddress</td>
<td>mac_address</td>
<td>MacAddress is mapped to the mac_address field of the cmdb_ci record.</td>
</tr>
<tr>
<td>u_netbiosName</td>
<td>netbios</td>
<td>NetbiosName is mapped to the NETBIOS field of the cmdb_ci record.</td>
</tr>
<tr>
<td>u_ip</td>
<td>ip</td>
<td>IP is mapped to the IP field of cmdb_ci record.</td>
</tr>
<tr>
<td>hostUniqueness</td>
<td>uuid</td>
<td>Host uniqueness is not mapped to any field but is used to determine uuid for the host.</td>
</tr>
<tr>
<td>u_family</td>
<td>category</td>
<td>Maps the name field in the family object of the plugin to the category column of third-party entry record.</td>
</tr>
<tr>
<td>Source field</td>
<td>Target field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>u_plugintext</td>
<td>proof</td>
<td>Plugin text is mapped to proof in tpe record.</td>
</tr>
<tr>
<td>[script]</td>
<td>source</td>
<td>The source of the integration is populated. The vulnerable items created from this integration have Tenable.sc as the source.</td>
</tr>
<tr>
<td>[script}</td>
<td>integration_instance</td>
<td>The integration_instance is the name of the instance from which the vulnerable item is imported.</td>
</tr>
<tr>
<td>u_vpr_score</td>
<td>source_risk_score</td>
<td>Maps VPR score from the scanner to the Source risk score in the third-party entry table.</td>
</tr>
</tbody>
</table>
| [script]                          | source_risk_rating    | Maps the vpr score to the standard risk rating based on the score ranges:  
  - 9 - 10 – Critical  
  - 7 – 9 – High  
  - 4 – 7 – Medium  
  - 0-4 - Low                                                                 |
<table>
<thead>
<tr>
<th>Source field</th>
<th>Target field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>u_vpr_context[id=exploit_code_maturity]</code></td>
<td><code>exploit_code_maturity</code></td>
<td>Maps exploit code maturity from the scanner to <code>exploit_code_maturity</code> in the third-party entry table.</td>
</tr>
<tr>
<td><code>u_vpr_context[id=product_coverage]</code></td>
<td><code>product_coverage</code></td>
<td>Maps product coverage from the scanner to <code>product_coverage</code> in the third-party entry table.</td>
</tr>
<tr>
<td><code>u_vpr_context[id=&quot;threat_sources_last_28&quot;]</code></td>
<td><code>threat_sources</code></td>
<td>Maps threat sources in the last 28 days from the scanner to <code>threat_sources</code> in the third-party entry table.</td>
</tr>
<tr>
<td><code>u_vpr_context[id=&quot;threat_intensity_last_28&quot;]</code></td>
<td><code>threat_intensity</code></td>
<td>Maps threat intensity in the last 28 days from the scanner to <code>threat_intensity</code> in the third-party entry table.</td>
</tr>
<tr>
<td><code>u_vpr_context[id=&quot;threat_recency&quot;]</code></td>
<td><code>threat_recency</code></td>
<td>Maps the threat recency information from the scanner to <code>threat_recency</code> in the third-party entry table.</td>
</tr>
<tr>
<td><code>u_vpr_context[id=--cvssV3_impactScore--]</code></td>
<td><code>v3_impact_subscore</code></td>
<td>Maps CVSS v3 impact score from the scanner to <code>v3_impact_subscore</code> in the third-party entry table.</td>
</tr>
<tr>
<td>Source field</td>
<td>Target field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>u_pluginname</td>
<td>name</td>
<td>Maps the name of the plugin to name column in third-party entry table.</td>
</tr>
<tr>
<td>u_stigseverity</td>
<td>stig_severity</td>
<td>Maps the stig_severity field in the plugin to stig_severity in third-party entry table.</td>
</tr>
<tr>
<td>u_checktype</td>
<td>check_type</td>
<td>Maps the check type to check_type in third-party entry table.</td>
</tr>
<tr>
<td>u_family.id</td>
<td>family_id</td>
<td>Maps the plugin family.id to family_id in the third-party entry table.</td>
</tr>
<tr>
<td>[script]</td>
<td>exploitAttack vector</td>
<td>The exploit_attack_vector column in the third_party_entry table is populated based on exploit_available and v3_attack_vector of columns.</td>
</tr>
</tbody>
</table>

**Source field**

<table>
<thead>
<tr>
<th>Source field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>u_cve</td>
<td>Inserts CVE-related data into the reference table (sn_vul_nvd_entry). If the same CVE in the NVD entry table (sn_vul_nvd_entry) is found, it associates the current vulnerability to the NVD entry. The mapping is found in sn_vul_m2m_entry_cve.</td>
</tr>
</tbody>
</table>
There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

<table>
<thead>
<tr>
<th>When the script is run</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>onStart (when an import set has started transformation)</td>
<td>This transform is used to initialize the values in the import_set for the integration process. For internal use. Modifying or deleting is not recommended.</td>
</tr>
<tr>
<td>onBefore (before an import set has completed transformation)</td>
<td>Function used to update the values in the vulnerability and verify if the vulnerability already exists. Based on the results, modifies the values in a vulnerable items table. For internal use. Modifying or deleting is not recommended.</td>
</tr>
<tr>
<td>onComplete (when an import set has completed transformation)</td>
<td>This transform is used to set the values of new VIs created, and VIs that have been updated and ignored. For internal use. Modifying or deleting is not recommended.</td>
</tr>
</tbody>
</table>
Tenable Vulnerability Integration reporting

View reports about vulnerabilities and vulnerable items on the Vulnerability Response dashboards.

The Vulnerability Response overview dashboard (Vulnerability Management) provides an executive view into vulnerabilities and vulnerable items, helping the Vulnerability Admin pinpoint areas of concern quickly. The Vulnerability Response remediation dashboard (Vulnerability Remediation) allows a remediation specialist to focus on the vulnerability groups and vulnerable items they own.

See *Using the default Vulnerability Response dashboards* on the product documentation website for more information.

Role required: Remediation owner

Persona and granular roles are available to help you manage what users can do and see in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see *Assign the Vulnerability Response persona roles using Setup Assistant* on the product documentation website.

For more information about managing granular roles, see *Manage persona and granular roles for Vulnerability Response* on the product documentation website.

to view the dashboard, navigate to Vulnerability Response > Remediation Overview.

Integration run status chart for the Tenable Vulnerability Integration

The Tenable Integration Run Status module provides you with a graphical view of the status of Tenable integration runs.

In the chart, point to any part of the graph to display a summary of data specific to that part. If you click any part on the bar graph, a list opens to provide more detailed information.

Role required: Vulnerability admin

Persona and granular roles are available to help you manage what users can do and see in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see *Assign the Vulnerability Response persona roles using Setup Assistant* on the product documentation website.

For more information about managing granular roles, see *Manage persona and granular roles for Vulnerability Response* on the product documentation website.
Tenable integration run status chart reports

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last 30 days Tenable Results</td>
<td>The number of integration runs completed for each integration. Shows both successful and failed runs. Each run displayed as a bar in the graph.</td>
</tr>
<tr>
<td>Last 30 Days Tenable New VIs</td>
<td>The number of new vulnerable items imported in the last 30 days. Shown as an integer.</td>
</tr>
<tr>
<td>Last 30 Days Tenable Updated VIs</td>
<td>The number of updated vulnerable items imported in the last 30 days. Shown as an integer.</td>
</tr>
<tr>
<td>Last 30 Days Tenable Unchanged VIs</td>
<td>The number of duplicate vulnerable items imported in the last 30 days. Shown as an integer.</td>
</tr>
<tr>
<td>Tenable Integration Runs</td>
<td>The integration run records in a list.</td>
</tr>
</tbody>
</table>

**Initiate rescan for the Tenable.sc integration**

Verify your vulnerable items have been remediated between scheduled scanning cycles by initiating rescans in the Tenable platform. You can initiate a rescan on-demand for vulnerable items for the Tenable.sc product from your Now Platform® instance.

**Before you begin**

Roles required: sn_vul.write_all or sn_vul.write_assigned
To help reduce the overhead and volume involved with scheduled, full scans, remediation owners, IT specialists, vulnerability analysts, or vulnerability managers can initiate targeted rescans on-demand for specific vulnerabilities on assets (configuration items) in their environments. You can initiate rescans from vulnerable item (VI), vulnerability groups (VGs), third-party entry (TPE), or discovered item records from your Now Platform instance.

Rescans permit you to verify that your remediation activities, patches, and other actions have successfully fixed specific vulnerabilities on your configuration items (CIs).

**Use case**

As an example, your entire environment is scanned once every three weeks. The most recent full scan was completed a week ago, but you applied a patch yesterday to fix a critical vulnerability. Due to the nature of this vulnerability, you cannot wait two weeks for the next scheduled scan to verify that it has been remediated. To verify that your patch successfully fixed a critical vulnerability discovered during an earlier scan, you can initiate a targeted rescan from your Now Platform for Tenable.sc vulnerable items.
Note: Your Vulnerability Response Integration with Tenable credentials are required when you request a rescan from your Now Platform® instance. The ServiceNow® Tenable.sc Scan Credential Integration imports and updates scanner credentials from the Tenable.sc product in your instance. This integration runs weekly to import and securely store your Tenable credentials data.

Note that this imported data does not include Tenable passwords or other sensitive Tenable account information. The ServiceNow® Tenable.sc Scan Credential Integration is enabled (Active) automatically from within the Setup Assistant in your instance when you configure the Tenable.sc Vulnerabilities integrations (Tenable.sc Open and Fixed Vulnerabilities Integrations).

Note the following information about the credentials you import so that your users can see them as needed from your Now Platform® instance:

- Credentials created with the Tenable.sc administrator user role are available to users across all your organizations.
- Credentials created with the Tenable.sc organizational users role are only available to users within that organization. These credentials are not imported into the Now Platform® for users outside of the creator’s organization unless they are shared with the user’s account being used to connect to the instance.

See the Tenable.sc documentation website for more information.

See Configure the Tenable Vulnerability Integration using Setup Assistant for more information about configuring the Tenable.sc application. To view more information about the Scan Credential Integration, navigate to Tenable Vulnerability Integration > Integrations > Tenable.sc Scan Credential Integration.

Procedure

1. Navigate to Vulnerability Response > Vulnerable items.
2. Locate the vulnerable item record that you want to trigger a rescan from and open it.

Note: You can only initiate rescans for VIs with Tenable.sc as the source. Verify Tenable.sc is displayed in the Source column on the VI List views, or in the Source fields on individual records. You can use the condition builder to group VIs by Source. Or, if the Source column is not displayed on the VI List view, in the upper left of the list, click the Personalize List icon (Gear icon) and use the Slushbucket to move Source from Available to Selected.
3. Alternatively, navigate to Vulnerability Response > Vulnerability Groups or Vulnerability Response > Libraries > Third-Party for the vulnerability group or third-party entry records, respectively, that you want to use for the rescan. Depending on your choice, the Rescan button is available on the following records:

- On a single VI record, the VI must be from the Tenable.sc product and in any state other than Closed. For multiple VI records, all the VIs must be from the Tenable.sc product and in any state other than Closed.
- On a VG record, the VG can be in any state other than Closed, and all the associated VIs must be from the Tenable.sc product.
- On a third-party entry (TPE) record, the record must have at least one associated VI record from the Tenable.sc product in any state other than Closed.

4. In the upper right of the record, click Rescan.
   You are prompted to choose the scanner credentials to access the scanner. These are the credentials imported by the Tenable.sc Scan Credential Integration.

5. In the dialog, select the filters and credential types you want.

6. Click Request Scan.
   A message is displayed that indicates your scan is being processed. Status for all rescans can be found at any time under the Scan related lists on the VI, VG, TPE records you used to launch the rescans. In the message, click View details to view the status of the rescan and view any other rescans launched from a given record.

   Your Now Platform® instance tracks the rescan status until it successfully completes, or, until the set tracking period times out, whichever happens first. The time-out does not stop the scan. The time-out refers to when the Now Platform stopped tracking your rescan status, not when the actual rescan stopped. All VIs that have transitioned, or will transition, to Closed/Fixed are imported with the next scheduled import of the Tenable.sc Fixed Vulnerabilities Integration.

**Update CIs with the network partition identifier for the Tenable Vulnerability Integration**

Create unique configuration items (CIs) that include different network partition identifiers for assets in your environment that share the same IP address. Identify the distinct assets across your environment and update the CIs on your existing discovered item, vulnerable item, and detection records to give you more details about your vulnerabilities.
Before you begin

You can create individual CIs for your assets with the same IP address starting from a fresh data import with a scheduled job, or, you can update your existing CIs with more granularity that includes the network partition identifier attribute by running a scheduled job on-demand.

When you upgrade starting with v13.0 of Vulnerability Response and v2.1 of the Tenable Vulnerability Integration, the upgrade includes the CMDB CI Class Models (1.0.21.) that has the Network Partition Identifier in the IRE identification rules.

The following system properties required to create or update CIs with network partition identifiers are disabled by default. Enable these properties for the Assets and Fixed and Open Vulnerabilities Integrations for the Tenable.io and Tenable.sc products as required.

- See the following tables for more information about assets that share the same IP address and the network_id or repository_id partition identifiers used to differentiate them.
- See the steps that follow the tables for more information about how to enable the system properties for the Assets and Fixed and Open Vulnerabilities Integrations for the Tenable.io and Tenable.sc products.

**sn_vul_tenable.lookup_network_partition_io**

When enabled, this system property includes the network partition identifier in the IP address lookup in Tenable.io imports with the Assets and Fixed and Open Vulnerabilities Integrations. This property also includes CIs created by IRE for unmatched items.

network_id is the network partition identifier.

**sn_vul_tenable.lookup_network_partition_sc**

When enabled, this system property includes the network partition identifier in the IP address lookup in Tenable.sc imports with the Assets and Fixed and Open Vulnerabilities Integrations. This property also includes CIs created by IRE for unmatched items.

repository.id is the network partition identifier.

After you enable the system properties, the following scheduled jobs run to create CIs with the network partition identifier starting with the next import. Alternatively, you can launch them on-demand to update your existing data.

**Tenable.io**

Update existing discovered items with network partition identifier.

**Tenable.sc**
Update existing discovered items with network partition identifier.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run the scheduled jobs on-demand.</td>
<td>Update your existing discovered items. CIs for your existing Tenable data are created or updated to include the network partition identifier granularity. Discovered items, vulnerable items, and detection records are all updated with the new CIs.</td>
</tr>
<tr>
<td>Wait for imports of fresh data from the integrations with the next scheduled jobs.</td>
<td>Create CIs for each new asset using the network partition identifier starting with the next scheduled job. CI, vulnerable item, and detection records are all updated to include the new granularity. New CIs are created when an exact match is not found.</td>
</tr>
</tbody>
</table>

Overview

By default in the Vulnerability Response application, one way to identify your assets is by their IP addresses.

For example, as shown in the following tables, when multiple assets in your environment share the same IP address but have unique network and repository ids, these assets are typically identified as a single CI during the IP address lookup and stored as one CI.

**Default IP lookup and CI creation**

<table>
<thead>
<tr>
<th>Source</th>
<th>IP address</th>
<th>Network_id</th>
<th>Configuration item</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable.io: Assets and Fixed and Open Vulnerabilities Integrations</td>
<td>123.12.12.141</td>
<td>03712</td>
<td>CI 1</td>
</tr>
<tr>
<td></td>
<td>123.12.12.141</td>
<td>03713</td>
<td>CI 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source</th>
<th>IP address</th>
<th>Repository_id</th>
<th>Configuration item</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable.sc: Assets and</td>
<td>123.12.12.141</td>
<td>12</td>
<td>CI 1</td>
</tr>
</tbody>
</table>
If you want to create new, distinct CIs for assets that share the same IP address but have unique Network_id (or) Repository_id values as shown in the following tables, in your Now Platform®, enable the system properties previously listed so that the network partition identifier is included in the IP address lookup and CI creation.

### Network partition identifier attribute included in IP lookup and CI creation

<table>
<thead>
<tr>
<th>Source</th>
<th>IP address</th>
<th>Repository_id</th>
<th>CI for assets without network partition identifier</th>
<th>CIs Assets with network partition identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable.io: Assets and Fixed and Open Vulnerabilities Integrations</td>
<td>123.12.12.141</td>
<td>03712</td>
<td>CI 1</td>
<td>CI 2</td>
</tr>
<tr>
<td>Tenable.sc: Assets and Fixed and Open Vulnerabilities Integrations</td>
<td>123.12.12.141</td>
<td>12</td>
<td>CI 1</td>
<td>CI 2</td>
</tr>
</tbody>
</table>

Role required: admin
Optional import modifications for the Tenable Vulnerability Integration

Configure optional modifications and streamline some of the data specifically for the Tenable Vulnerabilities import integration in the ServiceNow® Tenable Vulnerability Integration.

Before you begin
Role required: sn_vul.vulnerability_admin
This set of tasks requires coding and advanced knowledge about the Now Platform.

Follow these steps to create domain-separated imports for the Tenable Vulnerabilities Integrations. The following example is for the Tenable.io Open Vulnerabilities integration, but this content is applicable to the other Tenable integrations.

Procedure
1. Create a domain.
2. For every domain you create, create a user and assign the user to that domain.
   Think of this user as a run_as placeholder for the domain in Tenable.io
3. Open Vulnerabilities Integration.
   The user is the equivalent to the VR.System user in the global domain and must have the following roles: sn_vul.tenable_configure_integration, import_admin, and sn_vul.vulnerability_write. This user requires access to data sources, transform maps, and vulnerability data.

   ✉ Note: Consider this user as specific to this role. The user should not have any other purpose
4. In each domain, create a scheduled job by copying Scheduled Vulnerability Data Source Processor found under System Definition > Scheduled Jobs.
5. Append the domain to the name to identify the scheduled job.
6. Change the run_as user to the user you created in the previous step.

   ✉ Note: Edit the following UI action so that the integration runs in the run_as user domain.
7. Edit the Execute Now UI action in the Tenable.io Open Vulnerabilities Integration to add this code block to the top of the file.

```javascript
//sys id below is of Tenable.io integration
if(current.sys_id == "4df3f18d53730010d7f1ddeeff7b12a9"){
    current.run_as = gs.getUserID();
}
```

**Note:** Edit the following script includes so that integration runs in the run_as user domain.

8. Edit the VulnerabilityIntegrationUtils script include method addIntegrationRun to add the highlighted code.

9. Edit the VulnerabilityIntegrationUtils script include method addProcessRun to add the highlighted code.
10. Edit the DataSourceVulnReportRefreshProcessor script include method _processFromDataSourceGroups to change this original code: Original _processFromDataSourceGroups code to Edited _processFromDataSourceGroups code.

11. Edit the VulnerabilityDSAttachmentManager script include method, queueItem to add the following highlighted code blocks queueItem, _getNext, _processQueueEntry function.

You are ready for domain-separated host detection imports.

**Disable calculators prior to import**

Follow these steps to disable the default calculator if not used. If you do not use vulnerability calculators, it is best to disable the default calculators in addition to any others you have defined. Vulnerability calculators run every time a vulnerable item record is accessed and can impact instance performance.

Role required: sn_vul.vulnerability_admin

12. Navigate to Vulnerability > Administration > Vulnerability Calculators.

13. Open the Vulnerability Impact group.

14. Open the Score and Service Based Impact calculator.

15. Deselect the Active field to deactivate the calculator.

16. Click Update.

You have disabled the default calculator.

**Disable notification-based business rules prior to initial import**

Follow these steps to disable Disable notification-related business rules prior to initial record import. During the initial import of records, certain notification-related business rules can generate many notifications, impacting performance. These business rules should be modified to disable them during the import.

Role required: sn_vul.vulnerability_admin
17. Navigate to **System Definition > Business Rules**.


19. Open the business rule and insert the following condition:
   `current.sys_class_name != "sn_vul_vulnerable_item"`.

20. Click **Update**.

21. Repeat this procedure for the following business rules:
   - Affected cost center notifications
   - Affected group notifications
   - Affected location notifications

**Note:** After the completion of the initial record import, you have the option of re-enabling these business rules. However, consider leaving them disabled. They can generate large numbers of notifications and impact the performance of your instance.

**Modify an initial start date**

Follow these steps to Modify an initial start date. During installation using Setup Assistant, you set an initial start date for the Tenable integrations. You can reset that start date in Setup Assistant or from the primary integration as shown in the following steps.

22. Navigate to **Tenable Vulnerability Integration > Administration > Integrations**.

23. Click any integration.

24. Click Integration Details.

25. Set the Start time field to a value in the past, so all scanned and detected vulnerabilities since that time are detected.

   If you configured Tenable using Setup Assistant, the Start time field is pre-populated, initially to three months prior today’s date, and subsequently to today’s date. Note: Consider setting the value to a maximum of a month in the past. This keeps large amount of data from exceeding the Tenable API rate limitations, as well as triggering execution timeouts.

26. Click **Submit** or **Update**.

27. (Optional) Click **Execute Now** to run immediately.

**Create domain-separated imports for the Tenable Vulnerability Integration**

If you require vulnerability integration data to be imported to a specific domain, you must assign a user in that domain to run the integrations.
Before you begin
Role required: sn_vul_tenabe.configure_integration and import_admin
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task
This set of tasks requires coding or advanced ServiceNow expertise.

The import queues contain data attachments that the scheduled jobs (integrations) process. In a domain-separated environment, you must match the scheduled job with the correct import queue.

Procedure
1. Create a domain.

2. For every domain you create, create a user and assign the user to that domain.
   Think of this user as a run_as placeholder for the domain in one of your Tenable Vulnerability Integrations. It is the equivalent to the VR.System user in the global domain. This user needs access to data sources, and vulnerability data.

   📌 Note: Do not use this user for any other purpose.

3. In each domain, create a scheduled job.

   a. Navigate to System Definition > Scheduled Jobs.

   b. Copy Scheduled Vulnerability Data Source Processor into the domain.

   c. To identify the scheduled job, append the domain to the name.
d. In the **Run as** field change the **run_as** user to the user you created in the Step 2.

4. Ensure the integration runs in the **run_as** user domain.

   a. Edit the **Execute Now** UI action to add this code to the top of the file.

   **Example**

   ```javascript
   //sys id below is of host detection integration
   if(current.sys_id == "5d9cf0daff540300c68c9f783894fa4d"){
       current.run_as = gs.getUserID
   };
   ```

   b. Edit the **VulnerabilityIntegrationUtils** script include method **addIntegrationRun** to add the highlighted code.
c. Add the highlighted code to the **VulnerabilityIntegrationUtils** script include method **addProcessRun**.
   addProcessRun code

```javascript
gr.setValue("sys_domain", runGr.getValue("sys_domain"));
```

d. Add the highlighted code to the **VulnerabilityIntegrationUtils** script include method **copyProcess**.
   copyProcess code

```javascript
copyGr.setValue("sys_domain", runGr.getValue("sys_domain"));
```

e. Edit the **DataSourceVulnReportRefreshProcessor** script include method **_processFromDataSourceGroups**.

**Example**

Change the original line of code:

```
this.integrationProcessGr.getUniqueValues());
```

To

```
this.integrationProcessGr.getUniqueValue(),this.integrationProcessGr.getValue("sys_domain")
```

Edited _processFromDataSourcesGroups code

```javascript
var gr = new GlideRecord("sn_vulIntegration_process");
gr.initialize();
gr.setValue("sys_domain", runGr.getValue("sys_domain"));
```
f. Add the following highlighted code blocks to the `VulnerabilityDSAttachmentManager` script include method, `queueItem`.

```javascript
queueItem: function(dataSource, attachmentName, reportData, optIntegrationProcess, optDomain) {
    var gr = new GlideRecord(this.QUEUE_TABLE);
    gr.initialize();
    gr.setValue("status", "NEW");
    gr.setValue("data_source", dataSource);
    if (optIntegrationProcess)
        gr.setValue("integration_process", optIntegrationProcess);
    if (optDomain)
        gr.setValue("sys_domain", optDomain);
    var sysID = gr.insert();
}
```

g. Add the following highlighted code blocks to the `VulnerabilityDSAttachmentManager` script include function, `getNext`.

```javascript
_getNext: function() {
    var gruser = new GlideRecord("sys_user");
    gruser.getSysUser(sysDomainUser);
    var sysDomainUser = gruser.getValue("sys_domain");
    var gr = new GlideRecord(this.QUEUE_TABLE);
    gr.addQuery("status", "ACTIV");
    gr.addQuery("sys_domain", sysDomainUser);
    gr.query();
    if (gr.next())
        return gr;
}
```

h. Add the following highlighted code blocks to the `VulnerabilityDSAttachmentManager` script include function, `_processQueueEntry`.

```javascript
_gruser = new GlideRecord("sys_user");
_gruser.getSysUser(sysDomainUser);
var sysDomainUser = gruser.getValue("sys_domain");
var gr = new GlideRecord(this.QUEUE_TABLE);
gr.addQuery("status", "ACTIV");
gr.addQuery("sys_domain", sysDomainUser);
gr.query();
if (gr.next())
    return gr;
```
At this point, you are ready for domain-separated host detection imports.

💡 **Note:** If you have multiple deployments of the Tenable for Vulnerability Response vulnerability integration, repeat this process for each deployment.

**Manually create a vulnerability integration**

Vulnerability integrations provide the ability for customers and vendors to enrich the vulnerability data on their instance by retrieving data from external systems and vendors. This ability can simplify the vulnerability remediation life cycle by keeping the instance synchronized with other vulnerability management systems.

For detailed instructions on creating integrations, see [Define a new vulnerability integration](#).

**Define a new vulnerability integration**

A vulnerability integration pulls report data from a third-party system, generally to retrieve vulnerability data, and process that reporting data using data sources or a custom processor.

**Before you begin**

Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see [Assign the Vulnerability Response persona roles using Setup Assistant](#). For more information about managing granular roles, see [Manage persona and granular roles for Vulnerability Response](#).
**Procedure**

1. Navigate to Vulnerability > Administration > Integrations.
2. Click New.
3. Fill in the fields, as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A descriptive name for the integration.</td>
</tr>
<tr>
<td>Active</td>
<td>Whether the integration is active. If you do not want it to run for a specific time period, you can set up the parameters you want to use and deactivate the job.</td>
</tr>
<tr>
<td>Run</td>
<td>The frequency you want the integration to run, Daily, Weekly, Periodically, and so on. As noted, subsequent fields are displayed or not based on your setting in this field.</td>
</tr>
<tr>
<td>Day</td>
<td>The day you want the integration to run.</td>
</tr>
<tr>
<td></td>
<td>• If you selected Weekly in the Run field, this field displays the days of the week.</td>
</tr>
<tr>
<td></td>
<td>• If you selected Monthly in the Run field, this field displays the days of the month.</td>
</tr>
<tr>
<td>Time</td>
<td>The time you want the integration to start. This field appears only if you selected Daily, Weekly, or Monthly in the Run field.</td>
</tr>
<tr>
<td>Application</td>
<td>[Read only] The name of the application for which this integration was created.</td>
</tr>
<tr>
<td>Repeat Interval</td>
<td>If you selected Periodically in the Run field, this field displays the</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Field</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>number of days and hours before the integration runs again.</td>
</tr>
<tr>
<td><strong>Starting</strong></td>
<td>If you selected Periodically in the Run field, this field displays the dates and time to be used as the starting point for periodic updates.</td>
</tr>
<tr>
<td><strong>Conditional</strong></td>
<td>Select this field if you want to add conditional parameters.</td>
</tr>
<tr>
<td><strong>Condition</strong></td>
<td>If you selected the Conditional check box, enter the conditions here.</td>
</tr>
<tr>
<td><strong>Integration Details</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Integration script</strong></td>
<td>Select the script include that extends the VulnerabilityIntegrationBase to be executed when the integration runs. This script defines how to retrieve data from a third-party system.</td>
</tr>
<tr>
<td><strong>Integration factory script</strong></td>
<td>Enter a script that defines how to construct the script include selected for the Integration script.</td>
</tr>
<tr>
<td><strong>Report processor strategy</strong></td>
<td>Select the strategy you want to use to handle the data returned by the integration script when the integration runs.</td>
</tr>
<tr>
<td></td>
<td>• Select Data Source Attachment if you want to process data using a data source.</td>
</tr>
<tr>
<td></td>
<td>• Select Custom Report Processor to select a custom processor.</td>
</tr>
<tr>
<td><strong>Report processor</strong></td>
<td>If you selected Custom Report Processor in the Report processor strategy field, select the script include that extends the VulnerabilityReportProcessorBase</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2001
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration script</td>
<td>script include to be executed when the integration runs.</td>
</tr>
<tr>
<td></td>
<td>This script defines how to process the data returned by the integration script.</td>
</tr>
<tr>
<td>Processor factory script</td>
<td>Enter a script that defines how to construct the script include selected for the Report processor.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**Related information**

- Vulnerability integration script
- Report processor strategies
- Integration factory script fields
- Configure a vulnerability integration to use a scripted REST API
- Manually run a vulnerability integration

**Vulnerability integration script**

On the Vulnerability Integration form, the integration script is a reference to a script include that extends the VulnerabilityIntegrationBase script include.

The functionality contained in this script is called by the VulnerabilityIntegrationController to manage the means by which data is retrieved from an external data source. Each subclass of VulnerabilityIntegrationBase has access to contextual information about the calling process. That information is available through the following member variables:

- integrationGr — a GlideRecord of the vulnerability integration record that requested the integration to run.
- integrationProcessGr — a GlideRecord that provides contextual information for the current process of an integration.

The vulnerability process contains special parameters to be used within an integration, generally for pagination purposes. Each run of a vulnerability integration (called a Vulnerability Integration Run) has at least one associated vulnerability integration process. For multi-call integrations, there are one or more vulnerability integration process records for each Vulnerability Integration Run.
The script include must provide an implementation for the `retrieveData()` method and return an object that is processed by the report processor script. The object returned by `retrieveData()` is a simple object with properties for content, `contentType`, and extension.

Here is a screen shot of `VulnerabilityIntegrationBase.retrieveData()`:

```plaintext
VulnerabilityIntegrationBase.retrieveData()
```

The logic in the `retrieveData()` depends on the interface required for retrieving the data. For example, if the source of the data being pulled has a REST API, the body of this method could be calling the REST endpoint, likely via `RESTMessageV2`. The response of the call can then be parsed or put into an attachment, and the details could be used to construct the return object.

**Single call integrations**

Single call (single page) integration scripts are the simplest types of integrations. They require one call, often to an external source of data, to retrieve data. Only `retrieveData()` is required to be implemented for single page/single call integrations.

A sample that demonstrates a simple single call integration script follows. It creates a `RESTMessageV2` and executes it. It then returns an object using the response body as the contents, along with an assumed `contentType` and `extension`. 
Single call integration script

```javascript
var SingleRunVulnerabilityIntegration = Class.create();
SingleRunVulnerabilityIntegration.prototype = Object.extend(VulnerabilityIntegrationBase, { 
  initialize: function() { }, 

  retrieveData: function() {
    // Sample retrieveData() where fictional RESTMessage is executed and XML response body is returned.
    var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
    var response = message.execute();
    var responseBody = response.getErrorBody() ? response.getErrorBody() : response.getBody();
    return { contents: responseBody, contentType: "application/xml", extension: "xml"};
  },

  type: SingleRunVulnerabilityIntegration
});
```

Multiple call integrations

Multiple call (or multiple page) integration scripts are a bit more complicated. They require multiple calls to a data source to retrieve data.

Like a single call integration, a multiple call integration must also have retrieveData() implemented. In the body of retrieveData(), the integration uses the hasMoreData() and setNextRunParameters() methods provided by VulnerabilityIntegrationBase.

The hasMoreData() method accepts a single Boolean that instructs the VulnerabilityIntegrationController to insert more processes to pull more data. When passing true to hasMoreData(), a call to setNextRunParameters() is made to provide context to the next process.

The setNextRunParameters() method accepts a single object that provides context information to be used by the next call to retrieveData(). This object is used to pass state to subsequent calls to retrieveData(). An example use case is to pass an object that indicates the current page number and page size to a web service.

For multiple call integrations, each retrieveData() call first checks the current process parameters. The _getProcessParameters() method is provided to all VulnerabilityIntegrationBase as a convenience to get the parameters set by the previous process. If there are no parameters, it would indicate that it is the first process.

A screen shot of a sample multiple call integration script follows. Extending on the single call integration example, this script demonstrates making calls to a REST endpoint that has basic pagination support. It shows how you can get a single page of data, recognize that there is more data to retrieve, and then tell the next process which page to retrieve.
Attachments as retrieveData() return values

Sometimes, it is preferable to return an attachment from retrieveData(). The logic to create and/or retrieve an attachment is implementation-specific, but after the attachment is known, its information can be returned.

To provide an attachment, retrieveData() returns an object like:

```
{
  contents: "attachment-sys-id",
  contentType: "sys_attachment"
}
```

An example that extends on the previous example, but saves the response body of the REST Message to the integration process record follows. It then returns that attachment identifier as the contents of the return object.
Return attachment from retrieveData

```javascript
var MultiRunAttachVulnerabilityIntegration = Class.create();
MultiRunAttachVulnerabilityIntegration.prototype = Object.extendObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
    * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
    * returned. This call is paginated, so we need to figure out the range to pull
    * for each call.
    * For simplicity, we'll say that a status code != 200 means we've reached the end of data
    * from the server, or if we cap out past our maxPages member variable.
    */

    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn.ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);

        var table = this._integrationProcessGr.getTableName();
        var sysId = this._integrationProcessGr.getUniqueValue();
        var fileName = this._integrationProcessGr.getValue("name") + ".xml";
        message.saveResponseBodyAsAttachment(table, sysId, fileName);
        var response = message.execute();
        var resonsSysId = response.getResponseAttachmentSysId();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responsSysId, contentType: "sys_attachment", extension: "xml"};
    },

    type: 'MultiRunAttachVulnerabilityIntegration'
});
```

Report processor strategies

The Report processor strategy field on the Vulnerability Integration form is used to select the method to process the data returned by the vulnerability integration script when the vulnerability integration process is executed.

The default value is Data Source Attachment. This method is the baseline implementation that takes the retrieved data and pass it to a data source to be imported into the system. Selecting Custom Report Processor allows you to select a custom processor script for processing the data.

Use the data source attachment report processor strategy

The Data Source Attachment report processor strategy is used to pass data retrieved by the integration script to configured data sources.

Before you begin

Role required: sn_vul.vulnerability_write
Procedure
1. Navigate to Vulnerability > Administration > Integrations and create a new integration.
2. In the Report processor strategy field, select Data Source Attachment.
3. Right-click in the form header, and click Save.
4. In the Vulnerability Integration Data Sources related list, click New.
5. Define the data source to be used.
6. Click Submit.
7. Repeat steps 4 through 6 if you require additional data sources. Be sure to specify the order that the multiple data sources send information in the Order field.
8. Click Update.

About custom report processor scripts
On the Vulnerability Integration form, the Report processor is a reference to a script include that extends the VulnerabilityReportProcessorBase script include. The functionality contained in this script is called by the VulnerabilityIntegrationController and defines the means by which the data returned by the integration script are processed.

Each subclass of VulnerabilityReportProcessorBase has access to contextual information about the calling process. That information is available through the following member variables:

- integrationGr — a GlideRecord of the Vulnerability Integration record that requested the integration to run.
- integrationProcessGr — GlideRecord of the Vulnerability Process that provides contextual information for the current process of an integration.

The script include must provide an implementation for the processReport() method. The object passed to processReport() is the object returned by retrieveData, and as such, is a simple object with properties for content, contentType, and extension. The actual logic in processReport() is implementation-specific and dependent of the report data provided.

Here is a screen shot of the VulnerabilityReportProcessorBase.processReport():
Custom report processor script

```javascript
/*
 * Processes the reportData that was pulled by a Vulnerability Integration's retrieveData().
 * The expectation is that retrieveData() will return an object that matches this function's input parameter.
 * @param reportData = object with the following format:
 *  
 *  contents: raw contents of data to process, usually a string. If the integration creates an attachment
 *  this value should be the attachment sys_id.
 *  mimeType: the mimeType of the content. If the content is an attachment sys_id,
 *  this should be sys_attachment. The sys_attachment record itself should have the
 *  content type specified.
 *  extension: the file extension that should be used for this content in the event the processor
 *  needs to write the contents to a file (such as a new attachment).
 *  
 *  */

processReport: function(reportData) {
    return;
},
```

Integration factory script fields

The Vulnerability Integration form contains the integration factory script and, when the **Custom Report Processor** report processor strategy is selected, the Processor factory script. These fields are used to provide the logic to actually instantiate the object defined by the script include reference fields, Integration script, and Report processor, respectively.

When the script include is selected, both fields are pre-populated with a no-argument constructor call. Often, this is sufficient, but there can be occasions where more logic is required to instantiate the script object.

The integrationProcessGr record is exposed to the factory script fields so process-specific information can be used, as needed.

Pushing data to a vulnerability integration using a REST API

You can use a REST endpoint to push data to a vulnerability integration.

The REST resource at `/api/sn_vul/vulnerability_integration_svc` has been exposed to accept input data from an external system to be passed to a vulnerability integration. This resource requires the same authentication mechanism for other inbound REST messages. Only users with the v10.3 `sn_vul.vulnerability.admin` or `sn_vul.admin` (deprecated) role can issue requests to `/api/sn_vul/vulnerability_integration_svc`. The query parameters accepted by this resource are `integrationName` and `attachmentFileName`. The `integrationName` parameter is set to the name of the vulnerability integration. The `attachmentFileName` parameter is set to a string to be used as the file.

An attachment is generated with the request body being used as the attachment contents. The Content-type header that is sent with the request is used to determine the content type of the request body. The `attachmentFileName` parameter names the attachment internally. When the attachment is generated, a new vulnerability integration run is created based on the `integrationName` provided.
The details of the REST call to make to the vulnerability integration endpoint are:

- **HTTP Method:** POST
- **HTTP Query Params:**
  - attachmentFileName={name of file to be created as attachment}
  - integrationName={name of the integration to use}
- **Supported Content Types:** application/json, application/xml, text/xml, text/plain

**Configure a vulnerability integration to use a scripted REST API**

To allow data to be pushed from an external system, a scripted REST API provided in the base system, accepts a request and puts the request body into an attachment for a report processor to process that data.

**Before you begin**
Role required: sn_vul.vulnerability_write

**Procedure**

1. Navigate to **Vulnerability > Administration > Integrations** and create a new integration.
2. In the **Integration script** field, select **ScriptedRESTVulnerabilityIntegration**.
3. Select the appropriate **Report processor strategy** and, if you are using a custom report processor, the Report processor.

   **Note:** The ScriptedRESTVulnerabilityIntegration works by taking an attachment and passing it to the report processor. For proper functionality, the selected Report processor (if custom) must be able to support an attachment.

4. Click **Submit**.

**Create a custom outbound REST message for Qualys**

If needed, you can create your own outbound REST message to send to Qualys.

**Before you begin**
Role required: web_service_admin
Procedure

1. Navigate to Vulnerability > Vulnerability Scanning > Scanners.
2. Locate and open the Qualys scanner.
3. In the Scanner factory script, modify the parameter that is passed to QualysVulnerabilityScanner to the name of the REST message that you want to use.

   **Example**
   For example, if you created a REST message named MyQualys-REST, the field value is new sn_vul.QualysVulnerabilityScanner("MyQualys-REST").

   **Note:** The REST message passed to the Qualys vulnerability scanner must be available to the Vulnerability scope.
4. Click Update.

What to do next
If you have more complex scanning requirements, but still want to use the existing scanner implementation, you can Configure the ServiceNow-initiated Qualys IP scan. For example, to change how the REST message is built and sent to Qualys, create a script include that extends QualysVulnerabilityScanner and provides a new implementation for the _buildScanRequest function.

Manually run a vulnerability integration
A vulnerability integration is configured to run on a scheduled basis. However, you can run them manually when needed.

Before you begin
Role required: sn_vul.vulnerability_write

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure

1. Navigate to Vulnerability > Administration > Integrations.
2. Open the integration you want to run.
3. Click Execute Now.
Mobile experience for Vulnerability Response

As a remediation owner, you can access the Vulnerability Response (VR) application on your Now Platform® instance with your Android or iOS mobile device.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Vulnerability Response

To familiarize yourself with the concepts of vulnerability response and how this product can help your organization, see Understanding Vulnerability Response on the ServiceNow product documentation website.

<table>
<thead>
<tr>
<th>Release version with Paris</th>
<th>Release notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Response Mobile app v10.0, v11.0</td>
<td>Vulnerability Response release notes For compatibility information, see KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes</td>
</tr>
</tbody>
</table>

Note: Before you install the Vulnerability Response Mobile app mobile, familiarize yourself with the .

Overview

As a user with the remediation owner role (sn_vul.remediation_owner), the Vulnerability Response Mobile app allows you to view and search the vulnerabilities, vulnerability groups, and assignments on your Now Platform instance directly from your Android or iOS mobile device.

When Notifications have been set up, you are notified when VGs or VIs have been assigned to you or your assignment group. This app gives a remediation owner the flexibility to reassign, edit fields, and begin remediation without being tied to the desktop.

You have access to vulnerabilities, vulnerability items, modules, and all solutions. You can perform the following tasks on your mobile device:
• View and update vulnerability groups.
• View change requests.
• Reassign a vulnerability group or vulnerability item to another member of an assignment group.
• View notifications when a critical vulnerability group is assigned to you or one of your assignment groups.
• Edit a subset of fields on vulnerability group records.
• Search for vulnerability groups that match specific search criteria.

The following figure illustrates how you log in to your Now Platform instance from your mobile device and the landing screen of the Vulnerability Response Mobile app that is displayed after you log in.

For step-by-step instructions about how to set up your Now Platform instance and install the Vulnerability Response Mobile app, see Set up checklist for the Vulnerability Response Mobile app. For instructions about how to log in, see Log in to the Vulnerability Response Mobile app.
Applications

Applications are the ServiceNow software components such as Security Incident Response (SIR), Vulnerability Response (VR), Governance, Risk, and Compliance (GRC) and other ServiceNow products that provide specific features and functionalities within your Now Platform instance. After you install core applications that have mobile apps on your Now Platform instance, these applications are displayed as icons on the bottom of your mobile device.
Folders

Each ServiceNow® mobile application contains folders that separate the applets by categories. In the preceding image, **Vulnerability Groups (VGs)** and **Search (VGs)** are the folders for the Vulnerability Response Mobile app.

Applets

Applets are the different options within the application. In the preceding image, the icons under **Vulnerability Groups (VGs)** and **Search (VGs)** are the available applets for the Vulnerability Response Mobile app.

See the following topics for more information about the applets of the Vulnerability Response Mobile app.

Set up checklist for the Vulnerability Response Mobile app

The following checklist includes the set up tasks that you are required to complete in your Now Platform® instance and on your mobile device prior to using the Vulnerability Response Mobile app.

Before you begin

As an option, print this checklist and use it to guide you through the tasks that are required to install the Vulnerability Response Mobile app. Verify that each item on the list is completed so that you can log in to the Vulnerability Response Mobile app and add a Now Platform instance.

The check list items are displayed in **highlighted** text. More information follows each item in the right column. Estimated time to complete this task: 15-20 minutes.

Roles required: admin for installation, and sn_vul.remediation_owner for viewing

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see **Assign the Vulnerability Response persona roles using Setup Assistant.** For more information about managing granular roles, see **Manage persona and granular roles for Vulnerability Response.**
## Mobile checklist

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| ☐   | **As a user with the admin role, verify that you have the Vulnerability Response core application installed on a Now Platform instance. This is the Now Platform instance that you view on your mobile device.**  

**Note:** The Vulnerability Response core application and the Now Platform instance should be from the same family release.  

1. To verify the core application is installed on your instance, navigate to **Plugins** and search for Vulnerability Response.  
2. If the Vulnerability Response core application is not already installed, click **Install** to install it.  

For more information about installing the Vulnerability Response core application, see [Install and configure Vulnerability Response](#).  

For more information about obtaining the Vulnerability Response core application on the ServiceNow Store, getting entitlement, installing core applications, and activating dependencies, see [Security Operations and the ServiceNow Store](#). |

| ☐   | **As a user with the admin role, verify that you have the Vulnerability Response Mobile app installed on the Now Platform instance that you want to view on your mobile device.**  

**Note:** The Vulnerability Response Mobile app and the Now Platform instance should be from the same family release. Starting with version 12.0 of Vulnerability Response, Vulnerability Response Mobile app and the Vulnerability Response application should be compatible. For more information on Vulnerability Response application compatibility, see [Vulnerability Response and Configuration Compliance Compatibility Matrix](#).  

Download and install the Vulnerability Response Mobile app from the ServiceNow Store on your Now Platform instance. |
## Mobile checklist (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>When you install the Vulnerability Response Mobile app, its dependencies, com.glide.sg and com.glide.sg.agent_native_client, are also installed. To verify that these dependencies are installed: 1. Navigate to <strong>Plugins</strong>. 2. Search for the plugin IDs (com.glide.sg and com.glide.sg.agent_native_client). 3. If they are not activated, activate these plugins. These plugins are required for the Vulnerability Response Mobile app. For more information about obtaining the Vulnerability Response Mobile app application on the ServiceNow Store, getting entitlement, installing applications, and activating dependencies, see <a href="#">Security Operations and the ServiceNow Store</a>.</td>
</tr>
</tbody>
</table>

As a user with the admin role, in your Now Platform instance, verify that you have assigned mobile users with the required Now Platform roles.

1. To view the roles that are assigned to a user, navigate to **Users and Groups > Users**. 2. Select the user name followed by the roles related list. All roles assigned to this user are displayed. 3. Verify a user is assigned, or assign a user with the IT Infrastructure Library role (itil). Users with the itil role can create, open, update and close change requests and vulnerability groups. Only users with the itil role can have tasks assigned to them. 4. Verify a user is assigned, or assign a user with the remediation owner role (sn_vul.remediation_owner). Users with the sn_vul.remediation_owner role can read vulnerability and solution records. This role is automatically added when you assign the itil role. 5. Verify you have created any required assignment groups and assigned mobile users to these groups.
Mobile checklist (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td><strong>Note:</strong> If you have a large number of users for the mobile application, you alternatively can assign the sn_vul.remediation_owner role to a group. Each user you add to the group inherits this role. For more information about assignment rules and groups, see Vulnerability Response assignment rules overview. For more information on users and assigning roles to users and groups, see Create a user, Assign a role to a user and Assign a role to a group on the ServiceNow Product Documentation website.</td>
</tr>
<tr>
<td>☐</td>
<td><strong>As a user with the remediation owner role (sn_vul.remediation_owner), download the most current ServiceNow® Agent app on your mobile device.</strong> The most current Agent app is available on the Apple iOS App Store and the Google Play Store.</td>
</tr>
<tr>
<td>☐</td>
<td><strong>As a user with the sn_vul.remediation_owner role, verify notifications are enabled on your mobile device and in your Now Platform instance.</strong> Notifications inform you when critical vulnerability groups (VG) are assigned to you or to your assignment group. To assist you with timely remediation, after you enable notifications, click on a notification in the Vulnerability Response Mobile app and navigate directly to the record. To enable notifications in your Now Platform instance so they are displayed on your mobile device, follow these steps.</td>
</tr>
</tbody>
</table>
Mobile checklist (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Verify you have downloaded and installed the Vulnerability Response Mobile app on your Now Platform instance.</td>
</tr>
<tr>
<td>2.</td>
<td>In System Settings in your Now Platform instance, under Notifications, verify you have enabled the <strong>ServiceNow Mobile Application</strong>.</td>
</tr>
<tr>
<td></td>
<td>For more information about setting notifications, see <strong>User notification preferences in UI16</strong> on the ServiceNow documentation website.</td>
</tr>
<tr>
<td></td>
<td>Now Platform notifications are also displayed on the messages screen on your mobile device. Verify that notifications are also enabled in the settings of your mobile device.</td>
</tr>
</tbody>
</table>

You have successfully set up your mobile device for the Vulnerability Response Mobile app. The next step is to log in to the Vulnerability Response Mobile app and add a Now Platform instance to your mobile device.

**Log in to the Vulnerability Response Mobile app**

Open the Vulnerability Response Mobile app and add a Now Platform instance with Vulnerability Response to your mobile device.

**Before you begin**

Verify that you have completed the setup steps described in **Set up checklist for the Vulnerability Response Mobile app**.
Role required: Remediation owner (sn_vul.remediation_owner)

About this task
Time to complete this task: 5-7 minutes.

Procedure
1. On your mobile device, tap the ServiceNow Agent app.
If you are not already logged in to a Now Platform instance, the Instances screen is displayed.

2. If the Now Platform instance with the Vulnerability Response core application is not already added to your mobile device, follow these steps to add it.

   a. On the Instances screen that is displayed, tap the plus icon (+). A screen is displayed that prompts you to enter and save an address of a Now Platform instance.

   b. Fill in the fields.

   | Field name                        | Description
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the instance address or scan a QR code.</td>
<td>Choose one to continue:</td>
</tr>
<tr>
<td></td>
<td>• Before the .service-now.com, enter the name of your Now Platform instance, for example, vrmobileparisagent.</td>
</tr>
<tr>
<td></td>
<td>• Enter an address. This address is the URL of your Now Platform instance that you want to view on your mobile device.</td>
</tr>
<tr>
<td></td>
<td>• Scan a QR code.</td>
</tr>
<tr>
<td>(Optional) Enter nickname</td>
<td>Enter a nickname for this instance. If you have multiple instances added to the device, nicknames can help you quickly locate a Now Platform instance.</td>
</tr>
</tbody>
</table>

   c. Tap **Save and Login**

3. On the ServiceNow login screen that is displayed, enter the User name and Password for the Now Platform instance that you want to add and tap **Login**. The Vulnerability Response landing screen is displayed. You have successfully logged in to the Vulnerability Response Mobile app!

4. After you log in, verify notifications are enabled in the Vulnerability Response Mobile app.
a. On the landing screen on the bottom, tap Notification.

b. On the Notifications screen, tap Enable Notifications if not enabled. Notifications from the Now Platform are displayed on the Notifications screen in the Vulnerability Response Mobile app.

5. After you login to an instance on your mobile device, it is the default Now Platform instance on the device. If you want to view another Now Platform on the device, you must log out of the default instance. To log out:

a. Tap the Settings icon.

b. Tap Logout.

The Instances screen is displayed with any Now Platform instances you have added to the mobile device.

c. Optional: Tap another instance to log in to it, or, alternatively, follow the preceding steps to add another instance.

Results
If the instances screen for the Vulnerability Response Mobile app is not displayed after you tap the ServiceNow Agent app on your device, verify that the ServiceNow Agent is permitted as a trusted app on your device. To permit access as a trusted app, navigate to the settings and general device management on your device and tap the option (Trust app, etc.) to permit access.

If an error message is displayed after you enter your credentials in the log in screen, verify that your User name and password for the Now Platform instance is correct.

If you have problems viewing the landing screen, verify your network connection.

If you cannot view the Instances screen after you tap the ServiceNow Agent app, try uninstalling it from your device. Verify you have the most current version of the app from the Apple iOS App Store or the Google Play Store and try reinstalling it.

View, assign, and edit vulnerability groups with the Vulnerability Response Mobile app

View, assign, or edit the fields on Vulnerability Group (VG) records assigned to your group. Navigate through vulnerabilities, vulnerability items, and solutions
records and related lists to view solutions, deployment metrics, and items to address.

**Before you begin**
Role required: Remediation owner (sn_vul.remediation_owner)

**About this task**
Assign VG records to yourself or reassign them to another member of your group. Alternatively, view the details of active Vulnerability Group (VG) records, Vulnerable Items (VI), NVD vulnerabilities, and solutions prior to editing, assignment or remediation. Time to complete this task: 5-10 minutes.

**Procedure**

1. If you are not logged in to your Now Platform instance on your mobile device, for more information see Log in to the Vulnerability Response Mobile app.

2. With the Vulnerability Response landing screen displayed, tap **Assigned to My Groups**.
   
   If you navigate away from the Vulnerability Response Mobile app after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.

   ![ServiceNow Agent Mobile App](image)

   The list of open vulnerability group records assigned to your group is displayed.
3. **Optional:** Refer to Search for vulnerability groups with the Vulnerability Response Mobile app to search for vulnerability group records that match specific criteria. Alternatively, with the filter icon ( filtro) displayed, Set filters to limit the number of records on the list. Filtering records on screens in the mobile app works like filtering with a condition builder on the Now Platform.

4. To reassign or edit a record directly from the list, with the list of open vulnerability group records displayed, swipe left on a record to open the menu.
5. Choose one from the menu that is displayed to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assign to me</strong></td>
<td>If the VG record is already assigned to you, this option is not displayed.</td>
</tr>
<tr>
<td></td>
<td>Tap <strong>Assign to Me</strong> to assign the VG to yourself. Your name is displayed in the Assigned to field on the record.</td>
</tr>
<tr>
<td></td>
<td>A message is displayed that confirms the assignment.</td>
</tr>
<tr>
<td><strong>Reassign</strong></td>
<td>To reassign the VG to an assignment group:</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Tap</strong></td>
<td><strong>Assignment group</strong>.</td>
</tr>
<tr>
<td><strong>From the list, tap a group or enter text in the search field.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>To assign or reassign the VG to a member of an assignment group:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Tap</strong></td>
<td><strong>Assigned to</strong>.</td>
</tr>
<tr>
<td><strong>Tap a name from the list that is displayed or enter text in the search field.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Tap the send icon (✓) or Submit to save and submit your changes.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Tap</strong></td>
<td><strong>Edit</strong>.</td>
</tr>
<tr>
<td><strong>Expand the fields and select an option from the list that is displayed or enter text in the Search field.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Tap the send icon (✓) or Submit to save and submit your changes.</strong></td>
<td></td>
</tr>
</tbody>
</table>

6. Alternatively, to view the details of an open vulnerability record and to see more associated records and related lists, with the Assigned to My Groups screen displayed, tap a VG record on the list.

7. On the open vulnerability group record that is displayed, choose one option from the following table to the view work notes or the related lists.
With the Details tab selected, review the fields of the VG record. Tap the menu icon (☰) on the upper right of the screen to view the available options.

The options that are displayed in this expanded menu vary. The remediation actions you can take on your vulnerable items vary and depend on the value that is displayed in the State field of the Vulnerability Group record. For more information about the State field and your remediation
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Activity Stream tab** | With the Activity Stream tab selected, choose one to continue.  
• View the audit trail of work notes, activities, and additional comments of the record. Tap the plus icon (+) to add a work note or attach a file.  
• Tap the menu icon (⋮) on the upper right of the screen to view the available remediation options. |
| **Related Lists** | With the Related Lists tab selected, view any of the related lists of the VG record that are populated.  
• Tap **Vulnerable Items**. Tap a Vulnerable item (VI) record and navigate to the preferred solution record. Refer to the figure that follows the table for a navigation map and more details.  
• Tap **Change Requests**. View a list of the change requests that are associated with this record.  
• When displayed, tap the menu icon (⋮) on the upper right of a screen to view the available remediation options. |

The following image illustrates the navigation path from the Vulnerability Group record to the preferred solution record for the selected vulnerability. Navigate through the records and related lists to view solutions, deployment metrics, and items to address.
8. After reviewing, editing, or remediation, choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Tap an icon on the bottom of the screen. | On the bottom of the screen, choose one to continue.  
  - Tap the Vulnerability Response icon to return the landing screen.  
  - If displayed, tap an icon to open another ServiceNow® mobile app.  
  - Tap Notification to view notifications from the Now Platform and |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>the Vulnerability Response Mobile app</td>
<td></td>
</tr>
<tr>
<td>• Tap <strong>Settings</strong> and choose one to</td>
<td>continue.</td>
</tr>
<tr>
<td>◦ View information about the Now Platform</td>
<td>instance on your device.</td>
</tr>
<tr>
<td>◦ Log out of the current Now Platform</td>
<td>instance.</td>
</tr>
</tbody>
</table>

**View, reassign, and edit vulnerability groups assigned to you with the Vulnerability Response Mobile app**

View, assign, or edit the fields on Vulnerability Group (VG) records that are assigned to you. Navigate through records and related lists to view solutions, deployment metrics, and items to address.

**Before you begin**
Role required: Remediation owner (sn_vul.remediation_owner)

**About this task**
Reassign or edit Vulnerability Group (VG) records assigned to you. View the details of active Vulnerability Group (VG) records, Vulnerable Items (VI) records, Vulnerabilities, and Solutions prior to editing, assignment or remediation. Time to complete this task: 5-10 minutes.

**Procedure**

1. If you are not logged in to your Now Platform instance on your mobile device, for more information see Log in to the Vulnerability Response Mobile app.
2. With the **Vulnerability Response** landing screen displayed, tap **Assigned to Me**. If you navigate away from the Vulnerability Response Mobile app after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.
The list of vulnerability group records that are assigned to you is displayed.
3. **Optional:** Refer to Search for vulnerability groups with the Vulnerability Response Mobile app to search for vulnerability group records that match specific criteria. Alternatively, with the filter icon displayed, set filters to limit the number of records on the list. Filtering records on screens in the mobile app works like filtering with a condition builder on the Now Platform.

4. To reassign or edit the vulnerability group record directly from the list, with the Assigned to Me screen displayed, swipe left on a record to open the menu.
5. Choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Reassign | To reassign the VG to another assignment group:  
  a. Tap **Assignment group**.  
  b. Tap a group from the list that is displayed or enter text in the search field.  
  To assign or reassign the VG to a member of an assignment group: |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>a.</strong> Tap <strong>Assigned to</strong>.</td>
<td>Tap a name from the list that is displayed or enter text in the search field. Tap the send icon (&gt;) or <strong>Submit</strong> to save and submit your changes.</td>
</tr>
<tr>
<td><strong>b.</strong> Tap <strong>Edit</strong>.</td>
<td>Expand the fields and select an option from the list that is displayed or enter text. Tap the send icon (&gt;) or <strong>Submit</strong> to save and submit your changes.</td>
</tr>
</tbody>
</table>

6. Alternatively, to view the details of an open vulnerability record and to see more associated records and related lists, with the Assigned to Me screen displayed, tap a VG record on the list.

7. On the open vulnerability group record that is displayed, choose one option from the following table to view work notes or the related lists.
### Option Description

**Details tab**

With the Details tab selected, review the fields of the VG record. Tap the menu icon (⋮) on the upper right of the screen to view the available options.

The options that are displayed in this expanded menu vary. The remediation actions you can take on your vulnerable items vary and depend on the value that is displayed in the State field of the Vulnerability Group record. For more information about the State field and your remediation
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Activity Stream tab | With the Activity Stream tab selected, choose one to continue.  
|                 | • View the audit trail of work notes, activities, and additional comments of the record. Tap the plus icon (+) to add a work note or attach a file.  
|                 | • Tap the menu icon (⋮) on the upper right of the screen to view the available remediation options. |
| Related Lists tab   | With the Related List tab selected, view the related lists of the VG record that are populated.  
|                 | • Tap Change Requests. View a list of the change requests that are associated with this record. |
|                 | • Tap Vulnerable Items. Tap a Vulnerable item (VI) record and navigate to the preferred solution record. Refer to the figure that follows the table for a navigation map and more details.  
|                 | • When displayed, tap the menu icon (⋮) on the upper right of the screen to view the available remediation options. |

The following image illustrates the navigation path from the Vulnerability Group record to the preferred solution record for the selected vulnerability. Navigate through the records and related lists to view solutions, deployment metrics, and items to address.
8. Choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tap an icon on the bottom of</td>
<td>On the bottom of the screen, choose one to continue.</td>
</tr>
<tr>
<td>the screen.</td>
<td>• Tap the Vulnerability Response icon to return the landing screen.</td>
</tr>
<tr>
<td></td>
<td>• If displayed, tap an icon to open another ServiceNow® mobile app.</td>
</tr>
<tr>
<td></td>
<td>• Tap <strong>Notification</strong> to view notifications from the Now Platform and</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Tap Settings and choose one to continue. | • View information about the Now Platform instance on your device.  
• Log out of the current Now Platform instance. To log, tap Logout. |

**Search for vulnerability groups with the Vulnerability Response Mobile app**

Search for vulnerability groups (VGs) that match specific search criteria that you select.

**Before you begin**
Role required: Remediation owner (sn_vul.remediation_owner)

**About this task**
Time to complete this task: 5-7 minutes.

**Procedure**

1. If you are not logged in to your Now Platform instance on your mobile device, for more information see Log in to the Vulnerability Response Mobile app.
2. With the **Vulnerability Response** landing screen displayed, tap **Search VGs**.  
If you navigate away from the Vulnerability Response Mobile app after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.
3. On the Search screen that is displayed, tap the fields and fill out the form with your desired search criteria. Follow the instructions after the table to edit search criteria, clear search criteria, or submit a search.

<table>
<thead>
<tr>
<th>Tap this Field</th>
<th>To add an entry on Android devices</th>
<th>To add an entry on iOS devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Tap the screen and enter a VG number, for example, (VUL0002372) This number is displayed on the upper right of the VG record. Tap the check mark icon to add your entry and return to the Search VGs screen. Tap the close icon (X) to cancel your entry and return to the Search VGs field.</td>
<td>Enter a VG number, for example, (VUL0002372). This number is displayed on the upper right of the VG record. Tap <strong>Done</strong> to return to the Search VGs screen. From the expanded field, tap <strong>Cancel</strong> to clear the entry and return to the Search VGs screen.</td>
</tr>
<tr>
<td>Risk rating</td>
<td>Tap one or more items followed by the check mark icon to add your entry and return the Search VGs screen.</td>
<td>To add an entry, tap one or more items, or tap the search icon and type an entry in the search field. Tap <strong>Done</strong> to return to the Search VGs screen.</td>
</tr>
<tr>
<td>Tap this Field</td>
<td>To add an entry on Android devices</td>
<td>To add an entry on iOS devices</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Remediation status</td>
<td>Tap one or more items followed by the check mark icon to add your entry and return the Search VGs screen. Tap the close icon (X) to cancel your entry and return to the Search VGs field.</td>
<td>To add an entry, tap one or more items, or tap the search icon and type an entry in the search field. Tap <strong>Done</strong> to return to the Search VGs screen. From the expanded field, tap <strong>Cancel</strong> to clear the entry and return to the Search VGs screen.</td>
</tr>
<tr>
<td>State</td>
<td>Tap one or more items followed by the check mark icon to add your entry and return the Search VGs screen. Tap the close icon (X) to cancel your entry and return to the Search VGs field.</td>
<td>To add an entry, tap one or more items, or tap the search icon and type an entry in the search field. Tap <strong>Done</strong> to return to the Search VGs screen. From the expanded field, tap <strong>Cancel</strong> to clear the entry and return to the Search VGs screen.</td>
</tr>
<tr>
<td>Reason</td>
<td>Tap one or more items followed by the check mark icon to add your entry and return the Search VGs screen. Tap the close icon (X) to cancel your entry and return to the Search VGs field.</td>
<td>To add an entry, tap one or more items, or tap the search icon and type an entry in the search field. Tap <strong>Done</strong> to return to the Search VGs screen. From the expanded field, tap <strong>Cancel</strong> to clear the entry and return to the Search VGs screen.</td>
</tr>
<tr>
<td>Assignment group</td>
<td>Select one from the list or tap the search icon and type an entry in the search field.</td>
<td>Select one from the list or tap the search icon and type an entry in the search field.</td>
</tr>
<tr>
<td>Tap this Field</td>
<td>To add an entry on Android devices</td>
<td>To add an entry on iOS devices</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Assigned to</td>
<td>To clear a value for the Assignment group and Assigned to fields, for no entry, select <strong>None</strong>.</td>
<td>To clear a value for the Assignment group and Assigned to fields, for no entry, select <strong>None</strong>.</td>
</tr>
<tr>
<td>Short description</td>
<td>Tap the screen and enter text. The feature recognizes text strings and partial text strings in this field, but wildcards (*) are not accepted. Capital letters are not required. Tap the check mark icon to add your entry and return to the Search VGs screen.</td>
<td>On the screen enter text. The feature recognizes text strings and partial text strings in this field, but wildcards (*) are not accepted. Capital letters are not required. Tap <strong>Done</strong> to return to the Search VGs screen. From the expanded field, tap <strong>Cancel</strong> to clear the entry and return to the Search VGs screen.</td>
</tr>
<tr>
<td>Description</td>
<td>Tap the screen and enter text. The feature recognizes text strings and partial text strings in this field, but wildcards (*) are not accepted. Capital letters are not required. Tap the check mark icon to add your entry and return to the Search VGs screen.</td>
<td>On the screen enter text. The feature recognizes text strings and partial text strings in this field, but wildcards (*) are not accepted. Capital letters are not required. Tap <strong>Done</strong> to return to the Search VGs screen. From the expanded field, tap <strong>Cancel</strong> to clear the entry and return to the Search VGs screen.</td>
</tr>
</tbody>
</table>

For Android devices, with the Search VGs screen displayed and all your criteria entered, choose one to continue.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Clear or modify search criteria prior to executing a search | To clear all entered criteria, with the Search VGs screen displayed, tap the back arrow to clear all the fields and return to the Vulnerability Response landing screen. The search is not submitted and the search criteria are cleared. Alternatively, to edit a field:  
- With the Search VGs screen displayed, tap a field with search criteria to expand it.  
- Tap an item to deselect it. Tap All to select all items. Tap All again to clear all items. To clear a value for the Assignment group and Assigned to fields, for no entry, select None.  
- Tap the check mark icon to save the changes and return to the Search VGs screen. |
| Submit a search | With the Search VGs screen displayed with your entered search criteria, tap the send icon (>). The vulnerability group records that match your search criteria are displayed. After the search is completed, the search criteria are not saved. |

4. For iOS devices, with the Search VGs screen displayed, choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear or modify search criteria prior to executing a search</td>
<td>To clear all criteria and return to the landing screen, tap the close icon (X). Any entered search criteria are not saved. Alternatively, to edit a field:</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>a.</td>
<td>With the Search VGs screen displayed, tap a field with search criteria to expand it.</td>
</tr>
<tr>
<td>b.</td>
<td>Tap an item on the list to deselect it, or tap <strong>Clear All</strong>. To clear a value for the Assignment group and Assigned to fields, for no entry, select <strong>None</strong>.</td>
</tr>
<tr>
<td>c.</td>
<td>Tap <strong>Done</strong> to save the changes and return to the Search VGs screen.</td>
</tr>
</tbody>
</table>

Submit a search

With the Search VGs screen displayed with your entered search criteria, tap **Search**.

The vulnerability group records that match your search criteria are displayed. After the search is completed, the search criteria are not saved.

### 5. Optional: If your search returns multiple records, you can Filter records with the Vulnerability Response Mobile app to refine the search results.

**Filter records with the Vulnerability Response Mobile app**

Set additional filters to limit the number of records that are displayed on a screen. Filtering records in the mobile app works like filtering with a condition builder on the Now Platform.

**Before you begin**

Role required: Remediation owner (sn_vul.remediation_owner)

**About this task**

Time to complete this task: 5 minutes.

**Procedure**

1. To further refine your search results, or to enter additional filter criteria on any list of records that is displayed, tap the filter icon ( ![Filter icon](filter_icon.png)).

2. With the Filters screen displayed, tap a field to expand it.
   A common field to enter search criteria for Vulnerability Group records is the State field.
3. From the options that are displayed, tap the check box or tap an item for your filter. For many of the filters, you can select more than one option.

4. Tap the Back icon (Back) or DONE to save your changes to a field. The criteria you chose are displayed on the Filters screen. The number of records that match your criteria is also displayed at the top of the screen. Tap RESET to remove any filters and restore the default setting.

5. Optional: Repeat steps 1 - 4 with the Filters screen displayed to continue setting your filter criteria.

6. Tap the intersection icon ( ) to create AND conditions.

   Alternatively, tap the intersection icon ( ) to create OR conditions.

7. After you have added all the criteria you want, with the Filters screen displayed, tap DONE. On the screen, only the records that match your filter criteria are displayed.

 Related information

Search for vulnerability groups with the Vulnerability Response Mobile app

Vulnerability Response Orchestration

With Vulnerability Response Orchestration workflows and activities you can interact with and retrieve data from Windows or UNIX-based systems and environments using workflow orchestration. By enriching data, you can shorten the remediation life cycle.

For more information on editing workflows or creating custom workflows, see Workflow and Workflow Editor.

Vulnerability Response Orchestration workflows and activities

Several workflows are included with Vulnerability Response Orchestration. Workflows and activities automate and expedite your processes. Use workflows and activities to create scan records, scan vulnerable items, create scan records, and more.

Vulnerability Response - Scan Vulnerability workflow

Automate vulnerability scans for single or multiple vulnerable items using the Vulnerability Response - Scan Vulnerability workflow included in the base system.
Before you begin
Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task
The Vulnerability Response - Scan Vulnerability workflow creates a scan record for the vulnerability or group of vulnerabilities from which it was invoked.

⚠️ Note: It is good practice to rescan vulnerabilities or vulnerable items after remediation, when a vulnerability patch is applied to the affected records. You can perform the rescan using the method described or you can automate the rescans.

Workflow activities include:
• Variables for Create Scan Record for Vulnerabilities activity
Scan vulnerability workflow

The **Vulnerability Response > Scan Vulnerability** workflow rescans a vulnerability group.

**About this task**

This workflow is triggered by **Rescan vulnerable group** during a **Close/Ignore** action.

Workflow process activities include:

- **Variables for Create Scan Record for Vulnerabilities activity**
- **Log Message**
Procedure

1. Navigate to Vulnerability > Vulnerabilities > Vulnerability Groups.
2. Open a vulnerability group.
3. Click Close/Ignore.
5. Choose Fixed for the Substate.
6. Choose Wait for confirmation from the next scan for Close now?
   For the vulnerability group and vulnerable items, the State changes to Pending Confirmation, the Substate changes to Fixed, and a rescan runs.
Vulnerability Response - Scan Vulnerable Items workflow

Automate vulnerability scans for single or multiple vulnerable items using the **Vulnerability Response - Scan Vulnerable Items** workflow included in the base system.

**Before you begin**
Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see [Assign the Vulnerability Response persona roles using Setup Assistant](#). For more information about managing granular roles, see [Manage persona and granular roles for Vulnerability Response](#).

**About this task**
The **Vulnerability Response - Scan Vulnerable Items** workflow creates a scan record for the vulnerable item or group of items from which it was invoked.

⚠️ **Note:** It is good practice to rescan vulnerabilities or vulnerable items after remediation when a vulnerability patch is applied to the affected records. You can perform the rescan is using the method described or you can automate the rescans.

Workflow process activities include:

- Variables for Create Scan Record for Vulnerabilities activity
Scan vulnerability item workflow

The **Vulnerable Response > Scan Vulnerability Item** workflow rescans a vulnerable item.

**About this task**

This workflow is triggered by **Rescan vulnerability**, during a **Close/Ignore** action.

Workflow process activities include:

- Variables for Create Scan Record for Vulnerabilities activity
- Log Message
Procedure

1. Navigate to **Vulnerability > Vulnerabilities > Vulnerable Items**.
2. Open a vulnerability item.
3. Click **Close/Ignore**.
4. Choose **Closed** for the **Desired State**.
5. Choose **Fixed** for the **Substate**.
   The **State** of the group changes to **Pending Confirmation**, the **Substate** changes to **Fixed**, and a rescan runs.

**Vulnerability Response Orchestration workflow activities**

Vulnerability Response Orchestration activities allow users to determine whether a vulnerability has been seen before in other security incidents or on other systems using workflow orchestration.
Variables for Create Scan Record for Vulnerabilities activity

Vulnerability scans for single or multiple vulnerable items can be run using the Create Scan Record for Vulnerabilities workflow activity included in the base system. When the input is passed to the activity, it creates a scan record.

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskids</td>
<td>A string of comma-separated sysIds that define the expected inputs. This field is mandatory.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scanResult</td>
<td>Returns True if the input is not empty. A scan record is created for the taskIds.</td>
</tr>
</tbody>
</table>

Application Vulnerability Response

The ServiceNow® Application Vulnerability Response (AVR) feature of the ServiceNow® Vulnerability Response application imports application vulnerable items (AVIs) and, according to rules, allows you to remediate application vulnerabilities. It is available by separate subscription.

Overview of Application Vulnerability Response

Application vulnerabilities are vulnerabilities on custom software applications scanned throughout the application’s development life cycle.

Application Vulnerability Response (AVR) is the part of Vulnerability Response focused on Dynamic Application Security Testing (DAST) data.

DAST scans find vulnerabilities in the behavior of your overall application.
Note: SAST, SCA, Interactive Application Security Testing (IAST), and PEN testing data are not ingested and may account for differences between what is shown within Veracode and what appears in Application Vulnerability Response.

DAST use cases

In dynamic (DAST) scanning, a running service (URL) is scanned for vulnerabilities. Vulnerability results come with a URL location of the discovered vulnerability.

Some of the supported use cases are:

- Relate each vulnerability from scan results to some kind of cmdb_ci (child class).
- Relate DAST scan results to an existing application when there is a record in the CMDB from Discovery or a third-party integration.
- Relate DAST scan result to a newly inserted scanned application when a new Application has not previously been identified and/or stored in the CMDB.
- Store DAST scan results for a CMDB when you manage your applications in a product other than ServiceNow®.
- Store DAST scan results for a CMDB if you have previously customized for some other purpose.
- Create an application for Source code repository manually.

The common point for scans is the application release. An application release, which defines a Name string, is the tie-in point to group scanned vulnerability results on the scanner side. This way AVR knows which application release the results belong to when importing scan results through the integration.

A Configuration Item [cmdb_ci ] child table, Scanned Applications [sn_vul_app_scanned_application], was created in the Vulnerability Response application and scope. This table stores the Application Release abstraction and provides service graphing through its CMDB relationships. They can be viewed from the Application Vulnerability Response > Administration > Applications module. The list view for Scanned Applications contains the Department and Support Group added during setup.

Application Vulnerable Items (AVIs)

For application vulnerabilities, AVR relates a vulnerability to an application to create the application vulnerable item (AVI) record. Because of the multiple definitions of what constitutes an application in the CMDB, Application Vulnerability Response limits applications to scanned applications. Scanned applications are the applications scanned in your environment identified by AVR as Name and ID. AVIs are based on the latest scan summary until confirmed.
Fixed by the scanner. If an AVI is no longer found, it remains tied to the scan summary where it was last seen.

Application vulnerable items can be viewed from the Application Vulnerability Response > Vulnerabilities > Vulnerable Items module.

If an application is removed from the CMDB, any associated AVIs are closed.

For information on AVI form fields, see Application Vulnerable Item fields.

Application Vulnerability Response features:

**CI lookup rules:**
- Automatically search application data for matches in the Configuration Management Database (CMDB).

**Assignment rules:**
- Automatically assign application vulnerabilities based on user groups, user group fields, and scripts.

**Risk Calculators:**
- Automatically prioritize and rate the impact of AVIs using calculators, based on any criteria, by using condition filters.

**Severity mapping:**
- Automatically calculate initial values for fields on application vulnerable items. Vulnerability entries have both source severity and normalized severity (based on severity mapping). Severity is tied to the Common Weakness Enumeration (CWE).

**Remediation target rules**
- Define expected time frame for remediating an application vulnerable item.

**Reporting:**
- Quickly gain insight into your security posture, remediation trends and top 10 Applications or Business Units with the most critical AVIs.

**Application Vulnerability Response flow**

Use Application Vulnerability Response to follow the flow of information, from integration through investigation, and then on to resolution.
Available versions

<table>
<thead>
<tr>
<th>Release version</th>
<th>Release Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Response v13.0</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Response v12.1</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Response v12.0</td>
<td>Vulnerability Response</td>
</tr>
<tr>
<td></td>
<td>Release Notes</td>
</tr>
</tbody>
</table>

User groups and roles in Application Vulnerability Response

Often a team works together to create, manage, and oversee the management of application vulnerabilities. There are strategic roles, as well as operational roles, among the team members. In most organizations, you may participate in more than one role and often share roles with others. Application Vulnerability Response uses three user groups containing granular roles: App-Sec Manager, Application Security Champion, and Developer. See Manage Application Vulnerability Response user groups and roles for more information on these groups and roles.

Benefits of Application Vulnerability Response

- Integration with third party scanners.

  Vulnerability data is pulled from internal and external sources, such as the Common Weakness Enumeration (CWE) or third party integrations such as
Veracode. The Veracode Vulnerability Integration is available as a separate application in the ServiceNow Store and requires a separate subscription.

After vulnerability data is imported, compare the data to applications identified in Application Vulnerability Response. You can perform the following tasks.

- Compare application vulnerability-related data, if an application vulnerability is found in an application.
- Manage application vulnerable items. Each application vulnerability represents a vulnerability entry in the CWE, or third-party libraries.
- Relate a single third-party vulnerability to multiple CWE entries and find the primary CWE for the vulnerability in determining risk. For more information on the Primary CWE, see Application Vulnerability fields.
- Use CWE records, downloaded from the CWE database, or imported from Veracode, for reference when deciding whether a vulnerability must be escalated. Each CWE record also includes an associated knowledge article that describes the weakness. You cannot escalate a vulnerability from the Common Weakness Enumerations page. That page is for reference only.

- Prioritization of application vulnerabilities.
  Application Vulnerability Response data correlation is performed using calculators and libraries. You can perform the following tasks.

  - Create AVIs automatically using CI Lookup Rules. During import, third-party vulnerabilities are associated to a CWE to create an AVI.
  - Create assignment rules. Assignment rules are used to automate application vulnerable item assignments. There can be a performance impact associated with poorly constructed rules, so care should be taken with automated vulnerable item assignment.
  - Use calculator groups to determine business impact, specify varying conditions using filters, apply simple calculations, or use a script.
  - Create remediation target rules that define the expected timeframe for remediating application vulnerable items so you can monitor upcoming remediation activities.

- Remediation of application vulnerabilities.

  Application Vulnerability Response remediation is primarily a manual process performed at the application vulnerable item level.

  Update, Close, or Delete from the application vulnerable item form to expedite your investigation and remediation of vulnerabilities.
Application Vulnerability Response states

Application Vulnerability Response offers a state model for the status of your application vulnerable items (AVIs) and helps you to determine when and how to remediate your AVIs.

An application vulnerable item has several possible states, see Understanding Application Vulnerable Item (AVI) states for more information.

Application Vulnerability Response terminology

The following terms are used in Vulnerability Response.

**Application Vulnerable items (AVIs)**

Pairings of vulnerability entries and potentially vulnerable applications in your company environment.

**Assignment Rules**

Rules used to assign AVIs based on your defined criteria.

**Common Platform Enumeration (CPE)**

A NIST NVD structured naming scheme for information technology systems, software, and packages.

**Common Vulnerabilities and Exposures (CVE)**

Dictionary of publicly known information-security vulnerabilities and exposures.

**Common Weakness Enumeration (CWE)**

List of community-developed software weakness types.

**Integrations**

Scheduled jobs that pull report data from CWE or a third-party system, such as Veracode, to retrieve vulnerability data.

**Note:** If the NIST National Vulnerability Database integration in Vulnerability Response is activated and configured, CVE enrichment is available for CWEs but not required. For information on the NIST National Vulnerability Database integration, see Managing NVD, CWE, and third-party data libraries and prior to Vulnerability Response v13.0 Configure the scheduled job for updating NVD records (Prior to v13.0). (No configuration is not required for the Vulnerability Response integration with NVD application.

**National Vulnerability Database (NVD)**

**Remediation Target Rules**
Rules used to assign AVIs target dates for remediation based on your defined criteria.

**Vulnerability Calculators**
Calculators used to prioritize and categorize application vulnerabilities based on your defined criteria.

**Configure Application Vulnerability Response**
Before you run Application Vulnerability Response in your Now Platform instance, you must configure it.

**Before you begin**
Complete the following setup checklist prior to configuration.

<table>
<thead>
<tr>
<th>Setup tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that the Vulnerability Response application is installed and activated.</td>
<td>To verify that it is activated, navigate to Subscription Management &gt; Subscriptions in your instance. The list displays the subscriptions your organization has purchased. If the application is not installed and activated, see Install and configure Vulnerability Response.</td>
</tr>
<tr>
<td>Verify that the Performance Analytics for Vulnerability Response is installed and activated to see Application Vulnerability Response reports.</td>
<td>To verify that it is activated, navigate to Subscription Management &gt; Subscriptions in your instance. The list displays the subscriptions your organization has purchased. If the application is not installed and activated, see Install and configure the Performance Analytics for Vulnerability Response [PA] application.</td>
</tr>
<tr>
<td>Verify that the Veracode Vulnerability Integration is installed, activated.</td>
<td>To verify that it is activated, navigate to Subscription Management &gt;</td>
</tr>
<tr>
<td>Setup tasks</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>and configured. [Do not run the integrations at this point.]</td>
<td><strong>Subscriptions</strong> in your instance. The list displays the subscriptions your organization has purchased. If the application is not installed and activated, see <a href="#">Installation the ServiceNow Vulnerability Response Integration with Veracode</a>.</td>
</tr>
<tr>
<td>Verify that the CWE 2000 integration is running in Vulnerability Response.</td>
<td>To verify, see Verify that the scheduled job for updating NVD records is running.</td>
</tr>
<tr>
<td>[Optional] Verify that the NVD integration is running in Vulnerability Response.</td>
<td>To verify, see Verify that the scheduled job for updating CWE records is running.</td>
</tr>
<tr>
<td>Verify that you have the required ServiceNow roles for your instance.</td>
<td>The following roles are required for installation, configuration, and verification of expected results:</td>
</tr>
<tr>
<td></td>
<td>• If not already assigned, the System Administrator [admin] installs the application and assigns users to the following user groups: App-Sec Manager, Security Champion, and Developer. For information on Group roles see, Manage Application Vulnerability Response user groups and roles.</td>
</tr>
<tr>
<td></td>
<td>• The App-Sec Manager group oversees configuration and verifies expected results.</td>
</tr>
<tr>
<td></td>
<td>️ <strong>Note:</strong> Application Vulnerability Response configuration is not available from the Setup Assistant feature in Vulnerability Response.</td>
</tr>
</tbody>
</table>

Role required: App-Sec Manager user group
Procedure

1. Navigate to Security Operations > CMDB > CI Lookup Rules. See, Create a CI lookup rule to create or modify CI Lookup Rules for your environment.

2. Navigate to Application Vulnerability Response > Administration.

3. Select Assignment Rules. See, Create or edit Application Vulnerability Response assignment rules to create or modify application assignment rules for your environment.

4. Select Vulnerability Calculators. See, Calculate risk in Application Vulnerability Response automatically to create or modify application vulnerability calculators for your environment.
5. Select **Remediation Target Rules**. See, Create or edit application remediation target rules to create or modify application remediation targets for your environment.

6. Select **Normalized Severity Maps**. See, Map the severity of an application vulnerable item automatically to create or modify severity maps for your environment.

7. Navigate to **Veracode Vulnerability Integration > Integrations**.

8. Open the **Veracode Application List Integration**.

   **Note:** The other Veracode integrations are inactive by default.

9. If it has not already run, click **Execute Now**.
    For integration run statuses see, View the Veracode Vulnerability Integration import run status.

10. Once the **Veracode Application List Integration** has completed its run, navigate to **Application Vulnerability Response > Administration > Applications**.

11. For each application, manually enter a value for **Support Group** (used by assignment rules) and for **Department** (used in reporting).

   **Note:** To see the auto-updated **Business Unit**, refresh the page.
    For information on Scanned Application form fields see, Scanned application fields.

12. Return to the Integrations list, and activate the other Veracode integrations.
    See **Activate Application Vulnerability Response Integrations** to set your delta data integration imports.
    The Veracode integrations are chained and will run consecutively when activated.

13. [Optional] Navigate to **Application Vulnerability Response > Administration > Assignment Rules**.

   a. [Optional] If you chose **Configuration Item: Support group** for **User group field** when creating or editing your assignment rules earlier, the values you added to the Scanned Applications list view are available to use now. Edit your assignment rules accordingly.

   b. Click **Update**.

   c. From the Vulnerability Assignment Rules list view, click **Apply Changes** to reapply the assignment rules to your AVIs.

14. Your Application Vulnerability Response configuration is now complete.
What to do next
Navigate to Application Vulnerability Response > Overview and see View the Application Vulnerability Management [PA] dashboard for information on your overall security posture.

Verify that the scheduled job for updating CWE records is running
Use Common Weakness Enumeration (CWE) records downloaded from the CWE database for reference when deciding whether a vulnerability must be escalated. Update common weakness records from the Common Weakness Enumeration database on a regularly scheduled basis. You can also update the default script or write your own scripts, as needed.

Before you begin
Role required: App-Sec Manager group
Each CWE record also includes an associated knowledge article that describes the weakness.

Procedure
1. Navigate to Application Vulnerability Response > Administration > Integrations.
2. Select the CWE Comprehensive 2000 Integration scheduled job.
3. Verify that the Active check box is selected.
   - Note: The settings in this form are shared by Vulnerability Response and Application Vulnerability Response. Modifying the integration settings requires coordination with and expertise in Vulnerability Response and ServiceNow.
4. If the box is selected, you are done.
   - Note: If the box is not selected, this integration may need to be configured within Vulnerability Response. See Managing NVD, CWE, and third-party data libraries for more information before selecting it.

As needed, see View vulnerability libraries to see the imported entries.

Version 13.0: The Primary CWE field contains the CWE entry. If there is more than one CWE is associated with a vulnerability, see Application Vulnerability fields for information on how the primary CWE is determined.
Verify that the scheduled job for updating NVD records is running

Identify the repositories that you want updated regularly. You can execute a scheduled job to update National Vulnerability Database (NVD) records on a nightly or weekly basis. If it is not already running, you can enable the job.

Before you begin
Roles required: App-Sec Manager group

The NVD runs as a scheduled job weekly on Mondays at 01:00:00, by default.

Procedure
1. Navigate to Application Vulnerability Response > Administration > Integrations.
2. Select the NIST National Vulnerability Database scheduled job.
3. Verify that the Active check box is selected.

   Note: The settings in this form are shared by Vulnerability Response and Application Vulnerability Response. Modifying the integration settings requires coordination with and expertise in Vulnerability Response and ServiceNow.

4. If the box is selected, you are done.

   Note: If the box is not selected, this integration may need to be configured within Vulnerability Response. See Managing NVD, CWE, and third-party data libraries for more information before selecting it.

As needed, see View vulnerability libraries to see the imported entries.

Activate Application Vulnerability Response Integrations

Enable Application Vulnerability Response integrations to perform regular updates.

Before you begin
Role required: App-Sec Manager

Note: The NIST NVD integration for CPE v1.0, requires a different procedure, see Activate the NIST National Vulnerability Database - API CVE CPE Integration.

Procedure
1. Navigate to Application Vulnerability Response > Integrations.
2. Select an integration.
3. Select the **Active** check box.
4. Click **Update**.
5. Repeat as needed for each integration. After the initial run, the integrations are chained to do delta imports for subsequent runs.

**View vulnerability libraries**

You can view vulnerability data imported from the National Vulnerability Database (NVD), Common Weakness Enumeration (CWE), or third-parties to decide whether to escalate a vulnerability group.

**Before you begin**
Role required: App-Sec Manager group

**Procedure**

1. Navigate to **Application Vulnerability Response > for Libraries**.

   The following libraries are available:

<table>
<thead>
<tr>
<th>Libraries</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NVD</td>
<td>List of vulnerabilities found by NVD and includes security checklists, security-related software flaws, misconfigurations, product names, and impact metrics including exploits.</td>
</tr>
<tr>
<td>CWE</td>
<td>List of community-developed software weakness types. Each CWE record also includes an associated knowledge article that describes the weakness. You cannot escalate a vulnerability from the Common Weakness Enumerations screen, it is for reference only.</td>
</tr>
<tr>
<td>Third-party</td>
<td>List of imported third-party vulnerabilities in your instance. Contains a list of related references, vulnerable items, exploits, CWEs, and CVEs.</td>
</tr>
</tbody>
</table>

2. Choose a library to view vulnerabilities.
For information on specific fields, see Application Vulnerability fields.

**Application Vulnerability fields**

Vulnerabilities are created automatically when records are downloaded from the National Vulnerability Database (NVD), Common Weakness Enumeration (CWE) or third-party integrations. NVD and CWE are stored under Libraries in Vulnerability Response or under **Vulnerabilities** in Application Vulnerability Response.

**CWE vulnerability entry fields**

The fields in this table are read-only.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-ID</td>
<td>Identifier for this vulnerability entry. This identifier is used for both Categories and Weaknesses, and is unique between the two datasets.</td>
</tr>
<tr>
<td>Name</td>
<td>Descriptive name assigned to this CWE-ID.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Likelihood of exploit | How likely the weakness is to be exploited, on a qualitative scale. One of:  
  - Low  
  - Medium  
  - High  |
| OWASP Top 10 Position | This vulnerability’s numerical position in the OWASP top 10 list.                                                                           |
| SANS To 25 Position   | This vulnerability’s numerical position in the SAN top 25 list.                                                                             |
| Class                 | Type of weakness                                                                                                                             |
| Status                | One of:  
  - Incomplete  
  - Draft  
  - Stable  
  - Deprecated  
  - Obsolete  
  - Unstable  |
| Abstraction           | One of:  
  - Variant  
  - Class  
  - Base  
  - Compound  |
<p>| Updated               | Last time the record was updated in the instance.                                                                                           |
| Functional areas      | List of functional areas affected. For example, <strong>File Processing</strong>. Only populated for 24/862 weaknesses.                                    |
| Affected Resources    | List of affected resources. For example, <strong>File</strong> or <strong>Directory</strong>. Only populated for 51/863 weaknesses.                                     |
| URL                   | Knowledge base article associated with this vulnerability.                                                                                   |
| Description           | Description of the vulnerability.                                                                                                              |
| Integration run       | The integration run this CWE was imported in.                                                                                                  |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sections</td>
<td></td>
</tr>
<tr>
<td>Additional details</td>
<td>Software concept descriptions that further explain the weakness. Includes: • Extended description • Background details • Notes</td>
</tr>
<tr>
<td>Detection methods</td>
<td>Details on how you might detect this weakness in an application.</td>
</tr>
<tr>
<td>Modes of introduction</td>
<td>The phases in which the weakness is introduced, for example, Implementation, Architecture and Design, and so on.</td>
</tr>
<tr>
<td>Demonstrative examples</td>
<td>Code examples of the weakness with accompanying descriptions.</td>
</tr>
<tr>
<td>Potential mitigations</td>
<td>Details on how to prevent the weakness, including which phase of the application life cycle it occurs in, and the effectiveness of the mitigation.</td>
</tr>
</tbody>
</table>

**Related Lists**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relationships</td>
<td>CWEs associated to this vulnerability. Lists relationships between this CWE and others. Can include parent/child, follows/precedes, requiredby/requires (for composite weaknesses), CanAlsoBe, PeerOf, MemberOf.</td>
</tr>
<tr>
<td>Observed Examples</td>
<td>Some CVEs that are representative of this weakness.</td>
</tr>
<tr>
<td>Common Consequences</td>
<td>Consequences of a successful exploit, in terms of scope and impact. For example: Scope: Confidentiality Impact: Read Application Data</td>
</tr>
<tr>
<td>Memberships</td>
<td>CWE memberships with this vulnerability.</td>
</tr>
<tr>
<td>Applicable Platforms</td>
<td>Platforms associated with this vulnerability.</td>
</tr>
<tr>
<td>Application Vulnerability Entries</td>
<td>Other application vulnerability entries associated with one.</td>
</tr>
</tbody>
</table>
### Application vulnerability entry fields

The fields in this table are read-only.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identifier for this vulnerability entry.</td>
</tr>
<tr>
<td>Source</td>
<td>Origin of the vulnerability — whether a scanner or physical test.</td>
</tr>
<tr>
<td>Severity</td>
<td>Normalized degree of severity of this vulnerability.</td>
</tr>
</tbody>
</table>

**Severity mapping details:**

- Normalized degree of severity of this vulnerability. Severity maps are provided for NVD and with ServiceNow third-party integrations. For more information on creating or adjusting severity maps, see [Map the severity of an application vulnerable item automatically](#).

**Version 12.1:**

**Primary CWE**

- Reference to the Common Weakness Enumeration element that this vulnerability best fits into.

**Version 13.0:**

**Primary CWE**

- Reference to the Common Weakness Enumeration element that this vulnerability best fits into.

- If there is more than one CWE associated to the vulnerability, the primary CWE is determined as follows:
  - Is the CWE mapped to the OWASP Top 10. If so, use this CWE. If not, continue.
  - Is the CWE mapped to the SANs Top 25? If so, use this CWE. If not, continue.
  - Does the CWE have the highest severity? If so use this CWE. If not, continue.
  - Select the latest of all the CWEs. The latest CWE is the one with the latest Updated field value in the CWE record.

**Category name**

- Classification provided by the third-party integration. Aids in assignment.

### Vulnerability Details

- **Threat**
  - Description of the threat from this vulnerability.

- **Mitigation description**
  - Description of the steps that could be taken to mitigate the vulnerability.

## Related List
### Field | Description
--- | ---
Version 13.0: CWEs | List of the CWEs associated with this vulnerability. Non-applicable for the Veracode Vulnerability Integration.

### NVD entry fields
The imported fields in this table are read-only.

**Note:**

NVD data is not used in Application Vulnerability Response and entries represent Vulnerability Response data only.

CWEs, which are used in Application Vulnerability Response, can point to NVD entries, as examples of a weakness, and are provided here for informational purposes only.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identifier for this vulnerability entry.</td>
</tr>
<tr>
<td>Risk rating</td>
<td>(Hidden when no Vulnerability Response vulnerable items (VIs) are associated with the vulnerability) Quantified <strong>Risk Score</strong> separating VIs into Critical, High, Medium, Low, and None.</td>
</tr>
<tr>
<td>Risk score</td>
<td>(Hidden when no VIs are associated with the vulnerability) Calculated amount of risk the vulnerable item poses to your environment.</td>
</tr>
<tr>
<td>Severity</td>
<td>Normalized degree of severity of this vulnerability in Vulnerability Response. Severity maps are provided for NVD and with ServiceNow third-party integrations. Application Vulnerability Response <strong>Severity</strong> is derived from imported <strong>Source severity</strong> and not NVD. For information on Application Vulnerability Response severity mapping, see <a href="#">Map the severity of an application vulnerable item automatically</a>.</td>
</tr>
<tr>
<td>Exploit exists</td>
<td>Yes, if at least one exploit is associated with this vulnerability.</td>
</tr>
<tr>
<td>Exploit skill level</td>
<td>Lowest skill level required to exploit this vulnerability.</td>
</tr>
<tr>
<td>Exploit attack vector</td>
<td>Most vulnerable attack vector of the exploits for this vulnerability.</td>
</tr>
<tr>
<td>Active VIs</td>
<td>(Hidden when no VIs are associated with the vulnerability)</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Number of vulnerable items</td>
<td>Number of vulnerable items associated with this vulnerability, not in the Closed state. If there are no active AVIs for this vulnerability, <strong>Risk Rating</strong> and <strong>Risk Score</strong> are not displayed.</td>
</tr>
<tr>
<td>CWE entry</td>
<td>Reference to the Common Weakness Enumeration element that this vulnerability best fits into.</td>
</tr>
<tr>
<td>Date published</td>
<td>Date the vulnerability was published.</td>
</tr>
<tr>
<td>Last modified</td>
<td>Date the vulnerability was last modified.</td>
</tr>
<tr>
<td>Summary</td>
<td>Description of the vulnerability.</td>
</tr>
</tbody>
</table>

**Vulnerability Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVSS v2</td>
<td>Imported CVSS v2 data</td>
</tr>
<tr>
<td>CVSS v3</td>
<td>Imported CVSS v3 data, not available prior to 2015.</td>
</tr>
<tr>
<td>Preferred solution</td>
<td>(Hidden when no VIs are associated with the vulnerability) Solution of the highest-supersedence in the chain, derived from the solutions referenced in the vulnerability. If more than one highest-supersedence exists in the chain, no value is set. Any value set manually can be overwritten on subsequent imports. Setting this value manually should be done on the vulnerable item.</td>
</tr>
</tbody>
</table>

**Remediation Status**

(Hidden when no VIs are associated with the vulnerability)

**Excludes Deferred**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerable items</td>
<td>Number of active application vulnerable items with this vulnerability. This count excludes deferred vulnerable items.</td>
</tr>
<tr>
<td>Total VIs</td>
<td>Total number of vulnerable items with this vulnerability. This count excludes deferred vulnerable items.</td>
</tr>
<tr>
<td>%VIs remediated</td>
<td>Percent complete for remediation of vulnerable items with this vulnerability. This count excludes deferred vulnerable items.</td>
</tr>
</tbody>
</table>

**Includes Deferred**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerable items</td>
<td>Number of active vulnerable items with this vulnerability.</td>
</tr>
<tr>
<td>Total VIs</td>
<td>Total number of vulnerable items with this vulnerability.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>%VIs remediated</td>
<td>Percent complete for remediation of vulnerable items with this vulnerability.</td>
</tr>
</tbody>
</table>

**Related Links**

| Prior to v13.0: Force software vulnerability import | (Deprecated) Re-calculate product mapping with ITSM Software Asset Management based on information from NVD. Updates the Vulnerable Software library. |

**Note:**

Removed in v13.0

| Update status | Displays date and time of the last update. Updates the following: • Vulnerability group state • Risk score and rating • Metrics such as Active VIs, Total VIs from the Remediation Status section |

**Related Lists**

| Vulnerable Items | (Hidden when no VIs are associated with the vulnerability) Vulnerable items associated with this vulnerability. |
| Vulnerability References | Information about the vulnerability from external sources, cited by NVD. |
| Exploits | Exploits associated with this vulnerability. |
| Solutions | (Hidden when no VIs are associated with the vulnerability) All Vulnerability Solution Management integration solutions associated with this vulnerability. |
| Version 13.0: Weaknesses | Imported CWE Weakness data associated to a Common Vulnerabilities and Exposures (CVE). |
| Version 13.0: Vulnerable Software | (Hidden when no VIs are associated with the vulnerability) Imported Common Platform Enumeration (CPE) data associated with the vulnerability. |
Manage Application Vulnerability Response user groups and roles

Before you can successfully remediate vulnerabilities with Application Vulnerability Response (AVR), you must assign users to user groups.

Roles define what you and your groups can see and do in Application Vulnerability Response, Performance Analytics for Vulnerability Response, and third-party integrations with Application Vulnerability Response.

User groups

There are three default user groups supporting Application Vulnerability Response:

- **App-Sec Manager**: Contains security managers.
- **Security Champion**: Contains liaisons between the development group and security managers.
- **Developer**: Contains individual contributors.

The system admin [admin] role is required to assign users to the Application Vulnerability Response default user groups, using the User Administration module.

**Note:**

Assigning AVR users to the Application Vulnerability Response user groups for Application Vulnerability Response is not available in the Vulnerability Response Setup Assistant feature. Only Vulnerability Response roles are assigned there.

The following table lists the available Application Vulnerability Response user groups and the roles associated with them. Use this table to determine which users should be assigned which groups.

<table>
<thead>
<tr>
<th>User Group</th>
<th>Roles in this group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Champion</td>
<td>• sn_vul.app_read_assigned</td>
</tr>
<tr>
<td></td>
<td>• sn_vul.app_write_assigned</td>
</tr>
<tr>
<td></td>
<td>• sn_vul.app_update_assignment_group</td>
</tr>
<tr>
<td></td>
<td>• sn_vul.app_update_assigned_to</td>
</tr>
<tr>
<td>Members of this group can:</td>
<td></td>
</tr>
<tr>
<td>• Read and write application</td>
<td></td>
</tr>
<tr>
<td>vulnerable items (AVIs) assigned to you.</td>
<td></td>
</tr>
<tr>
<td>• Assign an AVI, that is assigned to you, to another individual or group.</td>
<td></td>
</tr>
<tr>
<td>User Group</td>
<td>Roles in this group</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>App-Sec Manager</td>
<td>• sn_vul.app_read_all&lt;br&gt;• sn_vul.app_write_all&lt;br&gt;• sn_vul.app_update_assignment_group&lt;br&gt;• sn_vul.app_update_assigned_to&lt;br&gt;• sn_vul.app_configure_integrations</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> By default, this role contains granular roles for third-party integration configuration. To define or edit an App-Sec Manager user group by single or specific integrations, see Vulnerability Response personas and granular roles.</td>
</tr>
<tr>
<td></td>
<td>• sn_vul.app_manage_assignment_rules&lt;br&gt;• sn_vul.app_manage_remediation_target_rules&lt;br&gt;• sn_vul.app_manage_risk_score_configurations&lt;br&gt;• sn_vul.app_manage_applications&lt;br&gt;• sn_vul.app_manage_app_vul_permissions&lt;br&gt;• sn_vul.app_manage_normalized_severity&lt;br&gt;• Version 13.0: sn_vul.app_manage_app_sc&lt;br&gt;• Version 12.0 only: sn_vul.app_read_application_release[Removed in v12.1. Do not use]&lt;br&gt;• sn_sec_int.admin&lt;br&gt;• Version 13.0: pa_power_user&lt;br&gt;• pa_viewer</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Starting with Vulnerability Response v13.0, pa_viewer is included in pa_power_user and no longer needed by itself.</td>
</tr>
</tbody>
</table>

Members of this group can:
• Read and write all AVIs.
• Configure AVR by create and manage rules, calculators, and severity maps.
• Configure integrations.
• Delete AVIs.
• Assign AVI to individuals or groups.
• Manage applications.
• Allows access to the Application module.
• Schedule, configure, execute integration.
• Read and execute integrations.
• View AVR Performance Analytics dashboards and reports.
<table>
<thead>
<tr>
<th>User Group</th>
<th>Roles in this group</th>
</tr>
</thead>
</table>
| Developer  | • sn_vul.app_read_assigned  
|            | • sn_vul.app_write_assigned  
|            | • sn_vul.app_update_assignment_group  
|            | • sn_vul.app_update_assigned_to  
|            | • sn_vul.app_pa_sc_view       |

Assign users to user groups in Application Vulnerability Response

Assign users to groups using the User Administration module in your instance.

**Before you begin**
Role required: admin

**Procedure**
To assign or remove a user from a group:

a. Navigate to Administration > Groups.

b. Locate and open the appropriate group, for example, App-Sec Manager. The group record is displayed.

c. Select the Group Members tab. The current members of the group are displayed.

d. Click Edit. The Edit members form is displayed.

e. From Collection list, select users to add to or remove from the group.

f. Once all users have been added to the Group Members List or removed, click Save. You are returned to the Group Members tab.

g. Click Update to save your changes and return to the Groups list.

**Related reference**
Components installed with Application Vulnerability Response
Understanding Application Vulnerable Item (AVI) states

Application Vulnerability Response offers a state model for the status of your application vulnerable items (AVIs), at any given time. Knowing how each state relates to and affects each other helps you to determine when and how to remediate your AVIs.

Application Vulnerable Item states

Understanding how states work helps with creating or editing application vulnerable item (AVI) rules.

Application vulnerable items have several possible states: Open, Deferred, Resolved and Closed. All these states are mapped from imported Remediation status from the third-party integration.

In an application vulnerable item, the State field is read-only.

The mapping for states is shown as follows.
**Identify applications in Application Vulnerability Response automatically**

When data is imported from a third-party integration, Application Vulnerability Response automatically uses application data to search for matches in the Configuration Management Database (CMDB). It does this using CI Lookup Rules. These rules identify applications for the application vulnerable item (AVI) record to aid in remediation.

As applications are imported, a lookup is performed on the Scanned Application [sn_vul_app_scanned_application] table using source_app_id and app_name to find matches to applications from prior imports. When an application ID match is found, its values are used in the Application and App release fields in the application vulnerable item record.

If a match is not found, or the application ID field is empty, the rules use the other application information to attempt to correctly identify the application. If a match is still not found, a placeholder scanned application record is created with only Application name and Application ID fields.

The Source Application Id and Application Name lookup rules are shipped with the Veracode Vulnerability Integration, by default.

⚠️ **Note:** Default CI lookup rules for Application Vulnerability Response are available only for the Veracode Vulnerability Integration.

When attempting a match, the lookup rules are evaluated by lowest Order value first. They stop when a rule returns a single CI as a match.

⚠️ **Note:** If a rule is created in such a way that it returns more than one CI, only the first match is used.

To make it easier to find matching issues, when a match is found, the CI lookup rule used to find it is added to the CI matching rule field for Scanned Applications. Click the Update Personalized List gear icon at the top of the Scanned Application list view to add it to the view.

⚠️ **Note:** Rules, once removed, cannot be recovered. Rather than removing existing rules, deactivate them when creating new ones.

CI lookup rules can be domain separated and are source-specific.

Importing vulnerability data can be taxing on an instance and performance issues with resources can occur if rules are not carefully constructed. The logic used to iterate through and perform matching within the CMDB can result in lengthy processing times. To avoid any potential degradation of resources
or performance complications, test any custom-written CI Lookup Rules or modifications to pre-defined CI Lookup Rules. See Prevent duplicate or orphaned records after running Application Vulnerability Response CI lookup rules for more information on preventing duplicate orphan records, deleting data, and cleaning up data.

Related information

Create a CI lookup rule

The CI Lookup Rules module contains rules that define what fields have matching data in the Configuration Management Database (CMDB). These rules are used to identify applications and application releases and add them to the application vulnerable item (AVI) record to aid in remediation.

Before you begin
Role required: App-Sec Manager group

About this task
Creating CI lookup rules requires advanced ServiceNow and Application Vulnerability Management expertise. Rather than modifying one of the existing lookup rules, consider copying it and modifying the copy. When you are satisfied that the new rule does what you want, deactivate the original.

Note: Rules, once removed, cannot be recovered. Rather than removing existing rules, deactivate them when creating new ones.

Procedure
2. Click New.
3. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>CI lookup rule form</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name</td>
<td>Name of the rule.</td>
</tr>
</tbody>
</table>
|                     | Lookup method | Method used for matching. Choices are:  
|                     |       | • **Script**: Pre-built or custom script.  
|                     |       | • **Field matching**: Search on table or field in the CMDB.  
<p>|                     | Type  | Type used with the Script Lookup method. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order</td>
<td>Order of precedence for the rule. Matches with the lowest order are evaluated first.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box for whether the rule is active or disabled.</td>
</tr>
<tr>
<td>Source</td>
<td>Source used as input to this rule.</td>
</tr>
<tr>
<td>Source field</td>
<td>Source field used as input to this rule. Fields must be a string or number.</td>
</tr>
<tr>
<td>Script</td>
<td>Editable sample script, based on the Type, is shown. Implement the custom script following the comments included in the template of the default function. Note: The process function has three parameters: rule, sourceValue, and sourcePayload</td>
</tr>
<tr>
<td>Search on table</td>
<td>Table to search within the CMDB. Used with field matching Lookup Method.</td>
</tr>
<tr>
<td>Search on field</td>
<td>Field that contains information that can be used to locate a CI. Used with the field matching Lookup method. This field may be on the CI record, or on a related record, such as a network adapter.</td>
</tr>
</tbody>
</table>
4. Click **Submit**.

**Example of a CI lookup rule using a script**

```javascript
1 // _queryMatch function checks if the query returns 0, 1 or more than 1 CI.
2 // it returns:
3 // null: if no CI found
4 // ci: if a unique CI was found
5 // _firstCI: if more than 1 CI was found and log a
6 // duplicate error message
7 function process(rule, sourceValue, sourcePayload) {
8   var sourceField = ();
9   sourceField[rule.source_field] = sourceValue;
10   var saGr = new GlideRecord("en_vul_app_seamed_Application");
11   saGr.addQuery("source", rule.source.source);
12   saGr.addQuery("source_app_id", sourceValue);
13   saGr.query();
14   saGr = _queryMatch(saGr, rule, sourceField);
15   if (saGr) {
16     return saGr.getUniqueValue();
17   }
18   return null;
19 })
```

**Related reference**

**Application Vulnerable Item fields**

**Prevent duplicate or orphaned records after running Application Vulnerability Response CI lookup rules**

Take steps to prevent duplicate or orphan records resulting from matching configuration items (CIs) within the CMDB.

Importing vulnerability data can be taxing on an instance and performance issues with resources can occur if rules are not carefully constructed. The logic used to iterate through and perform matching within the CMDB can result in lengthy processing times. Thorough testing and debugging of processing scripts in the rules helps alleviate the potential of issues later in the process.
Preventing duplicate or orphaned records

- Use small subsets of data that are specific to the CI lookup rule being tested.
  - Set all CI Lookup Rules, other than the one being tested, to Inactive.
  - Analyze the imported applications and configuration items (CIs) to ensure that you are observing the expected behavior and matching is occurring properly.
- Review CI states such as Retired.
- Remove Test Data.
  - Once you begin to observe the correct or expected behavior in CI matching, start over. This can be done by:
    - Deleting the data used for testing: (see the Deleting data from tables section)
      - Scanned applications
      - Application Vulnerable Items (AVIs)
      - Manually rerun the integrations.

Deleting data from tables

Sometimes you have imported data and realize something is wrong. If this happens in a development or performance environment, you could reclone from a better environment but, that isn’t always an option.

ℹ️ Note: Performing these actions requires advanced ServiceNow expertise.

There are four options for deleting data from tables:

- Using Delete All Records on Table Configuration.
- Configure the Table Cleaner by navigating to Auto Flushes (sys_auto_flush.list) and creating a new Auto-flush record.
- Truncate the gs.truncateTable using a background script.

ℹ️ Note: Never use truncateTable in a production environment. Consult your Support representative before executing large deletions in production or shared environments.

- Create a request in HI to have the data deleted.
Assign application vulnerable items in Application Vulnerability Response automatically

Automatically assign application vulnerabilities based on application tags, or any of the assignment groups in the Configuration Item [cmdb_ci] or platform assignment groups, to reduce the mean time to assignment.

Assigning application vulnerable items automatically
There are three different ways to assign AVIs using Assign using:

• User Group: This option allows you to select any of the existing Now Platform® user groups.

• User Group Field: This option allows you to choose any assignment group field available using the cmdb_ci table. By default, you see the following three group fields in the list menu under User group field.
  ◦ None: Indicates no default value for this mandatory field
  ◦ Configuration Item: Approval Group
  ◦ Configuration Item: Assignment Group
  ◦ Configuration Item: Support Group

• Script: This option allows you to define the conditions using a script. This option requires coding or advanced ServiceNow expertise.

Run high priority rules (items that need special handling, where risk is critical, or an AVI should be handled by regulatory compliance) first. Next, run your general rules, where no special handling is required, and you know who should be responsible for them. Finally, create a default rule to assign AVIs to the group that will figure out what assignment group it should belong to. This group could add another rule to cover their decisions. This default rule would run last.

Assignment rule evaluation process
When a new AVI is created, imported, or reopened after being closed, the assignment rules are evaluated against it. An AVI is only evaluated once, unless it is reopened after being closed. You can manually reapply rules after changes.

The following process is used for each new, updated, or reopened AVI:

• For each vulnerability assignment rule, the AVI is compared to the assignment filter, lowest order rule first.

• Where the condition matches, the AVI is assigned an assignment group. The lookup stops.
Where the conditions do not find a match among all the other rules, the AVI is assigned to the default assignment group, if a default rule exists.

**Note:** If there is no default rule, then the AVI remains unassigned.

**Assignment type**, whether **Manual** or **Rule** and **Assignment rule** are available from the Form Layout slushbucket on the application vulnerable item (AVI) form. Any AVI that was originally assigned by a rule but later manually reassigned contains a reference to the original rule.

**Note:** The assignment rules do not reevaluate manually created assignments.

Use **Assignment rule** and **Assignment type** information to identify cases where the assignment rules did not find a correct match for the intended recipient. Or which rules had the most reassignments.

**Reapplying assignment rules**
When you change an assignment rule, use the **Apply Changes** button on the Assignment Rules list view to rerun all the changed rules on all active Open AVIs (except those that were manually assigned).

**Note:**
- If the **Reapply all vulnerability assignment rules** scheduled job has not run before the first time you use **Apply Changes**, then it runs all the assignment rules on all Open AVIs except those AVIs that were manually assigned. After that, all subsequent uses of **Apply Changes** rerun only the changed rules and any dependent rules. Changes to one rule may result in an AVI matching a different unmodified rule.

The scheduled job [**Reapply all assignment rules**](#) is inactive, by default. When activated, it applies all the rules to all open AVIs except those manually assigned. It can run **Daily**, **Weekly**, **Monthly**, **Periodically**, **Once**, or **On Demand**. Depending on how many active AVIs you have in your environment, remember to set the **Run** field appropriately following the initial run to prevent performance impacts.

**Create or edit Application Vulnerability Response assignment rules**
You can create rules to automatically assign application vulnerable items (AVIs) based on filter conditions. These rules assign AVIs as they are imported or manually created.
Before you begin
Role required: App-Sec Manager group

About this task
With assignment rules, you define the condition of assignment and the order of execution. Once an AVI matches a rule condition, the assignment lookup stops. See Filtering within Application Vulnerability Management for more information.

Procedure
1. Navigate to Application Vulnerability Response > Administration > Assignment Rules.
2. Click New.
3. If New, fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Application Vulnerability Assignment Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Active</td>
</tr>
<tr>
<td>Execution order</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Condition</td>
</tr>
<tr>
<td>Condition fields</td>
</tr>
<tr>
<td>Assign using</td>
</tr>
<tr>
<td>Field</td>
</tr>
<tr>
<td>-----------------------</td>
</tr>
<tr>
<td>• User group:</td>
</tr>
<tr>
<td>• User group field:</td>
</tr>
<tr>
<td>• Script:</td>
</tr>
</tbody>
</table>

**Note:** Creating or edit a script requires ServiceNow expertise.

4. Click **Submit**. New or updated rules are evaluated on the next import.

### Calculate risk in Application Vulnerability Response automatically

Application vulnerability calculators automate calculating initial risk values for the fields on application vulnerable items (AVIs). Risk calculations offer insight into prioritizing remediation. The condition for each calculator is evaluated in order, and the first matching calculator is used.

#### Application Vulnerability Calculators

The Application Vulnerability Response base system includes two vulnerability calculators that set the base **Risk Score** on the application vulnerable item.

- **Basic Risk Calculator**
- **Advanced Risk Calculator**

Application vulnerability calculators can be built to prioritize and rate the impact of AVIs based on any criteria by using condition filters. Whether it is the business impact of the vulnerability, the class of the configuration item (CI), or the age of the AVI, you can create additional vulnerability calculators to set other fields on AVIs. Or you can customize the existing vulnerability calculators. A calculator can be written to reflect any set of priorities. See Filtering within Application Vulnerability Management for more information.

AVIs contain the **Risk Score** value derived from the risk calculators.

**Note:** An AVI displays **Source Severity** but not normalized severity. Normalized severity is used by the calculators to get the **Risk Score** value but is not shown on AVIs.

Each calculator contains a list of calculator rules, with a condition determining when to apply it. When the calculator is run, the condition for each calculator rule is evaluated in order, and the first matching calculator rule is used.
All enabled vulnerability calculators set the selected fields each time that an AVI is created, when an associated CI or vulnerability changes.

The **Basic Risk** calculator calculates **Risk Score** for AVIs using the normalized vulnerability severity.

⚠ **Note:** Only one calculator per target field (**Risk Score**) can be active at a time.

The **Basic Risk** is enabled by default. The **Advanced Risk Calculator** is disabled by default.

**Application vulnerability calculator rules**

The base system **Basic Risk Calculator** calculator contains calculator rules that assign each level of severity (None to Critical) a value (0-100) for **Risk Score** based on severity. **Unknown Severity** is automatically assigned a risk score of 100. These values can be adjusted and, like **Advanced Risk Calculator**, new calculator rules or new risk rules can be created.

The base system **Advanced Risk Calculator** calculator contains a specialized vulnerability calculator rule called **Default Risk Rule**. It calculates **Risk Score** based on multiple values:

- Vulnerability severity
- OWASP top 10
- SANS top 25

You can customize the criteria for the default risk rule. For more information, see .

You can adjust the values to use in the **Default Risk Rule** and how much weight to give each of these values. Weights are used to adjust how much each element counts when setting the **Risk Score**.

Each rule has an **Order** setting however, the first one to match the conditions updates the **Risk score** field in the AVI. Non-scripted calculator rules typically create less of a performance impact than scripted calculator rules.

**Create an application vulnerability calculator**

An application vulnerability calculator is a pre-defined formula to calculate a target field when certain criteria are met. Calculators, which calculate the application vulnerable item (AVI) **Risk Score**, can contain **Risk Rules**. Risk calculations offer insight in prioritizing remediation.

**Before you begin**

Role required: App-Sec Manager group
Note: You may notice performance degradation when running application vulnerability calculators that contain scripts. Order your rules to run the simplest rules first. Only run scripts on the items that cannot be handled with a condition and template value or a risk rule.

Procedure
1. Navigate to Application Vulnerability Response > Administration > Vulnerability Calculators.
2. Click New.
3. Fill in the fields on the form, as appropriate.

Vulnerability calculator form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the application vulnerability calculator.</td>
</tr>
<tr>
<td>Table</td>
<td>Auto-filled with the name of the AVI table.</td>
</tr>
<tr>
<td>Application</td>
<td>Auto-filled with Vulnerability Response.</td>
</tr>
<tr>
<td>Target field</td>
<td>Field to calculate.</td>
</tr>
<tr>
<td>Description</td>
<td>Text description of the calculator.</td>
</tr>
<tr>
<td>Active</td>
<td>Turn the calculator on or off.</td>
</tr>
</tbody>
</table>

4. Right-click in the header to Save. The Vulnerability Calculator Rules section appears.
5. Create a rule for the calculator by clicking New.

Note: For the New Risk Rules form (only available when the Target field is Risk Score) see step 10.
6. Fill in the fields, as appropriate.

Vulnerability Calculator Rule form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the calculator rule.</td>
</tr>
<tr>
<td>Order</td>
<td>The order in which to run the vulnerability calculator. A calculator with an order entry of 100 runs before a calculator with an order entry of 200.</td>
</tr>
<tr>
<td>Calculator</td>
<td>Auto-filled with the calculator parent.</td>
</tr>
</tbody>
</table>
7. Fill in the fields in the **When this condition is met** tab, as appropriate.

### When this condition is met tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition type</td>
<td>Available when you select the <strong>Advanced view</strong>. Choices include:</td>
</tr>
<tr>
<td></td>
<td>• Filter: Uses filter conditions.</td>
</tr>
<tr>
<td></td>
<td>• Filter group: See create and define filter groups to define the calculator criteria.</td>
</tr>
<tr>
<td></td>
<td>• Script: Script condition used to determine when to apply this calculator.</td>
</tr>
</tbody>
</table>

**Note:** Before you write scripts for determining when to apply the calculators, return to the Application Vulnerability Calculators list. Explore the vulnerability calculator records shipped with the base system.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Defines basic filter conditions for determining whether to use the calculator or not.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Selecting either the <strong>Filter group</strong> or <strong>Script</strong> condition types, hides this field.</td>
</tr>
</tbody>
</table>

8. Click the **Set these values** tab and fill in the fields on the form, as appropriate.

### Set these fields tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value type</td>
<td>Available when you select the <strong>Advanced view</strong>. Choices include:</td>
</tr>
<tr>
<td></td>
<td>• Template: Define the values to set on each field.</td>
</tr>
<tr>
<td></td>
<td>• Script: Used to set the values on each field.</td>
</tr>
</tbody>
</table>
9. When you have completed all entries, click Submit.

Note: When you edit an existing calculator, and you want to update all existing scores, you can use the Reapply Calculator button. It runs through all active AVIs, and if that calculator would be used to set its value, recalculates the value for those AVIs. Since reapplying a calculator can take a long time, a scheduled job handles it.

10. For the New Risk Rules form, fill in the fields as appropriate.

   Set each weight according to the percentage of the result that should come from that value. For any data that your scanner does not provide, or for data that should not be part of the risk score, set the weight to zero.

   As you update the weights, scenarios display the weights remaining, as well as anticipated Risk Score results.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the calculator rule.</td>
</tr>
<tr>
<td>Order</td>
<td>The order in which to run the calculator. A calculator with an order entry of 100 runs before a calculator with an order entry of 200.</td>
</tr>
<tr>
<td>Calculator</td>
<td>Auto-filled with the calculator parent.</td>
</tr>
<tr>
<td>Active</td>
<td>By default the Active check box is selected, which means the calculator rule is active. If you clear this check box, this rule does not apply to new vulnerable items created in the system.</td>
</tr>
<tr>
<td>Condition</td>
<td>Defines basic filter conditions for determining whether to use the calculator.</td>
</tr>
<tr>
<td></td>
<td>Selecting either the Filter group or Script condition types, hides this field.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Vulnerability Severity</td>
<td>Percentage of the result that comes from severity.</td>
</tr>
<tr>
<td>OWASP top 10</td>
<td>Percentage of the result that comes from the vulnerability’s presence in the OWASP top 10 list. If this information is not present in your vulnerabilities, set the weight to zero.</td>
</tr>
<tr>
<td>SANS top 25</td>
<td>Percentage of the result that comes from the vulnerability’s presence in the SANS top 25 list. If this information is not present in your vulnerabilities, set the weight to zero.</td>
</tr>
<tr>
<td>Running total</td>
<td>Auto-computed percentage totals. When this value reaches 100, the Scenario preview shows sample risk scores in different scenarios.</td>
</tr>
<tr>
<td>Sample scenarios</td>
<td>When all weights total 100%, risk score scenarios display, providing a preview of the risk score in some of the possible scenarios.</td>
</tr>
</tbody>
</table>

11. Click **Submit**.
Map the severity of an application vulnerable item automatically

Application Vulnerability Response severity mapping transforms third-party source severity fields to recognizable fields within Vulnerability Response.

Before you begin
Role required: App-Sec Manager group

About this task
Application Vulnerability Response third-party integrations such as the Veracode Vulnerability Integration provide severity mappings on installation. These maps can be adjusted by changing the fields in existing maps.

Creating or editing a severity map is intended only for customized or non-standard third-party mappings in your environment and requires Application Vulnerability Response and ServiceNow expertise.

Procedure
2. Click New.
3. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
</tr>
<tr>
<td>Source</td>
</tr>
<tr>
<td>Source value</td>
</tr>
</tbody>
</table>
| Target value | The target severity value. Choices are:  
  - 1 - Critical  
  - 2 - High  
  - 3 - Medium  
  - 4 - Low  
  - 5 - None |

4. Repeat Step 3 for each source severity level.
5. Click Submit.
Filtering within Application Vulnerability Management

Calculators, and Assignment Rules use conditions during import, created using the **condition builder**. Changes to their criteria can affect performance since each record is evaluated using these filters.

The rules and calculators shipped with the base system are optimized for performance. Editing or creating rules or calculators takes care and may require both ServiceNow and Application Vulnerability Response expertise. That said, some guidance is available.

**Avoid filtering based on subclass fields**

Some tables support extension. An example of that is the CMDB CI [cmdb_ci] table. Tables like cmdb_ci_hardware and cmdb_ci_computer extend this table. If you filter based on a field that is not on the parent table, that filter can be expensive to construct and evaluate.

For example, filtering on **Configuration Item > Cost** would not adversely affect performance because **Cost** is a class field, and not a subclass field, of **Configuration Item**.

**Configuration Item > Computer**, however, is a subclass requiring a dot-walk to another field, in this case, **Operating System**. This process can take many milliseconds which add up quickly, when millions of vulnerable items are being imported, and affect performance.

**Note**: Using the [contains] condition is like a wild-card search and can cause performance impact. Using [is], wherever possible, is more efficient.
Automate remediation target tracking in Application Vulnerability Response

Application Remediation Target Rules define the expected timeframe for remediating application vulnerable items (AVIs), providing a timeframe for remediating the vulnerability itself. For example, if an application vulnerable item contains a critical risk rating then the vulnerability on that item needs to be fixed within 15 days.

App-Sec Managers can create application remediation target rules by defining:

- The remediation target.
- The reminder target.

App-Sec Managers can see the remediation target date in the AVI form and list views, however dates are not updated for AVIs in the Deferred, Resolved, or Closed state.

The Remediation target date is color-coded on the AVI list view as dots, as follows:

- AVIs that have not reached their notification date are shown in green.
- AVIs approaching the remediation target date are shown in orange.
- AVIs past the remediation target date are shown in red.

Default rules
Application Vulnerability Response ships with three default rules which are inactive by default:

- Critical Risk Rating Rule: A remediation target with a 1-Critical risk rating, a remediation target of 15 days, and a reminder of 7 days before the target date.
- Medium-High Risk Rating rule: A remediation target with either a 2-High or 3-Medium risk rating a remediation target of 30 days, and a reminder of 7 days before the target date.
- Less Critical Risk Rating rule: A remediation target with a 4-Low risk rating a remediation target of 45 days, and a reminder of 7 days before the target date.

Remediation target rules can be deactivated or deleted

When a rule is deactivated, the current remediation target dates for the AVIs it was applied to, are cleared. If an AVI satisfies any active rule that rule is applied, otherwise the AVI has no rule or target date, and its status is No Target.
When rules are deleted, the **Remediation target** date and related fields on closed AVIs are preserved. The **Remediation target** date and related fields on non-closed AVIs are cleared and any dependent rules are reapplied.

**Remediation rule scenario**

- When multiple remediation target rules are applied to the same AVI, the most restrictive rule is applied.

For example, if an AVI meets the condition for two application remediation target rules:

**Scenario:** AVI last opened on 03/01/2018 at 10:00:00.

- Application remediation target rule 1: Last opened on 03/07/2018; remediation target is 15 days since it was last opened; calculated remediation target date is 03/16/2018 10:00:00.
- Application remediation target rule 2: Last opened on 03/10/2018; remediation target is 10 days since it was last opened; calculated remediation target date is 03/11/2018 10:00:00.

In this scenario, the Application remediation target rule 2 applies to the AVI since it has the more restrictive date, 10 days since the AVI was first identified versus 15 days.

**Note:** Application remediation targets are calculated from the **Last Opened** date plus the number of days (measured as 24-hour increments). You can add this field to the AVI form from the Form Layout slushbucket. It is the date the AVI was most recently opened in your instance.

**Note:** Once the application remediation target rule is defined, remediation target dates are calculated by the **Evaluate remediation targets** scheduled job or starting with v12.0, the **Apply Changes** button on the Remediation Target Rules list view.

**About the Evaluate remediation targets scheduled job**

**Evaluate remediation targets** runs once at 4:00:00 daily.

**Evaluate remediation targets** iterates through all active vulnerability rules, starting with those rules with the earliest remediation target date. It looks at all AVIs that:

- Are not in a **Closed**, **Deferred**, or **Resolved** state.
- Have no remediation target date.
- Have a remediation target date that is later than the date in the application remediation target rule.
**Evaluate remediation targets** adds a remediation target date, if one does not exist, or if this rule contains an earlier date than the one in the record, it updates the existing target date. Finally, it updates the **Remediation target date** and **Remediation status** fields in the AVI form. For inactive rules, **Evaluate remediation targets** clears the remediation fields on the AVI.

**Reapplying remediation target rules**
When you change a remediation target rule, use the **Apply Changes** button on the Remediation Target Rules list page to rerun all the changed rules on all active Open AVIs except those in the **Closed**, **Deferred** or **Resolved** state.

**Note:**
If the scheduled job, **Evaluate remediation targets** is running, you cannot initiate a reapply process. However, if a reapply process is already running, and the scheduled job is triggered, they run in parallel.

The reapply processes in Vulnerability Response and Application Vulnerability Response are independent and can run in parallel.

**Create or edit application remediation target rules**

Drive the remediation of high-risk vulnerabilities in a timely manner by setting up a remediation target rule at the application vulnerable item (AVI) level.

**Before you begin**
Role required: App-Sec Manager group

**Note:** The base system ships with three remediation target rules.
- Critical Risk Rating Rule
- Less Critical Risk Rating Rule
- Medium-High Risk Rating Rule

These rules are inactive by default. If you choose to edit one, rather than create a new one, remember to check the **Active** box before saving.

**Procedure**
1. Navigate to **Application Vulnerability Response > Administration > Remediation Target Rules**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the rule.</td>
</tr>
<tr>
<td>Target (days)</td>
<td>Specify the number of days within which the AVIs should be remediated, since last opened.</td>
</tr>
<tr>
<td>Active</td>
<td>By default the Active check box is selected, which means the remediation target rule is active. If this check box is cleared, this rule does not apply to new AVIs created in the system.</td>
</tr>
</tbody>
</table>
| Notify (days before due) | Number of days prior to the targeted remediation time for a reminder to be set. The notification date calculated using this value is used to show the remediation status and color coding. If the date is before the notification date, the remediation status is “In flight.” If it is past the notification date and before the remediation target date, the status is shown as approaching target.  

ℹ️ **Note:** If this field is set to 0, only a Target Missed notification is set. |
| Rule applies to          | Using the condition filter, select the criteria for applying the rule to the AVIs. To prevent performance impact, test your conditions at full production scale. Testing enables you to determine how long the Evaluate remediation targets job takes to execute, given the conditions and the size of your Configuration Management Database (CMDB). |
| Update history           | Unused for initial creation of a rule. Subsequently, system work notes are logged here.                                                      |
| Activities               | Unused for initial creation of a rule. Subsequently, system work notes are logged here.                                                      |

4. Click **Submit**.  
This rule goes into effect during the next run of the scheduled job, Evaluate remediation targets. The same is true when an existing rule is updated or when using the **Apply Changes** button on the Remediation Target Rules list view. The same is true when an existing rule is updated. For more information on
the scheduled job and **Apply Changes** see, *Automate remediation target tracking in Application Vulnerability Response.*

![Image of remediation target rule](image)

**View the remediation target status of an application vulnerable item**

When an application vulnerable item (AVI) has nearly reached (or passed) its remediation target date, as defined by a remediation target rule, the AVI record is updated with a status. This information can help you proactively monitor upcoming remediation activities.

**Before you begin**

Role required: App-Sec Manager group

**About this task**

A scheduled job called **Evaluate remediation targets**, runs once per day to compare the current date against the vulnerable item remediation date specified in the associated remediation target rule. When the current date falls within the number of days before the remediation is past due, a remediation status is added to the vulnerable item record.

**Procedure**

1. Navigate to **Application Vulnerability Response > Vulnerable Items**.
2. If the remediation date for the AVI is within range of the conditions set in the remediation target rule, check the Remediation Target Status columns, visible
on the Vulnerable Items list view. If the remediation target date has passed for an AVI, an annotation appears on the AVI form.

⚠️ **Note:** To view the number of AVIs that are Approaching Target, In-flight and Past Target, see View the Application Vulnerability Management [PA] dashboard.

### Related information

- Create or edit application remediation target rules

### Application Vulnerable Item fields

Application vulnerable items (AVIs) are automatically created during third-party vulnerability integration imports.

### Application Vulnerable Item fields

Except for the Assignment group, Assigned to fields and Notes, all other fields in the AVI are read-only.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Automatically generated AVI identifier for this record.</td>
</tr>
<tr>
<td>Scan type</td>
<td>Type of scanner that found this AVI.</td>
</tr>
<tr>
<td>Risk rating</td>
<td>Quantified <strong>Risk Score</strong> separating vulnerable items into Critical, High, Medium, Low, and None. For more information on risk ratings, see, <strong>Calculate risk in Application Vulnerability Response automatically</strong>.</td>
</tr>
<tr>
<td>Risk score</td>
<td>Calculated amount of risk the AVI poses to your environment. For more information, see <strong>Calculate risk in Application Vulnerability Response automatically</strong>.</td>
</tr>
<tr>
<td>Remediation target</td>
<td>Date by which the AVIs should be remediated, since first identified. Only appears when applicable. For more information on remediation targets, see <strong>Automate remediation target tracking in Application Vulnerability Response</strong>.</td>
</tr>
<tr>
<td>Remediation status</td>
<td>Status of the remediation for the AVI. It is determined by the AVI with the nearest due date, when applicable. States include:</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>• In-flight</td>
<td></td>
</tr>
<tr>
<td>• Approaching Target</td>
<td></td>
</tr>
<tr>
<td>• Past Target</td>
<td></td>
</tr>
<tr>
<td>Version 13.0: Category</td>
<td>Name of the category of the vulnerability.</td>
</tr>
<tr>
<td>Version 14.0: SAST</td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td>ID of the vulnerability associated with this application vulnerable item.</td>
</tr>
<tr>
<td>Application release</td>
<td>Version of the application.</td>
</tr>
<tr>
<td>Application module</td>
<td>Affected application in DAST scan.</td>
</tr>
<tr>
<td>Location:</td>
<td>URL location of the vulnerability within the application.</td>
</tr>
<tr>
<td>State</td>
<td>This field defaults to <strong>Open</strong> when created. See <strong>Understanding Application Vulnerable Item (AVI) states</strong> for more information on how states are mapped.</td>
</tr>
<tr>
<td>Reason</td>
<td>[Only visible when the AIV is in the <strong>Closed</strong> state.] Explanation of the State.</td>
</tr>
<tr>
<td>Assignment group</td>
<td>Group selected to work on this AVI. Can be manually added or edited by an App-Sec Manager.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>Individual from the selected assignment group that works on this AVI. Can be manually added or edited by an App-Sec Manager.</td>
</tr>
<tr>
<td>First found</td>
<td>Date the third-party source first found the application vulnerable item.</td>
</tr>
<tr>
<td>Last found</td>
<td>Date the third-party source last found the application vulnerable item.</td>
</tr>
<tr>
<td>Closed</td>
<td>[Only visible when the AVI is in the <strong>Closed</strong> state.] Date the AVI was closed.</td>
</tr>
<tr>
<td>Closed by</td>
<td>[Only visible when the AVI is in the <strong>Closed</strong> state.] Entity that closed the AVI.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Summary</td>
<td>Imported description of the vulnerability.</td>
</tr>
<tr>
<td><strong>Findings</strong></td>
<td>Read-only data imported from third-party integration.</td>
</tr>
<tr>
<td>Source AVIT ID</td>
<td>Imported identifier for the source AVI.</td>
</tr>
<tr>
<td>Source severity</td>
<td>Imported severity from the source application.</td>
</tr>
<tr>
<td>Source target fix date</td>
<td>Imported date by which the source expects the AVI to be remediated.</td>
</tr>
<tr>
<td>Source link</td>
<td>URL to the source AVI.</td>
</tr>
<tr>
<td>Source mitigation status</td>
<td>Imported mitigation status from the source application.</td>
</tr>
<tr>
<td>Source remediation status</td>
<td>Imported remediation status from the source application.</td>
</tr>
<tr>
<td>Version 12.1: Source finding status</td>
<td>[Only visible when populated] Imported issue status from the source application.</td>
</tr>
<tr>
<td>Complies with Policy</td>
<td>Imported compliance status. If not status is provided, this field is set to <strong>Not Applicable</strong>.</td>
</tr>
<tr>
<td>Source link</td>
<td>URL to the source AVI.</td>
</tr>
<tr>
<td>Version 13.0: Source notes</td>
<td>Imported notes from the source.</td>
</tr>
<tr>
<td>Version 13.0: Vulnerability summary</td>
<td>Imported summary from the source.</td>
</tr>
<tr>
<td>Version 13.0: Vulnerability explanation</td>
<td>Imported explanation from the source.</td>
</tr>
<tr>
<td>Version 13.0:</td>
<td>Imported recommendation from the source.</td>
</tr>
</tbody>
</table>
Scanned application fields

Applications are stored during import under Administration > Applications in Application Vulnerability Response.

Scanned Application fields

The imported fields in this table are read-only unless otherwise specified. Department and Support Group entries can be manually added or edited by an App-Sec Manager.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Imported name of the application.</td>
</tr>
<tr>
<td>Version</td>
<td>Imported version of the application, where applicable.</td>
</tr>
<tr>
<td>Operational status</td>
<td>Imported operational status of the application.</td>
</tr>
<tr>
<td>Department</td>
<td>Imported department to which the application belongs. If empty, it can be added manually.</td>
</tr>
<tr>
<td>Business unit</td>
<td>Imported business unit to which the department belongs. When the Department field is filled, this field is automatically</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
 | filled with the Business unit to which the department belongs. Otherwise, it is left empty and read-only.
Support group | Imported support group to which the application belongs. If empty, it can be added manually.
Description | Imported description of the application.

**Related List (visible only to an App-Sec Manager or Security Champion)**

| Version 13.0: Security champion | Lists the applications associated with a security champion. App-Sec Managers can add or remove members from the list.

### Components installed with Application Vulnerability Response

Several types of components are installed with activation of the Application Vulnerability Response feature, including tables, user roles, and scheduled jobs.

**Note:** The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

Demo data is available for this feature.

### Roles installed

Granular roles in Application Vulnerability Response are assigned to specific User Groups, by default.

**Note:** Using granular roles outside these user groups requires coding and advanced Application Vulnerability Response or ServiceNow expertise.

<table>
<thead>
<tr>
<th>Role title [name]</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sn_vul.app_read_assigned</td>
<td>View application vulnerable items (AVIs) assigned to you.</td>
</tr>
<tr>
<td>sn_vul.app_read_all</td>
<td>View all AVIs and related information.</td>
</tr>
<tr>
<td>sn_vul.app_write_assigned</td>
<td>Update AVIs assigned to you.</td>
</tr>
<tr>
<td>sn_vul.app_write_all</td>
<td>Update all AVIs and related information.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Role title [name]</th>
<th>Description</th>
<th>Contains</th>
</tr>
</thead>
<tbody>
<tr>
<td>sn_vul.app_update_assignment_group</td>
<td>Update AVI Assignment group.</td>
<td>Note:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When used outside of the default user group requires sn_vul.app_write_all</td>
</tr>
<tr>
<td></td>
<td></td>
<td>or sn_vul.app_write_assigned.</td>
</tr>
<tr>
<td>sn_vul.app_update_assigned_to</td>
<td>Update AVI assignee.</td>
<td>Note:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When used outside of the default user group requires sn_vul.app_write_all</td>
</tr>
<tr>
<td></td>
<td></td>
<td>or sn_vul.app_write_assigned.</td>
</tr>
<tr>
<td>sn_vul.app_configure_integrations</td>
<td>Configure third-party integrations.</td>
<td>sn_vul.app_configure_integrations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sn_vul.app_read_integrations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sn_vul_veracode.configure_integration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VR v13</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sn_vul.app_read_integrations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To define or edit an App-Sec Manager user group by single or specific integrations, see Vulnerability Response personas and granular roles.</td>
</tr>
<tr>
<td>sn_vul.app_read_integrations</td>
<td>View all third-party integrations.</td>
<td></td>
</tr>
<tr>
<td>sn_vul_veracode.configure_integration</td>
<td>Define, update, and delete Veracode integrations.</td>
<td></td>
</tr>
<tr>
<td>sn_vul.app_manage_assignment_rules</td>
<td>Define, update, and delete AVI assignment rules.</td>
<td>sn_vul.app_manage_assignment_rules</td>
</tr>
<tr>
<td>sn_vul.app_read_assignment_rules</td>
<td>View assignment rules.</td>
<td>sn_vul.app_read_assignment_rules</td>
</tr>
<tr>
<td>sn_vul.app_manage_remediation_target_rules</td>
<td>Define, update, and delete AVI remediation target rules.</td>
<td>sn_vul.app_manage_remediation_target_rules</td>
</tr>
<tr>
<td>sn_vul.app_manage_risk_score_configurations</td>
<td>Define, update, and delete AVR calculators and risk rules.</td>
<td>sn_vul.app_manage_risk_score_configurations</td>
</tr>
<tr>
<td>sn_vul.app_read_risk_score_configuration</td>
<td>View AVR calculators and risk rules.</td>
<td>sn_vul.app_read_risk_score_configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sn_sec_cmn.calc.write</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Role title [name]</th>
<th>Description</th>
<th>Contains</th>
</tr>
</thead>
<tbody>
<tr>
<td>sn_vul.app_manage_applications</td>
<td>View, update, and delete application records.</td>
<td></td>
</tr>
<tr>
<td><strong>Version 13.0:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sn_vul.app_manage_app_sc</td>
<td>Gives a Security Champion the ability to add or remove themselves from the Scanned Application related list.</td>
<td></td>
</tr>
<tr>
<td><strong>Version 13.0:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sn_vul.app_pa_sc_view</td>
<td>Provides relevant view to the specific Security Champion.</td>
<td></td>
</tr>
<tr>
<td>sn_vul.app_manage_app_vul_permissions</td>
<td>[internal] Used by sn_vul.app_manage_applications.</td>
<td></td>
</tr>
<tr>
<td>sn_vul.app_manage_normalized_severity</td>
<td>Update mapping to normalized severity.</td>
<td>sn_vul.</td>
</tr>
<tr>
<td>sn_vul.app_read_normalized_severity</td>
<td>View normalized severity records.</td>
<td></td>
</tr>
<tr>
<td><strong>Version 12.0:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sn_vul.app_read_normalized_severity</td>
<td>View normalized severity records.</td>
<td>[removed in v12.1. Do not use.]</td>
</tr>
<tr>
<td>sn_vul.app_read_application_release</td>
<td>View application release records.</td>
<td></td>
</tr>
<tr>
<td>sn_sec_int.admin</td>
<td>Provides access to integrations.</td>
<td></td>
</tr>
<tr>
<td><strong>Version 13.0:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>pa_power_user</td>
<td>Provides access to reports</td>
<td>pa_viewer</td>
</tr>
</tbody>
</table>

**Scheduled jobs installed**

For Vulnerability Response shared scheduled jobs see, Components installed with Vulnerability Response.

<table>
<thead>
<tr>
<th>Scheduled job</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version 13.0:</strong> Populate Entry and CVE M2M</td>
<td>Makes existing records consistent with multiple CWE records. Run once after upgrade to populate then disable.</td>
</tr>
<tr>
<td><strong>Version 13.0:</strong> Resync primary CWE</td>
<td>For customized primary CWE calculations. Run once after upgrade to resync then disable.</td>
</tr>
</tbody>
</table>
## Tables installed

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Release</td>
<td>Contains application version information.</td>
</tr>
<tr>
<td>[sn_vul_app_release]</td>
<td></td>
</tr>
<tr>
<td>Version 13.0: Application Security Champions</td>
<td>Contains the Application Vulnerability Response Security Champion group</td>
</tr>
<tr>
<td>[sn_vul_app_m2m_app_sc]</td>
<td>records.</td>
</tr>
<tr>
<td>Application Vulnerability Entry</td>
<td>Contains application vulnerability entries.</td>
</tr>
<tr>
<td>[sn_vul_app_vul_entry]</td>
<td></td>
</tr>
<tr>
<td>Application Vulnerability Integration</td>
<td>Contains Application Vulnerability Response integration records.</td>
</tr>
<tr>
<td>[sn_vul_app_integration]</td>
<td></td>
</tr>
<tr>
<td>Application Vulnerability Scan Location</td>
<td>Contains third-party scan location information.</td>
</tr>
<tr>
<td>[sn_vul_app_vul_scan_location]</td>
<td></td>
</tr>
<tr>
<td>Application Vulnerability Scan Summary</td>
<td>Contains third-party scan summary information.</td>
</tr>
<tr>
<td>[sn_vul_app_vul_scan_summary]</td>
<td></td>
</tr>
<tr>
<td>Application Vulnerable Item</td>
<td>Contains AVI records.</td>
</tr>
<tr>
<td>[sn_vul_app_vulnerable_item]</td>
<td></td>
</tr>
<tr>
<td>Scanned Application</td>
<td>Contains application information.</td>
</tr>
<tr>
<td>[sn_vul_app_scanned_application]</td>
<td></td>
</tr>
<tr>
<td>State Map</td>
<td>Contains state mapping from third-party integrations to application</td>
</tr>
<tr>
<td>[sn_vul_app_state_map]</td>
<td>vulnerable item (AVI) states.</td>
</tr>
<tr>
<td>Version 13.0: Vulnerability CWEs</td>
<td>Links CVE data to application vulnerable entries.</td>
</tr>
<tr>
<td>[sn_vul_m2m_entry_cwe]</td>
<td></td>
</tr>
</tbody>
</table>
Application Vulnerability Response remediation progress monitoring

Monitoring remediation is a process that begins with reviewing status and ends with closing application vulnerable items (AVIs). Application Vulnerability Response offers tools and procedures to make that process more productive and efficient.

Application Vulnerability Response remediation process

Application vulnerable item remediation is done manually.

An overview of the process:

- Log in to your Application Vulnerability Response instance.
- Validate that your rules (CI Lookup, Assignment) for application vulnerable items are working as expected. For information on revising CI Lookup Rules, see Identify applications in Application Vulnerability Response automatically. For information on Assignment rules, see Assign application vulnerable items in Application Vulnerability Response automatically.
- Validate that your remediation targets are correct. See Automate remediation target tracking in Application Vulnerability Response for information on how remediation target rules work and how to revise them. View the remediation target status of an application vulnerable item.

Note: Remediation target rules belong to AVIs. These rules are run when the AVI is imported.

- Review the dashboards or reports. For example, view dashboards that show AVIs aging by states.
Note:
For App-Sec Managers, Performance Analytics for Vulnerability Response contains the Application Vulnerability Response Overview, which can help you monitor areas of concern. See Using the Performance Analytics for Vulnerability Response content pack with Application Vulnerability Response and View the Application Vulnerability Management [PA] dashboard.

Version 13.0: For Security Champions, Performance Analytics for Vulnerability Response contains the My Application Vulnerabilities dashboard, which can help you monitor your areas of concern. See Using the Performance Analytics for Vulnerability Response content pack with Application Vulnerability Response and View the My Application Vulnerabilities dashboard.

Version 13.0: To limit the amount of data gathered for reports or related lists, see Define service classifications for Vulnerability Response reporting and related lists.

• Review the state of AVIs, in order of priority, searching for what has changed.
• Revise the risk for the AVIs, as needed. See Create an application vulnerability calculator for more information.
• Reassign the AVI to an assignment group for remediation, if needed.
• Rescans are triggered automatically by the third-party import schedule.
• After rescan, if the state is Fixed, AVIs are automatically closed during import.
• After the scan, if the state is not Fixed, the AVI is reopened.

Using the Performance Analytics for Vulnerability Response content pack with Application Vulnerability Response

The Performance Analytics for Vulnerability Response content pack contains a preconfigured dashboard for Application Vulnerability Response. This dashboard presents important metrics for analyzing your Application Vulnerability Management process, such as viewing remediation target attainment rates. The Performance Analytics for Vulnerability Response content pack is not automatically installed with the Vulnerability Response application. It is available on the ServiceNow Store as a separate subscription.
Enable your Performance Analytics Solutions for Vulnerability Response

For more information about setting up, installing, and configuring your Performance Analytics for Vulnerability Response application, see Install and configure the Performance Analytics for Vulnerability Response [PA] application.

Key terms

**Performance analytics (PA)**
Solution that creates management dashboards, reports on KPIs and metrics, and answers key business questions to help increase quality and reduce costs.

**Application Vulnerable item (AVI)**
An application vulnerability reported by a third-party vulnerability scanner that is present on a configuration item (CI).

**PA indicator**
Defines a performance measurement taken at regular intervals of an activity, or organizational behavior, for example, Top 10 Applications with the Most Critical Application Vulnerable Items.

**PA indicator source**
Data sets that filter records from one table or database view, for example, AVI Active.

Overview

The Application Vulnerability Management [PA] dashboard in the Performance Analytics for Vulnerability Response application provides you with important tools for your Application Vulnerability Management process.

View the Application Vulnerability Management [PA] dashboard

With the Application Vulnerability Management (PA) dashboard, vulnerability management can track the volume, performance and progress of vulnerabilities from initial analysis/detection to containment, or remediation. Quickly gain insight into your vulnerability exposure and security posture.

Using the dashboard

Organizations are dealing with increasing security incidents due to application vulnerabilities. Efficiently determine which application vulnerable items (AVIs) present the most risk to your organization. These dashboards provide a graphical view into AVI activity to help determine remediation plans and status progress.
You can focus on the KPIs associated with critical affected applications and high-visibility vulnerabilities.

View reports that show trending data over time. View trends of important metrics on a regular schedule to analyze your overall business processes and identify areas of improvement.

To view the dashboard, navigate to **Application Vulnerability Response > Overview**.

⚠️ **Note:** Version 13.0: The My Application Vulnerabilities dashboard is a subset of the Overview dashboard and only available when a member of the Security Champion user group logs into an instance. For information on the My Application Vulnerabilities dashboard, see [View the My Application Vulnerabilities dashboard](#).

**Application Vulnerability Management (PA) dashboard tabs**

The Overview dashboard communicates KPIs for vulnerability risk and prevalence, affected applications, remediation trends, and remediation progress. The default for trends is three months but can be changed to 7 day, one month, 3 months, 6 months, YTD, 1 year, or All.

Starting with v13.0, breakdown the data in the Application Vulnerability Management dashboard by **Scan Type**, **Application** or **Business unit**. Each of these choices has an additional filter, **Select elements**, to refine your selections.
Security Posture tab

The Security Posture tab helps you understand your security posture and the progress of your remediation actions.

Remediation Trend tab

The Remediation Trend tab helps you understand the progress of your remediation actions.
Scoreboard tab

The Scoreboard tab helps you understand the progress of your remediation actions, and which AVIs need the most assistance with their completion.

Report details

Security Posture

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Application Vulnerable Items (AVIs)</td>
<td>Single Score</td>
<td>Number of active (non-closed) application vulnerable items (AVIs).</td>
</tr>
<tr>
<td>Unassigned Application Vulnerable Items (AVIs)</td>
<td>Single Score</td>
<td>Number of active application vulnerable items (AVIs) without an assignment group.</td>
</tr>
<tr>
<td>AVI Distribution</td>
<td>Pie Chart</td>
<td>Distribution of all active application vulnerable items (AVIs) grouped by risk rating.</td>
</tr>
</tbody>
</table>
### Security Posture (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AVIs by Age</td>
<td>Heatmap</td>
<td>Number of active application vulnerable items (AVIs) grouped by risk rating and age (in days).</td>
</tr>
<tr>
<td>AVI trends</td>
<td>Trend</td>
<td>Trend of active application vulnerable items (AVIs) grouped by risk rating.</td>
</tr>
<tr>
<td>Average AVIs per application</td>
<td>Trend</td>
<td>Trend of average application vulnerable items (AVIs) per application, grouped by risk rating.</td>
</tr>
</tbody>
</table>

### Remediation Trend

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean time to RemEDIATE Application Vulnerable Items (AVIs)</td>
<td>Line</td>
<td>Trend of the average remediation time for application vulnerable items (AVIs) by risk rating.</td>
</tr>
<tr>
<td>Net change of AVIs</td>
<td>Trend</td>
<td>Trend of new application vulnerable items (AVIs) detected vs closed by month.</td>
</tr>
</tbody>
</table>

### Scoreboard

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 10 Applications with Most Critical Application Vulnerable Items (AVIs)</td>
<td>Score card and Distribution</td>
<td>Applications with most number of critical application vulnerable items (AVIs).</td>
</tr>
</tbody>
</table>
Scoreboard (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 10 Applications with Most Overdue Critical Application Vulnerable Items (AVIs)</td>
<td>Scorecard and Distribution Bar</td>
<td>Applications with the most number of active application vulnerable items (AVIs) that are past their remediation target dates.</td>
</tr>
</tbody>
</table>

Application Vulnerability Management breakdowns

The following breakdowns apply to the indicators on the Scoreboard dashboard:

- Application
- Business Unit

View the My Application Vulnerabilities dashboard

Starting with version 13.0, a Security Champion uses the My Application Vulnerabilities dashboard to track the volume, performance and progress of vulnerabilities from initial analysis/detection to containment, or remediation. Quickly gain insight into your vulnerability exposure and security posture.

Using the dashboard

View reports that show trending data over time. View trends of important metrics on a regular schedule to analyze your overall business processes and identify areas of improvement.

To view the dashboard, navigate to Application Vulnerability Response > My Application Vulnerabilities.

Note: The My Application Vulnerabilities dashboard is available only when a member of the Security Champion user group logs into an instance. For information on the Overview dashboard, see View the Application Vulnerability Management [PA] dashboard.
My Application Vulnerabilities dashboard tabs

The My Application Vulnerabilities dashboard communicates KPIs for vulnerability risk and prevalence, affected applications, remediation trends, and remediation progress. The default for trends is three months but can be changed to 7 day, one month, 3 months, 6 months, YTD, 1 year, or All.

Data is broken down in the dashboard by, Application. Use the Select elements list to refine your selections.

Security Posture tab

The Security Posture tab helps you understand your security posture and the progress of your remediation actions.
Remediation Trend tab

The Remediation Trend tab helps you understand the progress of your remediation actions.

Report details

Security Posture

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Application Vulnerable Items (AVIs)</td>
<td>Single Score</td>
<td>Number of active (non-closed) application vulnerable items (AVIs).</td>
</tr>
<tr>
<td>Application Vulnerable Item (AVI) Distribution</td>
<td>Pie Chart</td>
<td>Distribution of all active application vulnerable items (AVIs) grouped by risk rating.</td>
</tr>
<tr>
<td>AVI trends</td>
<td>Trend</td>
<td>Trend of active application vulnerable items (AVIs) grouped by risk rating.</td>
</tr>
</tbody>
</table>
Security Posture (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average AVIs per application</td>
<td></td>
<td>Trend of average application vulnerable items (AVIs) per application, grouped by risk rating.</td>
</tr>
</tbody>
</table>

Remediation Trend

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean time to Remediate Application Vulnerable Items (AVIs)</td>
<td>Line</td>
<td>Trend of the average remediation time for application vulnerable items (AVIs) by risk rating.</td>
</tr>
<tr>
<td>Net change of AVIs</td>
<td>Trend</td>
<td>Trend of new application vulnerable items (AVIs) detected vs closed by month.</td>
</tr>
</tbody>
</table>

Application Vulnerability Response integrations

Vulnerability Response includes support for third-party integrations.

Third-party integrations

Application vulnerability integrations help enrich the application vulnerability data on your instance by retrieving data from external systems and vendors.

⚠️ Note:

Multi-source integrations are not supported in Application Vulnerability Response. Third-party integrations are treated separately. If more than one third-party integration application is in use in your environment, there is no application vulnerable item (AVI) deduplication across integrations.

Vulnerability Response supports the following third-party integration:

• Veracode

For information on the configuration of the Veracode Vulnerability Integration, see Installation the ServiceNow Vulnerability Response Integration with Veracode and Configure the Veracode Vulnerability Integration.
Understanding the Veracode Vulnerability Integration

The Vulnerability Response Integration with Veracode application uses data imported from the Veracode product to help you determine the impact and priority of flaws in your code.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Veracode Vulnerability Integration

The Veracode product collects DAST scanner data and makes that data available to the Now Platform®. It easily integrates with the Application Vulnerability Response feature of Vulnerability Response to map third-party vulnerabilities enriching the data in your instance.

There is a configured run-as user for each integration record. The default value for this user is VR.System. Do not change this value.

Every day, scheduled jobs invoke the integrations automatically in the order they are listed. You can also execute individual scheduled jobs manually. Scheduled jobs simplify the vulnerability remediation life cycle by keeping the instance synchronized with other vulnerability management systems.

Available versions

<table>
<thead>
<tr>
<th>Release version</th>
<th>Release Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veracode 2.0</td>
<td>Vulnerability Response Integrations Release Notes</td>
</tr>
<tr>
<td>Veracode 1.0</td>
<td></td>
</tr>
</tbody>
</table>

User group and roles

The Veracode Vulnerability Integration is installed by a system administrator [admin] and configured by a member of the App-Sec Manager group. See Manage Application Vulnerability Response user groups and roles for more information.

Veracode Vulnerability Integrations

To view the Veracode vulnerability integrations, navigate to Veracode Vulnerability Integration > Integrations.
The following integrations are included in the base system. Only the Veracode Application List Integration integration is active, by default.

### Veracode Vulnerability Integrations

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veracode Application List Integration</td>
<td>Retrieves Veracode application scanner data (vulnerabilities, metadata) and enriches your application data. This integration is set to run daily at 00:00:00.</td>
</tr>
<tr>
<td>Veracode Scan Summary</td>
<td>Retrieves scan records from Veracode. This integration is chained to run following the Veracode Application List Integration when activated.</td>
</tr>
<tr>
<td>Veracode Application Vulnerable Item Integration</td>
<td>Retrieves scan results from Veracode, inserts AVIs and enriches your third-party vulnerability data. This integration is chained to run following the Veracode Scan Summary integration when activated.</td>
</tr>
</tbody>
</table>

For integration run statuses see, View the Veracode Vulnerability Integration import run status.

To view data in third-party vulnerabilities, see View vulnerability libraries.

### Preparing for the Veracode Vulnerability Integration

A successful Veracode Vulnerability Integration requires planning and the execution of pre-integration tasks. Prepare for the integration by performing these tasks. The Veracode Vulnerability Integration assumes that you are familiar with the Veracode product and API.

**Before you begin**

The Common Weakness Enumeration (CWE) integration is also used by Application Vulnerability Response and should be running prior to installing and configuring the Veracode Vulnerability Integration. It is installed with Vulnerability Response, by default.

⚠️ **Note:** NIST Vulnerability Database (NVD) data is not necessary to install the Veracode Application Vulnerability Integration, however they provide enrichment and would be useful to have. For information on NVD, see Managing NVD, CWE, and third-party data libraries.

There is a configured run-as user for each integration record. The default value for this user is VR.System. Do not change this value.
Role required: App-Sec Manager group

About this task

Note: Before running the integration, make any necessary configuration changes based on your requirements.

- Validate your instance sizing based on the number of application vulnerable items you expect to import. An undersized instance can lead to long load times. If you do not know the size of your instance, contact Customer Service and Support.

The Veracode Vulnerability Integration requires an API id and API key.

Procedure

To create the API ID and key credentials:

a. Log in to the Veracode Platform.

b. Go to the user account menu and select API Credentials.

c. Click Generate API Credentials.

d. Record your credentials for later use.

Installation the ServiceNow® Vulnerability Response Integration with Veracode

Before you run the integration on your instance, the installation and configuration steps must be completed so the Veracode product properly integrates with Application Vulnerability Response. This application is available as a separate subscription.

Before you begin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

Note: This process applies only to applications downloaded to production instances. If you're downloading applications to sub-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

<table>
<thead>
<tr>
<th>Setup tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that the Vulnerability Response application is installed and activated.</td>
<td>To verify that this application is activated, navigate to Subscription Management &gt; Subscriptions in...</td>
</tr>
<tr>
<td>Setup tasks</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Verify that you have the required</td>
<td>The following roles are required for installation, configuration, and verification of expected results:</td>
</tr>
<tr>
<td>ServiceNow roles for your instance.</td>
<td>• If not already assigned, the System Administrator [admin] installs the application and assigns users to the App-Sec Manager group. For information on Group roles see, Manage Application Vulnerability Response user groups and roles.</td>
</tr>
<tr>
<td></td>
<td>• The App-Sec Manager group oversees configuration and verifies expected results.</td>
</tr>
</tbody>
</table>

Role required: admin

**Procedure**

1. Log in to the instance you want to install the Veracode Vulnerability Integration on.
2. Navigate to the ServiceNow Store.
3. In the ServiceNow Store, search for Vulnerability Response Integration with Veracode application.
4. Click the application tile. Detailed information about the application you are installing is displayed.
   ❗ **Note**: Consider reading the Other Requirements and Dependencies sections, as applicable.
5. Click Request App and enter your Now Support login credentials.
6. Click Get.
7. Enter the Instance Name and Reason for the Instance, and click Validate Instance.
8. Click Request.
   You will receive an email with detailed installation instructions.

9. Navigate to **System Applications > Applications**.

10. Locate the application, select it, and click **Install**.
    Your application is automatically installed on your instance.

### What to do next
Configure the Veracode Vulnerability Integration for your environment. See Configure the Veracode Vulnerability Integration.

### Configure the Veracode Vulnerability Integration

Before you run the integration on your instance, the installation and configuration steps must be completed so the Veracode product properly integrates with Application Vulnerability Response. This application is available as a separate subscription.

### Before you begin
Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

**Note:** This process applies only to applications downloaded to production instances. If you're downloading applications to sub-production or development instances, it’s not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

<table>
<thead>
<tr>
<th>Setup tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that the Vulnerability Response application is installed and activated.</td>
<td>To verify that this application is activated, navigate to <strong>Subscription Management &gt; Subscriptions</strong> in your instance. The list displays the subscriptions your organization has purchased. If the application is not installed and activated see, Install and configure Vulnerability Response.</td>
</tr>
<tr>
<td>Verify that you have the required ServiceNow roles for your instance.</td>
<td>The following roles are required for configuration, and verification of expected results:</td>
</tr>
</tbody>
</table>
### Setup tasks

| Role required: App-Sec Manager user group |

#### Description

- If not already assigned, the System Administrator [admin] installs the app and assigns users to the App-Sec Manager user group.
- The App-Sec Manager oversees configuration and verifies expected results.

For the Veracode Application Vulnerability integration, have your API id and API key ready. Contact Veracode to obtain the API id and API key. See Preparing for the Veracode Vulnerability Integration.

### Procedure

1. Navigate to Veracode Vulnerability Integration > Configuration
2. Fill in the API id and API Key fields.
3. Choose your testing results.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Version 3.0: | Select DAST or SAST data types to include in the import.  

**Note:** You can choose one or the other, or both, but you must select at least one. |
| Version 1.0: | Dynamic Application Security testing results are selected, by default. |

4. Save and validate your choices.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Version 3.0: | Click Save and Test Credentials.  

**Note:** Configuration is successfully completed unless an error message is displayed. If an error message is displayed during the configuration, reenter your data.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><em>Click Save.</em> Verify successful configuration by clicking <strong>Test Credentials.</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Configuration is successfully completed unless an error message is displayed. If an error message is displayed during the configuration, reenter your data.

### Version 2.1

- **Veracode Configuration**
  - **API ID**
  - **API Key**
    - 
  - Include DAST
    - ✓
  - Include SAST
    - 

- **Save and Test Credentials**

### What to do next

If your environment requires domain-separated imports, see [Create domain-separated imports for the Veracode Vulnerability Integration](#).

On initial installation, refer to [Configure Application Vulnerability Response](#) for further instructions.

After initial installation, for modifications refer to [Optional Veracode Vulnerability Integration modification and activities](#).
View the Veracode Vulnerability Integration import run status

Use the Vulnerability Integration Runs related list to verify the success of your integration runs, locate any issues, and inform your remediation decisions.

Before you begin

To view the Veracode Vulnerability Integration import run status:

- Application Vulnerability Response and the Veracode Vulnerability Integration must be installed and configured.
- The Veracode Vulnerability Integration imports must be scheduled and running.

Role required: App-Sec Manager group

Procedure

1. Navigate to Veracode Vulnerability Integration > Integrations.
2. Select an integration.
3. Click the Vulnerability Integration Runs related list.
4. Verify that all imports have succeeded.

Trouble?

The most common causes for a failed run include:

- Network interruption.
- An issue in the data transfer resulting in corrupted data during the transform.

If you encounter any of these conditions, click Execute Now, and rerun the integration.

Optional Veracode Vulnerability Integration modification and activities

Configure optional modifications specifically for the Veracode Vulnerability Integration.

Note: Changing other Veracode Vulnerability Integration settings, other than the ones listed here, requires advanced ServiceNow and Application Vulnerability Response expertise and is beyond the scope of the product documentation.
Perform a manual Veracode application vulnerability import

If your initial import failed, or you do not want to wait for the scheduled initial import, you can perform a full data import independent of the daily scheduled job.

Before you begin
Role required: App-Sec Manager group

Procedure
1. Navigate to Veracode Vulnerability Integration > Integrations.
2. Choose an integration, for example, the Veracode Application List Integration.
3. Click Execute Now.

Note: Each of the Veracode application vulnerability integrations are intended to provide the most complete data retrieval. Running them out of order requires ServiceNow and Application Vulnerability Response expertise and could result in incomplete data.

Once the import is complete, scheduled imports resume.

4. For integration run statuses see, View the Veracode Vulnerability Integration import run status.

Set Veracode Vulnerability Integration import times

For your convenience, you can reset the start time for the Veracode Vulnerability Integrations.

Before you begin
Role required: App-Sec Manager group

About this task
After the initial import, Veracode vulnerability integrations do a full import each time it runs. See Perform a manual Veracode application vulnerability import for more information on performing imports.

Procedure
1. Navigate to Veracode Vulnerability Integration > Integrations.
2. Choose an integration.
3. Set the new Start time. Time is calculated as Hours in local time. The default time for the Veracode Application List Integration imports is 00:00:00.
other integrations are **On Demand** and chained to run after the Veracode Application List Integration. Changing the **Start time** for either of these requires advanced ServiceNow and Application Vulnerability Management expertise.

4. Click **Update**.
   The new time is used for the next scheduled import.

---

**Create domain-separated imports for the Veracode Vulnerability Integration**

If you require application vulnerability integration data to be imported to a specific domain, you must assign a user in that domain to run the integrations.

**Before you begin**

Role required: App-Sec Manager user group

**About this task**

This set of tasks requires coding or advanced ServiceNow expertise.

The import queues contain data attachments that the scheduled jobs (integrations) process. In a domain-separated environment, you must match the scheduled job with the correct import queue.

**Procedure**

1. Create a domain.

2. For every domain you create, create a user and assign the user to that domain.
   Think of this user as a **run_as** placeholder for the domain in your Veracode application integration. It is the equivalent to the **VR.System** user in the global domain. This user needs access to data sources, and vulnerability data.

   ⚠ **Note:** Do not use this user for any other purpose.

3. In each domain, create a scheduled job.

   a. Navigate to **System Definition > Scheduled Jobs**.

   b. Copy **Scheduled Vulnerability Data Source Processor** into the domain.

   c. To identify the scheduled job, append the domain to the name.
d. In the **Run as** field change the **run_as** user to the user you created in the Step 2.

4. Ensure the integration runs in the **run_as** user domain.

   a. Edit the **Execute Now** UI action to add this code to the top of the file.

   **Example**

   ```java
   //sys id below is of host detection integration
   if(current.sys_id == "5d9cf0daff540300c68c9f783894fa4d"){
       current.run_as = gs.getUserID
   }
   ```

   b. Edit the **VulnerabilityIntegrationUtils** script include method **addIntegrationRun** to add the highlighted code.
c. Add the highlighted code to the **VulnerabilityIntegrationUtils** script include method **addProcessRun**.

addProcessRun code

```javascript
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
}
```

d. Add the highlighted code to the **VulnerabilityIntegrationUtils** script include method **copyProcess**.

copyProcess code

```javascript
_copyProcess: function(listProcGr, isProcessErrored) {
    var copy = new GlideRecord("sn_vul_integration_process");
    copy.initialize();
    copy.setValue("integration_run", intProcGr.getValue("integration_run"));
    copy.setValue("parameters", intProcGr.getValue("parameters"));
    copy.setValue("state", "new");
    copy.setValue("notes", ");
    copy.setValue("sys_domain", intProcGr.getValue("sys_domain"));
    if (isProcessErrored) {
        copy.setValue("errored_retries", parseInt(intProcGr.getValue("errored_retries")) + 1);
        var nextRetryDue;
        if (intProcGr.getValue("next_retry_due_m") == ")
            nextRetryDue = new GlideDate().addSecond(intProcGr.getValue("next_retry_due_m") + 60);
        else
            nextRetryDue = new GlideDate().addSecond(intProcGr.getValue("next_retry_due_m"));
    } else {
        var intDistance = new sn_vul.VulnerabilityIntegrationHelper().getIntDistace();
        var nextRetryDelay = intDistance.getNovtRetry(intProcGr.getValue("errored_retries"));
        copy.setValue("next_retry_due_m", nextRetryDue); 
        copy.setValue("retries", intProcGr.retries + 1);
    }
    copy.insert();
    return copy;
}
```

e. Edit the **DataSourceVulnReportRefreshProcessor** script include method **_processFromDataSourceGroups**.

**Example**

Change the original line of code:

```javascript
this.integrationProcessGr.getUniqueValues());
```

to

```javascript
this.integrationProcessGr.getUniqueValue(), this.integrationProcessGr.getValue("sys_domain")
```

Edited **_processFromDataSourceGroups** code

```javascript
var mgr = new sn_vul.VulnerabilityOSAttachmentManager();
mgr.queueItem(isUniqueValue, this.integrationProcessGr.getUniqueValue(), this.integrationProcessGr.getValue("sys_domain"));
```
f. Add the following highlighted code blocks to the `VulnerabilityDSAttachmentManager` script include method, `queueItem`.

```javascript
queueItem: function(dataSource, attachName, reportData, optIntegrationProcess, optDomain) {
  var gr = new GlideRecord(this.QUEUE_TABLE);
  gr.initialize();
  gr.setValue("status", "NEW");
  gr.setValue("data_source", dataSource);
  if (optIntegrationProcess)
    gr.setValue("integration.process", optIntegrationProcess);
  if (optDomain)
    gr.setValue("sys_domain", optDomain);
  var sysID = gr.insert();
}
```

g. Add the following highlighted code blocks to the `VulnerabilityDSAttachmentManager` script include function, `getNext`.

```javascript
getNext: function() {
  var gr = new GlideRecord(this.QUEUE_TABLE);
  gr.getsysuserId();
  var sysDomainUser = gr.getValue("sys_domain");
  var gr = new GlideRecord(this.QUEUE_TABLE);
  gr.setQuery("status", "ACTIV");
  gr.setQuery("sys_domain", sysDomainUser);
  gr.query();
  if (gr.next()) {
    return gr;
  }
}
```

h. Add the following highlighted code blocks to the `VulnerabilityDSAttachmentManager` script include function, `_processQueueEntry`.

```javascript
// Then handle the regular queue items
gr = new GlideRecord(this.QUEUE_TABLE);
gr.setQuery("status", "QUEUED");
gr.query("queue on");
gr.setValue("sys_domain", sysDomainUser);
if (gr.next()) {
  return gr;
}
```
processQueueEntry function

At this point, you are ready for domain-separated host detection imports.

Configuration Compliance

Configuration Compliance is a Secure Configuration Assessment (SCA) application that aggregates scan results from integrations with configuration scanning applications, such as Qualys Cloud Platform. You can prioritize configuration compliance issues using the Configuration Management Database (CMDB). Configuration Compliance tightly integrates with the IT change management process to remediate non-compliant configurations.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

<table>
<thead>
<tr>
<th>Explore</th>
<th>Set up</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Understanding Configuration Compliance</td>
<td>• Configuration Compliance setup</td>
</tr>
<tr>
<td>• Upgrade to Paris.</td>
<td>• Install and configure Configuration Compliance</td>
</tr>
<tr>
<td>• Security Operations videos</td>
<td>• Configuration Compliance calculator groups</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use</th>
<th>Develop</th>
</tr>
</thead>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Understanding Configuration Compliance

Use test results obtained from third-party SCA integrations to verify compliance with security or corporate policies by identifying and remediating non-compliant configuration items.

What is Configuration Compliance

With Configuration Compliance you can do the following:

- Version 12.0: Include IT change management as part of your remediation process
- Version 12.0: Set the expected time frames for remediating test results with remediation target rules
- Automatically import policies, tests, authoritative sources, and technologies
- Automatically correlate policies and tests to configuration items
- Analyze test results
- Automatically group test results for remediation
- Automatically assign test results to groups or individuals for remediation
- RemEDIATE non-compliant configuration items

Who uses Configuration Compliance

Configuration Compliance activities can involve many levels of management.
• System administrators
• Vulnerability administrators
• Vulnerability managers
• Vulnerability analysts
• Compliance administrators

Configuration Compliance tasks involve the following roles.
• sn_vulc.admin — can read, write, delete
• sn_vulc.write — can read and write
• sn_vulc.remediation_owner — Can read and update assigned records

*Note:* The sn_vulc.remediation_owner role is also automatically assigned when any user is assigned the itil role.
• sn_vulc.read — can read

Configuration Compliance and Security Operations

Configuration Compliance works with third-party SCA scanner applications and integrates with Governance, Risk, and Compliance (GRC) for continuous monitoring. Configuration Compliance and GRC are available as separate subscriptions.

When the Qualys Vulnerability Integration is installed, access to Vulnerability Response becomes available. You can have multiple deployments of the Qualys Vulnerability Integration. Data sourced from each deployment is identified and available in a single instance of GRC.
Available versions for Paris

<table>
<thead>
<tr>
<th>Release version</th>
<th>Release notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Compliance v12.1</td>
<td>Configuration Compliance Release notes</td>
</tr>
<tr>
<td>Configuration Compliance v12.0</td>
<td>For more information about released versions of the Configuration Compliance application, compatibility with Paris, and schema changes, see KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes.</td>
</tr>
<tr>
<td>Configuration Compliance v11.1</td>
<td></td>
</tr>
<tr>
<td>Configuration Compliance v11.0</td>
<td></td>
</tr>
<tr>
<td>Configuration Compliance v10.3</td>
<td></td>
</tr>
<tr>
<td>Configuration Compliance v10.0</td>
<td></td>
</tr>
</tbody>
</table>

Configuration Compliance imported data

Configuration Compliance imports policies, tests, authoritative sources, and test results from third-party integrations and stores them in modules for viewing.

Policies

Policies are related to authoritative documents and test records. A group of configuration tests define policies. Policies typically align to a technology class (ex. Windows, Oracle databases, Cisco IOS) and are often derived from the primary industry standard. Policies can be modified to meet the needs of the organization. A single Configuration Test can belong to multiple policies.

If the Qualys Vulnerability integration is installed, policies are retrieved and Control IDs populated by the scheduled job, Qualys PC Policies at 1:00AM. You can view the scheduled job by navigating to Qualys Vulnerability Integration > Primary Integrations > Qualys PC Policies.

Notes: If you choose to run the integration manually, run Qualys PC Policies first.

Tests

Tests are libraries of data records that organize scans of computing assets. Configuration tests define how a class of technology assets should be governed.

A Configuration Compliance test is the mechanism third-party integration applications use to group assets by vulnerability type. Some third-party VA scanning solutions such as Qualys have very large libraries of tests (as many as 8,000) that are mapped to policies and "frameworks" of authoritative sources.
A Test can have many values, one-to-many, expected vs. actual, and so on. A test is anything that can be used to identify a class of software or hardware asset that is out of compliance. For example, a release or hardware number.

If the Qualys Vulnerability integration is installed, the scheduled job, Qualys PC Controls, retrieves the tests. You can view the scheduled job by navigating to Qualys Vulnerability Integration > Primary Integrations > Qualys PC Controls.

Note: If you choose to run the integration manually, run Qualys PC Controls after Qualys PC Policies.

Technologies

One of the techniques used by third-party vulnerability scanners to create test groups of software and hardware configuration items for analysis is to organize them by technology. Technologies are an imported library of OSes, network devices, databases, and apps that are associated with policies. Tests have multiple implementations for different technologies. Remediation is technology-specific, as well.

You can view the applicable technologies for a test, to better understand what kinds of software or hardware assets the control can be applied to. Examples of technologies that can be applied to controls include CentOS 7.x, Windows 8.1, Windows 2016 Server, and so on. The list of technologies is read-only and match the technologies defined in the Qualys Cloud Platform application.

Authoritative sources

Configuration Compliance uses Authoritative sources and citations when generating vulnerability alerts for tests. Authoritative sources usually map to sections of published industry standards, such as "NIST 800-53 version 3 (2009) 3: 2009, § SA-4".

Note: In the Qualys Vulnerability integration, this combination is referred to as framework.

Authoritative sources and citations (also known as mandates) are imported from the third-party vulnerability scanners (for example, Qualys Cloud Platform). Authoritative source records contain references to information about known software and hardware configuration issues from experts in the field of computer security. They define requirements for security policies and procedures. Configuration tests can reference multiple authoritative sources through citations. Authoritative sources can report on compliance for a given standard in preparation for an audit.

If the Qualys Vulnerability integration is installed, the scheduled job, Qualys PC Policies Detail, retrieves the authoritative sources and citations. You can view
this scheduled job by navigating to Qualys Vulnerability Integration > Primary Integrations > Qualys PC Policies Detail.

⚠️ Note: If you choose to run the integration manually, run Qualys PC Policies Detail after Qualys PC Policies.

**Test results**

Configuration Compliance does not calculate the test results, but imports them as part of a third-party integration. Once they are viewable in Configuration Compliance, they are remediated using Test Result Groups. See Configuration Compliance correlation for more information.

If the Qualys Vulnerability integration is installed, the scheduled job, Qualys PC Results, retrieves the test results. You can view this scheduled job by navigating to Qualys Vulnerability Integration > Primary Integrations > Qualys PC Results.

⚠️ Note: If you choose to run the integration manually, run Qualys PC Results after Qualys PC Policies and Qualys PC Policies Detail.

The Qualys PC Results import is the only integration that uses the Start Time parameter in the Integration Details tab. All other Configuration Compliance imports bring in all available data regardless of Start Time.

When the Qualys PC Results import is complete, an event is fired to trigger end-of-import calculations. For more information see, Configuration Compliance states.

**Configuration Compliance assignment rules overview**

Define the criteria by which test results are automatically assigned to an assignment group for remediation.

A default assignment rule, Assign to CI support group, is included in the base system assigning test results to the CI Support Group. Inactive by default.

The Assignment groups set by the Assignment Rules are used by Group Rules to assign owners to test result groups (TRGs).

**Assigning test results automatically**

There are three different ways to assign test results using Assign using:

- Assignment group: This option allows you to select any of the existing Now Platform® user groups.
- Assignment Group Field: This option allows you to choose any assignment group field available using the cmdb_ci table. By default you see the following three group fields:
None: Indicates no default value for this mandatory field
- Configuration Item: Approval Group
- Configuration Item: Assignment Group
- Configuration Item: Support Group

- Script: This option allows you to define the conditions using a script. This option requires coding or advanced ServiceNow® expertise.

See Create or edit Configuration Compliance assignment rules for more information on creating assignment rules.

With the sn_vulc.remediation_owner role, you can view and update test results and test result groups that are assigned to them or to their assignment groups. To view the modules, navigate to Configuration Compliance > Test Results > My Open Test Results, or Configuration Compliance > Test Result Groups > My Open Groups.

The sn_vulc.remediation_owner role can be assigned directly to a user, or, it is automatically assigned when you assign a user the itil role.

Assignment rule evaluation process

When a new test result is imported, or reopened after being closed, the assignment rules are evaluated against it. The assignment rules are evaluated after CI matching, and Risk Score calculations. A test result is only automatically evaluated upon initial import and when a rule is changed, unless it is reopened after being closed. You can manually reapply rules after changes.

The following process is used for each new or reopened test result:

- For each test result assignment rule, the test result is compared to the assignment filter, lowest order rule first.
- Where the condition matches, the test result is assigned an assignment group. The lookup stops.
- Where the conditions do not find a match among all the rules, the test result remains unassigned.

Reapplying assignment rules

When you change an assignment rule, use the Apply Changes button on the Assignment Rules list page to rerun all the changed rules on all active Open test results, except those that were manually assigned.

⚠️ Note: The assignment rules do not reevaluate manually created assignments.
The scheduled job [Reapply all assignment rules] is inactive, by default. When activated, it evaluates all the open test results against all active rules except those manually assigned. It can run Daily, Weekly, Monthly, Periodically, Once or On Demand.

Assignment rules and test result group assignment

Usually, you would assign your test result group (TRG) to the same assignment group as the test results in it. That is what the test result group rules do, by default.

For example, if your TRG groups by configuration item class, the test result group created can be broken apart by the different assignment groups. An Oracle Database TRG can be assigned to Group 1, and an Oracle Database TRG assigned to Group 2.

When the assignment group is changed at the test result group level, all the test results in that group which have same assignment group are updated to the new assignment group. The test results are marked as manually assigned and are not eligible for further rule evaluation.

Configuration Compliance test result groups and group rules overview

Automatically create test result groups (TRG) to analyze results in bulk using test result group rules. The criteria by which groups are formed is configured so that you do not have to manually assign test results into groups.

Understanding test result groups

Test result groups represent a set of test results to remediate. Grouping test results has many advantages. You can move test results through the remediation states, mark them under investigation, defer them, mark them resolved in bulk by using groups. You can create conditions to automatically group all results with specified results, technologies, risk scores, and any other data related to the test results. Test results can belong to more than one test result group giving you the flexibility to actively work with one group and monitor another. It all depends on your organizational needs. For example, you could group by assignment, and also create a group containing technologies.

Test result groups are created as follows.
• Manually, using one of two options, to add vulnerable items to the group.
  ◦ **Manual**: creates a group with no entries. Test results must be added manually.
  ◦ **Filter**: creates a group and uses conditions to automatically add test results to that group.

  **Note**: Manually added test results are not automatically removed from test result groups by test result group rules or group conditions.

• Automatically, using test result group rules. This option is the easiest option, once configured, test result group rules create all desired test result groups.

From a test result group, the group of test results may be assigned to a user, deferred until later, used to create a **Change Request**, and so on.

  **Note**: With the sn_vulc.remediation_owner role, you can view and update test results and test result groups that are assigned to you or to your assignment groups. To view the modules, navigate to **Configuration Compliance > Test Results > My Open Test Results**, or **Configuration Compliance > Test Result Groups > My Open Groups**.

When it is determined that a new test result can be added to a group, the test result is included in the **Test Results** related list of the test result group.

When updating the state of a test result group, associated test results can have their state updated to match this test result group. See **Configuration Compliance states** for more information on state changes.

**Understanding test result group rules**

Test result group rules allow you to define how test results are automatically grouped and assigned. A default rule, **Assignment group, Test**, is included in the base system grouping test results based on a test result **Assignment group** and the **Test** field. This rule is disabled, by default. You can group by any other set of values in columns accessible from the test result. You can use up to six keys and any number of conditions. See **Create or edit Configuration Compliance test result group rules** for more information.

For example, you can group your test results by assignment group or technology and configuration item (CI). A different set of rules can be used for test results that expose the company to more risk. You can have one group rule for low severity or low risk CIs. You can have another group rule for critical servers, and controls with exploits — test results that expose the company to more risk. See **Test Results fields** for more information on available fields.
When a new test result is imported, or reopened after being closed, the test result group rules are evaluated against it. A test result is only evaluated once, unless it is reopened after being closed.

Group rules are evaluated after CI matching, risk score calculations, and assignment rules.

The following process is used for each new or reopened test result:

- For each test result group rule, the test result is compared to the condition filter.
- For each rule where the rule condition matches, it pulls the data from the group key columns on the test result. The rule checks to see if there is a matching Open test result group that is assigned to the same assignment group as the test result.
- If the group is found, the test result is added to the existing group in the Open state.
- If no group in the Open state is found, the rule creates a group, assigns it based on the User Group or Key value in the rule, and places the test result in it.

More than one test result rule can be defined, to group different kinds of results. Since each result is compared with the rule conditions before putting it in a group, too many rules may have a performance impact.

When a group rule is deleted, you have the option to delete all open groups created by the rule. This applies to both the rule form view and list view.

When a test result group assignment is made or changed, the Assignment group and the Assigned to fields roll down to all test results, except for those where the test result has a different assignment group than the TRG. For more information on assignment rules, see Configuration Compliance assignment rules overview. These assignments are used automatically for this group on the next import.

**CI Lookup Rules for identifying configuration items from Configuration Compliance third-party vulnerability integrations**

When data is imported from a third-party integration, Configuration Compliance automatically uses host data to search for matches in the Configuration Management Database (CMDB). It does this using CI Lookup Rules. These rules are used to identify configuration items (CIs) and add them to the test result record to aid in remediation.

As assets are imported, a lookup is performed first on the Discovered Items list using third-party IDs to find matches to configuration item (CIs) from prior
imports. When a host ID match is found, it is used as the Configuration item field in the test result record.

You can see how imported assets are mapped to CIs using the Discovered Items list. If a match is not found, or the cmdb_ci field is empty, the rules use the other host information to attempt to correctly identify the CI. If a match is still not found, a placeholder CI is created and is designated as an Unmatched CI. See Unmatched CIs for more information on how those CIs are handled.

A new discovered item is created and mapped to this CI.

⚠️ **Note:** CI lookup rules are available only for the Qualys Integration for Security Operations.

CI lookup rules can be domain separated and are source-specific. Each source can have multiple deployments. Qualys can have multiple deployments of the Qualys Integration. Each deployment has its own set of CI Lookup Rules.

⚠️ **Note:** CI lookup rules are shared by all deployments of the vulnerability integration. If a rule is deleted or modified, the deletion or changes affect all deployments of the vulnerability integration.

When attempting a match, the first step is a vendor ID lookup for an exact match across source, source_instance, and vendor ID. Then, lookup rules are run in order, from lowest to highest and stop when a rule returns just a single CI as a match. If a rule is created in such a way that it returns more than one CI, only the first match is used.

⚠️ **Note:** To avoid matching on low-level networking elements, if a matched CI is one of dscy_switchport, cmdb_ci_network_adapter, cmdb_ci_nic, or cmdb_ci_ip_address, the parent CI is returned.

A system property to exclude CI classes is available. This property is not available with upgrade. See Ignore CI classes for upgrade information and instructions on setting the property.

To make it easier to find matching issues, when a match is found, the CI lookup rule used to find it is added to the Discovered Item record in the CI matching rule field. Lookup rules are evaluated by lowest Order value first.

These Qualys CI lookup rules are shipped with the base system.

- QUALYS HOST ID
- FQDN
- NetBIOS
• DNS
• IP

Importing test results data can be taxing on an instance and performance issues with resources can occur if rules are not carefully constructed. The logic used to iterate through and perform matching within the CMDB can result in lengthy processing times. To avoid any potential degradation of resources or performance complications, test any custom-written CI Lookup Rules or modifications to pre-defined CI Lookup Rules. See Prevent duplicate or orphaned records after running Vulnerability Response CI lookup rules for more information on preventing duplicate orphan records, deleting data, and cleaning up data.

**Reapplying updated CI lookup rules**
When you change a CI lookup rule, click **Apply Changes** on the CI Lookup Rules list page to rerun all the rules on the discovered items that:

• Were matched by the updated rules
• Are not matched by any rule

If the configuration item (CI) changes after reapplying the lookup rules, the discovered items are updated with the new CI. The test results are also updated. For more information, see **CI changes for discovered items**.

**Deduplicating existing configuration items for Configuration Compliance**
The Duplicate CI Remediator for deduplication tasks is updated with the `sn_sec_cmn_src_ci.cmdb_ci` property.

Whenever a deduplication task is used to update the configuration items (CIs), it also updates the discovered items related to those CIs. Hence, the test results are updated with the CI. For details, see **CI changes for discovered items for Configuration Compliance**.

**Creating CIs for Configuration Compliance using the Identification and Reconciliation Engine**
Starting with Configuration Compliance 11.1, you can create configuration items (CIs) in the Configuration Management Database (CMDB) using the Identification and Reconciliation engine (IRE) API. By using the IRE API to create CIs, you can prevent duplicate CIs from being created and you can reconcile CI attributes by allowing only authoritative data sources to write to CMDB.

A CI class (table) is the original table name in the instance database. CMDB contains base system classes that store data about CIs.
Using IRE for CI creation

Prior to version 11.1, if a matched CI was not found either in the Discovered Items list or CMDB, a CI was created in the Unmatched CI class (sn_sec_cmn_unmatched_ci).

For more information, see Unmatched CIs.

Starting with version 11.1, you can use the IRE API to create CIs in CMDB. Instead of using the Unmatched CI class, a CI is created in the Unclassed Hardware or Incomplete IP Identified Device class.

CMDB CI classes

**Note:** To use the new classes, activate the CMDB CI Class Models plugin. Otherwise, CIs are created in the Unmatched CI class.

Starting with version 11.1, if the host that you imported from a third-party scanner can’t be found in the Discovered Items list or CMDB, it is stored in one of the following new CMDB CI classes.

<table>
<thead>
<tr>
<th>CMDB CI Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incomplete IP Identified Device</td>
<td>CI is created in this table if only the IP address is available in the host information that is received from the scanner.</td>
</tr>
<tr>
<td>(cmdb_ci_incomplete_ip)</td>
<td></td>
</tr>
<tr>
<td>Unclassed Hardware</td>
<td>CI is created in this table if any of the following information is available in the host information that is received from the scanner:</td>
</tr>
<tr>
<td>(cmdb_unclassed_hardware_ci)</td>
<td>• Host name</td>
</tr>
<tr>
<td></td>
<td>• IP address</td>
</tr>
<tr>
<td></td>
<td>• DNS</td>
</tr>
<tr>
<td></td>
<td>• NETBIOS</td>
</tr>
<tr>
<td></td>
<td>• MAC address</td>
</tr>
</tbody>
</table>
The system automatically uses an Unmatched CI class if one of the following occurs:

- The CMDB CI Class plugin is not activated.
- IRE raises an exception while creating a new CI.

**Related information**

CMDB CI Class Models store app
Identification and Reconciliation engine (IRE)

**Discovered Items for Configuration Compliance**

Assets are automatically matched to configuration items (CIs) using CI lookup rules, when they are imported using the host and test results integrations. Discovered Items give you visibility into how asset identification is mapped to CIs in the CMDB.

Discovered Items are considered **Matched**, **Unmatched**, or **Reclassified**. Identified CIs are in the **Matched** state.

To make it easier to find potential matching issues, the CI Lookup Rule that matched the CI appears in the **CI matching rule** field.

**Note:** CI matching rule field support is available only for the Qualys integration.

If a match was not found, a CI is created in the unmatched CI class [sn_sec_cmn_unmatched_ci], [cmdb_ci_unclassed_hardware], or [cmdb_ci_incomplete_ip] of the CMDB. If the original unmatched CI was reclassified, Discovered item records are updated to reflect that state. For more information, see Unmatched CIs and View and reclassify unmatched configuration items for more information.
By default, the **Security Operations > CMDB > Discovered Items** module lists unmatched configuration items. You can view all discovered items from an import by removing the filter.

For a description of the fields in Discovered Items, see **Discovered Items form fields**.

**CI changes for discovered items for Configuration Compliance**

The default value of the property `sn_sec_cmn.update_on_ci_change` is **true**. So, when the configuration item (CI) for a discovered item is updated, the test results are updated as well.

The external ID for the test result is updated and the risk score, assignment rules, group rules, remediation target rule are reevaluated. If a test result exists with the same test and CI, the test results are updated with the existing test result and the current test result is closed with the substate `invalidCI`. Work notes are added accordingly.

If you do not want to update the CI for the existing test result, set the property to **false**. In this case, if a CI changes, a new test result is created and the existing one is closed as an `invalidCI`.

**Reconcile unmatched discovered items for Configuration Compliance**

Create a schedule job to reconcile unmatched discovered items. When a test result is created, the configuration item (CI) added to it at the time of creation might be an outdated one. If the information in the CMDB changes, unmatched CI information is not reconciled. To reconcile, apply CI lookup rules on the test results that are in an unmatched state when the CMDB is updated with the latest CIs.

**About this task**

A schedule job is run on demand to reapply the CI matching rule for the discovered items in an unmatched state. If the CI changes after reapplying the lookup rules, the discovered items are updated with the new CI. Impacted test results are also updated. For details, see **CI changes for discovered items for Configuration Compliance**.

**Procedure**

1. Navigate to **Security Operations > Reconcile Unmatched Discovered Items**.
2. On the Background Jobs page, click **Create reconciliation job**.
3. On the form, fill in the fields.

   **Note:** You can only edit the Parameters field.
### Background Job

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Unique job number.</td>
</tr>
<tr>
<td>Created by</td>
<td>User who created the job.</td>
</tr>
<tr>
<td>Parameters</td>
<td>Parameters to reconcile the unmatched discovered items:</td>
</tr>
<tr>
<td></td>
<td>• limit: Maximum number of discovered items to be reconciled.</td>
</tr>
<tr>
<td></td>
<td>If you do not enter a value, 10,000 discovered items are reconciled.</td>
</tr>
<tr>
<td></td>
<td>• firstDiscoveredItem: First discovered item that must be reconciled.</td>
</tr>
<tr>
<td></td>
<td>If you do not enter a value, the reconciliation process starts from the first discovered item.</td>
</tr>
<tr>
<td>State</td>
<td>Current state of the background job.</td>
</tr>
<tr>
<td>State description</td>
<td>Description of the current state of the background job.</td>
</tr>
<tr>
<td>Job type</td>
<td>Type of job. The value is <strong>Reconcile unmatched discovered items</strong>.</td>
</tr>
<tr>
<td>Started at</td>
<td>Time when the job started.</td>
</tr>
<tr>
<td>Ended at</td>
<td>Time when the job was completed.</td>
</tr>
<tr>
<td>Job duration</td>
<td>Total time taken to complete the job.</td>
</tr>
<tr>
<td>Substate</td>
<td>Substate for the selected state.</td>
</tr>
<tr>
<td>Notes</td>
<td>Number of records processed.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**Note:** To stop the running the job, click **Cancel**.

**Note:** You cannot reconcile unmatched CIs or reapply CI lookup rules while importing hosts or test results.
Reapply CI lookup rules on selected discovered items for Configuration Compliance

Reapply configuration item (CI) lookup rules on selected discovered items from the discovered item list view select actions. The administrator might have to edit or update a lookup rule for multiple reasons. If the lookup rule changes, they can reapply them on the discovered items.

About this task
If the CI changes after reapplying the CI lookup rules, the discovered items are updated with the new CI and test results. For more information, see CI changes for discovered items for Configuration Compliance.

Procedure
1. Navigate to Security operations > CMDB > Discovered Items.
2. Select the required discovered items and click Action on selected rows.
3. Select Reapply CI lookup rules from the list.
   The rules are reapplied on these discovered items.

Configuration Compliance change management (v 12.0)
As an IT remediation owner, starting with version 12.0 of Configuration Compliance, you can create and manage change requests (CHG) directly from test result groups (CRGs) in the Configuration Compliance application.

Change requests and the Configuration Compliance workflow
Change requests and change management are part of the remediation process of the Configuration Compliance workflow. During this remediation phase, you might use change requests to help you prioritize, track, and remediate test results.

The Configuration Compliance application works with the Now Platform® IT change management process to help you remediate non-compliant software and technologies in your environment.
With change management in the Configuration Compliance application, you can associate test results to existing change requests, or split a test result group and create a new test result group only for selected test results.

For creating change requests starting with v12.0 of Configuration Compliance, see Configuration Compliance remediation.

For creating change requests with versions of Configuration Compliance prior to v12.0, see Create a change request in Configuration Compliance (Prior to v12.0).

**Key terms**

**Tests**
Tests are libraries of data records that organize scans of computing assets. Configuration tests define how a class of technology assets should be governed. A test is anything that can be used to identify a class of software or a hardware asset that is out of compliance.

**Test results**
Test results are imported by third-party integrations. Once they are viewable in Configuration Compliance, they are remediated using **Test Result Groups**. Groups are assigned for remediation according to assignment rules.

**Test result group**
Test results are grouped into test result groups according to assignment rules and automatically assigned to remediation owners for remediation.

**Policies**
Policies are related to authoritative documents and test records. A group of configuration tests define policies.

**Change requests**
Change requests help you implement controlled processes for remediation. You might use change requests with test result groups in Configuration Compliance to help you identify, track, and resolve non-compliant assets (configuration items) that require additional resources, or that you might target for deferral.

For more information about test results and test result groups, see Understanding Configuration Compliance.

When to use change requests in Configuration Compliance
Change requests help you initiate and track remediation activities on your test results. When remediation owners have large numbers of unremediated test
results or configuration items, they might use change requests to identify test results for deferral. Alternatively, they might identify and regroup test results and configuration items that require more resources than initially identified in the original test result group.

**Create change requests from a test result group**

Create a change request directly from a test result group for all the test results in the group, or use filtering to identify only test results that match specific criteria. Create a change request with pre-populated information to expedite your investigation for test results that require manual intervention.

**Split group**

From an existing test result group, identify a subset of test results that you want to move to a new test result group. By creating a new CRG, you can work with a specific group of test results without impacting the original test result group.

**Associate test results to an existing change request**

Associate test results to existing tasks to avoid creating duplicate change requests as you work to resolve your test result groups. By associating a test result group to a change request that is already available in your instance, you can use an existing lists of tasks.

**Types of change requests for a test result group**

You can create, approve, implement, review, and close change requests directly from test result groups that are assigned to you. You can create three types of change requests with pre-populated information from a test result group:

- **Standard.** A pre-authorized change that is low risk, relatively common and follows a specified procedure or work instruction.
- **Normal.** Normal change requests follow a prescriptive process which requires two levels of approval before being implemented, reviewed, and closed.
- **Emergency.** A change to resolve a major incident.

**Configuration Compliance Exception Management overview**

When your organization can’t comply with a published vulnerability management or security policy, standard, or guideline, you can request an exception. Exception management entails requesting, reviewing, approving, or rejecting exceptions for a test result group that cannot be remediated according to the policy.
Some vulnerabilities might not have an existing patch, fix, or solution. When an exception is approved, it also means that you're accepting a risk because you're acknowledging and agreeing to the consequences of not remediating the configuration-related vulnerability.

**Life cycle of an exception**

An exception is a request to defer the remediation of a test result group for a specified period.

The life cycle of an exception is as follows:

- Requesting an exception
- Approving an exception request
- Tracking an exception request
- Expiry of an exception request

**Requesting an exception**

As the remediation owner, you can ask for an exemption for a test result group using the exception management process. During the approval process, the test result group remains in **In review** state. After the exception approver approves this request, the test result group moves to a **Deferred** state.

**Approving an exception request**

Test result groups that can't be remediated immediately are reviewed, assessed for risk, and approved for deferral until they can be remediated. Approving an exception request can be a two-level workflow. If only the first-level approver is present, the exception can be requested and approved. However, if there's no first-level approver, an exception can't be requested. See **Add an exception approver for Configuration Compliance** for more information.

Once an exception request for a test result group is approved, you can perform the following actions:

- Reopen
- Close
- Delete

ℹ️ **Note:** Rejection comments are shown in the Work notes for a test result group. If an exception request is rejected, this test result group reverts to its previous state.

**Tracking an exception request**
After raising the exception, you can track its status by using the **State Change Approvals** tab of the test result group. If an action is taken on a group, you can’t track the status of the individual test results in that group.

**Expiry of an exception request**

When an exception request for a test result group expires, the group reverts to its **Open** state.

### Exception management approval process

<table>
<thead>
<tr>
<th>Remediation Owner</th>
<th>Exception Approver L1</th>
<th>Exception Approver L2</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Diagram" /></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Configuration Compliance calculator groups**

Configuration Compliance calculators are used to update record values when pre-defined conditions are met. The calculators are grouped based on the criteria used to determine how the records are updated.

**Configuration Compliance calculator groups starting with v10.3**

From the Default Risk Calculator record, calculator rules can be applied to all affected test results and collections on-demand. Vulnerability managers may use this feature adjust their risk calculator configuration. They might experiment with several prioritization schemes early in their deployment and apply those changes on-demand to view how they impact import findings.

The Risk Score calculator group has been renamed to Risk Calculators.

Starting with v10.3, Risk Score Rollup Calculators are included with Configuration Compliance. There are two types of individual rollup calculators:

- **Configuration Test Risk Roll Up**
Calculators that roll up risk scores for all Test Results with the same Configuration Test to provide an overall risk score for the Configuration Test. The rolled-up value is displayed in the Risk Score fields.

**Test Result Group Risk Score Rollup**

These calculators roll up risk scores for all Test Results in a test result group to provide an overall risk score for that group. The rolled-up value is displayed in the Risk Score fields.

Both the Risk Score calculator group and Risk Score Rollup Calculators group are enabled by default.

For more information, review the following key terms for Configuration Compliance calculators introduced with v10.3:

**Test result**

A test result is the outcome of the configuration test on a configuration item (CI) and the associated technology. Test results in Failed, error, and Unknown states identify hardware, software, and assets that are out of compliance with your policies.

**Test result group**

Test results are grouped together at the time of data import based on the pre-defined group rules. These test result groups are similar to vulnerability groups in Vulnerability Response. Test result groups organize test results into groups for bulk analysis and represent a set of items to remediate.

**Risk score in a test result**

A value calculated by risk score calculators that is based on the business context, that is, the business criticality of the affected asset as defined in the CMDB, and the severity of the test as communicated by the scanner. The calculated value is displayed in the Risk Score fields of test results. The scores displayed values that range from 0-100. Fields are also color-coded to provide you with a severity at-a-glance.

**Risk score in test result group**

This score is displayed on the Test Result Group record and is the rolled up value of the risk scores for all the active test results in a test result group. This score changes as test results are remediated in the test result group.

**Risk score in configuration test**
This score is displayed on configuration tests and is the rolled up value of the risk scores for all the active test results with that configuration test. This score changes as the test results associated with this configuration test are remediated.

**Risk rating**

The amount of risk a failed test result poses to your system. It is based on a range of risk scores on a 1-5 numeric scale that rates risks as Critical (1) to None (5). The score is based on a range of risk scores and is displayed in Risk Rating fields.

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>Risk score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1- Critical</td>
<td>90 to 100</td>
</tr>
<tr>
<td>2- High</td>
<td>70 to 89</td>
</tr>
<tr>
<td>3- Medium</td>
<td>40 to 69</td>
</tr>
<tr>
<td>4- Low</td>
<td>1 to 39</td>
</tr>
<tr>
<td>5- None</td>
<td>0</td>
</tr>
</tbody>
</table>

**Risk score rollup calculators**

There are two types of rollup calculators:

- Configuration Test Risk Roll Up: These calculators roll up risk scores for all Test Results with the same Configuration Test to provide an overall risk score for the Configuration Test. The rolled-up value is displayed in the Risk Score fields. You can edit the script values for weight and score for these calculators.

- Test Result Group Risk Score Rollup: These calculators roll up risk scores for all Test Results in a test result group to provide an overall risk score for that group. The rolled-up value is displayed in the Risk Score fields. You can edit the script values for weight and score for these calculators. For an example of a Risk score rollup calculator and how it calculates scores, see Risk rollup calculation example for Configuration Compliance (v10.3).

**(Starting with v10.3) Historical risk score**

The inherent risk score across all the passed test results in a test result group. This field displays the amount of risk that was remediated.
Scores are calculated whenever the risk score changes or when test results are added or removed from a test result group.

**Note:** To work properly, this script requires the Service Mapping plugin. Service Mapping is available as a separate subscription and requires activation by ServiceNow personnel.

### Configuration Compliance calculator groups prior to v10.3

All enabled Configuration Compliance calculators in the **Calculator Groups** run each time a test result fails. If you change a test (within the third-party scanner application) or the logic in the risk calculator, **Risk Score** is calculated after the next import.

The Configuration Compliance base system includes one calculator group: **Risk Score**.

The calculator called **Basic Risk Score** is contained in the **Risk Score** calculator group. Its purpose is to calculate the risk score of a test result. As written, it is based on the **business criticality** and **test criticality** values of the test. If you do not have Service Mapping installed and configured, a middle value of 50 is used.

**Note:** To work properly, this script requires the Service Mapping plugin. Service Mapping is available as a separate subscription and requires activation by ServiceNow personnel.

When the computation is complete, the updated criticality is displayed in the **Risk Score** field in the **Test Results** record.

Configuration Compliance calculators can prioritize and categorize test results based on any custom criteria you want to use. The **Risk Score** calculator prioritizes based on the importance of the business services relying on an affected policy.

You can modify **Basic Risk Score** to calculate a score based on whatever risk factors you want. For example, you may have CI data indicating that the non-compliance is external-facing, posing a greater risk to your environment than internal-facing non-compliance. That data can be used as a factor.

**Note:** Editing **Basic Risk Score** or creating a calculator requires coding or advanced ServiceNow expertise.

The **Basic Risk Score** calculator is enabled by default.
Configuration Compliance remediation target rules (v 12.0)

Starting with version 12.0 of Configuration Compliance, you can view and edit remediation target rules.

Roles required: Configuration Compliance administrator (sn_vulc_admin), or a manager with the sn_vulc.manage_remediation_target_rules role

Remediation target rules

With remediation target rules, you can set the expected time frames for remediating test results. You can send notifications to users and groups when target dates are approaching and when they are past due.

A scheduled job, *Evaluate and notify remediation targets*, runs daily and uses active remediation target rules to evaluate active test result records. Whenever test result records associated with test result groups are updated or changed, the modified values are evaluated by the target rules, and changes are rolled up and displayed on associated test result groups.

You can edit, disable, or delete existing remediation target rules and create new ones. When you change, disable, or create a new rule, you have the option to click *Apply Changes* from the Remediation Target Rules list view and manually apply the changes you introduced before the next scheduled job. With this option, you can reevaluate your test result records without having to wait. If you do not choose to apply your changes manually, the next daily scheduled job picks up your changes and applies them.

1. Navigate to **Configuration Compliance > Administration > Remediation Target Rules** to view remediation target rules.

2. Click a rule in the Name column to open its record.

3. Select the **Active** check box on the Remediation Target Rule record to enable (true) any disabled rules (false).
Whenever you change or add a target rule, regardless of whether you choose to apply the changes manually or wait for the next scheduled job, your changes are used to evaluate all active test results along with any other target rules that are affected by your changes. When you choose to manually apply the changes, this evaluation may take some time if you have a large volume of active test results, because all the rules impacted by your changes are used for an evaluation.

For example, the default value for targeted remediation days is 30. If you create a new rule that also has 30 for Targeted remediation days, this rule, and any target rules with 30 days or greater as target dates are each applied to your test results.

**Deactivated and deleted target rules**

When a rule is active, `true` is displayed in the Active column on the Remediation Target rules list view. After a rule is deactivated (`false`), it is no longer applied to new test results. However, the scheduled job continues tracking any existing test results the rule was applied to. If the deactivated rule or rules are subsequently reactivated, any test result with an empty Remediation Target Date field is evaluated against the reactivated rules. This includes test results created while the rules were deactivated.

When rules are deleted, the Remediation Target Date and related fields on closed test results are preserved. The Remediation Target Date and related fields on non-closed test results are cleared, and any dependent rules are reapplied.

To deactivate a rule, from the remediation target rule record, disable the active check box and click Update. `false` is displayed in the Active column on the Remediation Target Rules list view.

To delete a rule, click Delete on the form, or, alternatively, from the list view, select the rule or rules, and click Delete from the Actions on rows list. The rule is no longer displayed on the list and the next rule in the order of operation replaces the deleted rule.

If you deactivate or delete a rule and choose to apply your changes prior to the next scheduled job, the rule reference is cleared from the field, but the remediation date and status data are preserved. If you do not apply your changes manually, the rule reference is cleared from the field with the next scheduled job.

**About Target rules and the Evaluate and notify remediation targets scheduled job**
The Evaluate and notify remediation targets scheduled job runs once at 4:30:00 daily. It picks up any active remediation target rules and evaluates all active
test results starting with the test results with the earliest remediation target date. It evaluates all test results that meet the following criteria:

- Are not in a Closed state.
- Have no remediation target date.
- Have remediation target dates that are later than the dates in the remediation target rules.
- Are created after a scanner import is completed. The scheduled job picks up and evaluates any new test results that are created as a result of an import.

After a target rule is defined, remediation target dates are calculated by the Evaluate and notify remediation targets scheduled job. The scheduled job adds a remediation target date, if one does not exist, or, if this rule contains an earlier date than the one in the record, it updates the existing target date.

Any expired records and reminder dates that match the target rules are picked up by the job and notifications are sent. For disabled rules, the job clears the remediation fields on test result records and stops sending notifications.

Viewing target dates and status on the list and form views

Configuration Compliance managers can see the remediation target date from both the test result form and list views. Remediation target rules are also run after a scanner import and rerun if a test result is reopened.

The scheduled job updates the Remediation target and Remediation status in the test result list view, and the Remediation target rule, Remediation target, and Remediation status fields on test result form.

**Note:** By default, the Remediation target and Remediation status columns are not displayed on the Test Results list view. To display these columns, you also must add them to the list view. Similarly, add the Remediation target rule, Remediation target, and Remediation status fields to the test result form.

Use the slushbuckets in the Settings and Additional action menus, respectively, as shown in the following images to display these columns and fields. For the Additional action menu on the test result record, click the menu icon, followed by Configure and Form layout to view the slushbucket and move the fields from Available to Selected.

The Remediation target date is coded on the Test Results list view as colored dots:
• Test results that have not reached their notification date are shown in green.
• Test results approaching the remediation target date are shown in orange.
• Test results past the remediation target date are shown in red.

Remediation target and status columns on the Test Results list view

Target Missed: the target date is past due
In-flight: the test result is in progress

Test result records are also displayed visually on the Configuration Compliance Dashboard. Navigate to Configuration Compliance > Overview and check the dashboard for status. The Overview includes existing widgets and remediation status. The colors of the graphs match the colors displayed in the Test Results list view and Test Result record.
Remediation target rule scenario
When multiple remediation target rules are applied to the same test result, the most restrictive rule is applied.

For example, if a test result first identified on 03/01/2018 meets the conditions for two remediation target rules:

- Remediation target rule 1: Defined on 03/07/2018; remediation target is 15 days since first seen; calculated remediation target date is 03/16/2018 10:00:00.
- Remediation target rule 2: Defined on 03/10/2018; remediation target is 10 days since first seen; calculated remediation target date is 03/11/2018 10:00:00.

Note:
Remediation targets are calculated from the First seen date plus the number of days (measured as 24-hour increments).

In this scenario, Remediation target rule 2 applies to the test result, because it has the more restrictive date: 10 days since the test result was first identified versus 15 days.

Create or modify target rules and reapply changes

1. Navigate to Configuration Compliance > Administration > Remediation Target Rules to view, edit, and create new remediation target rules.

2. In the Name column, click a rule to open a target rule and edit the record, or, alternatively, click New to create a new target rule.

3. Fill out the form to define the expected remediation time frame, specify which test results this rule to applies to with conditions, and determine when to send reminders to users or groups, or both.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for your rule.</td>
</tr>
<tr>
<td>Active</td>
<td>Enable or disable the rule. The rule is automatically enabled (true) by default and will be applied to your test results if you choose to apply changes manually or after the next scheduled job.</td>
</tr>
<tr>
<td>Target (days)</td>
<td>Set the targeted deadline date for remediation in number of days. The</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>default value for targeted remediation days is 30. For example, if you create a new rule that also has 30 for a Target value, your new rule and any other existing rules that also have 30 days or greater as target dates will be applied to your test results.</td>
<td></td>
</tr>
<tr>
<td>Notify (days before due)</td>
<td>Set a number of days before the deadline date to remind users and groups.</td>
</tr>
<tr>
<td>Description</td>
<td>Short description of the rule.</td>
</tr>
<tr>
<td>Condition</td>
<td>Use the condition builder to specify the test results this rule applies to. For example, set a remediation target date of 30 days for all test results with risk scores greater than 70. Send reminders to users or groups, or both, seven days prior to the remediation date. Starting with v12.0, case sensitivity for the search text you enter in the condition builder is not supported on this record or form. Prior to v12.0, case sensitivity is supported for the search text you enter in the condition builder.</td>
</tr>
<tr>
<td>User and user groups or both</td>
<td>Select users or groups, or both to send notifications about the approaching and past due target dates you have set.</td>
</tr>
</tbody>
</table>

4. Click **Submit**. Alternatively, to save edited rules, click **Update**.

The list view is displayed with your updated or new rule. Rules in the list are ordered and run starting with the rule with the lowest remediation target date. If you disable or delete a rule, the next rule in the order sequence replaces the inactive or deleted rule.

5. To apply your new changes now, click **Apply Changes**.
Configuration Compliance criticality maps

Configuration Compliance criticality mapping transforms criticality fields from the source to fields in Configuration Compliance.

The Configuration Compliance base system ships with a standard Qualys Cloud Platform to standard ServiceNow mapping. Creating or editing a criticality map is intended only for customized or non-standard third-party mappings in your environment.

Configuration Compliance states

Configuration Compliance offers a state model for the status of the test results group at any given time. Test result group states control test result states based on precedence.

Test Result Group States

Test result groups have many possible states. Automatic transition is available from the Resolved state based on the next scan results. If all test results pass on the next scan, the group is closed. Otherwise it transitions to Under Investigation. The system verifies this closed state, but it re-evaluates the group state if a test result is added to, or deleted from the group. Work notes are updated to reflect the transition. Work notes are updated to reflect the transition.

Note: Each group form contains Follow and Update buttons which are standard for ServiceNow tasks.
<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>State upon creation.</td>
</tr>
<tr>
<td>Under Investigation</td>
<td>Triggered by the <strong>Start Investigation</strong> button. From this state you can:</td>
</tr>
<tr>
<td></td>
<td><strong>Create a Change Request</strong></td>
</tr>
<tr>
<td></td>
<td>See Create a change request in Configuration Compliance (Prior to v 12.0) for more information.</td>
</tr>
<tr>
<td></td>
<td><strong>Defer</strong></td>
</tr>
<tr>
<td></td>
<td>Provide a reason and select a reopen date.</td>
</tr>
<tr>
<td></td>
<td><strong>Close</strong></td>
</tr>
<tr>
<td></td>
<td>Provide a resolution and notes. Closes the group.</td>
</tr>
<tr>
<td></td>
<td><strong>Delete</strong></td>
</tr>
<tr>
<td></td>
<td>Confirm the deletion. Removes the group</td>
</tr>
<tr>
<td>Deferred</td>
<td>Triggered by the <strong>Defer</strong> button.</td>
</tr>
<tr>
<td></td>
<td>From this state you can:</td>
</tr>
<tr>
<td></td>
<td><strong>Reopen</strong></td>
</tr>
<tr>
<td></td>
<td>Transitions back to an Open state.</td>
</tr>
<tr>
<td></td>
<td><strong>Close</strong></td>
</tr>
<tr>
<td></td>
<td>Provide a resolution and notes. Closes the group.</td>
</tr>
<tr>
<td></td>
<td><strong>Delete</strong></td>
</tr>
<tr>
<td></td>
<td>Confirm the deletion. Removes the group</td>
</tr>
<tr>
<td></td>
<td>Deferment information appears under the <strong>Defer/Close</strong> related tab. On the defer date, the group reopens for remediation.</td>
</tr>
<tr>
<td>Awaiting Implementation</td>
<td>Triggered by the <strong>Awaiting Implementation</strong> button. From this state you can:</td>
</tr>
<tr>
<td></td>
<td><strong>Create a Security Incident</strong></td>
</tr>
<tr>
<td></td>
<td>See Create a security incident for more information.</td>
</tr>
<tr>
<td></td>
<td><strong>Create a Change Request</strong></td>
</tr>
<tr>
<td></td>
<td>See Create a change request in Configuration Compliance (Prior to v 12.0) for more information.</td>
</tr>
<tr>
<td>State</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Resolve  | Select a Resolution and add notes. Choices are:  
• Result Invalid  
• Cancelled  
• Fixed  
State becomes **Resolved**. Notes appear under the **Resolution** related tab. |
| Close    | Select a Resolution and add notes. Choices are:  
• Result Invalid  
• Cancelled  
• Fixed  
State becomes **Closed**. Notes appear under the **Resolution** related tab. |
| Delete   | Confirm the deletion. Removes the group. |
| Resolved | Triggered from the Resolve button. From this state you can:  
**Create a Security Incident**  
See **Create a security incident** for more information.  
**Reopen**  
Transitions back to an Open state.  
**Close**  
Select a Resolution and add notes. Choices are:  
• Result Invalid  
• Cancelled  
• Fixed  
State becomes **Closed**. Notes appear under the **Resolution** related tab.  
**Delete** |

© 2021 ServiceNow, Inc. All rights reserved.  
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Confirm the deletion. Removes the group.</td>
</tr>
<tr>
<td></td>
<td>Notes appear under the Notes related tab. Resolution information appears under the Resolution related tab.</td>
</tr>
<tr>
<td>Closed</td>
<td>Triggered from the Close button. From this state you can:</td>
</tr>
<tr>
<td></td>
<td><strong>Reopen</strong></td>
</tr>
<tr>
<td></td>
<td>Transitions back to an Open state.</td>
</tr>
<tr>
<td></td>
<td><strong>Delete</strong></td>
</tr>
<tr>
<td></td>
<td>Confirm the deletion. Removes the group. Closure information appears under the Defer/Close related tab.</td>
</tr>
</tbody>
</table>

- If the **Test Result Group** is marked as **Closed**, with a non-fixed substate (such as False Positive, Risk Accepted, or Irrelevant), test results that are added to the group have their state updated to match the test result group.

- If **Test Result Group** is marked as **Closed** or **Fixed** and if the test result added is not itself **Closed** or **Fixed**, the test result state does not change, and the test result group state is changed to **Open**.

- If you determine that the results are a low priority, you can change their group to the **Deferred** state for a defined amount of time, or immediately **Close** them.

  🔄 **Note:** When test result groups are deferred or closed, you can specify substates to further define the reasons for doing so. Work notes are updated to reflect the transition.

**Test Result States**

The state of a test result group also changes the state of its associated test results. This mechanism has two cases.

**Test results that belong to only one group**

Results match the state of the group with three exceptions:

- If the group changes its state to be **Closed** and its resolution(substate) to be **Fixed**, the item ignores that change and then falls back to the **Open** state.

- If the group changes its state to be **Closed** and its resolution(substate) to be **Cancelled**, the item ignores that change and then falls back to the **Open** state.
• If the test result source status is Fixed (updated by a scan or import), then when the group changes its state, the test result changes its state to Closed(Fixed) no matter what state the group is in.

Test results that belong to multiple groups

Test results do not match the state of the group automatically, instead it searches among all the associated groups to find the state with the highest precedence to apply. This is the state of precedence:

Closed (substate: Result Invalid) > Deferred > Resolved > Awaiting Implementation > Under Investigation > Open

Note: Closed (substate: Fixed) and Closed (substate: Cancelled) are two special cases.

Test Result Group state examples

For example:

<table>
<thead>
<tr>
<th>Test Result Groups State</th>
<th>Test result State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group A: Open &gt; Under Investigation</td>
<td>Under Investigation</td>
</tr>
<tr>
<td>Group B: Open</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When Group A is Under Investigation and Group B is Open, the test result changes to Under Investigation, since after the search, between Group A and Group B, Group A has the state with the highest precedence.</td>
</tr>
<tr>
<td>Group A: Under Investigation</td>
<td>Under Investigation</td>
</tr>
<tr>
<td>Group B: Open &gt; Under Investigation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When Group B is Under Investigation and Group A is Under Investigation, the test result stays as Under Investigation, since after the search, between Group A and Group B, they have the state with the same precedence.</td>
</tr>
<tr>
<td>Group A: Under Investigation</td>
<td>Awaiting Implementation</td>
</tr>
<tr>
<td>Group B: Under Investigation &gt; Awaiting Implementation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When Group B is Awaiting Implementation and Group A is Under Investigation, the test result changes to Awaiting Implementation, since after the search, between Group A and Group B, they have the state with the same precedence.</td>
</tr>
</tbody>
</table>
### Test Result Groups State

<table>
<thead>
<tr>
<th>Test result State</th>
<th>Test result State</th>
</tr>
</thead>
<tbody>
<tr>
<td>search, between Group A and Group B, Group B has the state with the highest precedence</td>
<td></td>
</tr>
</tbody>
</table>

### Group A: Under Investigation > Deferred  
Group B: Awaiting Implementation

<table>
<thead>
<tr>
<th>Deferred</th>
</tr>
</thead>
<tbody>
<tr>
<td>When Group A is Deferred and Group B is Awaiting Implementation, the test result changes to Deferred, since after the search, item 1 found out that between Group A and Group B, Group A has the state with the highest precedence</td>
</tr>
</tbody>
</table>

### Group A: Deferred  
Group B: Awaiting Implementation > Closed (Result Invalid)

<table>
<thead>
<tr>
<th>Closed (Result Invalid) &gt; Deferred</th>
</tr>
</thead>
<tbody>
<tr>
<td>When Group B is Closed and the resolution(substate) is Result Invalid, and Group A is Deferred, the test result changes to Closed (Result Invalid), since after the search, between Group A and Group B, Group B has the state with the highest precedence.</td>
</tr>
</tbody>
</table>

### Group A: Deferred  
Group B: Closed (Result Invalid) > Open (via Reopen)

<table>
<thead>
<tr>
<th>Deferred</th>
</tr>
</thead>
<tbody>
<tr>
<td>When Group B is re-opened and its state changes to Open, and Group A is Deferred, the test result changes to Deferred, since after the search, between Group A and Group B, Group A has the state with the highest precedence.</td>
</tr>
</tbody>
</table>

### Test result state special cases

<table>
<thead>
<tr>
<th>Test result group State</th>
<th>Test result state</th>
</tr>
</thead>
</table>
| Group A: Under Investigation  
Group B: Awaiting Implementation > Closed (Fixed or Cancelled) |

<table>
<thead>
<tr>
<th>Under Investigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>When Group B is Closed (substate Fixed or substate Cancelled), and Group A is Under Investigation, the test result changes from Awaiting Implementation (previously the highest precedence) to</td>
</tr>
</tbody>
</table>
Test result state special cases (continued)

<table>
<thead>
<tr>
<th>Test result group State</th>
<th>Test result state</th>
</tr>
</thead>
<tbody>
<tr>
<td>Under Investigation (currently the highest precedence).</td>
<td></td>
</tr>
<tr>
<td>Group A: any state</td>
<td></td>
</tr>
<tr>
<td>Group B: any state</td>
<td></td>
</tr>
<tr>
<td>If the test result source status is Fixed (updated by a scan or import), then when the group changes its state, the test result changes its state to Closed(Fixed) no matter what states the other associated groups are in. The test result search for group state does not occur.</td>
<td></td>
</tr>
</tbody>
</table>

Domain separation and Configuration Compliance

This is an overview of domain separation and Configuration Compliance. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can then control several aspects of this separation, including which users can see and access data.

Support level: Standard

- Includes Basic level support.

- Business logic: Processes can be created or modified per customer by the service provider (SP). The use cases reflect proper use of the application by multiple SP customers in a single instance.

- The owner of the instance needs to be able to configure the minimum viable product (MVP) business logic and data parameters per tenant as expected for the specific application.

Use case: An admin needs to be able to make comments mandatory when a record closes for one tenant, but not for another.

How domain separation works in Configuration Compliance

With domain separation you can standardize (Configuration Compliance) procedures, across the customer base you serve, with lowered operational costs and a higher quality of service.

Separate customer work spaces for workflows, dashboards, reports, and so on, ensures that customer data is separated and never exposed to other clients.
## Domain separation support in Configuration Compliance by version releases

<table>
<thead>
<tr>
<th>Release</th>
<th>Support level</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geneva, Helsinki</td>
<td>No support</td>
<td></td>
</tr>
<tr>
<td>Istanbul</td>
<td>Data only</td>
<td>Initiation of data-level domain separation</td>
</tr>
<tr>
<td>Jakarta</td>
<td>Level 2 (Data, Requestor, Fulfiller)</td>
<td><strong>New features:</strong> third-party Integrations support with Level 2 domain separation under single instance of integration.</td>
</tr>
<tr>
<td>Kingston</td>
<td>Level 2 (Data, Requestor, Fulfiller)</td>
<td><strong>New features:</strong> third-party scanner integration can be enabled with multiple instances of Qualys, for example, but all instances still live under a single domain.</td>
</tr>
<tr>
<td>London</td>
<td>Level 2 (Data, Requestor, Fulfiller)</td>
<td></td>
</tr>
<tr>
<td>Madrid</td>
<td>Level 2 (Data, Requestor, Fulfiller)</td>
<td></td>
</tr>
<tr>
<td>New York</td>
<td>Level 2 (Data, Requestor, Fulfiller)</td>
<td></td>
</tr>
<tr>
<td>Orlando</td>
<td>Standard</td>
<td>Support standards and terminology for domain separation changed starting with this release. For more information about support levels, see Application support for domain separation</td>
</tr>
<tr>
<td>Paris</td>
<td>Standard</td>
<td></td>
</tr>
</tbody>
</table>

Domain separation for the Configuration Compliance application covers the following product functionality:
• Ingests the test results from third-party scanners (Qualys) in the correct domain.
  ◦ The data ingests in the same domain as that of the integration user, whose credentials are used for integration.
• Re-scans specific hosts from Configuration Compliance in the domain from which it was requested.
• Uses the CMDB CI lookup process to ensure that the CI information from the scanners matches the CIs in CMDB of the integration user’s domain.
• Calculates risk scores at the test result level as per the risk score calculator defined in the same domain as that of the integration user.
• Test result group rule(s) can be defined, assigned, and stay in, the same domain as the domain of the integration user.
• Test result groups created using the doc test result group rules stay in the same domain as where the group rules are created.
• Deferral workflow goes through the approval process in the same domain for which the deferral is requested.
• Reports and dashboards display the test result states such as age of test results, open test results by CI, test results by impact in the domain to which it belongs.
• Knowledge from third-party scanners (Qualys) can be ingested in the global domain and data can be shared across multiple clients.

⚠️ Note: In all the above cases the overarching principles of visibility in separated domains separation in the NOW Platform apply.

**Use cases**

The Configuration Compliance application manages the life cycle of a test result end to end. The following use cases are domain-separation aware:

• **Ingest** test results from Qualys
  ◦ Ingest data from multiple instances
  ◦ De-duplicate the test results
  ◦ Match up with CMDB CI

• **Enrichment** of test results with risk scores
  ◦ Asset enrichment (CMDB)
  ◦ Risk score

• **Group** test results and assign the test results group
Automatically group the test results
Automatically assign the test results group

**Remediate**
- Test result group assigned as a remediation task
- Comprehensive remediation life cycle
- Deferral workflow

**Measure** the security posture of the organization and compliance management program
- Results trend, by compliance, category, criticality and technology
- Status and distribution on policies, tests, hosts, test results, and risk score

**Setup**
Setting up domain separation for Configuration Compliance does not require any additional steps. All Configuration Compliance tables acquire the Domain column after the instance is domain separated. You can direct test result integration import data to specific domains. See Create domain-separated imports for the Qualys Host Detection Integration for more information.

**Domain-separated data**
Data can be domain separated, which means:
- Test results ingested from third-party scanners stays in the same domain as the domain of the integration user, and is not accessible from any other domain.
- Test results or hosts in one domain cannot be viewed from other domains.
- The risk scoring algorithm and the test results group rules cannot be viewed by anyone outside the domain.
- Deferral workflows created in one domain are not visible in another domain.
- All email notifications are contained within the domain they belong to.

**How compliance analysts manage their own application data**
- Analysts create their own application installation, multi-source application management, and CI lookup rules.
- Analysts can configure specific integrations exclusively for use within the domain.
- Analysts can create their own deferral and change management workflows.
• Analysts can create their own test result group rules, risk-scoring logic to accurately prioritize results, auto-assign test result groups and assign to the correct assignment group.

• Domain users create a manual test result group and then close it.

**Business logic and processes that can be domain-separated by instance owner**

• Configuration Compliance users and groups

• Configuration Compliance integrations (starting with the Madrid release)

• Complete setup configuration (user and group management, application installation, multi-source application management, CI lookup rules, test result group rules, risk calculators, etc.)

• Complete remediation life cycle including deferral

**Related information**

Domain separation for service providers

**Configuration Compliance setup**

Before you can use Configuration Compliance, you must install a third-party scanner integration, such as the Qualys Vulnerability Integration.

Other types of information can be set up to manage test results within the application.

• Configuration Compliance assignment rules overview

• Configuration Compliance test result groups and group rules overview

• Calculator Groups

• Criticality Mapping

**Install and configure Configuration Compliance**

Before you run Configuration Compliance in your Now Platform® instance, you must first download and install the Configuration Compliance application from the ServiceNow Store. This application is available as a separate subscription.

**Before you begin**

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.
Note: This process applies only to applications downloaded to production instances. If you’re downloading applications to sub-production or development instances, it’s not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

<table>
<thead>
<tr>
<th>Setup tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have the required ServiceNow roles for your instance.</td>
<td>The following roles are required for installation, configuration, and verification of expected results:</td>
</tr>
<tr>
<td></td>
<td>• If not already assigned, the System Administrator [admin] installs the application and assigns the Configuration Compliance Admin [sn_vulc.admin] role.</td>
</tr>
<tr>
<td></td>
<td>• The Configuration Compliance Admin [sn_vulc.admin] oversees configuration and verifies expected results.</td>
</tr>
<tr>
<td></td>
<td>• The Remediation Owner [sn_vulc.remediation_owner] reads and updates assigned records. The sn_vulc.remediation_owner role is also automatically assigned when any user is assigned the itil role.</td>
</tr>
</tbody>
</table>

Qualys Vulnerability Integration

If you plan to use the Qualys Vulnerability Integration with Configuration Compliance, verify that the Vulnerability Response application is installed and activated prior to configuring the Qualys Vulnerability Integration using Setup Assistant.

To verify that they are installed and activated, navigate to Subscription Management > Subscriptions in your instance. The list displays the subscriptions your organization has purchased.

If the Vulnerability Response application is not installed and activated see, Install and configure Vulnerability Response.
If the Qualys Vulnerability Integration is installed on your system, and your API credentials are different than the ones you want to use for Configuration Compliance, go into Setup Assistant (in Vulnerability Response) and assign them to each Qualys PC integration.

Navigate to Qualys Vulnerability Integration > Primary Integrations and edit the Qualys API Credentials field under the Qualys REST Details tab.

For more detailed information on the Qualys Vulnerability Integration, see Understanding the Qualys Vulnerability Integration.

Role required: admin

About this task
Separate third-party SCA plugins acquire and transform data in Configuration Compliance. Before you can use Configuration Compliance to remediate configuration items, you must perform at least one network scan.

Procedure
1. To get entitlement and download the Configuration Compliance core application, navigate to the ServiceNow Store.
2. In the upper right of the page, click Log In.
3. In the dialog that is displayed, enter your HI credentials and click **Login**.

4. On the page that is displayed, if not selected, click the **ServiceNow Products** tab.

5. To view the associated applications that you are eligible for with the Configuration Compliance application, on the product list page, click the **Configuration Compliance** product.
The page that is displayed lists all the applications you are eligible for if you opt-in. For more information on an application, click a link.

6. To get the Configuration Compliance application, click **Opt-in**.
7. To agree to the terms and conditions, at the prompt, select the check box and click **Accept**.
A message is displayed that indicates you have successfully opted-in for the application.

With the ServiceNow Products tab selected on the Products List, a green check mark replaces the plus sign to the right of the Configuration Compliance application, as shown in the following figure.

After you have accepted the terms and conditions and managed entitlements for any of the applications on the ServiceNow Products tab, on the Products List page, you can click the plus sign (+) to get entitlement and opt-in for the other applications on this page with a single click.

8. Skip to step 10 to install the application on your Now Platform instance.

9. **Optional:** Alternatively, if you want to manage your entitlement for the Configuration Compliance application on other Now Platform instances, follow these steps.

   a. If the Manage Entitlement button is not displayed, click the Configuration Compliance application on the Product List to display it.

   b. Click **Manage Entitlement**.
c. In the Manage Entitlements for Configuration Compliance dialog that is displayed, choose one:

Manage Entitlements for Configuration Compliance

Entitlement Type

- Remove all existing entitlements
- Entitle all Instances
- Entitle selected Instances

[OK] [Cancel]

d. Click **OK** or **Cancel** to continue.

You are ready to activate plugins and install the application on your Now Platform instance(s).

10. Log in to the Now Platform instance that you want to install the Configuration Compliance application on.

11. Navigate to **System Applications > All Available Applications > All**.
12. From the applications listed, locate the Configuration Compliance application (sn_vulc) and click **Install**.
The Application installation dialog is displayed. Any dependencies that will be installed are displayed.

13. If you want demo data, select the Load demo data check box and click **Install**.

**Note:** If you do not select the **Load demo data** check box, demo data is not available to install from the **Application Manager** later. For information on how to install or reinstall demo data after the initial installation, see the **Work around to install demo data if application is already installed [KB0722909]** article in the Now Support Knowledge Base.
This installation may take some time. A message is displayed in the Install dialog after the application and its dependencies are successfully installed.

14. Click **Close**.

15. After the installation successfully completes, see **Configuration Compliance calculator groups** and **Configuration Compliance criticality maps**.

### Components installed with Configuration Compliance

Several types of components are installed with activation of the Configuration Compliance plugin, including tables and user roles.

**Note:** The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see **Find components installed with an application**.

Demo data is available for this feature.

### Roles installed

<table>
<thead>
<tr>
<th>Role title [name]</th>
<th>Description</th>
<th>Contains roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Compliance administrator [sn_vulc.admin]</td>
<td>Able to modify application properties and configuration.</td>
<td>• sn_vulc.write</td>
</tr>
<tr>
<td>read [sn_vulc.read]</td>
<td>Read lists and records in Configuration Compliance.</td>
<td>• sn_sec_cmn.calc_read</td>
</tr>
<tr>
<td>write [sn_vulc.write]</td>
<td>Write lists and records in Configuration Compliance.</td>
<td>• sn_vulc.read • sn_vulc.remediation_owner</td>
</tr>
</tbody>
</table>
### Role title [name]

<table>
<thead>
<tr>
<th>Role title [name]</th>
<th>Description</th>
<th>Contains roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>write assignment</td>
<td>Write to Test Result assignment fields.</td>
<td>Contained in the sn_vulc.remediation_owner role.</td>
</tr>
<tr>
<td>[sn_vulc.write_assignment]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| remediation owner                 | View and update permission for test results assigned to you or your group. | Contained in the itil role. Contains:  
| sn_vulc.remediation_owner         |                                                  | • sn_sec_cmn.read  
|                                   |                                                  | • sn_vulc.write_assignment |

### Scheduled jobs installed

<table>
<thead>
<tr>
<th>Scheduled job</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version 12.0</strong></td>
<td>Calculates and updates values for status metrics on test result group records.</td>
</tr>
<tr>
<td>Calculate remediation metrics for all the test results groups</td>
<td></td>
</tr>
<tr>
<td><strong>Version 12.0:</strong> Calculate remediation metrics for all the test results</td>
<td>Calculates and updates values for status metrics on test results records.</td>
</tr>
<tr>
<td><strong>Version 12.0:</strong> Change Request State Synchronization</td>
<td>On-demand job that synchronizes the states of all existing test result groups (CRGs) with change requests (CHGs). As a change request moves through its life cycle, it also moves the states of any related test result groups automatically. Enables state synchronization going forward.</td>
</tr>
<tr>
<td><strong>Version 12.0:</strong> Change Request State Synchronization</td>
<td>On-demand job that synchronizes the states of all existing test result groups (CRGs) with change requests (CHGs). As a change request moves through its life cycle, it also moves the states of any related test result groups automatically. Enables state synchronization going forward.</td>
</tr>
<tr>
<td><strong>Version 11.1:</strong> Check Test Result</td>
<td>Sends notifications if test result groups have expired (and if they expire in one week).</td>
</tr>
<tr>
<td>Scheduled job</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Groups Deferment Expiration</td>
<td>Populates distinct configuration item (CI) count and the 90 day rolling average in the Configuration Item Count [sn_vulc_cc_configuration_item_count] table.</td>
</tr>
<tr>
<td>Configuration Compliance CI count</td>
<td>Version 11.1: Sets or updates remediation target dates on all test results. Determines the status of remediation target dates against rules. Sends notifications.</td>
</tr>
<tr>
<td></td>
<td>Version 12.0: Populates change requests on test result groups.</td>
</tr>
<tr>
<td>Re-open deferred test result groups</td>
<td>Reopens deferred groups when the due-date has passed.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>removed in Configuration Compliance v11.1. Deprecated for versions prior to 11.1. Do not use.</td>
</tr>
<tr>
<td></td>
<td>Reassesses the state of test result groups for entries where assess_state is false. Runs every 15 minutes.</td>
</tr>
<tr>
<td>Reapply all assignment rules</td>
<td>Reapplies all assignment rules.</td>
</tr>
<tr>
<td>Reassess the state of the test result groups</td>
<td>Reassesses the state of test result groups for entries where assess_state is false. Runs every 15 minutes.</td>
</tr>
<tr>
<td>Version 10.3: Rollup test result risk score to test result group and configuration test</td>
<td>Runs hourly and calculates the rollup scores for the changed configuration tests and test result groups.</td>
</tr>
<tr>
<td></td>
<td>• Calculates rollup risk score for all tests in sn_vulc_test_manifest and deletes the manifest record upon completion.</td>
</tr>
<tr>
<td></td>
<td>• Calculates the rollup risk score for all the tests in sn_vulc_result_group_manifest and deletes the manifest upon completion.</td>
</tr>
<tr>
<td>Scheduled job</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Version 12.0: Update policy remediation metrics</td>
<td>Calculates and updates values for status metrics on policy records.</td>
</tr>
<tr>
<td>Version 11.0: Update Risk Rating for Test Results</td>
<td>Updates Risk Rating for Test Results.</td>
</tr>
<tr>
<td>Version 11.0: Update Rollup risk score for all non closed Result groups and Configuration tests.</td>
<td>Updates the rollup risk score for all non-closed Result groups and Configuration Compliance tests.</td>
</tr>
</tbody>
</table>

### Tables installed

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignment Rule [sn_vulc_assignment_rule]</td>
<td>Contains the set of rules evaluated to set the assignment group on test results.</td>
</tr>
<tr>
<td>Authoritative Source [sn_vulc_auth_src]</td>
<td>Store imported authoritative sources.</td>
</tr>
<tr>
<td>Calculator [sn_vulc_calculator_risk_score]</td>
<td>Contains the calculator that sets certain test result fields when certain conditions are met.</td>
</tr>
<tr>
<td>CC Configuration Item Count [sn_vulc_cc_configuration_item_count]</td>
<td>Contains the total number of configuration items.</td>
</tr>
<tr>
<td>Version 12.0: Change request form [sn_vulc_cr_form]</td>
<td>Base table for change request management.</td>
</tr>
<tr>
<td>Version 12.0: Change request creation [sn_vulc_action_create_cr]</td>
<td>Staging table used for creating change request forms.</td>
</tr>
<tr>
<td>Version 12.0: Change request association [sn_vulc_action_associate_cr]</td>
<td>Staging table used for associating change requests to test result groups.</td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Version 12.0: Split test result group</td>
<td>Staging table used for splitting test result groups.</td>
</tr>
<tr>
<td>[sn_vulc_action_split_trg]</td>
<td></td>
</tr>
<tr>
<td>Citation</td>
<td>Contains imported citations</td>
</tr>
<tr>
<td>[sn_vulc_citation]</td>
<td></td>
</tr>
<tr>
<td>Configuration Test</td>
<td>Contains imported configuration test data.</td>
</tr>
<tr>
<td>[sn_vulc_test]</td>
<td></td>
</tr>
<tr>
<td>Version 10.3: Configuration Test Manifest</td>
<td>Contains the configurations tests for which the rollup risk score needs to be calculated.</td>
</tr>
<tr>
<td>[sn_vulc_test_manifest]</td>
<td></td>
</tr>
<tr>
<td>Configuration Test Technology</td>
<td>Contains imported configuration test technologies.</td>
</tr>
<tr>
<td>[sn_vulc_test_technology]</td>
<td></td>
</tr>
<tr>
<td>Group Rule</td>
<td>Contains the rules that define the criteria with which groups are automatically created for a set of test results.</td>
</tr>
<tr>
<td>[sn_vulc_grouping_rule]</td>
<td></td>
</tr>
<tr>
<td>Policy</td>
<td>Contains imported policies</td>
</tr>
<tr>
<td>[sn_vulc_policy]</td>
<td></td>
</tr>
<tr>
<td>Policy Configuration Test</td>
<td>Contains imported policy configuration test data.</td>
</tr>
<tr>
<td>[sn_vulc_policy_test]</td>
<td></td>
</tr>
<tr>
<td>Version 11.1: Remediation Target Rule</td>
<td>Defines the expected time frame for remediating a test result.</td>
</tr>
<tr>
<td>[sn_vulc_ttr_rule]</td>
<td></td>
</tr>
<tr>
<td>Risk Calculators</td>
<td>Contains the grouping of Configuration Compliance calculators. The order of the calculator group determines which group is evaluated first, and in each group, one calculator at most is used.</td>
</tr>
<tr>
<td>Version 10.3: Calculator Group</td>
<td></td>
</tr>
<tr>
<td>[sn_vulc_calculator_group]</td>
<td></td>
</tr>
<tr>
<td>Version 10.3: Risk Score Rollup Calculator</td>
<td>Contains rollup calculator configurations.</td>
</tr>
<tr>
<td>[sn_vulc_risk_score_rollup]</td>
<td></td>
</tr>
<tr>
<td>Version 11.1: State Change Approval</td>
<td>Contains approval state process data.</td>
</tr>
<tr>
<td>[sn_vulc_grouping_rule]</td>
<td></td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>[sn_vulc_state_change_approval]</td>
<td>Contains imported technologies.</td>
</tr>
<tr>
<td>Technology</td>
<td>[sn_vulc_technology]</td>
</tr>
<tr>
<td>Test Criticality Map</td>
<td>[sn_vulc_test_criticality_map] Contains criticality map data.</td>
</tr>
<tr>
<td>Test Result</td>
<td>[sn_vulc_result] Contains imported test results.</td>
</tr>
<tr>
<td>Test Result Group</td>
<td>[sn_vulc_result_group] Contains imported test result groups.</td>
</tr>
<tr>
<td>Version 12.0: Test Result Group Change Requests</td>
<td>Contains change requests for test result groups.</td>
</tr>
<tr>
<td>Version 10.3: Test result group manifest</td>
<td>[sn_vulc_result_group_manifest]</td>
</tr>
<tr>
<td>Test Result Groups</td>
<td>[sn_vulc_m2m_result_result_group] Contains test result group data.</td>
</tr>
<tr>
<td>Test Result History</td>
<td>[sn_vulc_result_history] Contains imported test result history.</td>
</tr>
<tr>
<td>Version 11.1: Test Result Remediation Status</td>
<td>Status of the test result against the closest applied remediation target rule.</td>
</tr>
</tbody>
</table>

**Configuring calculator groups and calculators for Configuration Compliance**

Configuration Compliance calculators are used to update record values when pre-defined conditions are met. The calculators are grouped based on the criteria used to determine how the records are updated.

**Configuration Compliance calculators starting with v10.3**

The Configuration Compliance application includes two types of calculators, Risk Calculators and Risk Score Rollup Calculators. These calculator groups are enabled by default.
The Risk Score calculator group has been renamed to Risk Calculators.
The Risk Score Rollup Calculators includes rollup calculators for configuration
tests and test result groups.

Configuring risk and rollup calculators for remediation of test results and test
result groups includes the following tasks:

- Create a risk calculator
- Create a risk score rollup calculator

After you create a risk calculator, it is available for calculations with the next
data ingestion. After you create it, you may also prefer to apply it on-demand.

For more information about calculators and calculator groups, see
Configuration Compliance calculator groups.

**Configuration Compliance calculators prior to v10.3**

All enabled Configuration Compliance calculators in the Calculator Groups run
each time a test result fails. If you change a test (within the third-party scanner
application) or the logic in the risk calculator, Risk Score is calculated after the
next import.

The Configuration Compliance base system includes one calculator group: Risk
Score.

**Create or edit Configuration Compliance assignment rules**
Create rules to automatically assign test results based on filter conditions. These
rules assign test results as they are imported.

**Before you begin**
Role required: sn_vulc.admin

**About this task**
The base system ships with one Configuration Compliance assignment rule,
Assign to CI support group, which assigns test results to the same assignment
group as the CI support group. This rule is inactive by default. You can modify
using filter conditions. With assignment rules, you define one or more conditions
of assignment and the order of execution. Once a test result matches a rule
condition, the assignment lookup stops.

⚠️ **Note:** New or updated rules are automatically evaluated on the next
import or manually using the **Apply Changes** button on the Assignment
Rules list.
Procedure

1. Navigate to Configuration Compliance > Administration > Assignment Rules.
2. Open the Assign to CI support group rule or click New.
3. Edit the Assign to CI support group rule, or if New, fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the group rule.</td>
</tr>
<tr>
<td>Execution order</td>
<td>Order in which the rules are evaluated. The lowest number is evaluated first.</td>
</tr>
<tr>
<td></td>
<td>High priority rules, test results that need special handling, where risk is critical, or a test result that should be handled by regulatory compliance, should be run first. Next, run your general rules, where no special handling is required, and you know who should be responsible for them. Finally, create a default rule to assign test results to the group that figures out what assignment group it should belong to. This group could add another rule to cover their decisions. This default rule would run last.</td>
</tr>
<tr>
<td>Active</td>
<td>Indicates whether the assignment rule is active.</td>
</tr>
</tbody>
</table>

**Condition**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition fields</td>
<td>Conditions that must be met.</td>
</tr>
<tr>
<td></td>
<td>Starting with v12.0, case sensitivity for the search text you enter in the condition builder is not supported on this record or form. Prior to v12.0, case sensitivity is supported for the search text you enter in the condition builder.</td>
</tr>
<tr>
<td>New Criteria</td>
<td>Adds more condition filter fields to choose from.</td>
</tr>
<tr>
<td>Description</td>
<td>Text describing the assignment rule.</td>
</tr>
<tr>
<td>Assign using</td>
<td>To automate the assignment of groups created based on this rule, choose one of the options available.</td>
</tr>
<tr>
<td></td>
<td>• User group: Select a user group from the lookup table</td>
</tr>
<tr>
<td></td>
<td>• User group field: Select a user group field from the drop-down menu.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>• Script:</td>
<td>Create or edit a script.</td>
</tr>
<tr>
<td>Note:</td>
<td>Creating or edit a script requires ServiceNow expertise.</td>
</tr>
<tr>
<td>(Starting with v10.3)</td>
<td></td>
</tr>
<tr>
<td>User group field</td>
<td>Select the user group responsible for remediating tests that match the</td>
</tr>
<tr>
<td></td>
<td>conditions of the assignment rules.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**Manually create a Configuration Compliance test result group**

You can manually create a test result group from the **Test Result Groups** module and perform remediation.

**Before you begin**

Role required: sn_vulc.admin

**About this task**

Using test result group rules automatically populates the **Test Results** tab. Manual creation is useful for a group that doesn't need a rule or to be repeated.

**Procedure**

1. Navigate to **Configuration Compliance > Test Result Groups**.
2. Starting with v10.3, in the navigation panel, click on **My Open Groups** or **All Open Groups** to view the list.
3. Prior to v10.3, click **New**.
4. Click **New**.
### (Starting with v10.3) Test Result Group form

<table>
<thead>
<tr>
<th>Open</th>
<th>Under Investigation</th>
<th>Deferred</th>
<th>Awaiting Implementation</th>
<th>Resolved</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Number**: CRS0001199
- **State**: Open
- **Assignment group**: 
- **Assigned to**: 
- **Created**: 
- **Updated**: 

**Short description**

**Description**

**Test**

**Group Configuration**

- **Grouping method**: Filter
- **Table**: Test Result (sn_vulc_result)
- **Test result condition**: Preview

All of these conditions must be met

- **-- choose field --**: 

**OR**

**AND**

New Criteria
5. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Auto-assigned ID in the system.</td>
</tr>
<tr>
<td><strong>Version 10.3: Risk score</strong></td>
<td>Auto-populated by risk score calculator.</td>
</tr>
<tr>
<td></td>
<td>This is a rollup risk score. This risk score is weighted, with 85% of the</td>
</tr>
<tr>
<td></td>
<td>score from the max risk score across all Test Results not 'Closed' (Open,</td>
</tr>
<tr>
<td></td>
<td>Under Investigation, Awaiting Implementation, Deferred, Resolved), and 15%</td>
</tr>
<tr>
<td></td>
<td>of the score from the number of test results that are not 'Closed'.</td>
</tr>
<tr>
<td><strong>Version 10.3: Risk rating</strong></td>
<td>Auto-populated by risk score calculator. Based on a range of risk scores on</td>
</tr>
<tr>
<td></td>
<td>a 1-5 numeric scale that rates overall risk based on a range of risk scores</td>
</tr>
<tr>
<td></td>
<td>as 1 - Critical to 5 - None. This field replaces the Priority field in</td>
</tr>
<tr>
<td></td>
<td>previous versions.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Version 10.3: Priority</td>
<td>Choose a remediation priority for the group. Choices are: • Critical • High • Moderate • Low • Minor</td>
</tr>
<tr>
<td><strong>Note:</strong> The Risk rating field replaces this field starting in v10.3.</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Initially <strong>Open</strong>, is the remediation state of the group. For more information, see Configuration Compliance states.</td>
</tr>
<tr>
<td>Assignment group</td>
<td>Assign the test result group to a remediation group.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>Assign personnel to remediate the test result group.</td>
</tr>
<tr>
<td>Created</td>
<td>Date you created this group.</td>
</tr>
<tr>
<td>Updated</td>
<td>Date you updated this group.</td>
</tr>
<tr>
<td>Short Description</td>
<td>Name of the test result group.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of this test result group.</td>
</tr>
<tr>
<td>Version 10.3: Test</td>
<td>Select a Configuration Test for this Test Result Group.</td>
</tr>
<tr>
<td><strong>Related tabs</strong></td>
<td></td>
</tr>
<tr>
<td>Group Configuration</td>
<td>Grouping Methods to use: • Manual (default): • Filter or Group Rule: Table: preselected as Test Result [sn_vulc_result] Test result condition: Choose the filters to use.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>The records match condition link above the filter conditions displays the test result records you have chosen in a new window. Prior to v10.3 Click the 📦 to see how many records match the ones you have chosen before you save. Version 10.3: Click Preview to see how many results your filter criteria returns before you save the new group. The Test Results related list must be created manually by clicking the Edit button in the Test Results related tab.</td>
</tr>
</tbody>
</table>

**Notes**

Work notes related to this test result group.

6. Right click in the header to Save or click Submit to save and return to the list of test result groups. Displays the Test Results and Change Request related lists.

Manually create a Configuration Compliance test result group from the Test Results list

You can manually create a test result group from the Test Result list and perform remediation from the resulting test result group.

**Before you begin**

Role required: sn_vulc.admin
About this task
This method requires selecting test results to include and creating the group from the **Actions on selected rows...** menu. This method is good for results that are not easily filtered or situations where you want to specify test results for remediation.

Procedure
1. Navigate to **Configuration Compliance > Test Results**.
2. Starting with v10.3, in the navigation panel, select a Test Result module to open a list.
3. Select the test results to include in the group by checking the box next to each one.
4. Open the **Actions on selected rows...** menu at the bottom of the list.
5. Choose **Create Test Result Group**.

The test result group is created and opens.
The test results you selected for the group are displayed on the Test Results related list along with any associated change requests.
<table>
<thead>
<tr>
<th>Number</th>
<th>Test</th>
<th>Result</th>
<th>Risk score</th>
<th>Risk rating</th>
<th>State</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTR0000003</td>
<td>Status of the 'Minimum Password Age' setting</td>
<td>Failed</td>
<td>75</td>
<td>2-High</td>
<td>Open</td>
<td></td>
</tr>
<tr>
<td>CTR0000004</td>
<td>Current list of Groups and User Accounts granted the 'Allow log on locally</td>
<td>Failed</td>
<td>75</td>
<td>2-High</td>
<td>Open</td>
<td></td>
</tr>
<tr>
<td>CTR0000004</td>
<td>Status of the 'Minimum Password Length' setting</td>
<td>Failed</td>
<td>65</td>
<td>3-Medium</td>
<td>Open</td>
<td></td>
</tr>
</tbody>
</table>

Actions on selected rows...
6. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Auto-assigned ID in the system.</td>
</tr>
<tr>
<td>Prior to version 10.3: Priority</td>
<td>Choose a remediation priority for the group.</td>
</tr>
<tr>
<td>Version 10.3: score</td>
<td>Auto-populated by risk score rollup calculator. This is a rollup risk score. This risk score is weighted, with 85% of the score from the max risk score across all Test Results not 'Closed' (Open, Under Investigation, Awaiting Implementation)</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Implementation, Deferred, Resolved), and 15% of the score from the number of test results that are not 'Closed'.</td>
<td></td>
</tr>
<tr>
<td><strong>Version 10.3: rating</strong></td>
<td>Auto-populated by risk score rollup calculator. Based on a range of risk scores on a 1-5 numeric scale that rates overall risk based on a range of risk scores as 1 - Critical to 5 - None. This field replaces the Priority field in previous versions.</td>
</tr>
<tr>
<td><strong>Version 10.3: Historical risk score</strong></td>
<td>Auto-populated by risk score rollup calculator. The inherent risk score across all the passed test results in a test result group. This field displays the amount of risk that was remediated by a test group and is only displayed after a test group is in the ‘Closed’ state and the risk score is zero.</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>Initially <strong>Open</strong>, is the remediation state of the group. For more information, see <strong>Configuration Compliance states</strong>.</td>
</tr>
<tr>
<td><strong>Assignment group</strong></td>
<td>Assign the test result group to a remediation group.</td>
</tr>
<tr>
<td><strong>Assigned to</strong></td>
<td>Assign personnel to remediate the group.</td>
</tr>
<tr>
<td><strong>Created</strong></td>
<td>Date you created this group.</td>
</tr>
<tr>
<td><strong>Updated</strong></td>
<td>Date you updated this group.</td>
</tr>
<tr>
<td><strong>Short Description</strong></td>
<td>Name of the test result group.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Text description of this test result group.</td>
</tr>
<tr>
<td><strong>(Starting with v10.3)</strong></td>
<td>Select a Configuration Test for this Test Result Group.</td>
</tr>
</tbody>
</table>
| **Related tabs** | Grouping Methods to use:  
  - Manual (default)  
  - Filter  
Table: preselected as Test Result  
Test result condition: Choose the filters to use. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong></td>
<td>The records match condition link above the filter conditions displays the test result records you have chosen in a new window.</td>
</tr>
<tr>
<td></td>
<td>(Prior to v10.3) Click the 📦 to see how many records match the ones you have chosen before you save.</td>
</tr>
<tr>
<td></td>
<td>(Starting with v10.3) Click <strong>Preview</strong> to see how many results your filter criteria returns before you save the new group.</td>
</tr>
<tr>
<td>Notes</td>
<td>Work notes related to this test result group.</td>
</tr>
<tr>
<td>Related lists</td>
<td></td>
</tr>
<tr>
<td>Test results</td>
<td>Test results included in this group.</td>
</tr>
<tr>
<td>Change requests</td>
<td>Change requests associated with this group.</td>
</tr>
</tbody>
</table>

7. Right click on the header to **Save** or click **Submit** to save and return to the list of test result groups.

**Create or edit Configuration Compliance test result group rules**

You can create rules to automatically group test results based on filter conditions. These rules automatically group test results as they are imported. Use the filter to limit the test results grouped by this rule, such as selecting all test results with exploits.

**Before you begin**
Role required: sn_vulc.admin

**About this task**
The base system ships with one test result group rule, **Assignment group**, **Test**, which groups test results by assignment group (pre-populated from Assignment Rules) and the test result **Test** field. This rule can be modified using filter conditions and group keys. Group keys are columns in the test results table. Select up to six keys to indicate what values should be used to group the test results.

**Note:** New or updated rules are automatically evaluated on the next import or manually using the **Reapply** button on the Group Rule form.
Procedure

1. Navigate to Configuration Compliance > Administration > Group Rules.
2. Open the Assignment group, Test rule or click New.

3. If New, fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the group rule.</td>
</tr>
<tr>
<td>Active</td>
<td>Indicates whether the group is active.</td>
</tr>
<tr>
<td>Description</td>
<td>Text description of this test result group rule.</td>
</tr>
<tr>
<td>Case sensitive</td>
<td>Determines whether the rule matching is case sensitive or not.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>The default value is case insensitive.</td>
</tr>
<tr>
<td>Conditions</td>
<td>Conditions that must be met.</td>
</tr>
</tbody>
</table>

Starting with v12.0, by default, **(Case sensitive check box disabled)**, the search text you enter in the condition builder on group rules records and forms is not case-sensitive. You have the
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>option to enable case-sensitive searches on group records and forms.</td>
</tr>
</tbody>
</table>

**Group By**

<table>
<thead>
<tr>
<th>Group test results from</th>
<th>Automate the creation of groups based on this rule. Choose one of the options available.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Test Result</td>
</tr>
<tr>
<td></td>
<td>• Test Result-&gt;Configuration Item</td>
</tr>
</tbody>
</table>

If an extended **Table** field is selected, test results that don’t use the corresponding extended table are grouped in a separate test result group.

**Assignment**

<table>
<thead>
<tr>
<th>Assign test result groups by</th>
<th>Automate the assignment of groups created based on this rule. Choose one of the options available.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Group key</td>
</tr>
<tr>
<td></td>
<td>When selected, a Key value field appears, available fields are listed in a drop-down menu.</td>
</tr>
<tr>
<td></td>
<td>• User group</td>
</tr>
<tr>
<td></td>
<td>When selected, a User group lookup field appears.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

⚠ **Note:** The Clear Group By Keys related link removes the group keys from the Group By tab on the form.

Create a Configuration Compliance calculator group

Configuration Compliance calculator groups are used to group calculators based on how you want to use them.

**Before you begin**

The Configuration Compliance base system includes one calculator group: **Risk Score**. As you create other calculators, you can add them to this group or create other groups and calculators. Within each group, the first calculator that matches the test result runs.

Role required: sn_vulc.admin
About this task
Starting with v10.3.0, there are two calculator groups that are included with the Configuration Compliance application:

- Risk Calculators
- Risk Score Rollup Calculators

Risk Calculators calculate the risk score and risk rating of a Test Result.
Risk Score Rollup Calculators roll up risk scores for all Test Results and Test Result groups with the same Configuration Test to provide an overall risk score.

Prior to v10.3, there is one calculator group included with the Configuration Compliance application, the Risk Score calculator group. It calculates the risk score of a test result. As written, it is based on the business criticality and test criticality values of the test.

You also create new calculators directly from these groups.

Procedure

1. Navigate to Configuration Compliance > Administration > Calculator Groups.
2. Starting with v10.3, Navigate to Configuration Compliance > Administration and select Risk Calculators or Risk Score Rollup Calculators.
3. Click New.
4. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the calculator.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of this calculator group.</td>
</tr>
<tr>
<td>Version 10.3:</td>
<td></td>
</tr>
<tr>
<td>Active</td>
<td>Enable or disable the calculator group.</td>
</tr>
</tbody>
</table>

5. Right-click Save in the form header or click Submit.
Starting with v10.3, the new calculator group is displayed on in the group list with the other calculators. Click the name of new calculator group to open the record. See Create, edit, and reapply risk calculators for Configuration Compliance (v. 10.3) for more information about setting conditions and displayed values and reapplying calculators.
Prior to v10.3, the **Security Calculators** related list is displayed.

Starting with v12.0, case sensitivity for the search text you enter in the condition builder is not supported on this record or form. Prior to v12.0, case sensitivity is supported for the search text you enter in the condition builder.

**What to do next**

Create a Configuration Compliance calculator (Prior to v. 10.3).

Create, edit, and reapply risk calculators for Configuration Compliance (v. 10.3)

Calculator rules can be applied to all affected test results and collections on-demand. Vulnerability managers may use this feature adjust their risk calculator configuration and apply changes on-demand to import findings.
Before you begin
Role required: sn_vulc.admin

Procedure

1. To create a new risk calculator, follow these steps.

   a. Navigate to **Configuration Compliance > Administration** and select **Risk Calculators**.

   b. In the Risk Calculator list, click **New**.

   c. Enter a name and description for your new calculator and click **Submit**. The new calculator is displayed on the Risk Calculator list.

   d. In the list, click the new calculator to create the conditions under which the calculator runs and specify the fields and values you want displayed on test result records and test result groups.

   e. In the record that is displayed, click **New**.

   f. Fill in out the fields in the tabs as appropriate.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>When this condition is met</td>
<td>Use the conditions builder to create the conditions under which the calculator runs. An example is: Result is Failed or Result is Error.</td>
</tr>
</tbody>
</table>
2. To reapply an existing calculator to test results or edit the rules and displayed values for an existing risk calculator, follow these steps.

   a. From the Risk Calculators or Risk Rollup calculator lists, select the calculator you want to edit.

   b. (Optional) To reapply a risk calculator to your existing test result data from the record, click **Reapply Calculator**.
      All test results that meet the conditions of the calculator are updated.

      Note: Depending on the number of test results, this update may take time.

   c. To edit the conditions and values, in the lower left in the Name column, click the calculator name.
      For risk calculators, the record and the **When this condition is met** and **Set these values** tabs are displayed.

   d. Fill in the form as appropriate.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Set these values</strong></td>
<td>Use the template to select the fields and values you want displayed.</td>
</tr>
<tr>
<td><strong>When this condition is met</strong></td>
<td>Use the filter conditions builder to create the conditions under which you want the calculator to run.</td>
</tr>
<tr>
<td><strong>Set these values</strong></td>
<td>Choose one to continue.</td>
</tr>
<tr>
<td></td>
<td>• Value type - Template. Choose fields from the list and corresponding values.</td>
</tr>
<tr>
<td></td>
<td>• Script - Enter your changes using the editor.</td>
</tr>
<tr>
<td></td>
<td>Note: Editing script requires advanced knowledge of the Now Platform and the Configuration Compliance application.</td>
</tr>
</tbody>
</table>
3. **Optional:** To apply the new rules on-demand to your existing test result data, follow these steps.

   a. With the Risk Calculators list displayed, click a calculator you want to apply. The record is displayed.

   b. Click **Reapply Calculator** to test and apply your changes on-demand to your import findings.

4. View your changes on test results and continue to edit your calculators as required.

### Create or edit risk rollup calculators for Configuration Compliance (v10.3)

Starting with version 10.3, this calculator group rolls up the risk scores of test results to test result groups and configuration tests. Use risk scores and risk ratings to assess the relative risks and potential impact that known configuration vulnerabilities pose to your organization.

**Before you begin**

Role required: Role required: sn_vulc.admin

**Procedure**

1. Navigate to **Configuration Compliance > Administration** and select **Risk Score Rollup Calculators**.

2. With the list of Risk Score Rollup Calculators displayed, click a calculator to open the record and edit the form.

3. Alternatively, to create a new calculator, click **New** and fill in the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the Configuration Test or Test Result Group rollup calculator.</td>
</tr>
<tr>
<td>Description</td>
<td>A description for the risk rollup calculator.</td>
</tr>
<tr>
<td>Script values</td>
<td>Edit the values in the script as required.</td>
</tr>
</tbody>
</table>

**Note:** Editing script requires advanced knowledge of the Now Platform and the Configuration Compliance application.

4. Click **Update** to save your edits.
Rollup calculators are scheduled jobs that run hourly to pick up changes. These scheduled jobs also overall risk scores for configuration tests and test result groups. The rolled-up values are displayed in the Risk Score fields.

For an example of how a risk rollup calculator determines scores, see Risk rollup calculation example for Configuration Compliance (v10.3).

**Risk rollup calculation example for Configuration Compliance (v10.3)**

The following example demonstrates how scores for risk rollup calculators are determined.

For the following test result group rollup calculator, the formula for calculating the test result Group Risk Score is:

\[(\text{Maximum risk score} / 100) \times 85 + (\text{factor} \times 15)\]

The factor in the previous equation is determined by the number of test results as shown in the following table.

<table>
<thead>
<tr>
<th>Test result count</th>
<th>Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;10</td>
<td>0.2</td>
</tr>
<tr>
<td>1-99</td>
<td>0.4</td>
</tr>
<tr>
<td>100-1000</td>
<td>0.6</td>
</tr>
<tr>
<td>1001-9999</td>
<td>0.8</td>
</tr>
<tr>
<td>&gt;1000</td>
<td>1</td>
</tr>
</tbody>
</table>

For the following test result group, CRG0003066, with three test results Risk scores, the maximum score is 90.

<table>
<thead>
<tr>
<th>Number</th>
<th>Risk score</th>
<th>Group</th>
<th>Result</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTR000123</td>
<td>90</td>
<td>CRG0003066</td>
<td>Failed</td>
<td>Open</td>
</tr>
<tr>
<td>CTR000124</td>
<td>70</td>
<td>CRG0003066</td>
<td>Failed</td>
<td>Open</td>
</tr>
<tr>
<td>CTR000125</td>
<td>40</td>
<td>CRG0003066</td>
<td>Failed</td>
<td>Open</td>
</tr>
</tbody>
</table>

For the Test result group, CRG0003066, the Risk Score is 79, \((90/100) \times 85 + 0.2 \times 15\) = Math.floor \((76.5 +3)\) =79.

The historical risk score is null, because the group is still 'Open'.
After the data ingestion, the test results are 'Passed', and the group transitions to 'Closed' as shown in the following table.

<table>
<thead>
<tr>
<th>Number</th>
<th>Risk score</th>
<th>Group</th>
<th>Result</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTR000123</td>
<td>0</td>
<td>CRG0003066</td>
<td>Passed</td>
<td>Closed</td>
</tr>
<tr>
<td>CTR000124</td>
<td>0</td>
<td>CRG0003066</td>
<td>Passed</td>
<td>Closed</td>
</tr>
<tr>
<td>CTR000125</td>
<td>0</td>
<td>CRG0003066</td>
<td>Passed</td>
<td>Closed</td>
</tr>
</tbody>
</table>

Test results History is displayed in the following table.

<table>
<thead>
<tr>
<th>Number</th>
<th>Risk score</th>
<th>Latest result</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTRH000111</td>
<td>90</td>
<td>CTR000123</td>
<td>Failed</td>
</tr>
<tr>
<td>CTRH000112</td>
<td>70</td>
<td>CTR000124</td>
<td>Failed</td>
</tr>
<tr>
<td>CTRH000113</td>
<td>40</td>
<td>CTR000125</td>
<td>Failed</td>
</tr>
</tbody>
</table>

The Risk score is zero, because there are no open test results in the group.

The maximum risk score of results that passed + the maximum risk score from the history - 90.

For the test result group CRG0003066, the Historical Risk Score is 79.

\[(90/100) \times 85 + 0.2 \times 15 = \text{Math.floor}(76.5 + 3) = 79.\]

**Create a Configuration Compliance calculator (Prior to v. 10.3)**

A calculator is a pre-defined formula to calculate the severity of a test result when certain criteria are met.

**Before you begin**

Roles required: sn_vulc.admin.

**About this task**

⚠️ **Note:** Editing **Basic Risk Score** or creating a calculator requires coding or advanced ServiceNow expertise.
Procedure

1. Navigate to Configuration Compliance > Administration > Calculator Groups.
2. Click the name of the group for which you want to create a calculator, or create a new group and then create a calculator for that group using the following steps.
3. In the Security Calculators related list, click New.
4. Fill in the fields on the form, as appropriate.

Vulnerability calculator form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the vulnerability calculator.</td>
</tr>
<tr>
<td>Calculator Group</td>
<td>Displays the group name for which you are creating this calculator.</td>
</tr>
<tr>
<td>Table</td>
<td>Select the table to be used for this calculator.</td>
</tr>
</tbody>
</table>

**Note:**
If you add calculators to tables other than Test Result [sn_vulc_result], add business rules and UI Actions to those tables.

To see examples:

- Navigate to System Definition > Business Rules and locate the Calculate Criticality business rule on the Vulnerable Item [sn_vul_vulnerable_item] table.
- Navigate to System UI > UI Actions and locate the Calculate Criticality UI action on the Vulnerable Item [sn_vul_vulnerable_item] table.

<table>
<thead>
<tr>
<th>Order</th>
<th>The order in which the calculator is run. A calculator with an order entry of 100 runs before a calculator with an order entry of 200.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Turn the calculator on or off.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of this calculator.</td>
</tr>
</tbody>
</table>

5. Right-click the form header and select Save. Two tabs, Conditions and Values to Apply, appear.
6. Fill in the fields in the Conditions tab, as appropriate.
Use filter group
Select this check box to use a predefined filter group or create a new filter group to define the calculator criteria.

Filter group
Select the filter group to use for defining a calculator. This field appears only if you selected the Use filter group check box.

Use advanced condition
Select this check box to indicate that a script condition is used to determine when this calculator is applied. When you select the check box, an Advanced condition scripting field appears. Set the answer variable to true to apply the calculator.

If you selected the Use filter group check box, this field is hidden.

Note: Before you define advanced conditions and write scripts for determining when the security incident calculators are applied, return to the Calculator Groups list. Explore the calculator records shipped with the base system.

Condition
Defines basic filter conditions for determining whether the calculator is used.

If you selected either of the Use filter group or Use advanced conditions check boxes, this field is hidden.

7. Click the Values to Apply tab and fill in the fields on the form, as appropriate. You have the choice of creating a script for defining the values to apply to the calculation or defining a template based on fields in the selected table.

Use script values
Select this check box to define field values with a script.

Script values
Defines what values to apply the calculations to. This field appears only if you selected the Use script values check box.

Template
Right-click the form header and select Save. Select the fields and values you want to use for the calculator.
8. When you have completed all entries, click **Submit**.

    **Note:** You may notice performance degradation when running Configuration Compliance calculators that contain scripts. If this impact occurs, deactivate them when they are not needed.

**Specify the duration of an exception requested for a test result group**

Use system properties to limit the duration for which an exception is requested for a test result group. Remediation of the test result group is deferred for the specified period.

**Before you begin**
Role required: sn_vulc.admin

**About this task**
The `sn_vulc.exception_max_request_days` property is used to specify the maximum number of days for which an exception for a test result group can be requested. The default value is 365 days.

    **Note:** You can use the `sn_vulc.exception_approval_required` property to disable the exception approval workflow for the test result group if it is not required. By default, this property is enabled and its value is `true`.

**Procedure**

1. Navigate to **System Properties > All Properties**.
2. On the System Properties page, search for `sn_vulc.exception_max_request_days`.
3. Click on the property name to open the System Property record.
4. To be able to edit this record, ensure that Configuration Compliance is selected as the current application.
5. Enter a positive **Value** and click **Update**. The record is updated and saved.

**Add an exception approver for Configuration Compliance**

Add users to the approver groups so that you can request an exception for a test result group in Configuration Compliance.

**Before you begin**
Role required: sn_vulc.admin
About this task
An exception request for a test result group is approved using the default two-level approval workflow. Adding users to the first-level group is mandatory. If there are no users in the second level, the request is automatically approved after the first-level approval.

⚠️ Note: If there's no first-level approver, an exception can't be requested.

Procedure
1. Navigate to **System Security > Users and Groups > Groups**.
2. In the Name column, search for **Exception**, and click **Exception Approver - Level 1 CC**.
3. On the Group Exception Approver - Level 1 CC form, navigate to **Group Members > New** (or **Edit**).
4. On the form, fill in the fields.

### User form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>Unique identifier for the user.</td>
</tr>
<tr>
<td>First name</td>
<td>User's first name.</td>
</tr>
<tr>
<td>Last name</td>
<td>User's last name.</td>
</tr>
<tr>
<td>Title</td>
<td>User's job title. Enter a title or job description, or select one from the list.</td>
</tr>
<tr>
<td>Department</td>
<td>User's department.</td>
</tr>
<tr>
<td>Password</td>
<td>Password assigned to the user. This password can be permanent or temporary.</td>
</tr>
<tr>
<td>Password needs reset</td>
<td>Option to enable the user to reset the password to ensure security.</td>
</tr>
<tr>
<td>Locked out</td>
<td>Option to lock the user out of the instance and terminate all the user's active sessions. The system prevents users with the admin role from locking themselves out.</td>
</tr>
<tr>
<td>Active</td>
<td>Option to make this user active. Only you can see an inactive user in these areas:</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>• Lists of users</td>
<td></td>
</tr>
<tr>
<td>• Selection list on reference fields (magnifying glass icon)</td>
<td></td>
</tr>
<tr>
<td>• Auto-complete list that appears when you type into a reference field</td>
<td></td>
</tr>
<tr>
<td>Web service access only</td>
<td>Option to designate this user as a non-interactive user.</td>
</tr>
<tr>
<td>Internal Integration User</td>
<td>Option to designate this user as an internal integration user.</td>
</tr>
<tr>
<td>Email</td>
<td>User's email address.</td>
</tr>
<tr>
<td>Language</td>
<td>User's preferred language.</td>
</tr>
<tr>
<td>Calendar integration</td>
<td>Calendar used to manage the work schedule. For example, Outlook.</td>
</tr>
<tr>
<td>Time zone</td>
<td>Time zone for this user's location.</td>
</tr>
<tr>
<td>Date format</td>
<td>User's preferred format for dates.</td>
</tr>
<tr>
<td>Business phone</td>
<td>User's business phone.</td>
</tr>
<tr>
<td>Mobile phone</td>
<td>User's mobile phone.</td>
</tr>
<tr>
<td>Photo</td>
<td>Photo that you can upload by clicking on <strong>Click to add...</strong></td>
</tr>
</tbody>
</table>

5. Click **Submit**.

6. **Optional:** Repeat steps 1–5 to create an Exception Approver - Level 2 CC.

1. **Note:** While creating a second level approver, select **Exception Approver - Level 2 CC**

7. **Optional:** If you select **Edit**, move users from the **Collection** to the **Group Members** panel and click **Save**.
   The approver must navigate to **Configuration Compliance > My Approvals** and approve requests.

**Configuration Compliance criticality maps**

Configuration Compliance criticality mapping transforms criticality fields from the source to fields in Configuration Compliance.
The Configuration Compliance base system ships with a standard Qualys Cloud Platform to standard ServiceNow mapping. Creating or editing a criticality map is intended only for customized or non-standard third-party mappings in your environment.

Create a Configuration Compliance criticality map

Configuration Compliance criticality mapping provides a transform map for third-party source criticality fields to recognizable fields in Configuration Compliance severity.

Before you begin
Role required: sn_vulc.admin

Procedure
1. Navigate to Configuration Compliance > Administration > Criticality Mapping.
2. Click New.
3. Fill in the fields on the form, as appropriate.

Field mapping

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>The name of the source for the criticality mapping.</td>
</tr>
<tr>
<td>Source value</td>
<td>The source criticality value.</td>
</tr>
<tr>
<td>Target value</td>
<td>The target value. Choices are:</td>
</tr>
<tr>
<td></td>
<td><strong>Critical</strong></td>
</tr>
<tr>
<td></td>
<td>The configuration issue associated with the control is causing a disruption</td>
</tr>
<tr>
<td></td>
<td>to one or more business-critical CIs.</td>
</tr>
<tr>
<td></td>
<td><strong>High</strong></td>
</tr>
<tr>
<td></td>
<td>The configuration issue associated with the control is a threat, but is</td>
</tr>
<tr>
<td></td>
<td>not causing a shutdown of critical network resources.</td>
</tr>
<tr>
<td></td>
<td><strong>Moderate</strong></td>
</tr>
<tr>
<td></td>
<td>The configuration issue associated with the control is a risk, but is not</td>
</tr>
<tr>
<td></td>
<td>an immediate threat.</td>
</tr>
<tr>
<td></td>
<td><strong>Low</strong></td>
</tr>
</tbody>
</table>
### Field | Description
---|---
**The configuration issue associated with the control is a low-level threat and can be ignored in favor of CIs that are at greater risk.**

**Minor**
The configuration issue associated with the control is a minor risk and can be ignored if necessary.

4. Click **Submit**.

### Configuration Compliance discovery

Configuration Compliance data is imported from third-party SCA scanner applications. They structure groups of software and hardware tests into data records to expedite conducting assessments.

When an import is complete, an event is sent to indicate end-of-import actions. For every active test result group, the following actions are taken:

- Resolved groups with failed results return to the **Awaiting Implementation** state.
- Test result groups where all results have passed, are **Closed**.
- The state of test results that are in active groups are updated.
- The flag indicating whether a result is part of an active group is updated.

### View Configuration Compliance policies

Once you have imported the results of a third-party scan into your instance, you can see your test compliance at the policy level. Use this view before an audit of that policy and any associated test records.

**Before you begin**
Role required: `sn_vulc.read` and `sn_vulc.remediation_owner` to view

**About this task**
Policies are imported records and uneditable inside Configuration Compliance.

**Procedure**
1. Navigate to Configuration Compliance > Policies.
2. Click the Short description of the policy you want to view.
## Configuration Compliance policy form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>System name of the third-party scanner, or the name entered in the ServiceNow plugin for the API that is used to communicate with Configuration Compliance.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Identifier assigned to this policy by the third-party scanner.</td>
</tr>
<tr>
<td>Short description</td>
<td>Summary description or title assigned to the policy in the third-party scanner application.</td>
</tr>
<tr>
<td>Description</td>
<td>Detailed description of the policy as defined in the third-party scanner application.</td>
</tr>
<tr>
<td>Technologies</td>
<td>List of technologies associated with the policy in the third-party scanner application.</td>
</tr>
<tr>
<td>Source created</td>
<td>Date the policy was defined in the third-party scanner application.</td>
</tr>
<tr>
<td>Source updated</td>
<td>Date the policy was last modified in the third-party scanner application.</td>
</tr>
<tr>
<td>Tests</td>
<td>List of tests that reference this policy. Imported from the third-party scanner. You can navigate the list to detailed information about a specific test, if necessary.</td>
</tr>
</tbody>
</table>

## Remediation Status (Version 12.0)

**Excludes Deferred**  
These values do not include CIs from deferred test results.

- **Remaining CIs**: The number (count) of configuration items (CIs) with active test results (any state other than **Closed**) for this policy.
## Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• % CIs remediated</td>
<td>Percent of compliant CIs for this policy. This number excludes CIs with deferred test results.</td>
</tr>
<tr>
<td>• Total CIs</td>
<td>The total number of CIs impacted by this policy. This count excludes deferred test results.</td>
</tr>
<tr>
<td>Includes Deferred</td>
<td>The values represent CIs from all active test results (any state other than Closed).</td>
</tr>
<tr>
<td>• Remaining CIs</td>
<td>The number of unique CIs associated with one or more test results not closed to which this policy has been applied.</td>
</tr>
<tr>
<td>• % CIs remediated</td>
<td>The percent of compliant CIs for this policy.</td>
</tr>
<tr>
<td>• Total CIs</td>
<td>Total number of CIs impacted by this policy.</td>
</tr>
</tbody>
</table>

Starting with version 12.0, to update these values on-demand, below the Remediation status tab, click the Update Status Related link. A message is displayed that indicates the data is being refreshed. Click the View status link to view progress on the update. After a few moments, any data that has changed or been updated since the last scheduled job are refreshed on the record. Updated field values are refreshed.

**View Configuration Compliance authoritative sources**

Use this module to view summary information about each authoritative source and to research the source publications that were used to create the record.

**Before you begin**

Role required:

- sn_vulc.admin to update
- sn_vulc.remediation_owner to view
Procedure

1. Navigate to **Configuration Compliance > Supporting Data > Authoritative Sources**.

2. Click the **Short description** of the authoritative source you want to view.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>ID number assigned to the authoritative source by your instance during the import process.</td>
</tr>
<tr>
<td>Source</td>
<td>System name of the third-party scanner application, or the name entered in the scanner plugin for the API that communicates with Configuration Compliance.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Identifier assigned to the authoritative source by the third-party scanner.</td>
</tr>
<tr>
<td>Short description</td>
<td>Name given to this authoritative source in the third-party scanner.</td>
</tr>
<tr>
<td>Publisher</td>
<td>Name of the organization or publication that was the original source of information for this authoritative source.</td>
</tr>
<tr>
<td>Citations</td>
<td>List of cited information about the test results. Imported from the third-party scanner. You can navigate this list to detailed information about a specific test, if necessary.</td>
</tr>
</tbody>
</table>

3. [Optional] Add a **Publisher**.

4. Click **Update**.

5. You can delete this record by clicking **Delete**.

   Removes the record from your instance. If it is still in use in your third-party integration, it returns in the next import.
View Configuration Compliance Technologies

Use this module to view summary information about each authoritative sources and citation (also known, in Qualys, as a framework). You can research the source publications that were used to create the record.

Before you begin
Role required:
- sn_vulc.admin to update
- sn_vulc.remediation_owner to view

Procedure
1. Navigate to Configuration Compliance > Supporting Data > Technologies.
2. Click the Short description of the authoritative source you want to view.

Configuration Compliance authoritative sources form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>ID number assigned to the authoritative source by your instance during the import process.</td>
</tr>
<tr>
<td>Source</td>
<td>System name of the third-party scanner, or the name entered in the third-party scanner plugin for the API that communicates with Configuration Compliance.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Identifier assigned to the authoritative source by the third-party scanner.</td>
</tr>
</tbody>
</table>

3. You can delete this record by clicking Delete.
   Removes the record from your instance. If it is still in use in your third-party integration, it returns in the next import.

View Configuration Compliance tests

Use this module to research detailed information about these tests. Included are the expert source citations that were used when creating them, the third-party configuration policies in which they are used, and the results obtained from the scan.
Before you begin
Role required:
• sn_vulc.admin to update
• sn_vulc.remediation_owner to view

Procedure
1. Navigate to Configuration Compliance > Controls.
2. Starting with v12.0, navigate to Configuration Compliance > Tests
3. Open the control you want to view.

Starting with version 12.0, to update these values on-demand, below the Remediation status tab, click the Update Status Related link. A message is displayed that indicates the data is being refreshed. Click the View status link to view progress on the update. After a few moments, any data that has changed or been updated since the last scheduled job are refreshed on the record. Field values such as the Risk Score, Risk Rating, Remediation target date, State, and the fields on the Remediation Status tab are refreshed.

<table>
<thead>
<tr>
<th><strong>Configuration Compliance test form fields</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
</tr>
<tr>
<td>Number</td>
</tr>
<tr>
<td>Source</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Source ID</td>
</tr>
<tr>
<td>Version 10.3: Risk score</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Field</td>
</tr>
<tr>
<td>-----------------------------</td>
</tr>
<tr>
<td>business criticality and test criticality values of test results.</td>
</tr>
<tr>
<td>Version 10.3: Risk rating</td>
</tr>
<tr>
<td>Result</td>
</tr>
<tr>
<td>Criticality</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Field</td>
</tr>
<tr>
<td>--------------------------------------</td>
</tr>
<tr>
<td>Low</td>
</tr>
<tr>
<td>Minor</td>
</tr>
<tr>
<td>Category</td>
</tr>
<tr>
<td>Sub-category</td>
</tr>
<tr>
<td>Technologies</td>
</tr>
<tr>
<td>Source created</td>
</tr>
<tr>
<td>Source updated</td>
</tr>
<tr>
<td>Short description</td>
</tr>
</tbody>
</table>

**Remediation Status (v 12.0)**

Includes Deferred | These values include deferred test results.

- **Open test results**: The number (count) of all active (any state other than Closed) test results for this test result group.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>% Test results remediated</td>
<td>The percent of remediated test results for this test result group.</td>
</tr>
<tr>
<td>Total test results</td>
<td>The total number of test results for this test result group.</td>
</tr>
</tbody>
</table>

Excludes Deferred These values do not include deferred test results.

- **Open test results**: The number (count) of active (any state other than Closed) test results for this configuration test.
- **% Test results remediated**: The percent of remediated test results for this test result group.
- **Total test results**: The total number of test results for this test result group.

Description Long description of the test. For the Qualys Vulnerability Integration, this field defaults to the contents of the Qualys Cloud Platform cover page.

Remediation Steps instructions describing how to remediate the non-compliance.

**Related Tabs**

<table>
<thead>
<tr>
<th>Citations</th>
<th>List of citations entered for each authoritative source associated with the test.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies</td>
<td>List of Configuration Compliance policies that use this test.</td>
</tr>
<tr>
<td>Test Results</td>
<td>List of CIs affected by the configuration issue or issues associated with this test. You can access individual tests, ServiceNow configuration items, or the list of affected technologies, if necessary.</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
GRC Policy Statements | If the GRC Policy and Compliance Management plugin is installed, this tab contains the related GRC policy. You can edit this list to add or remove policy statements. For more information, see Continuous monitoring for GRC assessment and policy.

Resolving Configuration Compliance import issues
Resolve issues with third-party integration import.

Import issue resolution

<table>
<thead>
<tr>
<th>Issue</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test results are missing</td>
<td>Check the <strong>Start Time</strong> on the <strong>Qualys PC Results</strong> integration. It might not be set back far enough. See <strong>Modify Qualys PC Results start date</strong>.</td>
</tr>
<tr>
<td>The integration is failing</td>
<td>Check the <strong>Vulnerability Integration Run</strong> status. Individual integration process entries hold the imported XML, which can be examined for unexpected information. Navigate to <strong>Qualys Vulnerability Integration &gt; Primary Integrations &gt; QualysPC Results &gt; Vulnerability Integration Runs</strong> related tab. Choose the latest run. Examine the status and notes of the entries in the related list <strong>Vulnerability Integration Process</strong> for anomalies.</td>
</tr>
</tbody>
</table>

Modify Qualys PC Results start date
If data is missing for the start date in the Qualys PC Results import, it can be modified.

**Before you begin**
Role required: sn_vul_qualys.admin
Procedure

1. Navigate to Qualys Vulnerability Integration > Administration > Primary Integrations.
2. Click Qualys PC Results integration.
3. Click Integration Details.
4. Set the Start time field to a value in the past, so all scanned and detected test results, since that time, are detected.

   Note: If the date is left empty, no data is returned on the first run. Set the value to a maximum of a month in the past. This setting keeps large amount of data from exceeding the Qualys API rate limitations, as well as triggering execution timeouts.

5. Click Submit or Update.
6. [Optional] Click Execute Now to run immediately.

Configuration Compliance correlation

Configuration Compliance provides prioritization and test result grouping to aid remediation of non-compliance issues.

Asset-Centric Prioritization

Configuration scans can produce large number of findings. Prioritize findings for greatest risk reduction. Priority includes both configuration test criticality and asset criticality. Configuration test result priority is expressed as a 0–100 scale risk score. Calculator groups compute risk score and can be customized.

When the third-party import is complete, Configuration Compliance sends an event to indicate end-of-import actions. For every active result group, the following actions are taken:

- Resolved groups with failed results return to the Awaiting implementation state.
- Groups where all results passed are Closed.
- The state of test results that are in active groups is updated.
- The flag indicating whether a result is part of an active group is updated.

Test Result Groups order of precedence

When test results belong to more than one group, the State of a test result is derived according to an order of precedence.
The State and Resolution fields in the Configuration Test form and the Result field in the Test Result form, are calculated following this order of precedence.

Tip:

The group membership precedence only applies to items where the item did not pass the configuration test. Passed items are always in the Closed-Fixed state.

The Result value determines the state. We ignore groups in the Closed-Fixed and Closed-Canceled state. The item state is computed from the states of all other test result groups it belongs to or is set to Open, if no other group exists for the item.

<table>
<thead>
<tr>
<th>Order of Precedence for Test Results belonging to multiple Test Result Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group A</strong></td>
</tr>
<tr>
<td><strong>Open</strong></td>
</tr>
<tr>
<td>Open</td>
</tr>
<tr>
<td>Under Investigation</td>
</tr>
<tr>
<td>Awaiting Implementation</td>
</tr>
<tr>
<td>Resolved</td>
</tr>
<tr>
<td>Deferred</td>
</tr>
<tr>
<td>Closed-Invalid</td>
</tr>
</tbody>
</table>

### Test Result Groups creation

Configuration Compliance Test Result Groups are created manually.

There are two ways to create and populate **Test Result Groups**.

- From the **Test Results Groups** module and using filters that automatically populate the **Test Results** tab.

  This way is good for when you know what filtering you want to use. For example, capturing all failed test results that are moderate and higher criticality, affect the windows-based infrastructure, and apply only to the SAP supply chain application.

- By selecting test results in the **Test Results** list and creating a group from the **Actions on selected rows...** menu.

  This method is good for results that are not easily filtered, or situations where you want to specify test results for remediation. For example, outliers that have nothing in common.
Note: If you create a group from the Test Results list and you later decide to use a filter for that group, your original entries are removed and replaced by the filter results.

Ungrouped Test Results

Ungrouped Test Results contain all non-pass test results that are not members of an active (non-Closed) group. This module is updated after every import and whenever test results are added or removed from a group.

View a test result group

You can view, or, alternatively, create a test result group and perform remediation.

Before you begin

Role required:

• sn_vulc.admin to update or create
• sn_vulc.remediation_owner to view

Procedure

1. Navigate to Configuration Compliance > Test Result Groups.
2. From the list, click the record you want to view.
3. Alternatively, click New to create a new test result group and fill in the fields.

Configuration Compliance Test Result Group form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>The automatically generated number for this record.</td>
</tr>
<tr>
<td>State</td>
<td>Progress status of the group.</td>
</tr>
<tr>
<td></td>
<td>• Open</td>
</tr>
<tr>
<td></td>
<td>• Under investigation</td>
</tr>
<tr>
<td></td>
<td>• Awaiting Implementation</td>
</tr>
<tr>
<td></td>
<td>• Deferred</td>
</tr>
<tr>
<td></td>
<td>• Resolved</td>
</tr>
<tr>
<td></td>
<td>• Closed</td>
</tr>
<tr>
<td>Risk score</td>
<td>This score is the rolled-up value of the risk scores for all the active test</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>results in a test result group. This score changes as test results are remediated in the test result group.</td>
</tr>
<tr>
<td>Assignment group</td>
<td>Group selected to work on this test result group.</td>
</tr>
<tr>
<td>Risk rating</td>
<td>The amount of risk a failed test result poses to your system. It is based on a range of risk scores on a 1-5 numeric scale that rates risks as Critical (1) to None (5).</td>
</tr>
<tr>
<td>Assigned to</td>
<td>Individual from the selected assignment group that works on this set of tasks.</td>
</tr>
<tr>
<td>Remediation target</td>
<td>Date by which the test results should be remediated, since first identified.</td>
</tr>
<tr>
<td>Created</td>
<td>The date and time this test result group was created.</td>
</tr>
<tr>
<td>Remediation status</td>
<td>Status of the remediation for the group. It is determined by the test result with the nearest due date.</td>
</tr>
<tr>
<td></td>
<td>For open groups states include:</td>
</tr>
<tr>
<td></td>
<td>• In-flight</td>
</tr>
<tr>
<td></td>
<td>• Approaching Target</td>
</tr>
<tr>
<td></td>
<td>• Target Missed</td>
</tr>
<tr>
<td></td>
<td>For closed groups states include:</td>
</tr>
<tr>
<td></td>
<td>• No Target</td>
</tr>
<tr>
<td></td>
<td>• Target Met</td>
</tr>
<tr>
<td></td>
<td>• Target Missed</td>
</tr>
<tr>
<td></td>
<td>For calculated remediation target dates, if the test result group is closed, the overall remediation status of all of the closed test results is shown in the test result group. Those determine whether the group met its date or not.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>A closed test result group remediation Status is <strong>No Target</strong> if none of its closed results had a remediation target date. It is <strong>Target Missed</strong> if any of its closed results missed their target date. It is <strong>Target Met</strong> if at least one closed result met its target and none of the others missed it.</td>
<td></td>
</tr>
<tr>
<td><strong>Updated</strong></td>
<td>The date and time this record was last modified.</td>
</tr>
<tr>
<td><strong>Short description</strong></td>
<td>Brief description of this test result group.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Long description of the test result group that includes the list of software associated with this test result group.</td>
</tr>
<tr>
<td><strong>Test</strong></td>
<td>The configuration test associated with this test result group.</td>
</tr>
<tr>
<td><strong>Remediation Status (Version 12.0)</strong></td>
<td>These values do not include deferred test results.</td>
</tr>
<tr>
<td><strong>Excludes Deferred</strong></td>
<td>The number (count) of active (any state other than <strong>Closed</strong>) test results for this test result group.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Open test results</strong>: The number (count) of active (any state other than <strong>Closed</strong>) test results for this test result group.</td>
</tr>
<tr>
<td></td>
<td>• <strong>% Test results remediated</strong>: The percent of remediated (closed) test results for this test result group.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Total test results</strong>: The total number of test results for this test result group.</td>
</tr>
<tr>
<td><strong>Includes Deferred</strong></td>
<td>The values represent all active test results (any state other than <strong>Closed</strong>).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>• <strong>Open test results</strong>: The number (count) of active (any state other than Closed) test results for this test result group.</td>
<td></td>
</tr>
<tr>
<td>• <strong>% Test results remediated</strong>: The percent of remediated (closed) test results for this test result group.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Total test results</strong>: The total number of test results for this test result group.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group Configuration</th>
<th>The type of filtering used to select the test results for the test result group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grouping method</td>
<td>Name of method used.</td>
</tr>
<tr>
<td>Group rule</td>
<td>Name of the group rule used.</td>
</tr>
<tr>
<td>Notes</td>
<td>System notes associated with the record.</td>
</tr>
</tbody>
</table>

**Related Links**

- **Version 12.0: Update status link.**
  Update the values on the test result record on-demand. View any data that has changed or been updated since the last scheduled job.

<table>
<thead>
<tr>
<th>Test Results</th>
<th>The test results in this test result group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change requests (v 12.0)</td>
<td>The list of change requests associated with this test result group.</td>
</tr>
<tr>
<td>State Change Approvals (v 12.0)</td>
<td>Status and states of change request approvals associated with this test result group.</td>
</tr>
</tbody>
</table>

**View Configuration Compliance test results**

View Configuration Compliance test results for auditing and remediation.

**Before you begin**

Role required:
• sn_vulc.read to view
• sn_vulc.remediation_owner to view and update
• sn_vulc.admin to delete

Procedure
1. Navigate to Configuration Compliance > Test Results.
2. Open the control you want to view.

Configuration Compliance test results form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>The number assigned to the test during the import process.</td>
</tr>
<tr>
<td>Source</td>
<td>The system name of the third-party SCA application, or the name entered in the application plugin for the API that is used to communicate with Configuration Compliance.</td>
</tr>
<tr>
<td>Source ID</td>
<td>The identifier assigned to the control by the SCA application.</td>
</tr>
<tr>
<td>Result</td>
<td>Passed, Failed, Error, or Unknown. Import from Qualys.</td>
</tr>
<tr>
<td>Risk score</td>
<td>Calculator result for this test.</td>
</tr>
<tr>
<td>Version 10.3: Risk rating</td>
<td>Based on a range of risk scores on a 1-5 numeric scale that rates overall risk based on a range of risk scores as 1 - Critical to 5 - None. This field replaces the Priority field in previous versions.</td>
</tr>
<tr>
<td>State</td>
<td>Calculated from the test result groups that the test result belongs to. If the test result belongs to multiple groups, an order of precedence is applied to determine state.</td>
</tr>
<tr>
<td>Resolution</td>
<td>Calculated from the test result groups that the test result belongs to. If the test result belongs to multiple</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>First seen</td>
<td>Date first imported into Configuration Compliance.</td>
</tr>
<tr>
<td>Last seen</td>
<td>Date last imported into Configuration Compliance.</td>
</tr>
<tr>
<td>Test</td>
<td>Name of the test.</td>
</tr>
<tr>
<td>Configuration item</td>
<td>Name of the CI attached to the test.</td>
</tr>
<tr>
<td>Technology</td>
<td>Software version running on the CI.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the test</td>
</tr>
<tr>
<td>Expected Values</td>
<td>Expected values configured in Qualys and imported by Configuration Compliance. This value is a Boolean expression that when evaluated to true makes the test result <strong>Passed</strong>. The expression can be a combination of logical, set, or regular expression operators.</td>
</tr>
<tr>
<td>Actual Values</td>
<td>Values returned by the test. These values are plugged into the expected values Boolean expression to determine if the result should pass or fail. They are imported from Qualys.</td>
</tr>
<tr>
<td>Remediation</td>
<td>Remediation instructions.</td>
</tr>
<tr>
<td>Related Tabs</td>
<td></td>
</tr>
<tr>
<td>Test Result Groups</td>
<td>Test result groups associated with this test result.</td>
</tr>
<tr>
<td>Test Result History</td>
<td>Related list of test results that show the history of pass/fail results for the same CI/technology/test.</td>
</tr>
</tbody>
</table>
Test Results fields
Test results are automatically created during third-part vulnerability integration imports.

Configuration Compliance does not create or update the test results, but imports them as part of a third-party integration. Once they are viewable in Configuration Compliance, they are remediated using Test Result Groups.

### Test results fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Number assigned to the test result during the import process.</td>
</tr>
<tr>
<td>Source</td>
<td>System name of the third-party integration application, or the name entered in the application for the API that is used to communicate with Configuration Compliance.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Identifier assigned to the test result by the third-party integration.</td>
</tr>
<tr>
<td>Risk Score</td>
<td>Score based on the Criticality value of the test. If you do not have installed and configured, a middle value of 50 is used.</td>
</tr>
<tr>
<td>Resolution</td>
<td>Resolution of the test result, calculated from associated groups.</td>
</tr>
<tr>
<td>Result</td>
<td>Status of the scan. Pass or Fail. If this test belongs to multiple test result groups, then its state is determined following an order of precedence.</td>
</tr>
<tr>
<td>State</td>
<td>State of the test result, calculated from associated groups.</td>
</tr>
<tr>
<td>Assignment group</td>
<td>Group selected to work on this test result.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>Individual from the selected assignment group to work on this test result.</td>
</tr>
<tr>
<td>Assignment type</td>
<td>Type of assignment. Choices are:</td>
</tr>
<tr>
<td></td>
<td>• Rule</td>
</tr>
<tr>
<td></td>
<td>• Manual</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assignment rule</td>
<td>Which assignment rule was used with this test result, when applicable.</td>
</tr>
<tr>
<td>First seen</td>
<td>Time and date the test result was first seen.</td>
</tr>
<tr>
<td>Last seen</td>
<td>Time and date the test result was last seen.</td>
</tr>
<tr>
<td>Test</td>
<td>The control that this result belongs to.</td>
</tr>
<tr>
<td>Configuration item</td>
<td>Configuration item associated with this test result.</td>
</tr>
<tr>
<td>Technology</td>
<td>Technology associated with this test result.</td>
</tr>
<tr>
<td>Description</td>
<td>Detailed description of the test result as defined in the third-party scanner application.</td>
</tr>
<tr>
<td>Expected Values</td>
<td>Description and expected values as defined in the third-party scanner application.</td>
</tr>
<tr>
<td>Expected values</td>
<td>Description and expected values as defined in the third-party scanner application.</td>
</tr>
<tr>
<td>Actual Values</td>
<td>Description and actual values as defined in the third-party scanner application.</td>
</tr>
<tr>
<td>Actual values</td>
<td>Description and actual values as defined in the third-party scanner application.</td>
</tr>
<tr>
<td>Remediation</td>
<td>Remediation action as defined in the third-party scanner application.</td>
</tr>
<tr>
<td>Remediation</td>
<td>Remediation action as defined in the third-party scanner application.</td>
</tr>
</tbody>
</table>

The following are the vulnerable items related lists.

<table>
<thead>
<tr>
<th>Related List</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Result Groups</td>
<td>Test Result Groups associated with this test result.</td>
</tr>
<tr>
<td>Test Result History</td>
<td>List of past records containing different results.</td>
</tr>
</tbody>
</table>

**Configuration Compliance reporting**

The Configuration Compliance homepage provides an executive view into policies, CIs, tests, and test results, helping security staff pinpoint areas of concern quickly. Configuration Compliance significance charts can be added.
as needed. You can also return Configuration Compliance-related information using the global search feature.

In each chart, you can point to any part of a chart (bar, pie, data point) to view general data specific to that part of the chart. If you click any part of a report, a list opens to provide detailed information.

Note: Anyone can view the dashboard. Anyone in the sn_vulc.write or sn_vulc.admin role can create and edit a dashboard. Only sn_vulc.admin can delete a dashboard.

**Version 10.3 Vulnerability Overview reports**

<table>
<thead>
<tr>
<th><strong>Test Results by Compliance</strong></th>
<th><strong>Policies</strong></th>
<th><strong>Tests</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Passed = 1,657</td>
<td>8</td>
<td>2,521</td>
</tr>
<tr>
<td>Failed = 969</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Failed Test Results by Risk Rating</strong></th>
<th><strong>Failed Test Results by Technology</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>3 - High = 117</td>
<td>Windows Server 2012 R2 = 17...</td>
</tr>
<tr>
<td>4 - Low = 285</td>
<td>Windows 2008 Server = 798</td>
</tr>
<tr>
<td>3 - Medium = 567</td>
<td></td>
</tr>
</tbody>
</table>
Version 10.3 Vulnerability Overview reports

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Results by</td>
<td>Donut</td>
<td>Displays the number of open tests that have</td>
</tr>
<tr>
<td>Compliance</td>
<td></td>
<td>passed or failed.</td>
</tr>
<tr>
<td>Polices</td>
<td>Number</td>
<td>Number of policies with failed test results.</td>
</tr>
<tr>
<td>Tests</td>
<td>Number</td>
<td>Number of tests with failed test results.</td>
</tr>
<tr>
<td>Hosts</td>
<td>Number</td>
<td>Number of hosts with failed test results.</td>
</tr>
<tr>
<td>Test Results</td>
<td>Number</td>
<td>Displays the number of test results.</td>
</tr>
</tbody>
</table>
### Version 10.3 Vulnerability Overview reports (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed Test Results by Risk Rating</td>
<td>Donut</td>
<td>Displays the number of failed tests by risk rating.</td>
</tr>
<tr>
<td>Failed Test Results by Technology</td>
<td>Donut</td>
<td>Displays models with failed tests.</td>
</tr>
<tr>
<td>Failed Test Results by Category</td>
<td>Bar</td>
<td>Displays categories with the most failed test results.</td>
</tr>
<tr>
<td>Open Test Result by Risk Rating</td>
<td>Bar</td>
<td>Displays the number of open test results by risk rating.</td>
</tr>
<tr>
<td>Version 10.3: Test Result Groups</td>
<td>Chart</td>
<td>Displays Test Result Groups by state and risk rating.</td>
</tr>
</tbody>
</table>
Reports prior to v10.3

Prior to v10.3 Vulnerability Overview reports

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Results by Compliance</td>
<td>Donut</td>
<td>Displays the number of open tests that have passed or failed.</td>
</tr>
<tr>
<td>Polices</td>
<td>Number</td>
<td>Number of policies with failed test results.</td>
</tr>
<tr>
<td>Tests</td>
<td>Number</td>
<td>Number of tests with failed test results.</td>
</tr>
<tr>
<td>Hosts</td>
<td>Number</td>
<td>Number of hosts with failed test results.</td>
</tr>
<tr>
<td>Test Results</td>
<td>Number</td>
<td>Displays the number of test results.</td>
</tr>
<tr>
<td>Failed Test Results by Criticality</td>
<td>Donut</td>
<td>Displays the number of failed tests by risk score.</td>
</tr>
</tbody>
</table>
Prior to v10.3 Vulnerability Overview reports (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed Test Results by Technology</td>
<td>Donut</td>
<td>Displays models with failed tests.</td>
</tr>
<tr>
<td>Failed Test Results by Category</td>
<td>Bar</td>
<td>Displays categories with the most failed test results.</td>
</tr>
<tr>
<td>Risk Score Distribution</td>
<td>Bar</td>
<td>Displays the number of failed test results by risk score.</td>
</tr>
<tr>
<td>Test Result Groups</td>
<td>Chart</td>
<td>Displays Test Result Groups by state and criticality.</td>
</tr>
</tbody>
</table>

**Configuration Compliance remediation**

Configuration Compliance remediation is primarily a manual process augmented by scheduled jobs (integrations), test result group tasks, workflows, and change requests.

Individual test failures are remediated from test result groups using change requests.

Starting with v12.0 of Configuration Compliance, the states of test result groups automatically transition as associated change requests move through their life cycles with State synchronization between change requests and test result groups (v 12.0). Users with the itil role can create and manage change requests directly from test result groups.

**Note:** Starting with v12.0, you can still manually move change requests and test result groups through the states of their life cycles on their respective records. If state synchronization is enabled, when the system registers that a change request associated with a test result group has changed its state, or you add a change request or remove it from a test result group, state synchronization potentially can override your manual intervention.

Prior to v12.0, with the sn_vulc.remediation_owner role, you can reassign or modify the State fields manually on test results and test result groups that are assigned to you or to your assignment groups.

**Create a change request in Configuration Compliance (v 12.0)**

You can create a change request from a test result group (CRG) in the Configuration Compliance application.
Before you begin
As an IT or remediation specialist, starting with version 12.0 of Configuration Compliance, create a change request (CHG) directly from a test result group for all the test results in the group. Create a change request with pre-populated information to expedite your investigation for vulnerabilities that require manual intervention.

Role required: user with the itil role
You can create, approve, implement, review, and close change requests directly from test result groups that are assigned to you. You can create three types of change requests with pre-populated information from a test result group:

**Standard**
A pre-authorized change that is low risk, relatively common, and follows a specified procedure or work instruction.

**Normal**
Normal change requests follow a prescriptive process which requires two levels of approval before being implemented, reviewed, and closed.

**Emergency**
A change to resolve a major incident.

The following image illustrates the basic flow for creating a change request from a test result group. The detailed steps for this flow follow the image.
Procedure

1. Navigate to Configuration Compliance > Test Result Groups > My Open Groups.
   The list of test result groups assigned to your groups is displayed.

2. In the Number column, click the test result group you want to create a change request for.
   You can create change requests from test result groups in any states other than Closed or In review.
   The test result group record is displayed.

3. In the upper right of the record, click Create Change.
   The change request form is displayed.

4. Fill in the fields.
   a. From the list of the Applies to field, choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All active test results in this group</td>
<td>If selected, all active test results from this test result group with a state other than Closed are added automatically.</td>
</tr>
</tbody>
</table>
Option | Description  
--- | ---  
| |  

cally to the change request after you click **Create Change**.  
| |  
If selected, the condition builder is displayed. Enter filter criteria to identify the test results that you want for the new change request.  
| **All active test results in this group matching a set of conditions** | An example of a filter you might create would locate only test results from the group that match a specific state and risk score:  
State is **Open** and Risk Score is greater than **50**.  
| |  
5. For the **Add CIs to CR** check box, choose one to continue.  
| **Option** | **Description**  
--- | ---  
| **Check box selected** | Default is selected. If the check box is selected, any configuration items (CIs) that belong to active test results from this test result group are added to this change request. The test result transitions to **Awaiting Implementation**.  
| **Check box cleared** | Clear the check box if you do not want the CIs from the active test results from this test result group added to the new change request. The test result group remains in its current state.  
| |  
6. From the list for the **Change type** field, choose one to continue.  
| **Option** | **Description**  
--- | ---  
| **Emergency** | A change to resolve a major incident.  
| **Normal** | A change type that is used to implement any change to a service that is not a standard or emergency change.  
| |  
© 2021 ServiceNow, Inc. All rights reserved.  
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard</strong></td>
<td>A pre-authorized, low-risk change request that is frequently implemented. Approved standard change requests can be predefined in a catalog of templates to make accessing and requesting a standard change more efficient. If selected, two fields are displayed. Select one from each list to fill in these fields:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Change category</strong>: Select a category for the change from your existing catalog, for example, Hardware, Server Standard Changes, Software.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Change template</strong>: Select one available template for change requests with pre-defined supporting tasks from your catalog.</td>
</tr>
</tbody>
</table>

For more information on ITSM change request categories, templates, and change types, see [Change types](#).

The feature automatically reads the types of change requests that you set up in your catalog in ITSM Change Management. For example, if you change the name for your Standard change requests in ITSM from Standard to Pre-approved, your new name is automatically displayed in the Change type list on the Create change request form.

7. The fields in the Change Request Preview section of the form are pre-populated with information from the test result group. If required, edit these fields.

8. Click **Create Change**.

The change request is displayed. On the Affected CIs related list, the CIs from the test results that matched your criteria are displayed. If the change request requires approval, the **Request Approval** button is displayed.

After the change request is created, the test result group moves to the **Awaiting Implementation** state. After the change request for this test result group is resolved, if there are no other open change requests associated with this test result group, the test result group is also moved to the **Resolved** state.
See State synchronization between change requests and test result groups (v 12.0) for more information.

**Note:** You can still manually move change requests and test result groups through the states of their life cycles on their respective records with state synchronization enabled, but when the system registers that a change request has changed its state, or you add a change request or remove it from a test result group, state synchronization potentially can override your manual intervention. However, change requests states do not automatically move the test result group from the Closed or Deferred states.

**Associate a test result group to an existing change request (v 12.0)**

Associate a test result group in Configuration Compliance application to an existing change request.

**Before you begin**

As an IT or remediation specialist, starting with version 12.0 of Configuration Compliance, avoid creating duplicate change requests (CHG) as you work to resolve your test result groups by associating a test result group (CRG) to a change request that is already available in your instance.

You can associate test result groups that are assigned to you or your assignment group to existing change requests directly from the test result group records. The following image illustrates the basic flow for associating an existing change request to a CRG. The detailed steps for this flow follow the image.

**Note:** You can associate an existing change request to a CRG in any state other than Canceled (Open, Under Investigation, Awaiting Implementation, Closed, and Deferred). Change requests, including those closed within the last 90 days, are available to associate from the form. When you associate a change request to an existing CRG, only the active test results and their configuration items are added to the change request.
Role required: a user with the itil role

Procedure

1. Navigate to Configuration Compliance > Test Result Groups > My Open Groups.
   The list of test result groups assigned to your groups is displayed.

2. In the Number column, click the test result group you want to create a change request for.
   The test result group record is displayed.

3. In the upper right of the record, click Create Change.
   The change request form is displayed.

4. Scroll to the Change Requests related list and select it.
   Any change requests associated with the CRG are displayed along with the Add button.

5. Click Add.
   The Add Existing Change Request to Test Result Group dialog is displayed.
6. Click the search icon and select an item from the list. You can filter the list that is displayed to narrow your search.

7. Click Submit.

The CRG is displayed along with a message that indicates the change request was successfully associated to the test result group. Under the change requests related list, the new change request is displayed. The CIs from the test result group are by default added to the change request and are displayed on the Affected CIs related list. You can also add CIs to the change request from this related list. A message indicates the number of test results that have moved to the new group, and the new CRG is displayed.

Note: For under 200 test results, the split operation is done synchronously, and the test results are displayed in the new group.

For over 200 test results, the split operation is done asynchronously in the background, and it may take a few seconds for the test results to appear in the new group. The following message is also displayed: n test results will be moved from CRGxxxxxxx to new test result group GRCxxxxx shortly.

You can associate any change requests to the CRG, with the following exceptions:

- Change requests in the Canceled state.
- Change requests in the Closed state older than 90 days.
- Change requests already associated with the CRG. The system will not permit you to associate a change request that is already associated with the CRG.

After the change request for this test result group is resolved, if there are no other open change requests associated with this test result group, the test result group is also moved to the Resolved state.

Note: You can still manually move change requests and test result groups through the states of their life cycles on their respective records with state synchronization enabled, but when the system registers that a change request has changed its state, or you add a change request or remove it from a test result group, state synchronization potentially can override your manual intervention. However, change requests states do not automatically move the test result group from the Closed or Deferred states.

See State synchronization between change requests and test result groups (v 12.0) for more information.
Split a test result group (v 12.0)

From an existing test result group (CRG) in the Configuration Compliance application, identify a subset of test results that you want to move to a new test result group.

Before you begin

As an IT or remediation specialist, starting with version 12.0 of Configuration Compliance, you can split existing test result groups in the Open, Under Investigation, or Awaiting Implementation states with more than one test result. By creating a new CRG with test results that match specific criteria, you can work with a specific group of test results without impacting the original group.

When you specify the conditions for the test results that you want to move to a new test result group with the condition builder, only the active test results that match your criteria are moved to the new group. You are not required to create change requests (CHGs) when you split a CRG. You have the option to split a CRG at the same time you create a change request, or, you can split a CRG without creating a change request.

The following image illustrates the basic flow for splitting a test result group. The detailed steps for this flow follow the image.

For a test result group in the following states with at least one test result:

- Open
- Under investigation
- Awaiting implementation (or Deferred)

1. Identify a subset of test results and create a new test result group for them

   ![Folder icon]

2. Optionally create a new change request for new group, or associate it with an existing change request

   ![List and plus sign]

3. Monitor the life cycle of the change request

4. When the change request is implemented and in review, the test result group is automatically resolved

   ![Folder icon]
Use cases for splitting test results from existing CRGs into new groups might include the following examples:

- When you want to create a change request or change requests for a split group.
- When you reassign a split group to another user in your assignment group.
- When you request a deferral or exception for a split group because you know that some test results on specific configuration items (CI) cannot be remediated in a given time frame.

Role required: a user with the itil role

Procedure

1. Navigate to **Configuration Compliance > Tests > Test Result Groups > My Open Groups**.
   The list of test result groups assigned to your groups is displayed.

2. In the Number column, click the test result group that you want to split.
   The test result group record is displayed.

3. To create a subset of test results for a new group that matches specific criteria, follow these steps. On the upper right of the record, click **Split Group**.
   You might prefer this method of creating a new group if you are working from a large group with multiple test results.
   The Split test result group form is displayed.

4. With the condition builder displayed, specify the conditions for the test results that you want to move to a new test result group. For example, you may prefer to filter out only test results that match the following conditions:
   - In the **Open** state.
   - Risk scores greater than 75.
   - Result is **Failed**.
   If test results match your filter after you enter the conditions, a message is displayed with the number of test results that match.
   If a message is displayed that no test results match your filter, or, that all your test results match your criteria, adjust the conditions so at least one test result matches your filter criteria.

5. Click **Preview items** to view the matched test results.
   A new window, Test Result Groups, displays the items.

6. To preview details about the test results that match your filter criteria, follow these steps before you click **Split Group** to create the new group. These
details include the assignment group and who the test result is assigned to. Viewing this information on the preview may help ensure that the new group is properly assigned.

a. With the Test Result Groups list displayed in the preview, click an item in the Result column. The Test Result record is displayed.

b. Verify the Assignment group and Assigned to fields are correct.

c. Click Update.

7. When you are ready to create the new group, click Split Group. A message indicates the number of test results that are moved to the new group, and the new CRG is displayed. To help you identify the new group, you might prefer to edit the text in the Short description field and edit the Assignment group or Assigned to fields again, if required.

Note: For under 200 test results, the split operation is done synchronously, and the test results are displayed in the new group.

For over 200 test results, the split operation is done asynchronously in the background, and it may take a few seconds for the test results to appear in the new group. The following message is also displayed: n test results will be moved from CRGxxxxxxx to new test result group GRCxxxxx shortly.

8. Alternatively, you can create a new test result group by selecting test results directly from the Test Results related list on a test result group.

You might prefer this method if you have only a few test results in a group, or you know exactly which tests you want to move to a new group.

a. With the test result group record displayed, scroll to the Test Results related list.

b. In the far left column, select check boxes for the test results you want to create a new CRG for.

c. From the Actions on selected rows list in the lower left of the record, click Split Group.

d. In the Split test result group form that is displayed, to help you identify the new group, you might prefer to edit the text in the Short description field.
e. Click **Split Group**.
A message indicates the number of test results that have moved to the new group, and the new CRG is displayed.

After the change request for this test result group is resolved, if there are no other open change requests associated with this test result group, the test result group is also moved to the **Resolved** state.

**Note:** You can still manually move change requests and test result groups through the states of their life cycles on their respective records with state synchronization enabled, but when the system registers that a change request has changed its state, or you add a change request or remove it from a test result group, state synchronization potentially can override your manual intervention. However, change requests states do not automatically move the test result group from the **Closed** or **Deferred** states.

See **State synchronization between change requests and test result groups (v 12.0)** for more information.

**What to do next**
You can create or associate change requests for your new test result groups.
See **Associate a test result group to an existing change request (v 12.0)** and **Create a change request in Configuration Compliance (v 12.0)**.

**State synchronization between change requests and test result groups (v 12.0)**
Starting with version 12.0 of Configuration Compliance, there is a synchronized relationship between the State fields of test result groups (CRGs) and the State fields of change requests (CHGs) in the Configuration Compliance application.

As a change request moves through its life cycle, it also moves the state of any related test result groups automatically. State synchronization is enabled by a system property by default in your instance when you download the Configuration Compliance application from the ServiceNow Store starting with v12.0.

When state synchronization is enabled, the CHG State field changes the test result group State field automatically in the following cases:
- When a new change request is created for a CRG, if it is not in **Awaiting Implementation**, the CRG state moves forward to **Awaiting Implementation**.

- When an existing change request is associated to a CRG, if it is not in **Awaiting Implementation**, the CRG state moves forward to **Awaiting Implementation**.

- After the tasks on a change request are completed (implemented), and the CHG is moved to the **Review** state, the CRG moves forward to **Resolved**.

For more information and examples of state synchronization, see the following sections.

**Note:** You can still manually move change requests and test result groups through the states of their life cycles on their respective records with state synchronization enabled, but when the system registers that a change request has changed its state, or you add a change request or remove it from a test result group, state synchronization potentially can override your manual intervention. However, change request states do not automatically move the test result group from the **Closed**.

**Forward state synchronization**

The following image illustrates how CHG states automatically move test result group states in a forward life cycle, that is, from **Open** to **Resolved**.

![Diagram](image)

You can create new change requests for any test result group in a state other than **Resolved** or **Closed**. State synchronization automatically moves the CRG bi-directionally through the **Open**, **Under Investigation**, **Awaiting Implementation**, and **Resolved** states. This movement is based on certain values of the state field on the change request. State synchronization between the change request and
the test result group is invoked automatically unless the check box (Add CIs to CR) is displayed on a form and you choose to clear the check box.

The test result group does not move forward to Resolved when a CHG is in its open states. Any CHG in states prior to Review in its life cycle such as, New, Assess, Authorize, Scheduled or Implement, as shown in the preceding figure, are considered open states for the CHG. Open states do not move the state field on the test result group, because investigations or tasks on the CHG are not completed. State synchronization is invoked when a CHG is created for, or associated to, the test result group, or when the state of an existing relationship changes on the CHG. The completed CHG states are Review and successfully Closed. When a CHG is closed successfully, its closed codes are: Successful, or Successful with issues, in which case the test result group moves forward to Resolved.

**Backward state synchronization**

As a CHG is processed during its life cycle, it may be canceled at some point. In this case, if the CHG is Canceled, or Closed (with a close code of Unsuccessful), the test result group automatically moves back to Under Investigation. The test result group moves back to Under Investigation, because there is no active plan to remediate the vulnerability.

If a test result group is in a Resolved state, and you create a new CHG or associate it to an existing CHG in one of the initial open states, the test result group automatically transitions back to Awaiting Implementation. The test result group moves back to this state, because more work is now assigned to the CHG.

**Test result groups with more than one CHG**

If a test result group in Awaiting Implementation has more than one CHG associated with it, state synchronization is based on the status of the CHG in the earliest state of its life cycle. For example, say a test result group has four CHGs associated with it, CHG1, CHG2, CHG3, and CHG4 as shown in the following table.

<table>
<thead>
<tr>
<th>CHG number</th>
<th>CHG state</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Implement</td>
</tr>
<tr>
<td>2</td>
<td>Canceled</td>
</tr>
<tr>
<td>3</td>
<td>Closed (close code of Unsuccessful)</td>
</tr>
<tr>
<td>4</td>
<td>Closed (close code Unsuccessful)</td>
</tr>
</tbody>
</table>
State synchronization between the CHG and the test result group in this case is based on CHG1, which is in the earliest state of the four CHGs, (Implement). In this case, the test result group remains in **Awaiting Implementation**.

In another example, if a test result group is in the **Resolved** state and has an existing CHG that has been implemented and is in the **Review** state, and a new CHG is created, the test result group moves back from **Resolved** to **Awaiting Implementation**. State synchronization is based on the CHG in the **New** state, which is the CHG in the earliest state.

<table>
<thead>
<tr>
<th>CHG number</th>
<th>CHG state</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Review</td>
</tr>
<tr>
<td>2</td>
<td>New</td>
</tr>
</tbody>
</table>

Also, when test result groups have more than one CHG, the state of the test result group transitions automatically in the following cases:

- When a CHG moves forward to **Review**, if all other CHGs associated with the test result group are in **Review** or **Closed** states (with a successful close code), the test result group automatically transitions to **Resolved**. Any other related CHGs that are canceled or closed unsuccessfully are ignored.

- When a CHG moves to **Canceled** or **Closed** (close code of **Unsuccessful**), if all other CHGs associated with the test result group are in the same state, then the test result group automatically transitions back to **Under Investigation**.

For more information about test result group states and what you can do in each state, see **Configuration Compliance states**.

**Create a change request in Configuration Compliance (Prior to v 12.0)**

You can create a change request from a test result group.

**Before you begin**
Role required: sn_vulc.admin

**Procedure**
1. Navigate to **Configuration Compliance > Test Result Groups**.
2. Open the test result group.
i Note: To request a change request, the group must be in the Under Investigation state.

3. Click Create Change.
   A pop-up window containing information about the group appears.

   ![Create Change pop-up window](image)

   The pop-up is pre-populated but you can edit the Short Description and Description fields.

4. Click Submit.
   Change requests are created and appear in the Change Requests related tab on the test result form.

   ![Change Requests tab](image)

   See Process a change request.
Close a test result group (Prior to v 12.0)

If you determine that the issue associated with a test result group can be immediately closed without further analysis, you can use the Close feature.

Before you begin
Role required:
• sn_vulc.admin
• sn_vulc.remediation_owner

⚠️ Note: With the sn_vulc.remediation_owner role, you can reassign or close test result groups that are assigned to you or to your assignment groups.

Procedure
1. Open the test result group record.
2. Click the Close button.
3. Describe why the issue is being closed in the pop-up window.
4. Click Close.

Related information
  Configuration Compliance states
  Requesting and approving an exception for a test result group

You can request to defer the remediation of a test result group for a specified period. Users who are a part of the approver group can approve exception requests.

To request or approve exception requests, see:
• Request an exception for a test result group in Configuration Compliance
• Approve an exception request in Configuration Compliance

⚠️ Note:
Email notifications are sent at every stage of exception management, providing the status and other details of a request. For example, when an exception is requested, the requester receives an email confirming that the request is raised. The approver also receives an email stating that an exception has been requested.
Request an exception for a test result group in Configuration Compliance

Request an exception to defer the remediation of a test result group for a specified period if it cannot be remediated immediately.

Before you begin
Role required: sn_vulc.remediation_owner

Procedure

1. Navigate to **Configuration Compliance > Test Result Groups > All Groups** and select the test result group that you want to request an exception for. The selected group must be in the Open, Under Investigation, or Awaiting Implementation state.

2. On the Test Result Group form, click **Request Exception**.

3. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Until</td>
<td>Date on which the exception request expires. This date must be a valid date in the future. When the exception request expires, the group reverts to its Open state.</td>
</tr>
<tr>
<td>Reason</td>
<td>Select the Reason. Choices are: Risk Accepted, Awaiting Maintenance Window, Fix Unavailable, Mitigating Control in Place, Other</td>
</tr>
<tr>
<td>Additional information</td>
<td>Details that are related to the reason why this request is being made. This required field is to be updated by the remediation owner.</td>
</tr>
</tbody>
</table>

4. Click **Request Approval** to submit the exception request. The state of the test result group changes to In Review. Use the **State Change Approval** tab to track the status of the exception request.
Approve an exception request in Configuration Compliance

Approve exception requests for test result groups that can't be remediated immediately. You must assess these requests for risk and then approve them for deferral until they can be remediated.

Before you begin
Role required: sn_vulc.exception_approver

Procedure
1. Navigate to Configuration Compliance > My Approvals.
2. Select a request from your queue.
3. Approve or reject the request with appropriate comments.

Note: In case of a two-level approval workflow, after the first-level approval, the request is submitted to the second level for further approval. If there are no users in the second level, the request is automatically approved after the first-level approval.

After the request is approved, the test result group moves to a Deferred state. In case of rejection, the test result group reverts to its earlier state.

Configuration Compliance integrations
Configuration Compliance includes third-party integration with the Qualys Cloud Platform.

Understanding the Qualys Vulnerability Integration
Qualys Cloud Platform sensors collect the data and automatically send it to the Qualys Cloud Platform application, which continuously analyzes and correlates the information. It easily integrates with Vulnerability Response as the Qualys Vulnerability Integration to map vulnerabilities to CIs and business services to determine impact and priority of potentially malicious threats.

Configure your Qualys Vulnerability Integration using Vulnerability > Administration > Setup Assistant to make data retrieval more flexible and scalable.

If you have multiple deployments of the Qualys Cloud Platform application, you can add an integration for each deployment. Assets, identified by multiple third-party deployments and their vulnerabilities, are consolidated and reconciled with your CMDB. This consolidation happens even when scan processes overlap between the multiple deployments. Data sourced from each deployment
is identified and available in a single instance of Vulnerability Response. Qualys vulnerability integration Knowledge Base records are normalized across deployments, ensuring that instances of the same vulnerability across deployments are treated as the same vulnerability.

**Note:** You cannot delete the original vulnerability integration but you can disable it. Integrations created from disabled templates are disabled by default.

There is a configured run-as user for each integration record. The default value for this user is **VR.System**. Do not change this value.

**Note:** While the **Qualys Vulnerability Integration** creates integrations for Appliance List, Asset Group, Dynamic Search List, and Static Search List, they are not required for normal operation.

### Available versions for Paris

<table>
<thead>
<tr>
<th>Release versions with Paris</th>
<th>Release Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualys Vulnerability Integration v12.1</td>
<td>Vulnerability Response integrations release notes</td>
</tr>
<tr>
<td>Qualys Vulnerability Integration v12.0</td>
<td>For compatibility information, see KB0856498</td>
</tr>
<tr>
<td>Qualys Vulnerability Integration v11.1</td>
<td>Vulnerability Response Compatibility Matrix and Release Schema Changes</td>
</tr>
<tr>
<td>Qualys Vulnerability Integration v11.0</td>
<td></td>
</tr>
<tr>
<td>Qualys Vulnerability Integration v10.3</td>
<td></td>
</tr>
<tr>
<td>Qualys Vulnerability Integration v10.0</td>
<td></td>
</tr>
</tbody>
</table>

### Primary and Supporting Integrations

Qualys primary and supporting integrations enrich the vulnerability data on your instance by retrieving data from the Qualys Vulnerability Integration. A series of scheduled jobs invoke the integrations automatically. You can also execute them manually. Scheduled jobs simplify the vulnerability remediation lifecycle by keeping the instance synchronized with other vulnerability management systems. Primary and supporting integrations can be modified.

The Qualys integrations are executed as scheduled jobs. There is a configured run-as user for each integration record. The default value for this user is **VR.System**. This value should not be changed.
Note: Failing to set a valid run-as user results in multiple, often duplicate, data retrieval attachments on the data source records, every time the integration runs. Multiple attachments on the data source increase processing time, resulting in inconsistent transform results.

Qualys Cloud Platform integration tasks involve the following roles.

- **sn_vul_qualys.admin** — can read, write, and delete records
- **sn_vul_qualys.user** — can read and write records
- **sn_vul_qualys.read** — can read records

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Primary integrations

A primary integration is an entry point to the Qualys Cloud Platform interacting with the Qualys API invoked on a schedule.

View the primary integrations by navigating to Qualys Vulnerability Integration > Administration > Primary Integrations.

The following primary integrations are included in the base system.

### Primary integrations

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualys Appliance List Integration</td>
<td>Retrieves scanner appliance information from Qualys.</td>
</tr>
<tr>
<td>Qualys Asset Group Integration</td>
<td>Retrieves asset group information from Qualys. Asset groups are used to identify which scanner appliances to use for scanning matching configuration items.</td>
</tr>
<tr>
<td>Qualys Dynamic Search List Integration</td>
<td>Synchronizes Qualys search lists for finding vulnerable entries, and retrieves dynamic list type records.</td>
</tr>
</tbody>
</table>
## Primary integrations (continued)

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualys Host Detection Integration</td>
<td>Retrieves host and vulnerability data from Qualys and processes it in your instance. It coordinates the REST message calls to the Host List Detection API. The outputs of this integration are vulnerable items. Version 10.0: Qualys host tags are imported in this integration.</td>
</tr>
<tr>
<td>Qualys Host List Integration</td>
<td>Retrieves authenticated and unauthenticated host scan data, and starting with v10.3, host tags from Qualys once a week and stores it in the Discovered Items module in your instance. Helps identify assets that haven't been scanned recently.</td>
</tr>
<tr>
<td>Qualys Knowledge Base</td>
<td>Retrieves Qualys knowledge base entries. The retrieved data is based on the date the vulnerabilities were updated by Qualys and since the last time the integration ran. This data is useful for populating historical data into your instance as well as ensuring the Qualys Identifiers (QIDs) are up to date.</td>
</tr>
<tr>
<td>Qualys Knowledge Base (Backfill)</td>
<td>Retrieves Qualys knowledge base entries. Scheduled to run after the Qualys Host Detection Integration. Updates your instance with any QIDs that were referenced in the Host Detection integration but did not exist in the system.</td>
</tr>
<tr>
<td>Qualys Static Search List Integration</td>
<td>Synchronizes Qualys search lists for finding vulnerable entries. Retrieves only static list type records.</td>
</tr>
<tr>
<td>Qualys Option Profile List Integration</td>
<td>Version 12.0: Retrieves option profiles from the Qualys product. Option profiles include scan settings which are required when you initiate scans from your Now Platform® instance.</td>
</tr>
<tr>
<td>Qualys Ticket Integration</td>
<td>Retrieves Qualys tickets and adds them to your instance. It coordinates the REST message calls to the ticket list API. There are often fewer tickets than Host Detections since Qualys settings can constrain the detections that result in a ticket.</td>
</tr>
</tbody>
</table>

## Supporting integrations

A supporting integration is a process that is not intended to run on a schedule nor without invocation by a primary integration.
View the supporting integrations by navigating to Qualys Vulnerability Integration > Administration > Supporting Integrations.

The following supporting integrations are included in the base system.

### Supporting integrations

<table>
<thead>
<tr>
<th>Integration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Group Pagination Handler</td>
<td>Directs the pagination of the Asset Group Integration.</td>
</tr>
<tr>
<td>Host Detection Import Set Reprocess Integration</td>
<td>Handles reprocessing of the Host List import set created by the Host Detection Integration. Processes detections found for each host and results in vulnerable items being inserted or updated in your instance.</td>
</tr>
<tr>
<td>Host Detection Pagination Handler</td>
<td>Directs the pagination of the Host Detection Integration. The Host List Detection API coordinates REST calls for each page request to the server.</td>
</tr>
</tbody>
</table>

### Search lists

Search lists are used in Qualys to create custom groups of vulnerabilities. You can save them and use for ticket creation and to customize vulnerability scans and reports. The Search Lists module allows you to download search list data from Qualys to your instance on a scheduled basis.

Search lists are pulled from Qualys using the Dynamic Search List Import and/or Static Search List Import data transformation maps. In each of these transforms, you can define schedules for performing the import.

### Option profiles (v 12.0)

Starting with v12.0, Option profiles are available with Qualys scan settings. An option profile is required when you initiate a scan from your Now Platform.

Option profiles are imported from the Qualys product by the Option Profile List Integration. You might prefer to run the Option Profile List Integration after an import from the Search Lists Integrations, the Qualys Dynamic Search List and Qualys Static Search List Integrations so that you can see which search lists are associated with option profiles.
**Asset groups**

Asset groups are setup in the Qualys platform. Asset groups identify which scanner appliances are used for scanning matching IP addresses when a scan is initiated from the Now Platform.

Asset groups that have associated appliances are pulled from Qualys by the Asset Group List Integration.

Initiate the Appliance List Integration after you import asset groups to populate the Appliance name and Appliance status fields on the Qualys Default Applications records in your Now Platform.

**Host tags**

Version 10.3: All host tags are imported as part of the Qualys Host List integration. Host tags are used primarily for filtering in Vulnerability Response Assignment and Vulnerability Group Rules. They are displayed in the Discovered Item form.

⚠️ **Note:** The Qualys Host List integration should be run prior to creating Assignment or Vulnerability Group Rules in Vulnerability Response so that all tags can be present in the rules and before vulnerable items are imported and grouped.

- Tag storage is not case sensitive. If a *San Diego* tag is created, then a *SAN DIEGO* tag cannot be stored in the Host tag table. “San Diego” and “SAN DIEGO” are considered to be the same host tag. Whichever tag was imported first wins.
- Using host tags as a Group Key in a Vulnerability Group Rule can have unexpected results. Host tags are intended for use only in the Condition builder.
- Host tags are controlled by the global system property `sn_vul.import_host_tags`. This property is set to true by default. Turning tags off turns them off across all instances.

Host tags (also called asset tags) are used for organizing and tracking the assets in your organization. You can assign tags to your host assets. Then, when launching scans, you can select tags associated with the hosts you want to scan. The Host Tags module allows you to download host tag data from Qualys to your instance on a scheduled basis.

**Reopen resolved vulnerable items not closed by scans**

Starting with v10.3, vulnerable items set to ‘Resolved’ in your Now Platform instance but not transitioned to ‘Closed/Fixed’ by the third-party integration runs are reopened if they are detected during rescans.
For Qualys detections, if the scanner continues to find VIs that were set to 'Resolved' but then not transitioned to 'Closed/Fixed' by subsequent scans, these VIs move back to 'Open' when the last found date is later than the Resolved date.

Data retrieval limitations

By default, there are no restrictions on how data is retrieved from Qualys. Many records can be related to low severity vulnerabilities that a customer is not willing to remediate using their vulnerability response process. Updating the corresponding REST message/method parameters can modify this behavior.

The REST message/method responsible for this update is **Qualys Host Detection – Standard/post**. To update the values, add a new HTTP Query Parameter to the post method with the following values:

- **Name**: severities
- **Value**: 3-5 (or whatever appropriate severities are desired)

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Related information

- Qualys REST messages

Preparing for the Qualys Vulnerability Integration

A successful integration requires planning and careful execution of pre-integration tasks. It is essential that you prepare for the integration by performing these procedures. The Qualys Vulnerability Integration assumes that you are familiar with and run Qualys Cloud Platform scans in your environment.

⚠️ **Note**: Make any necessary configuration changes based on your requirements before running the integrations.

Important prerequisites

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.
Validate your instance sizing based on the number of vulnerable items you expect to import. An undersized instance can lead to long load times. If you do not know the size of your instance, contact Customer Service and Support.

Use filtering to limit the number of items for initial import and phase your deployment by adjusting filters in subsequent imports.

**Actions to take**

- **Determine an initial start date** for Host Detection List Import integrations. Consider setting the **Start time** field to a few hours or days in the past. Ideally, choose the date of the last Qualys scan. The start date can include vulnerabilities discovered prior to using the vulnerability management solution. Set the earliest start time used to the start of your scanning cycle. So, if it takes a week before all hosts are scanned, set this value to a week prior to that time.

- **Add users** to the roles for admin, sn_vuln.admin, and sn_vul_qualys.admin. For more information see, Assign a role to a user. Assign a role to a user.

- **There is a configured run-as user** for each integration record. The default value for this user is **VR.System**. Do not change this value.

- **If you do not use vulnerability calculators**, disable the default calculator, in addition to any others you have defined. Vulnerability calculators run every time a vulnerable item record is created or updated, and can impact initial import performance.

- **During the initial import** of records, certain notification-related business rules can cause many notifications to be generated, impacting performance. Prior to your initial import, disable the business rules.

- **If you wish to use a different scanner than the Qualys default**, see set up scanner appliances.

- **Have your Qualys server URL and authentication credentials** ready. The credentials must provide adequate permissions for retrieving knowledge, scan, and detection information for a Qualys subscription.

- **Version 10.3:** If you plan to use host tags in Vulnerability Response Assignment or Vulnerability Group Rules, ensure the Qualys Host List integration was run prior to creating rules.

**Install the Qualys Vulnerability Integration**

Before you run the Qualys Vulnerability Integration in your instance, you must install and configure the Qualys Vulnerability Integration application. This application is available as a separate subscription.
Before you begin
Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

Note: This process applies only to applications downloaded to production instances. If you're downloading applications to sub-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Role required: admin to download and install the application

<table>
<thead>
<tr>
<th>Setup tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that the Vulnerability Response application is installed and activated.</td>
<td>To verify that it is activated, navigate to Subscription Management &gt; Subscriptions in your instance. The list displays the subscriptions your organization has purchased. If the application is not installed and activated see, Install and configure Vulnerability Response.</td>
</tr>
<tr>
<td>Get entitlements for the Qualys Vulnerability Integration application and download it to your Now Platform® instance.</td>
<td>If the application is not already downloaded on your instance, see Download an application from the ServiceNow Store for the first time.</td>
</tr>
<tr>
<td>Prepare for the integration.</td>
<td>See Preparing for the Qualys Vulnerability Integration.</td>
</tr>
</tbody>
</table>

Procedure
1. Navigate to Vulnerability Response > Administration > Setup Assistant.
   After a few moments, the applications that are available for installation on your instance are displayed.
2. Locate the Qualys Vulnerability Integration tile and click Install.
3. Follow the prompts in the Setup Assistant.
4. For more information about installing applications using Setup Assistant, see Install Vulnerability Response third-party applications using Setup Assistant.

What to do next
After you complete the installation in Setup Assistant, navigate to Integration Configuration>Scanner Integrations in Setup Assistant to continue with the
configuration. If you want more information to supplement the prompts provided in Setup Assistant, see Configure the Qualys Vulnerability Integration using Setup Assistant.

**Optional Qualys modifications**

Configure optional modifications and streamline some of the data specifically for the Qualys integration.

**Create domain-separated imports for the Qualys Host Detection Integration**

If you require imported host detection data to be in a specific domain, the user assigned to run the integrations must belong to that domain.

**Before you begin**

Role required: sn_qualys.admin and import_admin

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

**About this task**

This set of tasks require coding or advanced ServiceNow expertise.

The import queues contain data attachments that the scheduled jobs (integrations) process. In a domain-separated environment, you must match the scheduled job with the correct import queue.

**Procedure**

1. Create a domain.

2. For every domain you create, create a user and assign the user to that domain.
   Think of this user as a run_as placeholder for the domain in, for example, the Qualys Host Detection Integration. It is the equivalent to the VR.System user in the global domain. This user needs access to data sources, transform maps, and vulnerability data.

   **Note:** Do not use this user for any other purpose.

3. In each domain, create a scheduled job by copying Scheduled Vulnerability Data Source Processor found under System Definition > Scheduled Jobs.
Append the domain to the name to identify the scheduled job. Change the run_as user to the user you created in the previous step.

4. **Note:** Edit the following UI action so that the integration runs in the run_as user domain.

Edit the Execute Now UI action in the Qualys Host Detection Integration to add this code block to the top of the file.

**Example**

```java
//sys id below is of host detection integration
if(current.sys_id == "5d9cf0da0540300c68c9f783894fa4d"){
    current.run_as = gs.getUserID()
    ;
}
```

5. **Note:** Edit the following script includes so that integration run in the run_as user domain.

Edit the VulnerabilityIntegrationUtils script include method addIntegrationRun to add the highlighted code
6. Edit the `VulnerabilityIntegrationUtils` script include method `addProcessRun` to add the highlighted code.

```javascript
define.addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
}
```

7. Edit the `VulnerabilityIntegrationUtils` script include method `copyProcess` to add the highlighted code.

```javascript
define.copyProcess: function(intProcGr, stProcessErrored) {
    var copy = new GlideRecord("sn_vul_integration_process");
    copy.initialize();
    copy.setValue("sys_domain", intProcGr.getValue("sys_domain"));
    if (stProcessErrored) {
        copy.setValue("error retries", parseInt(intProcGr.getValue("error retries")) + 1);
    } else {
        copy.setValue("next_retry_day", new GlideDateTime(intProcGr.getValue("next_retry_day")));
    } copy.insert();
    return copy;
}
```
8. Edit the **DataSourceVulnReportRefreshProcessor** script include method _processFromDataSourceGroups to change this original code:

**Original _processFromDataSourceGroups code**

```javascript
function(payload, fileName) {
  var gr = new GlideRecord("sn_vul_int_data_src");
  gr.addQuery("sn_vul_integration", this.IntegrationGr.sys_id + "");
  gr.orderBy("ds_group_number");
  gr.query();
  var lastGroup = true;
  if (gr.getRowCount() == 0) {
    throw new Error("There are no data sources to provide data to.");
  }
  while (gr.next()) {
    var thisGroup = gr.getValue("ds_group_number");
    var lastGroup = thisGroup && lastGroup != undefined {
      continue;
    } else {
      var ds = new GlideRecord("sys_data_source");
      if (ds.get("sys_data_source")) {
        continue;
      }
      var mnr = new sn_vul.VulnerabilityDSAttachmentManager();
      mnr.queueItem(ds, getUniqueValue(), fileName, payload,
      this.integrationProcessor, getUniqueValue(), this.integrationProcessor, getValue("sys_domain"));
      gr.setValue("last_used", new GlideDateTime().getValue());
      gr.update();
      lastGroup = thisGroup;
    }
}
```

**To:**

**Edited _processFromDataSourceGroups code**

```javascript
function(payload, fileName) {
  var gr = new GlideRecord("sn_vul_int_data_src");
  gr.addQuery("sn_vul_integration", this.IntegrationGr.sys_id + "");
  gr.orderBy("ds_group_number");
  gr.query();
  var lastGroup = true;
  if (gr.getRowCount() == 0) {
    throw new Error("There are no data sources to provide data to.");
  }
  while (gr.next()) {
    var thisGroup = gr.getValue("ds_group_number");
    var lastGroup = thisGroup && lastGroup != undefined {
      continue;
    } else {
      var ds = new GlideRecord("sys_data_source");
      if (ds.get("sys_data_source")) {
        continue;
      }
      var mnr = new sn_vul.VulnerabilityDSAttachmentManager();
      mnr.queueItem(ds, getUniqueValue(), fileName, payload,
      this.integrationProcessor, getUniqueValue(), this.integrationProcessor, getValue("sys_domain"));
      gr.setValue("last_used", new GlideDateTime().getValue());
      gr.update();
      lastGroup = thisGroup;
    }
}
```

9. Edit the **VulnerabilityDSAttachmentManager** script include method, **queueItem** to add the following highlighted code blocks

**queueItem**

```javascript
function(dataSource, attachmentName, reportData, optIntegrationProcess, optDomain) {
  var gr = new GlideRecord(this.QUEUE_TABLE);
  gr.initialize();
  gr.setValue("status", "NEW");
  gr.setValue("dsSource", dataSource);
  if (optIntegrationProcess) {
    gr.setValue("integration_process", optIntegrationProcess);
    if (optDomain) {
      gr.setValue("sys_domain", optDomain);
    }
  } else {
    gr.setValue("sys_domain", optDomain);
  }
  var sysId = gr.insert();
```

**_getNext**
_processQueueEntry function

At this point, you are ready for domain-separated host detection imports.

⚠️ **Note:** If you have multiple deployments of the Qualys Vulnerability Integration, repeat this process for each deployment.

**Disable the default vulnerability calculator if not used**

If you do not use vulnerability calculators, it is best to disable the default calculators in addition to any others you have defined. Vulnerability calculators run every time a vulnerable item record is accessed, and can impact instance performance.

**Before you begin**

Role required: **admin**
Procedure

1. Navigate to Vulnerability > Administration > Vulnerability Calculators.
2. Open the Vulnerability Impact group.
3. Open the Score and Service Based Impact calculator.
4. Deselect the Active field to deactivate the calculator.
5. Click Update.

Disable notification-related business rules prior to initial record import

During the initial import of records, certain notification-related business rules can generate many notifications, impacting performance. These business rules should be modified to disable them during the import.

Before you begin
Role required: admin

Procedure

1. Navigate to System Definition > Business Rules.
2. Search for Affected ci notifications.
3. Open the business rule and insert this condition: current.sys_class_name != "sn_vul_vulnerable_item".
4. Click Update.
5. Repeat this procedure for the following business rules:
   - Affected cost center notifications
   - Affected group notifications
   - Affected location notifications

Note: After the completion of the initial record import, you have the option of re-enabling these business rules. However, consider leaving them disabled. They can generate large numbers of notifications and impact the performance of your instance.

Modify an initial start date

During installation using Setup Assistant, you set an initial start date for the Qualys integrations. You can reset that start date in Setup Assistant or from the primary integration as shown below.
Before you begin
Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure
1. Navigate to Qualys Vulnerability Integration > Administration > Primary Integrations.
2. Click Qualys Host Detection Integration.
3. Click Integration Details.
4. Set the Start time field to a value in the past, so all scanned and detected vulnerabilities since that time are detected.
   If you configured Qualys using Setup Assistant, the Start time field is pre-filled, initially to three months prior today's date, and subsequently to today's date.
   
   Note: Consider setting the value to a maximum of a month in the past. This keeps large amount of data from exceeding the Qualys API rate limitations, as well as triggering execution timeouts.

5. Click Submit or Update.
6. Optional: Click Execute Now to run immediately.

Advanced Qualys configurations and modifications
Configure advanced optional modifications and streamline some of the data specifically for the Qualys integration. Most of these modifications require coding or advanced ServiceNow or Qualys Cloud Platform expertise.

Modify the Qualys to ServiceNow priority and state mapping values
Modify mapping values for priority and state for your requirements.

Before you begin
Role required: admin
About this task
This is an advanced customization option.

Procedure
1. Navigate to **System Definition > Business Rules**.
2. Search for **Map Qualys Values** and open it.
3. Click the **Advanced** tab.
4. Modify per your requirements. The most common modifications include adding new state values or revising criticality or priority.
5. Click **Update**.

Restrict the ability to write to a record based on an assignment group
You can restrict write/read rights on records based on membership to an assigned group. Modify conditions and script based on specific requirements.

Before you begin
Role required: security_admin (elevated role from admin)
⚠️ Note: This action is performed in the Vulnerability scope.

Procedure
1. Navigate to **System Security > Access Control (ACL)**.
2. Search for ACLs that start with **sn_vul**.
3. Choose an Access Control record, for example, **sn_vul_vulnerable_item**, **Operation write**.
4. Check the **Advanced** box in the record, if necessary, to display the **Role** entries.
5. Modify the **Role** script for your requirements.
Script Example of modifying access by group.

```javascript
answer = (current.assigned_to == gs.getUserID() ||
    isMemberOfForScopedApp(current.assignment_group));
// Note: standard 'isMemberOf' does not work within Scoped App
// gs.getUser().isMemberOf(current.assignment_group);
function isMemberOfForScopedApp(groupID){
    var result = false;
    if (groupID != ''){
        var userID = gs.getUserID();
        var now_GR = new GlideRecord("sys_user_grmember");
        now_GR.addQuery("group", groupID);
        result = now_GR.addQuery("group", groupID);
    }
}
```
6. Click **Update**.

### Set up scanner appliances

If you are initiating scans from ServiceNow®, instead of directly from Qualys, you can set up scans for IP address ranges.

**Before you begin**

The data comes from the Qualys integration based on Qualys asset groups and their related default appliances (scanners).

If no appliances are configured for the targeted IP address ranges, the appliance that is set as the default for the integration instance is used for the scan.

Role required: sn_vul_qualys.admin

**Procedure**

1. Navigate to **Qualys Vulnerability Integration > Scanner Appliances**.
2. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance name</td>
<td>Enter the name for the Qualys scanner appliance to be used for invoking scans for matching configuration items.</td>
</tr>
<tr>
<td></td>
<td>If you have manually created records that do have an Appliance ID provided, the appliance name is used.</td>
</tr>
<tr>
<td></td>
<td>Use the External value when you want the scan to be launched with an external scanner.</td>
</tr>
<tr>
<td>Appliance ID</td>
<td>Enter the appliance identifier for the Qualys scanner appliance to be used for invoking scans for matching configuration items.</td>
</tr>
<tr>
<td></td>
<td>If you entered both an Appliance name and an Appliance ID, the identifier is used.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the 0 value when you want the scan to be launched with an external scanner.</td>
<td>Appliance status Displays the last status of the scanner appliance on the data returned by the Qualys integration. For manually created records, the status is updated only if a valid Appliance ID is specified.</td>
</tr>
<tr>
<td>Displays the Qualys asset group identifier that created this record. This field displays a value only for records created by the Qualys integration.</td>
<td>Asset group ID</td>
</tr>
<tr>
<td>Displays the Qualys asset group name that created this record. This field displays a value only for records created by the Qualys integration.</td>
<td>Asset group name</td>
</tr>
<tr>
<td>Enter a value to be used for determining scanning priority. For appliance that have conflicting criteria, an appliance with a lower order value is given a higher priority.</td>
<td>Order</td>
</tr>
<tr>
<td>Indicates whether this record was created manually by the user.</td>
<td>Manually created</td>
</tr>
<tr>
<td>Select this check box to specify a filter group for finding matching configuration items for scanning.</td>
<td>Use filter group</td>
</tr>
<tr>
<td>Select the filter group you want to use for finding matching configuration items for scanning. This field appears only if you selected Use filter group.</td>
<td>Filter group</td>
</tr>
<tr>
<td>A comma-separated list of IP addresses or ranges of IP addresses to be used by this appliance when invoking scans.</td>
<td>IPs</td>
</tr>
<tr>
<td>Starting with v12.0, the Qualys integration instance associated with this appliance.</td>
<td>Integration instance</td>
</tr>
<tr>
<td>Starting with v12.0, select the option profile you want to use for scans for matching configuration items.</td>
<td>Option profile</td>
</tr>
</tbody>
</table>

3. Click **Update**.

**Configure and manage Qualys vulnerability scanners and scans**

Qualys vulnerability scans can be performed to find software vulnerabilities that affect your CIs. You can initiate scans from a vulnerable item record or by creating a scan record directly for configuration items (CIs) and IP addresses.
If you scan Qualys vulnerable items directly from the Vulnerable Items screen, you also have the option of scanning multiple vulnerable items at the same time.

If Security Incident Response is activated, you can also initiate a scan from the security incident catalog, a security incident record, or a security scan request. Scans submitted from Qualys vulnerable items, the Security Incident Catalog, security incidents, or security scan requests are performed by the default Qualys scanner.

Starting with v12.0 of the Qualys Vulnerability Integration, you can select the option profile you want to use for scans for matching configuration items.

- Option profiles contain Qualys scan settings.
- An option profile is required when you initiate a Qualys scan from your Now Platform®.

**Configure the ServiceNow-initiated Qualys IP scan**

The Qualys scanner included with the base system provides a baseline integration to initiate scans based on IP addresses.

**Before you begin**

Starting with v12.0 of the Qualys Vulnerability Integration, you can select the option profile you want to use for scans for matching configuration items.

- Option profiles contain Qualys scan settings.
- An option profile is required when you initiate a Qualys scan from your Now Platform®.

Role required: web_service_admin

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

**Procedure**

1. Navigate to **Vulnerability Response > Vulnerability Scanning > Scanners**.
2. Open the Qualys record.
3. Select the **Active** and **Default** check boxes.
Starting with v12.0, selecting **Active** is required to use the Qualys scanner to scan Qualys VIs automatically. You also don't need to select **Default** to have it run automatically.

Prior to v12.0, **Active** is required to use the scanner. If **Default** is also selected, the scanner is automatically used without having to be selected during scanning.

4. Starting with v12.0, for the Source integration field, click the search icon and select the option for **Qualys**, for example, **Qualys Cloud Platform**.

5. Click **Update**.

6. Navigate to **Qualys Vulnerability Integration > Administration > Primary Integrations**.

7. Open the **Qualys Asset Group List Integration**.
   a. Select the **Active** check box.
   b. Click **Execute Now**.

8. Starting with v12.0, follow these steps to populate your scanner appliances.

   **Note:** You might prefer to run the Option Profile List Integration after an import from the Search Lists Integrations, the Qualys Dynamic Search List, and Qualys Static Search List Integrations, so that you can see which search lists are associated with option profiles.

   a. Open the **Qualys Option Profile List Integration**.
   b. Select the **Active** check box.
   c. Click **Execute Now**.
   d. Follow the steps listed in **Set up scanner appliances** to configure your scanner appliances. Return here after you complete those steps to continue with the configuration.
   e. Navigate to **Qualys Vulnerability Integration > Administration > Primary Integrations**.
   f. Open the **Qualys Appliance List Integration**.
   g. Select the **Active** check box.
h. Click **Execute Now**.

Your Qualys scanner appliances are now correctly populated.

**Related information**

**Understanding the Qualys Vulnerability Integration**

**Scan multiple Qualys vulnerabilities or vulnerable items**

You can simultaneously scan multiple Qualys vulnerabilities or vulnerable items that contain at least one affected configuration item (CI) or an IP address populated on the form.

**Before you begin**

Role required: sn_vul.vulnerability_write

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see **Assign the Vulnerability Response persona roles using Setup Assistant**. For more information about managing granular roles, see **Manage persona and granular roles for Vulnerability Response**.

**Procedure**

1. Do one of the following:
   - Navigate to **Vulnerability Response > Vulnerabilities > Vulnerability Groups**.
   - Navigate to **Vulnerability Response > Vulnerabilities > All Vulnerable Items**.

2. Select the check boxes for the records you want to scan.

3. Click the **Actions on selected rows** list, and click **Scan for Vulnerabilities**. A message appears with a link to the scan and the work notes are updated.

4. Click the link to see the progress or results of the scan.
Prior to v13.0 of Vulnerability Response and v12.0 of the Qualys Vulnerability Integration, the Scan screen includes a Source related list that shows the individual vulnerabilities or vulnerable items scanned.

### Scan results prior to v13.0 of Vulnerability Response and v12.0 of the Qualys Vulnerability Integration

<table>
<thead>
<tr>
<th>Number</th>
<th>Time requested</th>
<th>Requested by</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSCAN0001002</td>
<td>2016-05-03 15:05:04</td>
<td>System Administrator</td>
<td>Error</td>
</tr>
</tbody>
</table>

#### Configure the Qualys auto scan for resolved vulnerability groups (v 12.0)

Starting with v12.0 of the Qualys Vulnerability Integration, you can schedule the scan that runs automatically to update your Qualys vulnerable items.

#### Before you begin

After a vulnerability group (VG) is transitioned to **Resolved**, a scan is initiated automatically to update the state of the associated vulnerable items.

- The scan is disabled by default.
- Enable the scan with the `scan_on_resolved` integration instance parameter in the Qualys record located at **Qualys Vulnerability Integration > Integration Instances > Qualys**. See the following steps for more information.
• This scan is instance-specific. If you have multiple instances and you want to enable or disable this scan, you must disable the `scan_on_resolved` parameter in the integration instance parameters in each instance you want changed.

• When the scan is enabled, you can initiate the scan on-demand, or you can schedule the scan to run only within a specified time window. See Configure Qualys rescans to run only within scheduled intervals (v 12.0) for how to set the start and end times for the time window.

Role required: sn_vul_qualys.admin

Procedure

1. Navigate to Qualys Vulnerability Integration > Integration Instances > Qualys.
2. Click Qualys to open the record.
   The integration instance parameters for Qualys are displayed.
3. To enable the auto scan, locate the `scan_on_resolved` parameter.
4. In the Value column for the property, enter `true`.
5. Click Update.

Configure Qualys rescans to run only within scheduled intervals (v 12.0)

Starting with v12.0 of the Qualys Vulnerability Integration, set the scan start and end time parameters so that rescans run, or are available, only during the hours that you want.

Before you begin

This configuration applies to both scheduled rescans and the rescans you initiate manually in the Qualys product from your Now Platform® instance.

Setting the scan start and end time parameters for integration instances permits you to specify time windows when rescans in the Qualys product are available. For example, you might prefer to specify that rescans are only available during off-hours, for example, midnight to 10 AM.

This setting is instance-specific. If you have multiple instances, you must configure the `scan_start_time` and `scan_end_time` values in the integration instance parameters in each instance you want to change.

Role required: sn_vul_qualys.admin

Procedure

1. Navigate to Qualys Vulnerability Integration > Integration Instances > Qualys.
2. Click Qualys to open the record.
The integration instance parameters for Qualys are displayed.

3. For the scan_start_time parameter, in the Value column, enter the time in the UTC time zone in 24 hour format (00:00 through 24:00) for the start time of the window that you want rescans available.

4. For the scan_end_time, in the Value column, enter times in the same format (00:00 through 24:00) for the end time of the available window.
   For example, if you enter a start time of 00:00 for the scan_start_time parameter, and an scan_end_time of 10:00 AM that same morning, scans scheduled or manually launched outside of the midnight to 10 AM time window are queued and launched at the start time of the following day's time window, 00:00.
   In the same example, if a remediation owner manually initiates a rescan at 11:00 AM, the rescan is not immediately launched, because it lies outside of the available configured scan times. The scan request remains queued until the start of the following day's time window, in this example, (00:00).

5. Click Update to save your settings.

View the Qualys vulnerability scan queue

Vulnerability scan requests submitted to Qualys vulnerability scanning integration are queued so as not to overload system resources. You can view the status of queued requests, as needed.

Before you begin
Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task
In the list of queued scans, each scan includes an automatically generated scan name that identifies the CI that was scanned.

Procedure

1. Navigate to Vulnerability Response > Vulnerability Scanning > Scan Queue. All Qualys scan requests that have been submitted are shown in a list. The State column shows the current state of each queued entry. A state of Complete indicates that the scan has left the queue. It does not necessarily
indicate that the scan has completed processing. When the scans have been completed or if they failed, the **Processing** column shows the appropriate work notes text.

**Note:** If a hash value was submitted for scanning and the scanner fails to find a result, the **State** shows **Complete** and the work note in the **Processing** column indicates **Unknown**.

2. After a scan has finished processing, click a queued record to view details for the scan request.

**Initiate rescan for the Qualys Vulnerability Integration (v 12.0)**

Starting with version 12.0 of the Qualys Vulnerability Integration, verify your vulnerable items have been remediated between scheduled scanning cycles by initiating rescans in the Qualys product from your Now Platform.

**Before you begin**

You can initiate a rescan on-demand for vulnerable items for the Qualys product from your Now Platform® instance.

To help reduce the overhead and volume involved with scheduled, full scans, remediation owners, IT specialists, vulnerability analysts, or vulnerability managers can initiate targeted rescans on-demand for specific vulnerabilities on assets (configuration items) in their environments. You can initiate rescans in the Qualys product from vulnerable item (VI), vulnerability groups (VG), third-party entry (TPE), or discovered item records from your Now Platform instance.

Rescans permit you to verify that your remediation activities, patches, and other actions have successfully fixed specific vulnerabilities on your configuration items (CIs).

**Use case**

As an example, say your entire environment is scanned once every three weeks. The most recent full scan was completed a week ago, but you applied a patch yesterday to fix a critical vulnerability. Due to the nature of this vulnerability, you cannot wait two weeks for the next scheduled scan to verify that it has been remediated. To verify that your patch successfully fixed a critical vulnerability discovered during an earlier scan, you can initiate a targeted rescan from your Now Platform for Qualys vulnerable items.

**Required setup for rescans in the Qualys product initiated from your Now Platform**

Verify you have completed the following setup required for rescans. See the steps starting with **Configure and manage Qualys vulnerability scanners and scans** listed in the previous sections for more information.
Role required: sn_vul_manually_initiate_rescan

Procedure

1. Navigate to Vulnerability Response > Vulnerable items.
2. Locate the vulnerable item record that you want to trigger a rescan from and open it.

   Note: You can only initiate rescans for VIs with Qualys as the source. Verify Qualys is displayed in the Source column on the VI List views, or in the Source fields on individual records. You can use the condition builder to group VIs by Source. Or, if the Source column is not displayed on the VI List view, in the upper left of the list, click the Personalize List icon (Gear icon) and use the Slushbucket to move Source from Available to Selected.

3. Alternatively, navigate to Vulnerability Response > Vulnerability Groups, Vulnerability Response > Libraries > Third-Party, or to Discovered items for the vulnerability group, third-party entry, or discovered items records, respectively, that you want to use for the rescan.

   Depending on your choice, the Rescan button is available on the following records:

   • On a single VI record, the VI must be from the Qualys product and in any state other than Closed. For multiple VI records, all the VIs must have Qualys as the source and in any state other than Closed.
   • On a VG record, the VG can be in any state other than Closed, and all the associated VIs must have Qualys as the source.
   • On a third-party entry (TPE) record, the record must have at least one associated VI record in any state other than Closed with Qualys as the source.
   • On a discovered item record, the configuration item has at least one associated VI with Qualys as the source in any state other than Closed.

4. In the upper right of the record you chose, click Rescan.

   In the dialog that is displayed, choose one to continue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the Specify option profiles check box.</td>
<td>From the list, choose the option profile for the Qualys scanner you want to use for the rescan. These are the appliances (scanners) you have</td>
</tr>
</tbody>
</table>
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configured and listed at <strong>Qualys Vulnerability Integration &gt; Scanner Appliances</strong>.</td>
</tr>
<tr>
<td>Clear the <strong>Specify option profiles</strong> check box (not selected).</td>
<td>The Qualys option profile for the scanner you have set as your default scanner on the Scanner Appliances list is used for the scan. For more information about setting the default scanners you initiate from your Now Platform, <strong>Setup scanner appliances</strong> listed in the previous section for more information.</td>
</tr>
</tbody>
</table>

5. Click **Request Scan**.

A message is displayed that indicates your scan is being processed. Status for all rescans can be found at any time under the Scan related lists on the VI, VG, TPE, and discovered item records you used to launch the rescans. In the message, click **View details** to view the status of the rescan and view any other rescans launched from a given record.

Your instance tracks the rescan status until it successfully completes, or until the set tracking period times out, whichever happens first. The time-out does not stop the scan. The time-out refers to when the Now Platform stopped tracking your rescan status, not when the actual rescan stopped.

After the rescan is successfully completed, the Qualys Host Detection Integration is automatically initiated to update your vulnerable items. Depending on how many VIs you have, your detections, VIs and VGs are updated after the completion of the Qualys Host Detection Integration scan. Navigate to these records to view the updates after the Host Detection Integration is completed.

This scan is instance-specific and can be disabled. For more information about the Qualys integrations and how to view the integrations, see **Understanding the Qualys Vulnerability Integration**.

**What to do next**

You can view a **.csv** attachment on the scan record to see details about the rescans.
As shown in the previous image, during the rescan, if hosts (configuration items) in your environment are not accessible, any detections and VIs associated with these assets are not updated when the rescan is completed. To help you understand why they are not included, after the rescan is completed, the asset IP addresses for these CIs are listed on Vulnerability records in the Hosts not scanned field.

**Scan a new or existing Qualys vulnerable item (Prior to v 12.0)**

You can scan a new or existing Qualys vulnerable item that contains at least one affected configuration item (CI) or has an IP address populated on the form.

**Before you begin**
The vulnerable item that you want to scan must contain an affected CI or IP address.
Role required: sn_vul.vulnerability_write

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response.
application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure

1. Navigate to Vulnerability Response > Vulnerabilities > Vulnerable Items.
2. Create a new vulnerable item or open an existing one.
3. Click the Scan for Vulnerabilities related link.
   A message appears with a link to the scan and the work notes are updated.
4. Click the link to see the progress or results of the scan.

   Note: It is a good practice is to rescan vulnerabilities or vulnerable items after they have been remediated and a vulnerability patch has been applied to the affected records. The rescan can be performed using the preceding procedure, but you can also automate the rescans.

Qualys vulnerability scan rate limits

You can define the rate that different types of scans are performed to limit the number of requests that are sent to an external scanner. After you have defined rate limits, you can apply them to the Qualys scanners.

Define Qualys scan rate limits

You can define the rate that different types of scans are performed to balance the load in your scan queue. Conditions defined in the rate limit determine whether the rate limits are applied to queued entries.

Before you begin

Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.
**Procedure**

1. Navigate to **Vulnerability Response > Vulnerability Scanning > Rate Limit Definitions**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Provide a descriptive name that identifies the conditions the queue entry must meet. For example, scans per minute</td>
</tr>
<tr>
<td>Queue conditions</td>
<td>Enter conditions used to determine whether a queued scan entry is subject to this rate limit. The conditions should not be specific to a particular scanner.</td>
</tr>
<tr>
<td>Evaluation script</td>
<td>Write a script with the logic to evaluate the queued entry. It is important that the script return true/false to define whether the entry is processed. Also, base the evaluation script on the queued entry being evaluated.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**Apply scan rate limits to Qualys scanners**

After you have defined scan rate limits using **Rate Limit Definitions**, you can apply rate limits to specific Qualys scanners.

**Before you begin**

Role required: sn.vul_admin

Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see **Assign the Vulnerability Response persona roles using Setup Assistant**. For more information about managing granular roles, see **Manage persona and granular roles for Vulnerability Response**.

**Procedure**

1. Navigate to **Vulnerability Response > Vulnerability Scanning > Scanner Rate Limits**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Scanner rate limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
</tr>
<tr>
<td>Scanner</td>
</tr>
<tr>
<td>Rate limit</td>
</tr>
<tr>
<td>Threshold</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**Resolving Qualys Vulnerability Integration issues**

Some commonly encountered issues, along with workarounds are discussed.

**Attachments not appearing after import**

If attachments are not appearing as expected for data sources or on a security incident after third-party integration imports, check your IP restrictions.

IP access restrictions can prevent attachments from being seen unless you are logged in from a safe IP. Since a new attachment is added with each import, this can result in duplicates you have to remove.

For example, when you run a third-party host import integration, if you do not see any attachments on your data sources, check your IP restrictions and add users to the safe list prior to import.

**CVE data is missing from the vulnerability entry**

If Common Vulnerability Enumeration (CVE) data is missing from your Qualys third-party vulnerability entries, this means the NIST National Vulnerability Database (NVD) database is not populated in Vulnerability Response. Set the `insert_nvd` parameter to `true`, perform an NVD on-demand update and rerun the Qualys Knowledge Base integration.

**Before you begin**

Role required: v10.3 sn_vul.vulnerability.admin or sn_vul.admin (deprecated)  
Starting with v10.3, persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see
Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure
1. Navigate to Qualys Vulnerability Integration > Administration > Integration Instances.
2. Change insert_nvd to true.
3. Navigate to Vulnerability > Administration > On-Demand Update.
4. Update the NVD vulnerability records. See the instructions in Update NVD on-demand (Prior to v13.0).
5. Set the Start date to an earlier date and rerun the Qualys Knowledge Base integration.

Modify transform maps
Transform maps are provided with base configurations and are sufficient usually. You can modify transform mappings depending on the needs of your organization.

Before you begin
Role required: sn_vul_qualys.admin + import_admin

Procedure
1. Navigate to System Import Sets > Administration > Transform Maps to view the REST messages.
2. Filter the resulting list by application, and limit the list to the Qualys Vulnerability Integration application.
3. Modify the transform maps per the customer requirements.
   
   For details on the data provided by the Qualys API, see the Qualys API documentation (https://www.qualys.com/docs/qualys-api-v2-user-guide.pdf).

Check XML attachment property size
Verifies that the XML attachment property is sufficient for large files.

Before you begin
Role required: admin
Procedure

1. Navigate to **System Properties > Import Export**.

2. Scroll down to **Import Properties > XML Format** at the bottom of the page.

3. If necessary, change the value to 250 and click **Save**.

Related information

Data retrieval limitations

By default, there are no restrictions on how data is retrieved from Qualys. Many records can be related to low severity vulnerabilities that a customer is not willing to remediate using their vulnerability response process. Updating the corresponding REST message/method parameters can modify this behavior.

The REST message/method responsible for this update is **Qualys Host Detection – Standard/post**. To update the values, add a new HTTP Query Parameter to the post method with the following values:

- Name: severities
- Value: 3-5 (or whatever appropriate severities are desired)

Qualys Vulnerability Integration reporting

The Qualys Cloud Platform overview is an executive view into vulnerability activity. By providing trends, reports, and drill-downs into specific data, an administrator or analyst can quickly pinpoint areas of concern. The charts are populated with data after vulnerable items and Qualys knowledge base data has been retrieved.

**Note:** Using the Qualys Cloud Platform Vulnerability integration assumes that tuning, testing and deployment have occurred in your instance. These functions are areas beyond the scope of product documentation. For assistance, contact Customer Service and Support.
In each chart, you can point to any part of a chart (bar, pie, data point, and so on) to view general data specific to that part. If you click any part of a report, a list opens to provide detailed information.

The following reports are available on the Qualys Cloud Platform homepage.

### Qualys Vulnerability Integration Overview reports

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIs Synchronized With Qualys</td>
<td>Bar</td>
<td>Displays the number of open vulnerable items recorded for each CI, from most to least.</td>
</tr>
<tr>
<td>Open Qualys Vulnerable Items</td>
<td>Bar</td>
<td>Displays the number of open vulnerable items associated with vulnerabilities (CVE records), from most to least.</td>
</tr>
<tr>
<td>Total Qualys Vulnerable Items</td>
<td>Bar</td>
<td>Displays the number of ignored vulnerable items scheduled to be expired within 7 days.</td>
</tr>
</tbody>
</table>
Qualys Vulnerability Integration Overview reports (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerable Items by Priority</td>
<td>Trend</td>
<td>Displays the number of vulnerability entries recorded each week.</td>
</tr>
<tr>
<td>QID Prevalence</td>
<td>Bar</td>
<td>Displays the number of vulnerable items recorded for each model, from most to least.</td>
</tr>
<tr>
<td>Open Qualys Vulnerable Items</td>
<td>List</td>
<td>Displays the number of vulnerable items recorded for each publisher, from most to least.</td>
</tr>
</tbody>
</table>

Qualys integration run status chart

The Qualys Integration Run Status module is a graphical view of the status of Qualys integration runs.

In the chart, point to any part (bar, pie, data point, and so on) to view general data specific to that part. If you click any part of a report, a list opens to provide detailed information.

Multiple factors can impact the performance of the integration run, like the amount of data and time taken to process this data. Starting with v10.3, two new graphs have been added to compare the performance metrics:

- Qualys Vulnerable Item Ingestion Performance Metrics: Compare daily performance metrics for assignment rules, group rules, risk rules, queue wait time, queue processing time, and other statistics for vulnerable items for the last 30 days, to identify the cause for any deviations in performance.
- Qualys Vulnerable Item Ingestion Performance Throughput: Compare daily vulnerable item ingestion throughput for the Qualys Host Detection integration. Throughput is measured in items per hour.
Sample Qualys Integration Run Status chart (v10.0)

Starting with v10.0:

- The values in the Imported Items column represents the total number of vulnerable items that are created from an integration run.

- The New items column displays the number of vulnerable items that are created from an integration run.

- The Duplicate items column is no longer populated. You may prefer to remove this column from the display.

- The Updated items column displays the number of times vulnerable items are updated during an integration run. This value is not the number of unique vulnerable items that are updated. If for example, a vulnerable item is updated two times during the integration run, it is counted two times and displayed as 2 updated items.

- The Unchanged items column displays vulnerable items found during the integration run that already exist in the database but were not updated, because none of the relevant field values had changed.

Note: Integration runs with zero results for all four of the following values: New CIs, Existing CIs, New Items, and Updated Items are filtered out of the Qualys Integration Runs list.

<table>
<thead>
<tr>
<th>Qualys integration run status chart reports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td>Last 30 Days Qualys Results</td>
</tr>
</tbody>
</table>
Qualys integration run status chart reports (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last 30 Days Qualys New VIs</td>
<td>The number of new vulnerable items imported in the last 30 days. Shown as an integer.</td>
</tr>
<tr>
<td>Last 30 Days Qualys Updated VIs</td>
<td>The number of updated vulnerable items imported in the last 30 days. Shown as an integer.</td>
</tr>
<tr>
<td>Last 30 Days Qualys Duplicates</td>
<td>The number of duplicate vulnerable items imported in the last 30 days. Shown as an integer.</td>
</tr>
<tr>
<td>Qualys Integration Runs</td>
<td>The integration run records in a list.</td>
</tr>
<tr>
<td>Version 10.3: Last 30 Days Qualys Vulnerable Item Ingestion Performance Metrics</td>
<td>Daily performance metrics for vulnerable items compared for the last 30 days.</td>
</tr>
<tr>
<td>Version 10.3: Last 30 Days Qualys Vulnerable Item Ingestion Performance Throughput</td>
<td>Daily vulnerable item ingestion throughput measured for the Qualys Host Detection integration for the last 30 days.</td>
</tr>
</tbody>
</table>

Qualys data transformation

The data retrieved from Qualys is processed through a set of data sources and transforms.

Most transforms for the Qualys Vulnerability Integration are performed using transform scripts. These scripts are for internal use deleting is not recommended. Modifications require coding or advanced ServiceNow or Qualys Vulnerability Integration expertise. The remaining maps are listed in this section and use field maps.

⚠️ Note: During installation, normalized severity maps, that transform imported Qualys Cloud Platform severity levels to standard ServiceNow severity levels, are installed in the Vulnerability Response Normalized Severity Mapping module. See Create a Vulnerability Response severity map for more information.
Dynamic Search List Import

The Qualys dynamic search list transform map is used to transform and import Qualys Dynamic Search Lists. Changes to this transform alter how Dynamic Search Lists are processed and inserted into the system.

To access this transform map, navigate to Qualys Vulnerability Integration > Import Set Tables > Dynamic Search List Import.

The table shows the fields currently being transformed.

<table>
<thead>
<tr>
<th>Source Field</th>
<th>Target field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>u_id</td>
<td>id</td>
<td>Used as the identifier for the Qualys Dynamic Search List.</td>
</tr>
<tr>
<td>[Script]</td>
<td>list_type</td>
<td>The type of search list. Dynamic is the default for the Dynamic Search List transform.</td>
</tr>
<tr>
<td>u_title</td>
<td>title</td>
<td>The name in Qualys for this search list.</td>
</tr>
</tbody>
</table>

In addition to field mappings, there is also a transform script that is executed during the transformation process.

The following table shows when this script runs and what it is used for.

<table>
<thead>
<tr>
<th>When the script is run</th>
<th>Purpose of the script</th>
</tr>
</thead>
<tbody>
<tr>
<td>onAfter (after an import set has completed transformation).</td>
<td>Creates the relationships between Search Lists and their related vulnerabilities. For internal use. Modifying or deleting is not recommended.</td>
</tr>
</tbody>
</table>

Static Search List Import

The Qualys static search list transform map is used to transform and import Qualys Static Search Lists. Changes to this transform alter how Static Search Lists are processed and inserted into the system.

To access this transform map, navigate to Qualys Vulnerability Integration > Import Set Tables > Static Search List Import.

The table shows the fields currently being transformed.
Qualys static search list transform map fields

<table>
<thead>
<tr>
<th>Source Field</th>
<th>Target field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>u_id</td>
<td>id</td>
<td>Used as the identifier for the Qualys Static Search List.</td>
</tr>
<tr>
<td>u_title</td>
<td>title</td>
<td>The name in Qualys for this search list.</td>
</tr>
<tr>
<td>[Script]</td>
<td>list_type</td>
<td>The type of search list. Static is the default for the Static Search List transform.</td>
</tr>
</tbody>
</table>

In addition to field mappings, there is also a transform script that is executed during the transformation process.

The following table shows when this script runs and what it is used for.

Qualys static search list transform map script timing and purpose

<table>
<thead>
<tr>
<th>When the script is run</th>
<th>Purpose of the script</th>
</tr>
</thead>
<tbody>
<tr>
<td>onAfter (after an import set has</td>
<td>Creates the relationships between Search Lists and their related vulnerabilities.</td>
</tr>
<tr>
<td>completed transformation)</td>
<td>For internal use. Modifying or deleting is not recommended.</td>
</tr>
</tbody>
</table>

Asset Group Import

The Qualys Asset Group Appliance Transform map is used to transform Qualys Asset Group data to create scanner appliance records. Changes to this transform alter how scanner appliances are created and modified.

To access this transform map, navigate to Qualys Vulnerability Integration > Import Set Tables > Asset Group Import.

The table shows the fields currently being transformed.

Qualys asset group transform map fields

<table>
<thead>
<tr>
<th>Source Field</th>
<th>Target field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>u_id</td>
<td>id</td>
<td>Used as identifier for the Qualys Asset Group.</td>
</tr>
<tr>
<td>[Script]</td>
<td>manual</td>
<td>Scripted value to determine how the target record was created. When created through</td>
</tr>
</tbody>
</table>
Qualys asset group transform map fields (continued)

<table>
<thead>
<tr>
<th>Source Field</th>
<th>Target field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>transforms, this field is always false.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Script]</td>
<td>ips</td>
<td>The IP addresses that are associated with the asset group being transformed.</td>
</tr>
<tr>
<td>u_default_appliance_id</td>
<td>appliance_id</td>
<td>The Qualys appliance identifier for the default appliance in this asset group.</td>
</tr>
<tr>
<td>u_title</td>
<td>asset_group_name</td>
<td>The name of the Qualys asset group.</td>
</tr>
</tbody>
</table>

In addition to field mappings, there is also a transform script that is executed during the transformation process.

The following table shows when this script runs and what it is used for.

Qualys asset group transform map script timing and purpose

<table>
<thead>
<tr>
<th>When the script is run</th>
<th>Purpose of the script</th>
</tr>
</thead>
<tbody>
<tr>
<td>onBefore (before an import set has completed transformation)</td>
<td>The script that constrains the asset group imports to only asset groups with a default appliance and a set of mapped IP addresses. For internal use. Modifying or deleting is not recommended.</td>
</tr>
</tbody>
</table>

Appliance Import

The Qualys Appliance Transform map is used to transform Qualys Appliance data into appliance records. This is used to update the appliance records that would initially be created from the Asset Group Import. Changes to this transform alter how appliance records are updated with appliance details.

To access this transform map, navigate to Qualys Vulnerability Integration > Import Set Tables > Appliance Import.

The table shows the fields currently being transformed.
Qualys appliance transform map fields

<table>
<thead>
<tr>
<th>Source Field</th>
<th>Target Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>u_name</td>
<td>appliance_name</td>
<td>The name of the Qualys scanner appliance.</td>
</tr>
<tr>
<td>u_status</td>
<td>appliance_status</td>
<td>The last reported status of the Qualys scanner appliance.</td>
</tr>
<tr>
<td>u_id</td>
<td>appliance_id</td>
<td>The Qualys appliance identifier.</td>
</tr>
</tbody>
</table>

In addition to field mappings, there is also a transform script that is executed during the transformation process.

The following table shows when this script runs and what it is used for.

Qualys appliance transform map script timing and purpose

<table>
<thead>
<tr>
<th>When the script is run</th>
<th>Purpose of the script</th>
</tr>
</thead>
<tbody>
<tr>
<td>onBefore (before an import set has completed transformation).</td>
<td>Used to update appliance names and statuses for the given ID. For internal use. Modifying or deleting is not recommended.</td>
</tr>
</tbody>
</table>

Qualys REST messages

Qualys REST messages are used to make calls to the Qualys API.

Qualys Host Detection REST message

The Qualys Host Detection REST message makes the initial call to the Host List Detection API for the Qualys Host Detection Integration.

Qualys host detection REST message parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>list</td>
<td>Indicates the type of operation requested. Required parameter. Changes are not required.</td>
</tr>
<tr>
<td>output_format</td>
<td>XML</td>
<td>Sets the format of the report returned by Qualys.</td>
</tr>
</tbody>
</table>
Qualys host detection REST message parameters (continued)

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detection_updated_since</td>
<td>${lastScanDate}</td>
<td>Shows only detections whose detection status changed after a certain date and time. For detections that have never changed the date is applied to the last detection date.</td>
</tr>
<tr>
<td>truncation_limit</td>
<td>500</td>
<td>The number of hosts to retrieve data from, per request. This parameter is used for pagination purposes. The default value is 500, but larger or smaller values can be used. Do not set at less than 100 since it significantly increases system load. Smaller values require more calls to the Qualys API and larger values result in larger result sets to process and potential data retrieval/processing timeouts.</td>
</tr>
<tr>
<td>status</td>
<td>New, Fixed, Active, Re-opened</td>
<td>Detection statuses to retrieve from Qualys. The default is to retrieve all statuses. For large data pulls (often the initial pull of data), it can be beneficial to exclude Fixed statuses from this list. It is important to include the Fixed status when updating vulnerabilities already in the system.</td>
</tr>
</tbody>
</table>
**Qualys host detection pagination REST message**

The Host Detection Pagination REST message handles pagination requests to the Host Detection API.

When the primary host detection runs, if the Qualys API provides a URL to fetch the next page of data, this REST message retrieves that additional data. This data is used by Host Detection Pagination Handler.

Host detection pagination REST is a specialized REST message and is not intended to be modified.

**Qualys knowledge base (backfill) REST message**

The Qualys Knowledge Base (Backfill) REST message retrieves Qualys knowledge base data based on the last modified timestamp of the vulnerability data for the Qualys Knowledge Base integration.

Changes to the REST message method record impact the request made to Qualys to retrieve knowledge base information.

The following table shows the request parameters that are sent.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>list</td>
<td>Indicates the type of operation being requested. Required parameter. Changes are not recommended.</td>
</tr>
<tr>
<td>details</td>
<td>All</td>
<td>Indicates the level of detail shown for vulnerabilities retrieved. Safe to modify as needed.</td>
</tr>
<tr>
<td>ids</td>
<td>${qids}</td>
<td>Specifies which QIDs to retrieve from Qualys. Referenced in code. Modifications are not recommended.</td>
</tr>
</tbody>
</table>

**Qualys knowledge base (date-based) REST message**

The Qualys Knowledge Base (Date-Based) REST message is used to retrieve Qualys knowledge base data based on the last modified timestamp of the vulnerability data. This message is used by the Qualys Knowledge Base integration.

Changes to the REST message method record impact the request made to Qualys to retrieve knowledge base information.

The following table shows the request parameters that are sent.
Qualys knowledge base (date-based) REST message parameters

<table>
<thead>
<tr>
<th>Source Field</th>
<th>Target Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>list</td>
<td>Indicates the type of operation requested. Required parameter. Changes are not recommended.</td>
</tr>
<tr>
<td>details</td>
<td>All</td>
<td>Indicates the level of detail shown for vulnerabilities retrieved. Safe to modify as needed.</td>
</tr>
<tr>
<td>last_modified_after</td>
<td>${dateStart}</td>
<td>Indicates when to start retrieving historical data. Used by code to determine both the start time and to assist with pagination. Modifications or removal is not recommended.</td>
</tr>
<tr>
<td>last_modifiedbefore</td>
<td>${dateEnd}</td>
<td>Indicates when to end retrieving historical data. Used by code to determine both the end time and to assist with pagination. Modifications or removal is not recommended.</td>
</tr>
</tbody>
</table>

Qualys tickets REST message

The Qualys tickets REST message retrieves Qualys ticket information for the Qualys Ticket Integration. Changes to the REST message method record impact the requests made to Qualys to retrieve ticket information.

The table shows the request parameters that are sent.

Qualys tickets REST message parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>modified_since_datetime</td>
<td>${lastRunDatetime}</td>
<td>Indicates the last run date of the integration and the date after which to pull data. Used by code. Changes are not recommended.</td>
</tr>
<tr>
<td>since_ticket_number</td>
<td>${lastTicketNumber}</td>
<td>Indicates which ticket was last retrieved from Qualys.</td>
</tr>
</tbody>
</table>
Qualys tickets REST message parameters (continued)

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show_vuln_details</td>
<td>1</td>
<td>Indicates whether the vulnerability details are retrieved.</td>
</tr>
</tbody>
</table>

Used for pagination. Changes are not recommended.

**Threat Intelligence**

The ServiceNow® Threat Intelligence application allows you to find indicators of compromise (IoC) and enrich security incidents with threat intelligence data.

<table>
<thead>
<tr>
<th>Explore</th>
<th>Set up</th>
<th>Administer</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Understanding Threat Intelligence</td>
<td>• Install Threat Intelligence</td>
<td>• Set Threat Intelligence properties</td>
</tr>
<tr>
<td>• Domain separation and Threat Intelligence</td>
<td>• Define a threat source</td>
<td></td>
</tr>
<tr>
<td>• Upgrade to Paris.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Threat Intelligence Orchestration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Security Operations videos</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use</th>
<th>Develop</th>
<th>Integrate</th>
</tr>
</thead>
<tbody>
<tr>
<td>• IoC Repository</td>
<td>• Developer training</td>
<td>• Threat Intelligence integrations</td>
</tr>
<tr>
<td>• Threat Intelligence administration</td>
<td>• Developer documentation</td>
<td>• ServiceNow Security Operations integration development guidelines</td>
</tr>
<tr>
<td>• Security Case Management</td>
<td>• Find components installed with an application</td>
<td>• Tips for writing integrations</td>
</tr>
</tbody>
</table>
Understanding Threat Intelligence

The Threat Intelligence application allows you to access and provide a point of reference for your company’s Structured Threat Information Expression (STIX™) data. Included in Threat Intelligence is the Security Case Management application, which provides a means for analyzing threats to your organization posed by targeted campaigns or state actors.

STIX is a language for describing cyber threat information in a standardized and structured manner. Using STIX data and Trusted Automated Exchange of Indicator Information (TAXII™) profiles, threat professionals can use shared cyber threat information to isolate threats that have been previously identified by your company and from other sources. TAXII makes widespread automated exchange of cyber threat information possible.

Threat Intelligence supports STIX versions 1.1, 2.0, and 2.1.

STIX™ and TAXII™ are trademarks of The MITRE Corporation.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Domain separation and Threat Intelligence

Domain separation is supported in the Threat Intelligence module that is available as part of Security Incident Response. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can then control several aspects of this separation, including which users can see and access data.
Support level: Standard

- Includes **Basic** level support.
- Business logic: Processes can be created or modified per customer by the service provider (SP). The use cases reflect proper use of the application by multiple SP customers in a single instance.
- The owner of the instance needs to be able to configure the minimum viable product (MVP) business logic and data parameters per tenant as expected for the specific application.

Use case: An admin needs to be able to make comments mandatory when a record closes for one tenant, but not for another.

Overview

In the Threat Intelligence module (as part of the Security Incident Response application), domain separation enables service providers (SPs) to create and manage the threat intelligence repository in the following ways:

- Threat sources and Trusted Automated Exchange of Indicator Information (TAXII) profiles
- Observables
- Indicators of compromise
- Threat attack modes / methods and case management across the customer base they serve with lowered operational costs and a higher quality of service

Having separate customer work spaces for workflows, dashboards, reports, and so on, ensures that customer data is separated and never exposed to other clients.

Domain separation support in Threat Intelligence by version release

<table>
<thead>
<tr>
<th>Release</th>
<th>Support level</th>
<th>Notes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Geneva, Helsinki</td>
<td>No support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Istanbul</td>
<td>Data only</td>
<td>Security incident observables are stored as fields in the IOC table (source IP, destination IP, malware hash, malware URL, referrer URL, other IOC) and are</td>
<td></td>
</tr>
</tbody>
</table>
Domain separation for the Threat Intelligence module (as part of the Security Incident Response application) covers the following product functionality:

- Security incident observables are directed to the appropriate domain of the user whose ID/ Credential/ Scope generates the incident. The observables extracted from the incident are stored in the domain of the security incident.

- Setting up of TAXII service profiles to download one or more TAXII collections that offer cyber-threat information feeds. The configuration is stored in the domain under which the profile is being set up.

- Setting up the download of threat feeds into the IOC repository in the domain under which the configuration is being performed.
• Creation of attack mode/methods in the domain of the threat intelligence source that provides the information automatically or the domain under which a new attack mode/method is being added manually by the user

• Creation of cases for long-term investigation of incidents, observables, CIs, users, and indicators of compromise (IOC) associated with the case. The case is stored in the domain created by the user.

Note: In all the above cases, the overarching principles of visibility in separated domains in the NOW Platform apply. As always, an incident in the parent domain can reference artifacts in the child domain, but not the other way around.

How domain separation works in Threat Intelligence (as part of Security Incident Response)

Threat Intelligence is part of Security Incident Response in the Professional and Enterprise Tiers, but not with the Standard Tier. Therefore a separate plugin is needed. The Threat Intelligence module (as part of the Security Incident Response application) creates and manages the threat intelligence information associated with security incidents in an organization. The following use cases are domain-separation aware:

• Creation of security incident observables at the time of incident creation
  ◦ From email parsers (Platform-based, user-reported phishing, custom)
  ◦ From applications in third-party Security Information and Event Management (SIEM) stores
  ◦ Manually keyed in by the SOC analyst

• Collection of observables from threat feed sources
  ◦ Threat intelligence sources from TAXII collections

• Manage security incident observables
  ◦ Associate observables with related indicators
  ◦ Associate observables with security incidents
  ◦ Associate observables with child observables
  ◦ Associate observable to threat feed source
  ◦ Add security annotations to observables

• Manage indicators of compromise
  ◦ Associate indicators with related observables
  ◦ Associate indicators with attack mode/method
Associate indicators with indicator types
Associate indicators to threat feed source
Add security annotations to indicators

• Manage cases
  ○ Create case (manually or from an incident)
  ○ Edit a new case to add details (choose case type and severity, add incidents, observables, configuration items, users, indicators)
  ○ Delete a case

Domain separation setup
Setting up domain separation for Threat Intelligence does not require any additional steps. All Threat Intelligence tables acquire the Domain column after the instance is domain separated.

Domain-separated data
Data can be domain separated, which means:

• Security incident observables in one domain cannot be viewed from the scope of other domains.
• Indicators of compromise in one domain cannot be viewed from the scope of other domains.
• Attack modes/methods associated with one domain cannot be viewed from the scope of other domains.
• TAXII service profiles associated with one domain cannot be viewed from the scope of other domains.
• Threat intelligence sources associated with one domain cannot be viewed from the scope of other domains.
• Cases associated with one domain cannot be viewed from the scope of other domains.

Threat Intelligence properties are set at the global level and are not, therefore, domain-separated. The settings include:

• The domain name to retrieve additional information for IP addresses/URLs
• The API key to be used for retrieval
• Lookup of local IoC tables before sending to remote scanner
• Number of days local observables are considered
• Marking an attack mode/method as inactive when not received from threat intel sources
• Marking an indicator as inactive when not received from any source for a specified number of days

Configuration
All aspects of the threat intelligence functionality configuration are self-contained in a domain-separated environment.

The following tasks can be configured per domain:

1. Creation of TAXII service profiles
   • Choose a Discovery service configuration
   • Choose a Collection service configuration
     ◦ Assign roles to users and groups of users

2. Creation of threat intelligence sources
   • Configure the REST service that supplies the threat intel information
   • Schedule the download of threat intel information
   • Choose threat details information to assign to the source

3. Creation of attack mode/methods (manual)
   • Source, malware type, attack mechanism, threat actor type, description, handling, intended effect, first seen, last seen
   • Related indicators, child attack mode/method, associated security incidents

   Note: Attack modes/methods are auto-created from the threat feed sources as well.

4. Setting default lists for the following threat information categories:
   • Attack mechanisms
   • Discovery methods
   • Feeds
   • Indicator types
   • Intended effects
   • Notifications
   • Observable types
   • Rate limit definitions
• Threat actor types
• Attack motivations
• Infrastructure types
• Malware capabilities
• Malware types
• Report types
• Threat actor roles
• Tool types

How tenant domains manage their own application data
• Tenant domain owners can create their own TAXII service profiles.
• Tenant domain owners can create their own threat intelligence sources.
• Tenant domain owners can create their own attack mode/methods.
• Tenant domain owners can create their own default lists for threat information categories.

⚠️ Note: Business logic and processes enable threat intelligence source download schedules to be domain separated by instance owner.

Related information
Domain separation for service providers

Set up Threat Intelligence
Before you run Threat Intelligence in your instance, you must download it from the ServiceNow Store. You can also set up properties and define a threat source.

Install Threat Intelligence
Before you run Threat Intelligence in your instance, you must download it from the ServiceNow Store.

Before you begin
Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.
Setup tasks

<table>
<thead>
<tr>
<th>Description</th>
<th>Setup tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that you have the required ServiceNow roles for your instance.</td>
<td></td>
</tr>
</tbody>
</table>

The following roles are required for installation, configuration, and verification of expected results:

- If not already assigned, the System Administrator [admin] installs the application and assigns the Threat Admin [sn_ti.admin] role.
- The Threat Admin [sn_ti.admin] oversees configuration and verifies expected results.

Role required: admin

Procedure

Follow the instructions for downloading an application from the ServiceNow Store.

What to do next

Set Threat Intelligence properties.

Components installed with Threat Intelligence

Several types of components are installed with activation of the Threat Intelligence plugin, including tables and user roles.

Note: The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

Demo data is available for this feature.

Roles installed

<table>
<thead>
<tr>
<th>Role title [name]</th>
<th>Description</th>
<th>Contains roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Administrator [sn_ti.admin]</td>
<td>Has full control over all threat properties, SLAs, and notifications.</td>
<td>• sn_ti.write</td>
</tr>
<tr>
<td>Threat Reader</td>
<td>Has read access to threat information.</td>
<td>• sn.sec_cmn.int_read</td>
</tr>
</tbody>
</table>
### Role title [name]  
<table>
<thead>
<tr>
<th>Role title [name]</th>
<th>Description</th>
<th>Contains roles</th>
</tr>
</thead>
</table>
| [sn_ti.read]      | Has write access to threat information. Cannot delete attack modes, indicators nor observables. Only a Threat Administrator can delete them. | • sn_sec_cmn.int_write  
• sn_ti.read |

### Tables installed

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack mechanism [sn_ti_attack_mechanism]</td>
<td>Organizes attack patterns hierarchically based on mechanisms that are frequently employed when exploiting a vulnerability. The categories that are members of this view represent the different techniques used to attack a system.</td>
</tr>
<tr>
<td>Attack mode/method [sn_ti_attack_mode]</td>
<td>Attack modes and methods are representations of the behavior of cyber adversaries. They characterize what an adversary does and how they do it in increasing levels of detail.</td>
</tr>
<tr>
<td>Discovery method [sn_ti_discovery_method]</td>
<td>An expression of how an incident was discovered.</td>
</tr>
<tr>
<td>Feed [sn_ti_feed]</td>
<td>Used for configuring the Threat Feed (RSS) in the Threat Overview.</td>
</tr>
<tr>
<td>Indicator Attack mode/method [sn_ti_m2m_indicator_attack_mode]</td>
<td>Used to map attack modes/methods to indicators.</td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Indicator of Compromise</td>
<td>Used to convey specific observable patterns combined with contextual information intended to represent artifacts and/or behaviors of interest within a cyber security context.</td>
</tr>
<tr>
<td>Indicator of Compromise Metadata</td>
<td>Used to populate TAXII records.</td>
</tr>
<tr>
<td>Indicator Source</td>
<td>Used to collect all the sources reporting the specific indicator.</td>
</tr>
<tr>
<td>Indicator Type</td>
<td>Characterizes a cyber threat indicator made up of a pattern identifying certain observable conditions as well as contextual information about the patterns meaning, how and when it is acted on, and so on.</td>
</tr>
<tr>
<td>Associated Indicator Type</td>
<td>Links indicators with their applicable types</td>
</tr>
<tr>
<td>Incident count</td>
<td>Number of security incidents associated with an observable.</td>
</tr>
<tr>
<td>Intended effect</td>
<td>Used for expressing the intended effect of a threat actor.</td>
</tr>
<tr>
<td>IP Scan Result</td>
<td>Used to show the results of an IP lookup.</td>
</tr>
<tr>
<td>Malware Rate limit</td>
<td>Defines a rate limit to be used on a lookup source.</td>
</tr>
<tr>
<td>Malware Scan</td>
<td>A lookup. Contains what to look up, with what lookup</td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Malware Scan Queue Entry</td>
<td>A lookup record queued for lookup or processing. Facilitates the requests within stated rate limits.</td>
</tr>
<tr>
<td>[sn_ti_scan_q_entry]</td>
<td></td>
</tr>
<tr>
<td>Malware Scan Result</td>
<td>Displays the result of a lookup.</td>
</tr>
<tr>
<td>[sn_ti_scan_result]</td>
<td></td>
</tr>
<tr>
<td>Malware Scanner</td>
<td>Defines third-party lookup sources to use in performing lookups.</td>
</tr>
<tr>
<td>[sn_ti_scanner]</td>
<td></td>
</tr>
<tr>
<td>Malware Scanner Rate Limit</td>
<td>Associates a lookup source with a rate limit.</td>
</tr>
<tr>
<td>[sn_ti_scanner_rate_limit]</td>
<td></td>
</tr>
<tr>
<td>Malware Type</td>
<td>Used for expressing the types of malware instances.</td>
</tr>
<tr>
<td>[sn_ti_malware_type]</td>
<td></td>
</tr>
<tr>
<td>Observable</td>
<td>Observables in STIX represent stateful properties or measurable events pertinent to the operation of computers and networks.</td>
</tr>
<tr>
<td>[sn_ti_observable]</td>
<td></td>
</tr>
<tr>
<td>Observable Context Type</td>
<td>Stores the context (source, destination of an IP address, and so forth) for an observable.</td>
</tr>
<tr>
<td>[sn_ti_observable_context_type]</td>
<td></td>
</tr>
<tr>
<td>Observable Indicator</td>
<td>Used to relate observables to indicators.</td>
</tr>
<tr>
<td>[sn_ti_m2m_observable_indicator]</td>
<td></td>
</tr>
<tr>
<td>Observable Source</td>
<td>Used to relate observables to threat sources.</td>
</tr>
<tr>
<td>[sn_ti_observable_source]</td>
<td></td>
</tr>
<tr>
<td>Observable Type</td>
<td>Lists the various types of observables, such as IP addresses.</td>
</tr>
<tr>
<td>[sn_ti_observable_type]</td>
<td></td>
</tr>
<tr>
<td>Observable Type Category</td>
<td>Stores the first categorization of observables (for example,</td>
</tr>
<tr>
<td>[sn_ti_observable_type_category]</td>
<td></td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Related attack mode/method</td>
<td>Used to relate attack modes to each other.</td>
</tr>
<tr>
<td>[sn_ti_m2m_attack_mode_attack_mode]</td>
<td></td>
</tr>
<tr>
<td>Related Observables</td>
<td>Used to relate observables to each other.</td>
</tr>
<tr>
<td>[sn_ti_m2m_observables]</td>
<td></td>
</tr>
<tr>
<td>Scan type</td>
<td>The definition of a lookup type, with initial records for File, URL, and IP.</td>
</tr>
<tr>
<td>[sn_ti_scan_type]</td>
<td></td>
</tr>
<tr>
<td>Security Case</td>
<td>Stores security case records created using Case Management.</td>
</tr>
<tr>
<td>[sn_ti_case]</td>
<td></td>
</tr>
<tr>
<td>Security Case IoC</td>
<td>Used to manage the relationship between observables and cases.</td>
</tr>
<tr>
<td>[sn_ti_case_ioc]</td>
<td></td>
</tr>
<tr>
<td>Security Case Related Task</td>
<td>Used to manage the relationship between tasks (security incidents, change requests, and so forth) with security cases.</td>
</tr>
<tr>
<td>[sn_ti_m2m_case_task]</td>
<td></td>
</tr>
<tr>
<td>Security Case Relationship Exclusion</td>
<td>Provides the definition of inclusion and exclusion of related records in security cases.</td>
</tr>
<tr>
<td>[sn_ti_case_relationship_exclusion]</td>
<td></td>
</tr>
<tr>
<td>Sighting</td>
<td>The m2m link between the observable and the Sightings Search detail result used in the execution of a Sighting Search request.</td>
</tr>
<tr>
<td>[sn_ti_sighting]</td>
<td></td>
</tr>
<tr>
<td>Sighting Configuration Items</td>
<td>Maps configuration items to a Sightings Search.</td>
</tr>
<tr>
<td>[sn_ti_m2m_sighting_ci]</td>
<td></td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Sighting Search Detail</td>
<td>Details of a Sighting Search for example the number of internal external items found.</td>
</tr>
<tr>
<td>[sn_ti_sighting_search_detail]</td>
<td></td>
</tr>
<tr>
<td>Sighting Search Result</td>
<td>The header for a Sightings Search execution.</td>
</tr>
<tr>
<td>[sn_ti_sighting_search]</td>
<td></td>
</tr>
<tr>
<td>Supported Observable Types</td>
<td>Relates indicator types to valid observable types.</td>
</tr>
<tr>
<td>[sn_ti_m2m_ind_type_obs_type]</td>
<td></td>
</tr>
<tr>
<td>Supported Scan Type</td>
<td>Maps the lookup type to a lookup source/vendor-specific implementation. Indicates that a specific lookup source supports the type.</td>
</tr>
<tr>
<td>[sn_ti_supported_scan_type]</td>
<td></td>
</tr>
<tr>
<td>Task Attack mode/method</td>
<td>Relates attack modes to tasks.</td>
</tr>
<tr>
<td>[sn_ti_m2m_task_attack_mode]</td>
<td></td>
</tr>
<tr>
<td>Task Indicator</td>
<td>Relates indicators to tasks.</td>
</tr>
<tr>
<td>[sn_ti_m2m_task_indicator]</td>
<td></td>
</tr>
<tr>
<td>Task Observable</td>
<td>Relates observables to tasks.</td>
</tr>
<tr>
<td>[sn_ti_m2m_task.observable]</td>
<td></td>
</tr>
<tr>
<td>Task Sighting</td>
<td>Stores task records (security incidents and cases) related to a sighting record.</td>
</tr>
<tr>
<td>[sn_ti_m2m_task_sighting]</td>
<td></td>
</tr>
<tr>
<td>TAXII Collection</td>
<td>Defines a cyber-risk intelligence feed that can be imported by a TAXII server.</td>
</tr>
<tr>
<td>[sn_ti_taxii_collection]</td>
<td></td>
</tr>
<tr>
<td>TAXII Profile</td>
<td>Defines a repository for sharing cyber-risk intelligence. Contains TAXII collections.</td>
</tr>
<tr>
<td>[snTi_taxii_profile]</td>
<td></td>
</tr>
<tr>
<td>Threat Actor type</td>
<td>Provides characterizations of malicious actors (or adversaries) representing</td>
</tr>
<tr>
<td>[sn_ti_threat_actor_type]</td>
<td></td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Threat Intelligence Source [sn_ti_source]</td>
<td>Defines a source for importing threat data.</td>
</tr>
<tr>
<td>Associated Attack Motivation [sn_ti_stix2_m2m_object_attack_motivation]</td>
<td>Collects all attack motivations associated with a STIX Object.</td>
</tr>
<tr>
<td>Associated Infrastructure Type [sn_ti_stix2_m2m_infra_type]</td>
<td>Links infrastructure with their types.</td>
</tr>
<tr>
<td>Associated Kill Chain Phase [sn_ti_stix2_m2m_indicator_kill_chain_phase]</td>
<td>Links kill chain phases to indicators.</td>
</tr>
<tr>
<td>Associated Kill Chain Phase [sn_ti_stix2_m2m_object_kill_chain_phase]</td>
<td>Links kill chain phases to STIX objects.</td>
</tr>
<tr>
<td>Associated Malware Capability [sn_ti_stix2_m2m_malware_capability]</td>
<td>Links malware with their capabilities.</td>
</tr>
<tr>
<td>Associated Malware Type [sn_ti_stix2_m2m_malware_malware_type]</td>
<td>Links malware with their types.</td>
</tr>
<tr>
<td>Associated Observable [sn_ti_stix2_m2m_malware.observable]</td>
<td>Collects all observables associated with a malware.</td>
</tr>
<tr>
<td>Associated Observable [sn_ti_stix2_m2m_observed_data.observable]</td>
<td>Collects all observables associated with an observed data.</td>
</tr>
<tr>
<td>Associated Report Type [sn_ti_stix2_m2m_report_report_type]</td>
<td>Links threat reports with their types.</td>
</tr>
<tr>
<td>Associated Threat Actor Role [sn_ti_stix2_m2m_threat_actor_threat_actor_role]</td>
<td>Links threat actors with their roles.</td>
</tr>
<tr>
<td>Associated Threat Actor Type [sn_ti_stix2_m2m_threat_actor_threat_actor_type]</td>
<td>Links threat actors with their types.</td>
</tr>
<tr>
<td>Associated Tool Type</td>
<td>Links tools with their types.</td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>[sn_ti_stix2_m2m_tool_tool_type]</td>
<td>Attack Motivation shapes the intensity and the persistence of an attack. Threat Actors and Intrusion Sets usually act in a manner that reflects their underlying emotion or situation, and this informs defenders of the manner of attack.</td>
</tr>
<tr>
<td>Attack Pattern</td>
<td>A TTP type that describes methods that adversaries use to attempt to compromise targets.</td>
</tr>
<tr>
<td>Campaign</td>
<td>A grouping of adversarial behaviors that describe a set of malicious activities or attacks (sometimes named as waves) that occur over a period against a specific set of targets.</td>
</tr>
<tr>
<td>Course of Action</td>
<td>A recommendation from a producer of intelligence to a consumer on the actions that they might take in response to intelligence.</td>
</tr>
<tr>
<td>External Reference</td>
<td>Pointers to information represented outside of STIX.</td>
</tr>
<tr>
<td>Identity Sighting</td>
<td>Collects all Identities associated with a Sighting.</td>
</tr>
<tr>
<td>Identity</td>
<td>Actual individuals, organizations, or groups (example ACME, Inc.) as well as classes of individuals, organizations, systems, or groups</td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Indicator External Reference</td>
<td>Represents external references associated with indicators.</td>
</tr>
<tr>
<td>[sn_ti_stix2_indicator_external_reference]</td>
<td>(example the finance sector).</td>
</tr>
<tr>
<td>Indicator Sighting</td>
<td>Represents sightings of indicators.</td>
</tr>
<tr>
<td>[sn_ti_stix2_indicator_sighting]</td>
<td></td>
</tr>
<tr>
<td>Infrastructure Type</td>
<td>Represents the various infrastructure types.</td>
</tr>
<tr>
<td>[sn_ti_stix2_infrastructure_type]</td>
<td></td>
</tr>
<tr>
<td>Infrastructure</td>
<td>A TTP type that describes any systems, software services, and any associated physical or virtual resources, intended to support some purpose (example C2 servers used as part of an attack, device, or server that are part of defense, database servers targeted by an attack, and the like).</td>
</tr>
<tr>
<td>[sn_ti_stix2_infrastructure]</td>
<td></td>
</tr>
<tr>
<td>Installed software</td>
<td>Collects all software (SCO software types) associated with a malware analysis.</td>
</tr>
<tr>
<td>[sn_ti_stix2_m2m_malware_analysis_sw]</td>
<td></td>
</tr>
<tr>
<td>Intrusion Set</td>
<td>A grouped set of adversarial behaviors and resources with common properties that is believed to be orchestrated by a single organization.</td>
</tr>
<tr>
<td>[sn_ti_stix2_intrusion_set]</td>
<td></td>
</tr>
<tr>
<td>Kill Chain Phase</td>
<td>Represents kill chain phases associated with a kill chain.</td>
</tr>
<tr>
<td>[sn_ti_stix2_kill_chain_phase]</td>
<td></td>
</tr>
<tr>
<td>Kill Chain</td>
<td>Represents various kill chains.</td>
</tr>
<tr>
<td>[sn_ti_stix2_kill_chain]</td>
<td></td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Location</td>
<td>Represents a geographic location provided through STIX.</td>
</tr>
<tr>
<td>[sn_ti_stix2_location]</td>
<td></td>
</tr>
<tr>
<td>Malware Analysis</td>
<td>The metadata and results of a particular static or dynamic analysis performed on a malware instance or family.</td>
</tr>
<tr>
<td>[sn_ti_stix2_malware_analysis]</td>
<td></td>
</tr>
<tr>
<td>Malware Capability</td>
<td>Represents common capabilities that a malware family or instance exhibits.</td>
</tr>
<tr>
<td>[sn_ti_stix2_malware Capability]</td>
<td></td>
</tr>
<tr>
<td>Malware Operating System</td>
<td>Collects all Operating Systems (SCO software types) associated with malware.</td>
</tr>
<tr>
<td>[sn_ti_stix2_m2m_malware_operating_system]</td>
<td></td>
</tr>
<tr>
<td>Malware</td>
<td>A TTP type that represents malicious code.</td>
</tr>
<tr>
<td>[sn_ti_stix2_malware]</td>
<td></td>
</tr>
<tr>
<td>Marking Definition</td>
<td>Represents handling or sharing requirements for STIX Objects.</td>
</tr>
<tr>
<td>[sn_ti_stix2_marking_definition]</td>
<td></td>
</tr>
<tr>
<td>Object Sighting</td>
<td>Represents sightings of STIX Objects.</td>
</tr>
<tr>
<td>[sn_ti_stix2_object_sighting]</td>
<td></td>
</tr>
<tr>
<td>Object-Indicator Relationship</td>
<td>Collects all relationships between STIX objects and STIX indicators.</td>
</tr>
<tr>
<td>[sn_ti_stix2_m2m_object_indicator]</td>
<td></td>
</tr>
<tr>
<td>Object-Object Relationship</td>
<td>Collects all relationships between STIX Objects and other STIX objects excluding the indicators.</td>
</tr>
<tr>
<td>[sn_ti_stix2_m2m_object]</td>
<td></td>
</tr>
<tr>
<td>Object-Observable Relationship</td>
<td>Collects all relationships between STIX observables and STIX objects.</td>
</tr>
<tr>
<td>[sn_ti_stix2_m2m_object_observable]</td>
<td></td>
</tr>
<tr>
<td>Observed Data Sighting</td>
<td>Collects all the observed data objects associated to a sighting.</td>
</tr>
<tr>
<td>[sn_ti_stix2_m2m_sighting_observed_data]</td>
<td></td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Observed Data [sn_ti_stix2_observed_data]</td>
<td>Conveys information about cyber security-related entities such as files, systems, and networks using the STIX Cyber-Observable Objects (SCOs).</td>
</tr>
<tr>
<td>Report Type [sn_ti_stix2_report_type]</td>
<td>Represents primary purpose or subject of Threat Reports.</td>
</tr>
<tr>
<td>Reported Observable [sn_ti_stix2_m2m_malware_analysis.observable]</td>
<td>Collects all observables associated to Malware Analysis.</td>
</tr>
<tr>
<td>STIX V2 Object [sn_ti_stix2_object]</td>
<td>Common parent table for STIX Object.</td>
</tr>
<tr>
<td>STIX V2 Sighting [sn_ti_stix2_sighting]</td>
<td>Common parent table for STIX sighting tables.</td>
</tr>
<tr>
<td>Threat Actor Role [sn_ti_stix2_threat_actor.role]</td>
<td>Represents roles that can be played by threat actors.</td>
</tr>
<tr>
<td>Threat Actor [sn_ti_stix2_threat_actor]</td>
<td>Threat Actors are actual individuals, groups, or organizations believed to be operating with malicious intent.</td>
</tr>
<tr>
<td>Threat Grouping [sn_ti_stix2_threat_grouping]</td>
<td>Groups all the STIX Objects that share some common context.</td>
</tr>
<tr>
<td>Threat Note [sn_ti_stix2_threat_note]</td>
<td>Provides context and additional analysis not contained in the corresponding STIX Object.</td>
</tr>
<tr>
<td>Threat Opinion [sn_ti_stix2_threat_opinion]</td>
<td>Provides assessment of accuracy of information in a STIX object produced by a different entity.</td>
</tr>
<tr>
<td>Threat Report</td>
<td>Reports are collections of threat intelligence focused</td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>[sn_ti_stix2_threat_report]</td>
<td>on one or more topics, such as a description of a threat actor, malware, or attack technique, including context and related details. They are used to group-related threat intelligence together to publish as a comprehensive cyber threat story.</td>
</tr>
<tr>
<td>Tool Type</td>
<td>The categories of tools that can be used to perform attacks.</td>
</tr>
<tr>
<td>[sn_ti_stix2_tool_type]</td>
<td></td>
</tr>
<tr>
<td>Tool</td>
<td>Tools are legitimate software that is used by threat actors to perform attacks.</td>
</tr>
<tr>
<td>[sn_ti_stix2_tool]</td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td>Represents weakness or defect in the requirements, designs, or implementations of the computational logic (example code) found in software and some hardware components (example firmware). They can be directly exploited to negatively impact the confidentiality, integrity, or availability of that system.</td>
</tr>
<tr>
<td>[sn_ti_stix2_vulnerability]</td>
<td></td>
</tr>
</tbody>
</table>

**Set Threat Intelligence properties**

Threat Intelligence properties allow you to control how different aspects of the system function, including the setting of API keys.

**Before you begin**

Role required: sn_ti.admin
Procedure

1. Navigate to **Threat Intelligence > Administration > Properties**.
2. Set the following properties, as needed.

### Properties for Threat Intelligence

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sn_ti.ip_lookup.web_site</td>
<td>The domain name to retrieve additional information for IP addresses/URLs. The domain name to use for retrieving additional information into your IoC database. This property is used by the ThreatAdditionalInfo script include to populate additional information on the Observables form.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong>: String</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default value</strong>: <a href="http://api.ipinfodb.com/v3/ip-country/">http://api.ipinfodb.com/v3/ip-country/</a></td>
</tr>
<tr>
<td></td>
<td>• <strong>Location</strong>: Threat Intelligence &gt; Administration &gt; Properties</td>
</tr>
<tr>
<td>sn_ti.ip_lookup.api_key</td>
<td>The API key to use for retrieving additional information into your IoC database. This property is used (along with the sn_ti.ip_lookup.web_site property) by the ThreatAdditionalInfo script include to populate additional information on the Observables form.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Location</strong>: Threat Intelligence &gt; Administration &gt; Properties</td>
</tr>
</tbody>
</table>

**Note:** The pinfodb.com third-party API is available at no extra charge and used in many commercial software programs. If you replace it with a different domain name, you must also provide the API key in the next field.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sn_ti.scan.use_file_hash</td>
<td>For file lookups from lookup requests, lookup only their hash values.</td>
</tr>
<tr>
<td>sn_ti.scan.delete_attachment_on_detection</td>
<td>For threat file scans, delete an attachment if malware was detected.</td>
</tr>
<tr>
<td>sn_ti.scan.delete_attachment_after_hash</td>
<td>For threat hash scans, delete an attachment after it has been hashed.</td>
</tr>
<tr>
<td>sn_ti.scan_ioc_before_sending</td>
<td>Lookup local IoC tables before sending to remote scanner.</td>
</tr>
<tr>
<td>sn_ti.observable</td>
<td>If set to True, the Observable [sn_ti.observable] table is checked against</td>
</tr>
<tr>
<td></td>
<td>the lookup request for a matching value. If a match is found (that is, the</td>
</tr>
<tr>
<td></td>
<td>same IP address, URL, or hash file value exists), the lookup result is</td>
</tr>
<tr>
<td></td>
<td>populated from information in the Observable [sn_ti.observable] table. This</td>
</tr>
<tr>
<td></td>
<td>setting prevents unneeded lookups. In the lookup request, the State field</td>
</tr>
<tr>
<td></td>
<td>is set to Complete, the Result field is set to Failed, and the Internally</td>
</tr>
<tr>
<td></td>
<td>populated field is set to True.</td>
</tr>
<tr>
<td></td>
<td>If a matching value or attachment is not found in the Observable [sn_ti.observable] table, the lookup proceeds normally.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **Number of days local Observables are considered**<br>sn_ti.scan_ioc_num_days | If the **Lookup local IoC tables before sending to lookup source** property is set to **True**, observables that were updated in the past number of days specified in this property is compared with the value in the lookup. If a match is found within the specified number of days, or if an attachment in the lookup exists in an IoC observable, the lookup is not performed. The **State** field is set to **Complete**, and the **Result** field is set to **Failed**. If a matching value or attachment is not found in the Observable [sn_ti.observable] table, the lookup proceeds normally.  
  
  - **Type**: integer  
  - **Default value**: 30  
  - **Location**: Threat Intelligence > Administration > Properties |
| When an attack mode/method has not been received from any source for the specified number of days, mark it as inactive<br>sn_ti.attack_mode_inactivate_days | Number of days from when an attack mode/method was last received for the record to be marked inactive.  
  
  - **Type**: integer  
  - **Default value**: 30 |

© 2021 ServiceNow, Inc. All rights reserved.  
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Type**: integer  
**Default value**: 360  
**Location**: Threat Intelligence > Administration > Properties |
| Note: The Active check box is not visible on the Attack mode/method form by default. However, you can add it. When attack modes/methods are inactive, they cannot be selected on other forms. |

When an indicator has not been received from any source for the specified number of days, mark it as inactive  
**sn_ti.indicator_inactivate_days**

Number of days from when an indicator was last received for the record to be marked inactive.  
**Type**: integer  
**Default value**: 180  
**Location**: Threat Intelligence > Administration > Properties

Note: The Active check box is not visible on the Indicator form by default. However, you can add it. When indicators are inactive, they cannot be selected on other forms.

Maximum time in seconds an outbound HTTP connection waits to fetch TAXII collection data  
**sn_ti.taxii.http.max_timeout**

Specifies the maximum amount of time an outbound HTTP connection waits before fetching the next packet of TAXII collection data.  
**Type**: integer  
**Default**: 300

© 2021 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
### Property | Description
---|---
Maximum number of objects retrieved in one REST call from a TAXII server (Applicable only for TAXII versions 2.0 and 2.1)  
*sn_ti.taxii.max_page_size*  
Specifies the maximum number of objects retrieved in one REST call from the TAXII server for one page.  
- **Type**: integer  
- **Default**: 5000  
- Maximum allowed value is 50000.

Maximum number of retries for a failed TAXII 2.X REST call  
*sn_ti.taxii2.retry_count*  
Specifies the maximum number of retries for a failed TAXII REST call.  
- **Type**: integer  
- **Default**: 3

3. Click **Save**.

### Define a threat source

You can maintain a list of Threat Intelligence threat sources. Each source includes the ability to define how often a source is queried. You can also execute a threat source on demand to import the needed Structured Threat Information eXpression (STIX) data.

### Before you begin

Threat Intelligence employs two technologies for importing threat-related information: STIX and Trusted Automated Exchange of Indicator Information (TAXII).

STIX provides a standardized, structured language for representing an extensive set of cyber threat information that includes indicators of compromise (IoC) activity (for example, IP addresses and file hashes), as well as contextual information regarding threats, such as attack modes/methods, that together more completely characterize the motivations, capabilities, and activities of a cyber adversary. As such, STIX data provides valuable information on how your organization can best to defend against cyber threats.

Trusted Automated Exchange of Indicator Information (TAXII) is used to facilitate automated exchange of cyber threat information. TAXII defines a set of services and message exchanges that enable sharing of actionable cyber threat information across organization and product/service boundaries for the detection, prevention, and mitigation of cyber threats. TAXII profiles can be set
up as repositories for sharing STIX-formatted information. Each profile contains one or more TAXII collections or feeds.

Role required: sn_ti.admin

Procedure

1. Navigate to Threat Intelligence > Sources > Threat Sources.
2. Click New.
3. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the threat source.</td>
</tr>
<tr>
<td>Application</td>
<td>The application that contains this record.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to activate the threat source.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Select this check box to display the scripts in the Integration factory script and Report processor fields.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of this threat source.</td>
</tr>
</tbody>
</table>

4. Fill in the fields in the Schedule section, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run</td>
<td>The frequency you want the integration to run, Daily, Weekly, Periodically, and so on. As noted, subsequent fields are displayed based on the setting of this field.</td>
</tr>
<tr>
<td>Day</td>
<td>The day you want the integration to run.</td>
</tr>
<tr>
<td>Time</td>
<td>The time you want the integration to start.</td>
</tr>
<tr>
<td>Repeat Interval</td>
<td>If you selected Periodically in the Run field, this field displays the number of days and hours before the integration runs again.</td>
</tr>
</tbody>
</table>
### Field Description

**Starting**  
If you selected *Periodically* in the Run field, this field displays the dates and time to be used as the starting point for periodic updates.

**Conditional**  
Select this field if you want to add conditional parameters.

**Condition**  
If you selected the Conditional check box, enter the conditions here.

#### 5. Fill in the fields in the **Threat Details** section, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicator</td>
<td>The indicator to use when the data does not explicitly provide one. For blocklists, if empty, a new indicator is created for each observable.</td>
</tr>
<tr>
<td>Indicator type</td>
<td>The indicator type to use for indicators that are created and the data does not explicitly provide an indicator type.</td>
</tr>
<tr>
<td>Attack Mode/Method</td>
<td>The attack mode/method to use when the data does not explicitly provide one.</td>
</tr>
<tr>
<td>Observable Type</td>
<td>The observable type to use for observables that are created and the data does not explicitly provide an observable type. [SI1]</td>
</tr>
<tr>
<td>Weight</td>
<td>Enter a weight value for this source to be used in the confidence calculation.</td>
</tr>
</tbody>
</table>

**Note**: The usage of the **Indicator**, **Indicator Type**, **Attack Mode/Method**, and **Observable Type** fields is implementation-specific. The default processor, SimpleBlocklistProcessor, behaves as the hints describe. However, a TAXII threat source is fully data driven. Any custom threat source processor would be able to use its own strategy. These fields are basically items to expose to the integration/processor and the implementation decides how to use them.

#### 6. Fill in the fields in the **Source Details** section, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint</td>
<td>Enter the web service endpoint URL where the threat source is accessed by Threat Intelligence. Click the lock icon to lock the URL.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use REST Message</td>
<td>If you require a REST message to access the threat source, select this check box. The <strong>REST message</strong> and <strong>REST method</strong> fields become required.</td>
</tr>
<tr>
<td>REST message</td>
<td>Click the lookup icon, and select the REST message from the list or click <strong>New</strong> to define a new REST message.</td>
</tr>
<tr>
<td>REST method</td>
<td>Click the lookup icon, and select the REST method from the list or click <strong>New</strong> to define a new REST method.</td>
</tr>
<tr>
<td>Integration script</td>
<td>The default integration script is SimpleRESTSecurityDataIntegration. It runs a simple REST call, saves the response as an attachment, and then returns the attachment to the processor. This script meets the needs of most organizations. But if you want, you can click the lookup icon, and select a different integration script or define a new one.</td>
</tr>
<tr>
<td>Integration factory script</td>
<td>If the <strong>Advanced</strong> check box is selected, this field displays the actual script for constructing the integration script. You can edit the script as needed. This ability is useful for custom implementations. Integrations in the base system usually do not need any custom constructor logic.</td>
</tr>
<tr>
<td>Report processor</td>
<td>The default integration script is SimpleBlocklistProcessor. This script is a simple processor that accepts a simple blocklist (simple, meaning a single column document with observables such as URLs or IP addresses) and creates observables. It uses the various <strong>Threat Details</strong> fields to determine which fields to set when observables are created.</td>
</tr>
<tr>
<td>Processor factory script</td>
<td>If the <strong>Advanced</strong> check box is selected, this field displays the actual script for constructing the processor. You can edit the script as needed. This script is generally useful for custom implementations. The integrations in the base system usually do not need custom constructor logic.</td>
</tr>
</tbody>
</table>

7. Click **Submit**.

**Create a TAXII profile**

You can maintain TAXII profiles for sharing STIX-formatted information. Each profile contains one or more TAXII collections or feeds.
Before you begin
Role required: sn_ti.admin

Procedure

1. Navigate to Threat Intelligence > Sources > TAXII Profiles.
2. Click New.
3. Complete the following fields as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the TAXII profile</td>
</tr>
<tr>
<td>Application</td>
<td>The application that contains this record.</td>
</tr>
<tr>
<td>Use REST messages as template</td>
<td>If you require a REST message to access the TAXII profile, select this check box.</td>
</tr>
<tr>
<td>TAXII Version</td>
<td>Specify the TAXII version. The supported STIX versions are 1.1, 2.0, and 2.1.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of this TAXII profile.</td>
</tr>
</tbody>
</table>

4. Fill in the fields in the Discovery Service Configuration section, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery Service endpoint</td>
<td>Discovery Endpoint authorizes clients to obtain information about a TAXII Server and get a list of API Roots.</td>
</tr>
<tr>
<td>Use REST message</td>
<td>Select this option if you require a REST message to access the TAXII profile. The Discovery Service REST message and Discovery Service REST method fields become required.</td>
</tr>
<tr>
<td>Discovery Service REST message</td>
<td>Click the lookup icon, and select the REST message from the list or click New to define a new REST message.</td>
</tr>
<tr>
<td>Discovery Service REST method</td>
<td>Click the lookup icon, and select the REST message from the list or click New to define a new REST method.</td>
</tr>
</tbody>
</table>

5. Fill in the fields in the Collection Service Configuration section, as appropriate.
A TAXII Collection is an interface to a logical repository of CTI objects provided by a TAXII Server and is used by TAXII Clients to send information to the TAXII Server or request information from the TAXII Server.

A TAXII Server can host multiple Collections per API Root, and Collections are used to exchange information in a request–response manner.

Select this option if you require a REST message to access the TAXII profile. The Collection Info Service REST message and Collection Info Service REST method fields become required.

Click the lookup icon, and select the REST message from the list or click New to define a new REST message.

Click the lookup icon, and select the REST message from the list or click New to define a new REST method.

6. Click Submit.

**IoC Repository**

IoC repository contains STIX objects, each of these objects contain a specific piece of information.

When you combine STIX objects together through relationships, you allow for easy or complex representations of Cyber Threat Intelligence (CTI).

Threat Intelligence supports STIX versions 1.1, 2.0, and 2.1.

**Attack modes and methods**

Attack modes and methods, sometimes referred to as Tactics, Techniques, and Procedures (TTPs), are representations of how cyber adversaries behave. They characterize what these adversaries do and how they do it, in increasing levels of detail. Attack modes and methods apply for STIX 1.1.
For example, an attack mode/method might be to use malware to steal credit card credentials. Or another, related tactic (at a lower level of detail) might be to send targeted emails with attachments that contain malicious code, which executes upon opening, captures credit card information from keystrokes, and uses http to communicate with a command and control server to transfer information.

Attack modes and methods apply for STIX 1.1.

**Define an attack mode/method**

Attack modes and methods are imported with STIX data, but you can add new modes/methods, as needed.

**Before you begin**

Role required: sn_ti.admin

**Procedure**

1. Navigate to **Threat Intelligence > IoC Repository > Attack Mode/Method**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Select classification tag | If you set up and activated *classification tags* to add metadata to the record, you can select one or more tags to specify the degree of sensitivity of the attack mode/method.  
If you did not set up or activate classification tags, this drop-down list is not displayed. |
<p>| Title               | Enter a descriptive name for this attack mode/method.                                                                                                                                                   |
| Malware Type        | Select the malware type for this attack mode/method. The available malware types are retrieved from the vendor server as STIX data.                                                                 |
| Source              | Select the threat data source for this attack mode/method. Some data sources are included with the base system. You can create new data sources as needed.                                                   |
| Attack mechanism    | Select the attack mechanism for this attack mode/method. Attack mechanisms represent the different techniques used to attack a system. The available attack mechanisms are retrieved from the vendor server as STIX data. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Seen</td>
<td>This date is retrieved from the vendor server as STIX data.</td>
</tr>
<tr>
<td>Last Seen</td>
<td>This date is retrieved from the vendor server as STIX data.</td>
</tr>
<tr>
<td>Threat Actor Type</td>
<td>Select the threat actor type for this attack mode/method. Threat actor types characterize malicious actors (or adversaries) representing a cyber attack threat, including presumed intent and historically observed behavior. The available threat actor types are retrieved from the vendor server as STIX data.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the attack mode/method.</td>
</tr>
<tr>
<td>Handling</td>
<td>Enter instruction for how to handle this attack mode/method.</td>
</tr>
<tr>
<td>Intended effect</td>
<td>Enter the intended effect of this type of attack.</td>
</tr>
</tbody>
</table>

4. Right-click in the form header and click **Save**. You can view any of the following related lists to view additional information.

<table>
<thead>
<tr>
<th>Related List</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related Indicators</td>
<td>Lists related Indicators of Compromise (IoC) that have been identified by the threat source.</td>
</tr>
<tr>
<td>Child Attack mode/method</td>
<td>Lists attack modes/methods that are children of the parent attack mode/method.</td>
</tr>
<tr>
<td>Associated Tasks</td>
<td>Lists changes associated with the parent attack mode/method.</td>
</tr>
</tbody>
</table>

**Add an IoC to an attack mode/method**

In addition to importing indicators as STIX data, you can add IoCs to an attack mode/method manually.

**Before you begin**
Role required: sn_ti.admin

**Procedure**
1. Navigate to **Threat Intelligence > IoC Repository > Attack Mode/Method**.
2. Click the attack mode to which you want to add an IoC.
3. Click the Related Indicators related list.
4. Click Edit.
5. As needed, use the filters to locate the IoC you want to add.
6. Using the slushbucket, add the IoC to the Related Indicators list.
7. Click Save.

Add a related attack mode method

In addition to importing attack modes/methods as STIX data, you can add related attack modes/methods manually.

Before you begin
Role required: sn_ti.admin

Procedure
1. Navigate to Threat Intelligence > IoC Repository > Attack Mode/Method.
2. Click the attack mode to which you want to add a related attack mode/method.
3. Click the Child Attack mode/method related list.
4. Click Edit.
5. As needed, use the filters to locate the attack mode/method you want to relate to the current one.
6. Using the slushbucket, add the attack mode/method to the Child Attack mode/method list.
7. Click Save.

Add associated task to an attack mode/method

In addition to importing associated tasks (such as changes and incidents) as STIX data, you can add them to an attack mode/method manually.

Before you begin
Role required: sn_ti.admin

Procedure
1. Navigate to Threat Intelligence > IoC Repository > Attack Mode/Method.
2. Click the attack mode to which you want to add an associated task.
3. Click the Associated Tasks related list.
4. Click **Edit**.

5. As needed, use the filters to locate the tasks you want to associate with the attack mode/method.

6. Using the slushbucket, add the task to the **Associated Tasks** list.

7. Click **Save**.

**Indicators of compromise**

Indicators of Compromise (IoC) are artifacts observed on a network or operating system that are likely to indicate an intrusion. Typical IoCs are virus signatures and IP addresses, MD5 hashes of malware files or URLs, or domain names. IoC applies for STIX 1.1 and 2.x.

An IoC can be a single observable or a collection of observables (for example, a single known bad URL or the presence of a specific file and a couple of specific registry key values).

After IoCs have been identified in a process of incident response and computer forensics, they can be used for early detection of future attack attempts using intrusion detection systems and antivirus software.

IoC applies for STIX 1.1 and 2.x.

**View an IoC**

IoCs, sometimes referred to as indicators, are most typically retrieved from a threat data source as STIX data. If needed, you can also create IoCs.

**Before you begin**

Role required: sn_ti.write

**Procedure**

1. After the scheduled job has retrieved IoC data from the **defined data source**, navigate to **Threat Intelligence > IoC Repository > Indicators**.
   
The retrieved IoCs are listed.

2. Click the IoC you want to view.

3. The following information displays.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select classification</td>
<td>If you set up and activated security tags to add metadata to the record,</td>
</tr>
<tr>
<td>tag</td>
<td>you can select one or more tags to specify the degree of sensitivity of the</td>
</tr>
<tr>
<td></td>
<td>IoC.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>If you did not set up or activate security tags, this drop-down list is not displayed.</td>
</tr>
<tr>
<td>Title</td>
<td>A descriptive name for this indicator.</td>
</tr>
<tr>
<td>First Seen</td>
<td>The first date this indicator was observed in the system.</td>
</tr>
<tr>
<td>Last Seen</td>
<td>The most recent date this indicator was observed in the system.</td>
</tr>
<tr>
<td>Encountered count</td>
<td>The number of times the indicator has been encountered.</td>
</tr>
<tr>
<td>Sourced count</td>
<td>The number of times the indicator was imported from defined threat sources.</td>
</tr>
<tr>
<td>Notes</td>
<td>Any additional notes about the indicator. This field can also contain JSON key/value pairs.</td>
</tr>
</tbody>
</table>

4. You can click any of the following related lists to view additional information.

<table>
<thead>
<tr>
<th>Related Links and Related Lists</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Relationships</td>
<td>Opens the STIX Visualizer where you can view the relationship of the STIX object.</td>
</tr>
<tr>
<td></td>
<td>Show Relationships appears only when the object has an associated object.</td>
</tr>
<tr>
<td>Related Observables</td>
<td>Lists observables that are linked to the current indicator.</td>
</tr>
<tr>
<td>Related Attack mode/method</td>
<td>Lists related attack modes/methods that have been identified as related to this indicator.</td>
</tr>
<tr>
<td>Associated Type</td>
<td>Lists other indicator types that are associated with this IoC.</td>
</tr>
<tr>
<td>Indicator Sources</td>
<td>Lists the sources of this indicator, along with the confidence level of the source.</td>
</tr>
<tr>
<td>Associated Tasks</td>
<td>Lists all tasks, changes, and incidents associated with the IoC.</td>
</tr>
<tr>
<td>Related Links and Related Lists</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Indicator Metadata</td>
<td>If the <strong>Notes</strong> field contains valid JSON key/value pairs, they are parsed and displayed. If no JSON key/value pairs are present, or if the JSON is invalid, this related list is not displayed.</td>
</tr>
<tr>
<td>Security Annotations</td>
<td></td>
</tr>
<tr>
<td>Indicator External References</td>
<td></td>
</tr>
<tr>
<td>Associated Kill Chain Phases</td>
<td>Lists kill chain phases associated with this object.</td>
</tr>
<tr>
<td>Attack Patterns</td>
<td>Lists the attack patterns that help categorize attacks that are associated with this object.</td>
</tr>
<tr>
<td>Campaigns</td>
<td>Lists campaigns associated with this object.</td>
</tr>
<tr>
<td>Intrusion Set</td>
<td>Lists a set of adversarial behaviors and resources with common properties associated with this object.</td>
</tr>
<tr>
<td>Malware</td>
<td>Lists malicious code associated with this object.</td>
</tr>
<tr>
<td>Threat Actors</td>
<td>Lists individuals, groups, or organizations who act with malicious intent associated with this object.</td>
</tr>
</tbody>
</table>

**Add a related observable to an IoC**

In addition to importing observables as STIX data, you can add related observables to an IoC manually.

**Before you begin**

Role required: sn_ti.write

**Procedure**

1. Navigate to **Threat Intelligence > IoC Repository > Indicators**.
2. Click the indicator to which you want to add a related observable.
3. Click the **Related Observables** related list.
4. Click **Edit**.
5. As needed, use the filters to locate the observable you want to relate with the IoC.
6. Using the slushbucket, add the observable to the **Related Observables** list.

7. Click **Save**.

**Add a related attack mode/method to an IoC**

In addition to importing related attack modes/methods as STIX data, you can add related attack modes/methods to an IoC manually.

**Before you begin**
Role required: sn_ti.write

**Procedure**
1. Navigate to **Threat Intelligence > IoC Repository > Indicators**.
2. Click the indicator to which you want to add a related attack mode/method.
3. Click the **Related Attack mode/method** related list.
4. Click **Edit**.
5. As needed, use the filters to locate the attack mode/method you want to relate with the IoC.
6. Using the slushbucket, add the attack mode/method to the **Related Attack mode/method** list.
7. Click **Save**.

**Identify associated indicator types**

If an IoC has no associated indicator types defined, it tracks all types of observables. However, if you associate one or more types of indicators to an IoC, it limits the types of observables that can be associated with the IoC.

**Before you begin**
Role required: sn_ti.write

**Procedure**
1. Navigate to **Threat Intelligence > IoC Repository > Indicators**.
2. Click the indicator to which you want to associate an indicator type.
3. Click the **Associated Type** related list.
4. Click **Edit**.
5. As needed, use the filters to locate the indicator type you want to associate with the IoC.
6. Using the slushbucket, add the indicator type to the Associated Type list.
7. Click Save.

**Identify indicator sources**

Indicator sources are normally tracked automatically as part of the threat import process, but more sources can be manually added.

**Before you begin**
Role required: sn_ti.write

**Procedure**

1. Navigate to Threat Intelligence > IoC Repository > Indicators.
2. Click the indicator to which you want to add indicator sources.
3. Click the Indicator Sources related list.
4. Click Edit.
5. As needed, use the filters to locate the indicator source you want to associate with the IoC.
6. Using the slushbucket, add the indicator source to the Indicator Sources list.
7. Click Save.

**Add associated tasks to an IoC**

In addition to importing associated tasks (such as changes and incidents) as STIX data, you can add them to an IoC manually.

**Before you begin**
Role required: sn_ti.write

**Procedure**

1. Navigate to Threat Intelligence > IoC Repository > Indicators.
2. Click the IoC to which you want to add an associated task.
3. Click the Associated Tasks related list.
4. Click Edit.
5. As needed, use the filters to locate the tasks you want to associate with the IoC.
6. Using the slushbucket, add the task to the Associated Tasks list.
7. Click Save.
Observables

Observables represent stateful properties (such as the MD5 hash of a file or the value of a registry key) or measurable events (such as the creation of a registry key or the deletion of a file) that are pertinent to the operation of computers and networks. Observables apply for STIX 1.1 and 2.x.

Sets of cyber observables are useful for identifying indicators of compromise when they are combined with contextual information that represents the behaviors of cyber threats.

Observables apply for STIX 1.1 and 2.x

Define an observable

Observables are retrieved from the vendor server as STIX data. However, you can create observables, as needed.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to Threat Intelligence > IoC Repository > Observables.
2. Click New.
3. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select classification tag</td>
<td>If you set up and activated security tags to add metadata to the record, you can select one or more tags to specify the degree of sensitivity of the observable. If you did not set up or activate security tags, this drop-down list is not displayed.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Value</td>
<td>The value (for example, IP address or hash) associated with the observable.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If a failure occurs on an IP address or hash, returned malware or some other failure, the IP address or hash value is automatically added to the Observable [sn_ti_observable] table. As such, it can be searched for from the Observables form.</td>
</tr>
<tr>
<td>Observable type</td>
<td>Select the observable classification, such as an IP address or file hash. These observable types are defined in the Observable Types module.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For a File type observable, select the Observable Type: File to upload the file attachment.</td>
</tr>
<tr>
<td>Incident count</td>
<td>The number of times the observable value has been encountered.</td>
</tr>
<tr>
<td>Is composition</td>
<td>This field displays only after the observable record has been saved.</td>
</tr>
<tr>
<td></td>
<td>If the Observable Type is set to anything other than Observable Composition, and this new observable is a composition, select this check box.</td>
</tr>
<tr>
<td></td>
<td>If the Observable Type is already set to Observable Composition, the check box is selected and read-only.</td>
</tr>
<tr>
<td></td>
<td>An observable composition is an observable that contains child observables.</td>
</tr>
<tr>
<td>Finding</td>
<td>Select one of the following: None, Unknown or Malicious. Unknown is the default.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> After an upgrade, existing observables are marked Malicious.</td>
</tr>
<tr>
<td>Operator</td>
<td>This field appears only when the Is composition check box is selected. Depending on your setting in this field, the observables and their children are considered when deciding whether an associated indicator is present.</td>
</tr>
<tr>
<td></td>
<td>Set this field to AND if all the child observables must be present for an associated indicator to be considered present.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Field</td>
<td>Set it to <strong>OR</strong> if <strong>any</strong> of the child observables are present for an associated indicator to be considered present.</td>
</tr>
<tr>
<td>Must not be present</td>
<td>This field displays only after the observable record has been saved. If selected, this field signifies that the absence of the observable is the potential issue (for example, a missing registry key).</td>
</tr>
<tr>
<td>Location</td>
<td>Using the settings in two properties and a script include definition, you can load <strong>Load more IoC data</strong> in this field.</td>
</tr>
<tr>
<td>Notes</td>
<td>Enter any additional notes about the observable.</td>
</tr>
</tbody>
</table>

4. Right-click in the form header and click **Save**. You can now click any of the following related lists to view additional information.

<table>
<thead>
<tr>
<th>Related List</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related Indicators</td>
<td>Lists indicators that have been identified by the threat source.</td>
</tr>
<tr>
<td>Associated Tasks</td>
<td>Lists changes associated with the observable.</td>
</tr>
<tr>
<td>Child Observables</td>
<td>Lists related observables that have been identified by the threat source.</td>
</tr>
<tr>
<td>Matching Resources for IP</td>
<td>If the observable is an IP address, this list shows any resources (configuration items) that have a matching IP address.</td>
</tr>
<tr>
<td>Observable Sources</td>
<td>Lists the sources of this observable, along with the confidence level of the source.</td>
</tr>
<tr>
<td>Security Annotations</td>
<td>Lists security annotations added to this observable.</td>
</tr>
</tbody>
</table>

**Add a related IoC to an observable**

In addition to importing observables as STIX data, you can add related observables to an IoC manually.

**Before you begin**

Role required: sn_ti.admin
Procedure
1. Navigate to Threat Intelligence > IoC Repository > Observables.
2. Click the observable to which you want to add a related IoC.
3. Click the Related Indicators related list.
4. Click Edit.
5. As needed, use the filters to locate the indicator you want to relate with the observable.
6. Using the slushbucket, add the indicator to the Related Indicators list.
7. Click Save.

Add associated tasks to an observable
In addition to importing associated tasks (such as changes and incidents) as STIX data, you can add them to an observable manually.

Before you begin
Role required: sn_ti.admin

Procedure
1. Navigate to Threat Intelligence > IoC Repository > Observables.
2. Click the observable to which you want to add an associated task.
3. Click the Associated Tasks related list.
4. Click Edit.
5. As needed, use the filters to locate the tasks you want to associate with the observable.
6. Using the slushbucket, add the task to the Associated Tasks list.
7. Click Save.

Add a related observable
In addition to importing observables as STIX data, you can add related observables manually.

Before you begin
Role required: sn_ti.admin
Procedure
1. Navigate to Threat Intelligence > IoC Repository > Observables.
2. Click the observable to which you want to add a related observable.
3. Click the Child Observables related list.
4. Click Edit.
5. As needed, use the filters to locate the observable you want to relate to the current one.
6. Using the slushbucket, add the observable to the Child Observables list.
7. Click Save.

Load more IoC data
Depending on settings in two properties and a script include definition, you can load geolocation information for IP addresses and websites in the Observables form. With further customization, you can also add other information, such as country codes, city names.

Before you begin
The following two properties must be set:
• The domain name to retrieve additional information for IP addresses/URLs [sn_ti.ip_lookup.web_site]
• The API key to be used for the above domain, if any [sn_ti.ip_lookup.api_key]

Role required: sn_ti.admin

Procedure
1. Navigate to Threat Intelligence > IoC Repository > Observables.
2. Click the IP address or URL of the observable to which you want to view more IoC data.
   The Location field shows the geolocation of the IoC.
3. Click the Enrich data button to load the additional IoC data.
4. You can also configure the Observable form to add other location-related fields, such as the country code and city code.

Note: To load more location-related information, edit the ThreatAdditionalInfo script include and provide the appropriate API key from the website that provides the additional information.
**Identify observable sources**

If an observable has no sources defined, it uses all types of sources. However, if you add one or more threat sources to an observable, it limits the sources used.

**Before you begin**
Role required: sn_ti.admin

**Procedure**
1. Navigate to Threat Intelligence > IoC Repository > Observables.
2. Click the observable to which you want to add observable sources.
3. Click the Observable Sources related list.
4. Click Edit.
5. As needed, use the filters to locate the source you want to associate with the observable.
6. Using the slushbucket, add the observable source to the Observable Sources list.
7. Click Save.

**Perform lookups on observables**

You can perform threat intelligence lookups on one or more observables to determine whether they are associated with known security threats. The scanning implementations that run depend on the ones you have activated.

**Before you begin**
Before you can perform lookups, you must activate the Threat Intelligence plugin. You must also install the plugin for one or more of the scanning implementations:

- CrowdStrike Falcon Intelligence integration
- OPSWAT Metadefender
- Recorded Future
- Security Operations Have I been pwned?
- VirusTotal

Role required: sn_ti.write
Procedure

1. Navigate to Threat Intelligence > IoC Repository > Observables.

2. Do one of the following steps:
   - To perform a lookup on more than one observable, select the observables, click Actions on selected rows, and select Run threat lookup.
   - To perform a lookup on a single observable, open the observable record, and click the Run threat lookup related link.

3. Select the threat lookup implementations you want to use, or select All to perform lookups using all of the active implementations, then click Submit. A message indicates that the threat lookups have begun. The Security Operations Integration - Threat Lookup workflow runs and also executes the implementation workflows for the threat lookup implementations you selected. The lookups are performed and the results are generated.

4. When the lookups are completed, you can click the Threat Lookup Results tab to view the results.

Note:
5. To see additional details, including raw results for a specific lookup, click the Result value.

**Note:** When the VirusTotal or OPSWAT Metadefender implementations are used, the details are consolidated, as shown below.

---

**Perform threat enrichment on observables**

You can perform threat intelligence enrichment on one or more observables to determine whether they are associated with known security threats. The implementations that run depend on the ones you have activated.

**Before you begin**

Before you can perform enrichment, you must activate the Threat Intelligence plugin. You must also install the plugin for one or more of the enrichment implementations:

- **CrowdStrike Falcon Intelligence integration**
- **OPSWAT Metadefender**
- **Recorded Future**
- **Security Operations Have I been pwned?**
- **VirusTotal**
- **WhoIs?**

Role required: sn_ti.admin
Procedure

1. Navigate to Threat Intelligence > IoC Repository > Observables.

2. Do one of the following steps:
   - To perform a lookup on more than one observable, select the observables, click Actions on selected rows, and select Run threat lookup.
   - To perform a lookup on a single observable, open the observable record, and click the Run threat lookup related link.

3. Select the threat lookup implementations you want to use, or select All to perform lookups using all of the active implementations, then click Submit. A message indicates that the threat lookups have begun. The Security Operations Integration - Threat Lookup workflow runs and also executes the implementation workflows for the threat lookup implementations you selected. The lookups are performed and the results are generated.

4. When the lookups are completed, you can click the Threat Lookup Results tab to view the results.

Note:
5. To see additional details, including raw results for a specific lookup, click the Result value.

**Note:** When the VirusTotal or OPSWAT Metadefender implementations are used, the details are consolidated, as shown below.

### Attack patterns

Attack patterns are a type of Tactics, Techniques, and Procedures (TTPs) that describe the methods that adversaries attempt to compromise targets. Attack Patterns apply for STIX 2.x.

Attack patterns are used to help categorize attacks. They generalize specific attacks to the patterns that they follow, and provide detailed information about how attacks are performed.

For example, spear phishing is a common type of attack where an attacker sends a carefully crafted email message to a party with the intent of getting them to click a link or open an attachment to deliver malware. Attack Patterns are more specific, such as spear phishing by a particular threat actor (example - that the target won a contest) can also be an Attack pattern.

**Define an attack pattern**

Define an attack pattern to help categorize attacks.

**Before you begin**

Role required: sn_ti.admin
Procedure

1. Navigate to **Threat Intelligence > IoC Repository > Attack Patterns.**
2. Click **New.**
3. Complete the fields in the form as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name for this attack pattern.</td>
</tr>
<tr>
<td>Spec Version</td>
<td>The version of the STIX specification used to represent this object.</td>
</tr>
<tr>
<td></td>
<td>The value of this property must be 2.1 for STIX Objects defined according to</td>
</tr>
<tr>
<td></td>
<td>this specification.</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies the threat source from which this record is created.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the attack pattern.</td>
</tr>
<tr>
<td>Aliases</td>
<td>Alternative names to identify this attack pattern.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Unique identifier for this object in the threat source.</td>
</tr>
<tr>
<td>Created Time in Source</td>
<td>Specifies the time the object is created in the source.</td>
</tr>
<tr>
<td>Modified Time in Source</td>
<td>Specifies the time the object is modified in the source.</td>
</tr>
</tbody>
</table>

4. Click **Submit.**

**What to do next**
You can now click any of the following related lists to view additional information about objects associated with the attack pattern.

<table>
<thead>
<tr>
<th>Related Links and Related Lists</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Relationships</td>
<td>Opens the STIX Visualizer where you can view the relationship of the STIX object.</td>
</tr>
<tr>
<td>Related Links and Related Lists</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Show Relationships</td>
<td>Show Relationships appears only when the object has an associated object.</td>
</tr>
<tr>
<td>External References</td>
<td>Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.</td>
</tr>
<tr>
<td>Associated Kill Chain Phases</td>
<td>Lists kill chain phases associated with this object.</td>
</tr>
<tr>
<td>Campaigns</td>
<td>Lists campaigns associated with this object.</td>
</tr>
<tr>
<td>Course of Actions</td>
<td>Lists the associated course of actions with this object that are technical or automated responses (applying patches, reconfiguring firewalls) to prevent an attack.</td>
</tr>
<tr>
<td>Identities</td>
<td>List of identities associated with this object.</td>
</tr>
<tr>
<td>Indicators</td>
<td>Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.</td>
</tr>
<tr>
<td>Intrusion Set</td>
<td>Lists a set of adversarial behaviors and resources with common properties associated with this object.</td>
</tr>
<tr>
<td>Locations</td>
<td>Lists locations that provide geographic context to this object.</td>
</tr>
<tr>
<td>Malware</td>
<td>Lists malicious code associated with this object.</td>
</tr>
<tr>
<td>Threat Actors</td>
<td>Lists individuals, groups, or organizations who act with malicious intent associated with this object.</td>
</tr>
<tr>
<td>Tools</td>
<td>Lists legitimate software that is used by threat actors to perform attacks associated with this object.</td>
</tr>
</tbody>
</table>
| Vulnerabilities | Lists a weakness or defect in a software or hardware that attackers
Related Links and Related Lists

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>exploit which is associated with this object.</td>
</tr>
</tbody>
</table>

Campaigns

A Campaign is a grouping of adversarial behaviors. These behaviors describe a set of malicious activities or attacks that occur over time against a specific set of targets. Campaigns apply for STIX 2.x.

Campaigns usually have well-defined objectives and may be part of an Intrusion Set.

Campaigns are often attributed to an intrusion set and threat actors. The threat actors may reuse known infrastructure from the intrusion set or may set up new infrastructure specific for conducting that campaign.

Campaigns have a common objective in the incidents they cause, to people, or to the resources they target, and the resources they use.

For example, a crime syndicate attacks the executives of ACME Bank. They attack by using a specific variant of malware, and new servers to gain secret information about an upcoming merger with another bank.

Define a campaign

Define a campaign to group adversarial behaviors.

**Before you begin**

Role required: sn_ti.admin

**Procedure**

1. Navigate to Threat Intelligence > IoC Repository > Campaigns.
2. Click New.
3. Complete the fields in the form as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name for this campaign.</td>
</tr>
<tr>
<td>Spec Version</td>
<td>The version of the STIX specification used to represent this object. The value of this property must be 2.1 for STIX Objects defined according to this specification.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies the threat source from which this record is created.</td>
</tr>
<tr>
<td>Description</td>
<td>A description that provides more details and context about the campaign. This includes its purpose and its key characteristics.</td>
</tr>
<tr>
<td>Aliases</td>
<td>Alternative names to identify this campaign.</td>
</tr>
<tr>
<td>Objective</td>
<td>The campaign's primary goal, objective, desired outcome, or intended effect. What the threat actor or intrusion set hopes to accomplish with this campaign.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Unique identifier for this object in the threat source.</td>
</tr>
<tr>
<td>Created Time in Source</td>
<td>Specifies the time the object is created in the source.</td>
</tr>
<tr>
<td>Modified Time in Source</td>
<td>Specifies the time the object is modified in the source.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**What to do next**

You can now click any of the following related lists to view additional information about objects associated with the campaign.

<table>
<thead>
<tr>
<th>Related Links and Related Lists</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Relationships</td>
<td>Opens the STIX Visualizer where you can view the relationship of the STIX object.</td>
</tr>
<tr>
<td></td>
<td>Show Relationships appears only when the object has an associated object.</td>
</tr>
<tr>
<td>External References</td>
<td>Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.</td>
</tr>
<tr>
<td>Related Links and Related Lists</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Attack Patterns</td>
<td>Lists the attack patterns that help categorize attacks that are associated with this object.</td>
</tr>
<tr>
<td>Identities</td>
<td>List of identities associated with this object.</td>
</tr>
<tr>
<td>Indicators</td>
<td>Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>Lists systems, software services, and any associated physical or virtual resources that are associated with this object.</td>
</tr>
<tr>
<td>Intrusion Set</td>
<td>Lists a set of adversarial behaviors and resources with common properties associated with this object.</td>
</tr>
<tr>
<td>Locations</td>
<td>Lists locations that provide geographic context to this object.</td>
</tr>
<tr>
<td>Malware</td>
<td>Lists malicious code associated with this object.</td>
</tr>
<tr>
<td>Threat Actors</td>
<td>Lists individuals, groups, or organizations who act with malicious intent associated with this object.</td>
</tr>
<tr>
<td>Tools</td>
<td>Lists legitimate software that is used by threat actors to perform attacks associated with this object.</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.</td>
</tr>
</tbody>
</table>

**Course of actions**

A course of action is an action taken either to prevent an attack or to respond to an attack that is in progress. Course of actions apply for STIX 2.x.
Course of actions describes technical or automated responses (applying patches, reconfiguring firewalls). It can also describe higher-level actions like employee training or policy changes.

For example, a course of action to mitigate a vulnerability could describe applying the patch that fixes it.

**Define a course of action**

Define a course of action to prevent an attack or to respond to an attack that is in progress.

**Before you begin**

Role required: sn_ti.admin

**Procedure**

1. Navigate to Threat Intelligence > IoC Repository > Course of Actions.
2. Click New.
3. Complete the fields in the form as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name for this course of action.</td>
</tr>
<tr>
<td>Action</td>
<td>To capture structured or automated courses of action.</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies the threat source from which this record is created.</td>
</tr>
<tr>
<td>Description</td>
<td>A description that provides more details and context about the course of action, potentially including its purpose and its key characteristics.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Unique identifier for this object in the threat source.</td>
</tr>
<tr>
<td>Created Time in Source</td>
<td>Specifies the time the object is created in the source.</td>
</tr>
<tr>
<td>Modified Time in Source</td>
<td>Specifies the time the object is modified in the source.</td>
</tr>
</tbody>
</table>

4. Click Submit.
What to do next

Click any of the following related lists to view additional information about objects associated with the course of action.

<table>
<thead>
<tr>
<th>Related Links</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Relationships</td>
<td>Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.</td>
</tr>
<tr>
<td>External References</td>
<td>Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.</td>
</tr>
<tr>
<td>Attack Patterns</td>
<td>Lists the attack patterns that help categorize attacks that are associated with this object.</td>
</tr>
<tr>
<td>Indicators</td>
<td>Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.</td>
</tr>
<tr>
<td>Malware</td>
<td>Lists malicious code associated with this object.</td>
</tr>
<tr>
<td>Tools</td>
<td>Lists legitimate software that is used by threat actors to perform attacks associated with this object.</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.</td>
</tr>
</tbody>
</table>

Identities

Identities represent actual individuals, organizations, or groups (ACME, Inc.) and classes of individuals, systems, or groups (the finance sector). Identities apply for STIX 2.x.

The Identity SDO can capture basic identifying information, contact information, and the sectors that the Identity belongs to. Identity represents targets of attacks, information sources, object creators, and threat actor identities.
Define identities
Define identities who represent actual individuals, organizations, or groups.

Before you begin
Role required: sn_ti.admin

Procedure
1. Navigate to Threat Intelligence > IoC Repository > Identities.
2. Click New.
3. Complete the fields in the form as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name for this identity. When referring to a specific entity (an individual or organization), this property must contain the canonical name of the specific entity.</td>
</tr>
<tr>
<td>Identity Class</td>
<td>The type of entity that this identity describes. For example, individual or organization.</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies the threat source from which this record is created.</td>
</tr>
<tr>
<td>Description</td>
<td>A description that provides more details and context about the identity, potentially including its purpose and its key characteristics.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Unique identifier for this object in the threat source.</td>
</tr>
<tr>
<td>Created Time in Source</td>
<td>Specifies the time the object is created in the source.</td>
</tr>
<tr>
<td>Modified Time in Source</td>
<td>Specifies the time the object is modified in the source.</td>
</tr>
</tbody>
</table>

4. Click Submit.
What to do next
Click any of the following related lists to view additional information about objects associated the identity.

<table>
<thead>
<tr>
<th>Related Links and Related Lists</th>
<th>Description</th>
</tr>
</thead>
</table>
| Show Relationships                    | Opens the STIX Visualizer where you can view the relationship of the STIX object.  
                                            Show Relationships appears only when the object has an associated object.        |
| External References                   | Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers. |
| Attack Patterns                       | Lists the attack patterns that help categorize attacks that are associated with this object. |
| Campaigns                             | Lists campaigns associated with this object.                                 |
| Intrusion Set                         | Lists a set of adversarial behaviors and resources with common properties associated with this object. |
| Locations                             | Lists locations that provide geographic context to this object.              |
| Malware                               | Lists malicious code associated with this object.                           |
| Threat Actors                         | Lists individuals, groups, or organizations who act with malicious intent associated with this object. |
| Tools                                 | Lists legitimate software that is used by threat actors to perform attacks associated with this object. |

Infrastructure
The Infrastructure SDO represents a type of Tactics, Techniques, and Procedures (TTPs). They describe any systems, software services, and any associated
physical or virtual resources intended to support some purpose of an attack. Infrastructure applies for STIX 2.x.

The elements of an attack are represented by other SDOs or SCOs. However, the Infrastructure SDO represents a named group of data that constitutes the infrastructure.

Examples of infrastructure include, C2 servers used in an attack, a device, or a server that is part of a defense, or database servers targeted by an attack.

**Define infrastructure**

Define an Infrastructure that is any systems, software services, and any associated physical or virtual resources intended to support some purpose of an attack.

**Before you begin**

Role required: sn_ti.admin

**Procedure**

1. Navigate to **Threat Intelligence > IoC Repository > Infrastructure**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name to identify the infrastructure.</td>
</tr>
<tr>
<td>First Seen</td>
<td>The time that this infrastructure was first seen performing malicious activities.</td>
</tr>
<tr>
<td>Last Seen</td>
<td>The time that this infrastructure was last seen performing malicious activities.</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies the threat source from which this record is created.</td>
</tr>
<tr>
<td>Description</td>
<td>A description that provides more details and context about the Infrastructure, potentially including its purpose, how it is being used, how it relates to other intelligence activities captured in related objects, and its key characteristics.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Aliases</td>
<td>Alternative names to identify this infrastructure.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Unique identifier for this object in the threat source.</td>
</tr>
<tr>
<td>Created Time in Source</td>
<td>Specifies the time the object is created in the source.</td>
</tr>
<tr>
<td>Modified Time in Source</td>
<td>Specifies the time the object is modified in the source.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**What to do next**

You can now click any of the following related lists to view additional information. You can also associate other objects with the infrastructure.

<table>
<thead>
<tr>
<th>Related Links and Related Lists</th>
<th>Description</th>
</tr>
</thead>
</table>
| Show Relationships              | Opens the STIX Visualizer where you can view the relationship of the STIX object.  
<pre><code>                                | Show Relationships appears only when the object has an associated object.     |
</code></pre>
<p>| External References             | Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers. |
| Associated Types                | Lists indicator types associated with this object.                          |
| Associated Kill Chain Phases    | Lists kill chain phases associated with this object.                        |
| Associated Observables          | Lists observables associated with this object.                               |
| Associated Infrastructure       | Lists systems, software services, and any associated physical or virtual resources that are associated with this object. |</p>
<table>
<thead>
<tr>
<th>Related Links and Related Lists</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Campaigns</td>
<td>Lists campaigns associated with this object.</td>
</tr>
<tr>
<td>Indicators</td>
<td>Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.</td>
</tr>
<tr>
<td>Intrusion Set</td>
<td>Lists a set of adversarial behaviors and resources with common properties associated with this object.</td>
</tr>
<tr>
<td>Locations</td>
<td>Lists locations that provide geographic context to this object.</td>
</tr>
<tr>
<td>Malware</td>
<td>Lists malicious code associated with this object.</td>
</tr>
<tr>
<td>Observed Data</td>
<td>Lists observed data associated with this object.</td>
</tr>
<tr>
<td>Threat Actors</td>
<td>Lists individuals, groups, or organizations who act with malicious intent associated with this object.</td>
</tr>
<tr>
<td>Tools</td>
<td>Lists legitimate software that is used by threat actors to perform attacks associated with this object.</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.</td>
</tr>
</tbody>
</table>

**Intrusion set**

An Intrusion Set is a grouped set of adversarial behaviors and resources with common properties. An Intrusion Set usually involves a single organization. Intrusion set applies for STIX 2.x.

An Intrusion Set may capture multiple Campaigns or other activities. These activities share attributes indicating a commonly known or unknown Threat Actor.

New activity can be attributed to an Intrusion Set even if the Threat Actors behind the attack are not known. Threat Actors can move from supporting one Intrusion Set to supporting another, or they may support multiple Intrusion Sets.
An Intrusion Set is the entire attack package and may be used over a long period in multiple Campaigns to achieve potentially multiple purposes.

**Define an intrusion set**

Define an intrusion set that is a grouped set of adversarial behaviors and resources with common properties.

**Before you begin**

Role required: sn_ti.admin

**Procedure**

1. Navigate to **Threat Intelligence > IoC Repository > Intrusion Set**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name to identify the intrusion set.</td>
</tr>
<tr>
<td>First Seen</td>
<td>The time that this intrusion set was first seen performing malicious activities.</td>
</tr>
<tr>
<td>Last Seen</td>
<td>The time that this intrusion set was last seen performing malicious activities.</td>
</tr>
<tr>
<td>Primary Motivation</td>
<td>The primary reason, motivation, or purpose behind this intrusion set. The motivation is why the Intrusion Set wants to achieve the goal (what they are trying to achieve). For example, an intrusion set with a goal to disrupt the finance sector in a country might be motivated by ideological hatred of capitalism.</td>
</tr>
<tr>
<td>Resource Level</td>
<td>This property specifies the organizational level at which this intrusion set typically works, which in turn determines the resources available for use in an attack.</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies the threat source from which this record is created.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Description</td>
<td>A description that provides more details and context about the intrusion set, potentially including its purpose and its key characteristics.</td>
</tr>
<tr>
<td>Aliases</td>
<td>Alternative names to identify this intrusion set.</td>
</tr>
<tr>
<td>Goals</td>
<td>The high-level goals of this intrusion set, namely, what are they trying to do. For example, they may be motivated by personal gain, but their goal is to steal credit card numbers. To do this, they may execute specific campaigns that have detailed objectives like compromising point of sale systems at a large retailer.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Unique identifier for this object in the threat source.</td>
</tr>
<tr>
<td>Created Time in Source</td>
<td>Specifies the time the object is created in the source.</td>
</tr>
<tr>
<td>Modified Time in Source</td>
<td>Specifies the time the object is modified in the source.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**What to do next**

Click any of the following related lists to view additional information about objects associated with the intrusion set.

<table>
<thead>
<tr>
<th>Related Links and Related Lists</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Relationships</td>
<td>Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.</td>
</tr>
<tr>
<td>External References</td>
<td>Lists external references which refer to non-STIX information. This property is</td>
</tr>
<tr>
<td>Related Links and Related Lists</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Associated Attack Motivations</td>
<td>Lists any secondary motivations why this intrusion set wants to achieve.</td>
</tr>
<tr>
<td>Attack Patterns</td>
<td>Lists the attack patterns that help categorize attacks that are associated with this object.</td>
</tr>
<tr>
<td>Campaigns</td>
<td>Lists campaigns associated with this object.</td>
</tr>
<tr>
<td>Identities</td>
<td>List of identities associated with this object.</td>
</tr>
<tr>
<td>Indicators</td>
<td>Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.</td>
</tr>
<tr>
<td>Locations</td>
<td>Lists locations that provide geographic context to this object.</td>
</tr>
<tr>
<td>Malware</td>
<td>Lists malicious code associated with this object.</td>
</tr>
<tr>
<td>Threat Actors</td>
<td>Lists individuals, groups, or organizations who act with malicious intent associated with this object.</td>
</tr>
<tr>
<td>Tools</td>
<td>Lists legitimate software that is used by threat actors to perform attacks associated with this object.</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.</td>
</tr>
</tbody>
</table>

**Locations**

A Location represents a geographic location. Locations are primarily used to give context to other SDOs. Locations apply for STIX 2.x.

The location may contain, some or all of the following: region (North America), civic address (New York, US), latitude, and longitude.
The Location SDO may relate to an Identity or Intrusion Set to indicate that the identity or intrusion set is in that location. It can also relate to a malware or attack pattern to indicate that the target victim is in a particular location.

For example, a Location could be used in a relationship to describe that the Bourgeois Swallow intrusion set originates from Eastern Europe.

At least one of the following properties or sets of properties must be provided:

- region
- country
- latitude and longitude

### Define Location

Define a geographic location to provide more context to other SDOs.

#### Before you begin

Role required: sn_ti.admin

#### Procedure

1. Navigate to **Threat Intelligence > IoC Repository > Locations**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name to identify the location.</td>
</tr>
<tr>
<td>Street Address</td>
<td>The street address that this location describes. This property includes all aspects or parts of the street address.</td>
</tr>
<tr>
<td>City</td>
<td>The city that this location is in.</td>
</tr>
<tr>
<td>Postal Code</td>
<td>The postal code that this location is in.</td>
</tr>
<tr>
<td>Region</td>
<td>The region that this location is in.</td>
</tr>
<tr>
<td>Country</td>
<td>The country that this location is in.</td>
</tr>
<tr>
<td>Latitude</td>
<td>The latitude of the Location in decimal degrees. Positive numbers describe latitudes north of the equator,</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>and negative numbers describe latitudes south of the equator. The value of this property must be from -90.0 through 90.0 respectively.</td>
<td></td>
</tr>
<tr>
<td>Longitude</td>
<td>The longitude of the location in decimal degrees. Positive numbers describe longitudes east of the prime meridian and negative numbers describe longitudes west of the prime meridian. The value of this property must be from -180.0 through 180.0, inclusive.</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies the threat source from which this record is created.</td>
</tr>
<tr>
<td>Description</td>
<td>A description that provides more details and context about the intrusion set, potentially including its purpose and its key characteristics.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Unique identifier for this object in the threat source.</td>
</tr>
<tr>
<td>Created Time in Source</td>
<td>Specifies the time the object is created in the source.</td>
</tr>
<tr>
<td>Modified Time in Source</td>
<td>Specifies the time the object is modified in the source.</td>
</tr>
</tbody>
</table>

4. Click Submit.

What to do next
Click any of the following related lists to view additional information about objects associated with the location.

<table>
<thead>
<tr>
<th>Related Links and Related Lists</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Relationships</td>
<td>Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.</td>
</tr>
<tr>
<td>Related Links and Related Lists</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>External References</td>
<td>Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.</td>
</tr>
<tr>
<td>Attack Patterns</td>
<td>Lists the attack patterns that help categorize attacks that are associated with this object.</td>
</tr>
<tr>
<td>Campaigns</td>
<td>Lists campaigns associated with this object.</td>
</tr>
<tr>
<td>Identities</td>
<td>List of identities associated with this object.</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>Lists systems, software services, and any associated physical or virtual resources that are associated with this object.</td>
</tr>
<tr>
<td>Intrusion Set</td>
<td>Lists a set of adversarial behaviors and resources with common properties associated with this object.</td>
</tr>
<tr>
<td>Malware</td>
<td>Lists malicious code associated with this object.</td>
</tr>
<tr>
<td>Threat Actors</td>
<td>Lists individuals, groups, or organizations who act with malicious intent associated with this object.</td>
</tr>
<tr>
<td>Tools</td>
<td>Lists legitimate software that is used by threat actors to perform attacks associated with this object.</td>
</tr>
</tbody>
</table>

**Malware**

Malware is a type of TTP that represents malicious code. It refers to a program that is covertly inserted into a system. Malware applies for STIX 2.x.

The intent of a malware is to compromise the confidentiality, integrity, or availability of the victim’s data, applications, or operating system (OS).

The Malware SDO characterizes, identifies, and categorizes malware instances and families from data that is derived from analysis. This SDO captures detailed information about how the malware works and what it does.
Define a Malware

Define a malware that represents malicious code.

Before you begin
Role required: sn_ti.admin

Procedure
1. Navigate to Threat Intelligence > IoC Repository > Malware.
2. Click New.
3. Complete the fields in the form as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name to identify the malware instance or family, as specified by the producer of the SDO. For a malware family, the name must be defined.</td>
</tr>
<tr>
<td>First Seen</td>
<td>The time that this malware instance or family was first seen performing malicious activities.</td>
</tr>
<tr>
<td>Last Seen</td>
<td>The time that this malware instance or family was last seen performing malicious activities.</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies the threat source from which this record is created.</td>
</tr>
<tr>
<td>Description</td>
<td>A description that provides more details and context about the malware instance or family, potentially including its purpose and its key characteristics.</td>
</tr>
<tr>
<td>Aliases</td>
<td>Alternative names to identify this malware instance or family.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Unique identifier for this object in the threat source.</td>
</tr>
<tr>
<td>Is Family</td>
<td>Specifies if the object represents a malware family or a malware instance.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Created Time in Source</td>
<td>Specifies the time the object is created in the source.</td>
</tr>
<tr>
<td>Modified Time in Source</td>
<td>Specifies the time the object is modified in the source.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**What to do next**

Click any of the following related lists to view additional information about objects associated with the malware.

<table>
<thead>
<tr>
<th>Related Links and Related Lists</th>
<th>Description</th>
</tr>
</thead>
</table>
| Show Relationships              | Opens the STIX Visualizer where you can view the relationship of the STIX object.  
<pre><code>                             | Show Relationships appears only when the object has an associated object.       |
</code></pre>
<p>| External References             | Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers. |
| Associated Types                | Lists indicator types associated with this object.                          |
| Associated Capabilities         | Lists the capabilities identified and associated with this object.           |
| Associated Kill Chain Phases    | Lists kill chain phases associated with this object.                         |
| Associated Observables          | Lists observables associated with this object.                               |
| Associated Malware              | Lists the associated malware identified with this object.                    |
| Associated Operating Systems    | The operating systems that the object is executable on. This applies to virtualized operating systems as well as those running on bare metal. |</p>
<table>
<thead>
<tr>
<th>Related Links and Related Lists</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Patterns</td>
<td>Lists the attack patterns that help categorize attacks that are associated with this object.</td>
</tr>
<tr>
<td>Campaigns</td>
<td>Lists campaigns associated with this object.</td>
</tr>
<tr>
<td>Course of Actions</td>
<td>Lists the associated course of actions with this object that are technical or automated responses (applying patches, reconfiguring firewalls) to prevent an attack.</td>
</tr>
<tr>
<td>Identities</td>
<td>List of identities associated with this object.</td>
</tr>
<tr>
<td>Indicators</td>
<td>Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>Lists systems, software services, and any associated physical or virtual resources that are associated with this object.</td>
</tr>
<tr>
<td>Intrusion Set</td>
<td>Lists a set of adversarial behaviors and resources with common properties associated with this object.</td>
</tr>
<tr>
<td>Locations</td>
<td>Lists locations that provide geographic context to this object.</td>
</tr>
<tr>
<td>Malware Analysis</td>
<td>Lists malware analysis records associated with this object.</td>
</tr>
<tr>
<td>Reported Observables</td>
<td>Lists observables reported as part of this object.</td>
</tr>
<tr>
<td>Threat Actors</td>
<td>Lists individuals, groups, or organizations who act with malicious intent associated with this object.</td>
</tr>
<tr>
<td>Tools</td>
<td>Lists legitimate software that is used by threat actors to perform attacks associated with this object.</td>
</tr>
</tbody>
</table>
Malware analysis

Malware Analysis captures the metadata and results of a malware. Malware analysis applies for STIX 2.x.

Malware Analysis includes static or dynamic analysis performed on a malware instance or family.

Define malware analysis

Define malware analysis that captures the metadata and results of a particular static or dynamic analysis performed on a malware instance or family.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to Threat Intelligence > IoC Repository > Malware Analysis.
2. Click New.
3. Complete the fields in the form as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name to identify the intrusion set.</td>
</tr>
<tr>
<td>Analysis Engine Version</td>
<td>The version of the analysis engine or product (including AV engines) that was used to perform the analysis.</td>
</tr>
<tr>
<td>Analysis Definition Version</td>
<td>The version of the analysis definitions used by the analysis tool (including AV tools).</td>
</tr>
<tr>
<td>Analysis Started</td>
<td>The date and time that the malware analysis was initiated.</td>
</tr>
<tr>
<td>Analysis Ended</td>
<td>The date and time that the malware analysis was ended.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies the threat source from which this record is created.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Unique identifier for this object in the threat source.</td>
</tr>
<tr>
<td>Result</td>
<td>The classification result as determined by the scanner or tool analysis process.</td>
</tr>
<tr>
<td>Result Name</td>
<td>The classification result or name assigned to the malware instance by the scanner tool.</td>
</tr>
<tr>
<td>Created Time in Source</td>
<td>Specifies the time the object is created in the source.</td>
</tr>
<tr>
<td>Modified Time in Source</td>
<td>Specifies the time the object is modified in the source.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**What to do next**
Click any of the following related lists to view additional information on the objects associated with malware analysis.

<table>
<thead>
<tr>
<th>Related Links and Related Lists</th>
<th>Description</th>
</tr>
</thead>
</table>
| Show Relationships                       | Opens the STIX Visualizer where you can view the relationship of the STIX object.  
                                          | Show Relationships appears only when the object has an associated object.       |
| External References                      | Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers. |
| Associated Malware                       | Lists the associated malware identified with this object.                   |
| Reported Observables                     | Lists observables reported as part of this object.                          |
### Related Links and Related Lists

<table>
<thead>
<tr>
<th>Related Links and Related Lists</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed Software</td>
<td>Lists any non-standard software installed on the operating system used for the dynamic analysis of the malware instance or family.</td>
</tr>
</tbody>
</table>

### Observed data

Observed Data conveys information about cyber security-related entities such as files, systems, and networks using the STIX Cyber-observable Objects (SCOs). Observed data applies for STIX 2.x.

Observed Data captures both a single observation of a single entity (file, network connection) as well as the aggregation of multiple observations of an entity.

You can use Observed Data by itself (without relationships) to convey raw data collected from any source. Sources include analyst reports, sandboxes, and network and host-based detection tools.

For example, Observed Data can capture information about an IP address, a network connection, a file, or a registry key. Observed Data is not an intelligence assertion, it is simply the raw information without any context for what it means.

### Define observed data

Define observed data that conveys information about cyber security-related entities such as files, systems, and networks using the STIX Cyber-observable Objects (SCOs).

### Before you begin

Role required: sn_ti.admin

### Procedure

1. Navigate to **Threat Intelligence > IoC Repository > Observed Data**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Observed</td>
<td>The initial time when the data was seen.</td>
</tr>
<tr>
<td>Last Observed</td>
<td>The last time when the data was seen.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Observed Count</td>
<td>The number of times that each Cyber-observable object was seen. The value must be an integer from 1 through 999,999,999.</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies the threat source from which this record is created.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Unique identifier for this object in the threat source.</td>
</tr>
<tr>
<td>Created Time in Source</td>
<td>Specifies the time the object is created in the source.</td>
</tr>
<tr>
<td>Modified Time in Source</td>
<td>Specifies the time the object is modified in the source.</td>
</tr>
</tbody>
</table>

4. Click Submit.

**What to do next**
Click any of the following related lists to view additional information about objects associated with the observed data.

<table>
<thead>
<tr>
<th>Related Links and Related Lists</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Relationships</td>
<td>Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.</td>
</tr>
<tr>
<td>External References</td>
<td>Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.</td>
</tr>
<tr>
<td>Associated Observables</td>
<td>Lists observables associated with this object.</td>
</tr>
<tr>
<td>Indicators</td>
<td>Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>Lists systems, software services, and any associated physical or virtual</td>
</tr>
</tbody>
</table>
Threat actors

Threat Actors are individuals, groups, or organizations who act with malicious intent. Threat actors applies for STIX 2.x.

A Threat Actor is not an Intrusion Set but may support or be affiliated with various Intrusion Sets, groups, or organizations over time.

Threat Actors use their resources, and the resources of an Intrusion Set, to conduct attacks, and run Campaigns against targets.

You can identify Threat Actors by their motives, capabilities, goals, sophistication level, past activities, resources they have access to, and their role in the organization.

Define threat actors

Define threat actors who are individuals, groups, or organizations who act with malicious intent.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to Threat Intelligence > IoC Repository > Threat Actors.
2. Click New.
3. Complete the fields in the form as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name to identify the malware instance or family, as specified by the producer of the SDO. For a malware family, the name must be defined.</td>
</tr>
<tr>
<td>First Seen</td>
<td>The time that this malware instance or family was first seen performing malicious activities.</td>
</tr>
<tr>
<td>Last Seen</td>
<td>The time that this malware instance or family was last seen performing malicious activities.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Primary Motivation</td>
<td>The primary reason, motivation, or purpose behind this threat actor. The motivation is why the threat actor wants to achieve the goal (what they are trying to achieve). For example, a threat actor with a goal to disrupt the finance sector in a country might be motivated by ideological hatred of capitalism.</td>
</tr>
<tr>
<td>Resource Level</td>
<td>The organizational level at which this threat actor typically works, which in turn determines the resources available to this Threat Actor for use in an attack.</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies the threat source from which this record is created.</td>
</tr>
<tr>
<td>Description</td>
<td>A description that provides more details and context about the threat actor, potentially including its purpose and its key characteristics.</td>
</tr>
<tr>
<td>Aliases</td>
<td>A list of other names to identify this threat actor.</td>
</tr>
<tr>
<td>Goals</td>
<td>The high-level goals of this threat actor, namely, what are they trying to do. For example, they may be motivated by personal gain, but their goal is to steal credit card numbers.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Unique identifier for this object in the threat source.</td>
</tr>
<tr>
<td>Created Time in Source</td>
<td>Specifies the time the object is created in the source.</td>
</tr>
<tr>
<td>Modified Time in Source</td>
<td>Specifies the time the object is modified in the source.</td>
</tr>
</tbody>
</table>

4. Click Submit.
What to do next
Click any of the following related lists to view additional information about objects associated with the threat actor.

<table>
<thead>
<tr>
<th>Related Links and Related Lists</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Relationships</td>
<td>Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.</td>
</tr>
<tr>
<td>External References</td>
<td>Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.</td>
</tr>
<tr>
<td>Associated Types</td>
<td>Lists indicator types associated with this object.</td>
</tr>
<tr>
<td>Associated Roles</td>
<td>Lists the associated roles with the threat actor.</td>
</tr>
<tr>
<td>Associated Attack Motivations</td>
<td>Lists the associated attack motivations with the threat actor.</td>
</tr>
<tr>
<td>Attack Patterns</td>
<td>Lists the attack patterns that help categorize attacks that are associated with this object.</td>
</tr>
<tr>
<td>Campaigns</td>
<td>Lists campaigns associated with this object.</td>
</tr>
<tr>
<td>Identities</td>
<td>List of identities associated with this object.</td>
</tr>
<tr>
<td>Indicators</td>
<td>Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>Lists systems, software services, and any associated physical or virtual resources that are associated with this object.</td>
</tr>
<tr>
<td>Related Links and Related Lists</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Intrusion Set</td>
<td>Lists a set of adversarial behaviors and resources with common properties associated with this object.</td>
</tr>
<tr>
<td>Locations</td>
<td>Lists locations that provide geographic context to this object.</td>
</tr>
<tr>
<td>Malware</td>
<td>Lists malicious code associated with this object.</td>
</tr>
<tr>
<td>Tools</td>
<td>Lists legitimate software that is used by threat actors to perform attacks associated with this object.</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.</td>
</tr>
</tbody>
</table>

**Threat groupings**

A Threat Groupings object explicitly asserts that the referenced STIX Objects have a shared context. Threat groupings applies for STIX 2.x.

A Threat Groupings object represents a set of data that, given sufficient analysis, matures to convey an incident or threat report as a STIX Report object. For example, a Grouping could be used to characterize an ongoing investigation into a security event or incident.

A Threat Groupings object could also be used to assert that the referenced STIX Objects are related to an ongoing analysis process. For example, a threat analyst may collaborate with others in their trust community to examine a series of Campaigns and Indicators.

The Threat Grouping SDO contains a list of references to SDOs, SCOs, and SROs, along with an explicit statement of the context shared by the content, a textual description, and the name of the grouping.

**Define threat groupings**

Define threat groupings as objects that have a shared context.

**Before you begin**

Role required: sn_ti.admin
Procedure

1. Navigate to **Threat Intelligence > IoC Repository > Threat Groupings.**
2. Click **New.**
3. Complete the fields in the form as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name to identify the threat grouping.</td>
</tr>
<tr>
<td>Context</td>
<td>A description of the particular context shared by the content referenced by the grouping.</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies the threat source from which this record is created.</td>
</tr>
<tr>
<td>Description</td>
<td>A short description that provides details and context about the grouping. This includes its purpose and its key characteristics.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Unique identifier for this object in the threat source.</td>
</tr>
<tr>
<td>Created Time in Source</td>
<td>Specifies the time the object is created in the source.</td>
</tr>
<tr>
<td>Modified Time in Source</td>
<td>Specifies the time the object is modified in the source.</td>
</tr>
</tbody>
</table>

4. Click **Submit.**

What to do next

Click any of the following related lists to view additional information about objects associated with the threat grouping.

<table>
<thead>
<tr>
<th>Related Links and Related Lists</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Relationships</td>
<td>Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.</td>
</tr>
</tbody>
</table>
### Marking definitions

The marking definitions object represents a specific marking. Data markings represent restrictions, permissions, and other guidance for how data can be used and shared.

For example, data may be shared with the restriction that it must not be reshared, or that it must be encrypted at rest.

In STIX, data markings are specified using the marking definition object. These definitions are applied to STIX Objects using object markings and to individual properties of STIX Objects via granular markings.

#### Define marking definitions

Define marking definitions that represent a specific data marking.

**Before you begin**

Role required: sn_ti.admin

#### Procedure

1. Navigate to Threat Intelligence > IoC Repository > Marking Definitions.
2. Click New.
3. Complete the fields in the form as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definition</td>
<td>Specify the marking object (example, TLP) or some other marking definition that has been defined.</td>
</tr>
<tr>
<td>Definition Type</td>
<td>Identifies the type of marking definition - statement or TLP (Traffic Light Protocol).</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Specifies the threat source from which this record is created.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Unique identifier for this object in the threat source.</td>
</tr>
<tr>
<td>Created Time in Source</td>
<td>Specifies the time the object is created in the source.</td>
</tr>
<tr>
<td>Modified Time in Source</td>
<td>Specifies the time the object is modified in the source.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**What to do next**

Click any of the following related lists to view additional information about objects associated with the marking definition.

<table>
<thead>
<tr>
<th>Related Links and Related Lists</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Relationships</td>
<td>Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.</td>
</tr>
<tr>
<td>Marked Objects</td>
<td>Lists of objects marked with the marking definition.</td>
</tr>
<tr>
<td>Marked Indicators</td>
<td>Lists of indicators marked with the marking definition.</td>
</tr>
</tbody>
</table>

**Threat notes**

A Threat Note conveys informative text to provide additional analysis not contained in the STIX Objects, Marking Definition objects, or Language Content objects which the Note relates to. Threat notes applies for STIX 2.x.

For example, an analyst may add a Note to a Campaign object created by another organization. The note may indicate that they’ve seen posts related to that Campaign on a hacker forum.

Notes are usually created by human analysts and are composed of human-oriented text, they contain an extra property to capture the author that created the Note.
**Define threat notes**

Define threat notes that convey information to provide further context or analysis that is not available in existing objects.

**Before you begin**
Role required: sn_tiability

**Procedure**
1. Navigate to Threat Intelligence > IOC Repository > Threat Notes.
2. Click New.
3. Complete the fields in the form as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract</td>
<td>Specify a brief summary of the note content.</td>
</tr>
<tr>
<td>Content</td>
<td>Specifies the content of the note.</td>
</tr>
<tr>
<td>Authors</td>
<td>Specifies the name of the author (example, an analyst).</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies the threat source from which this record is created.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Unique identifier for this object in the threat source.</td>
</tr>
<tr>
<td>Created Time in Source</td>
<td>Specifies the time the object is created in the source.</td>
</tr>
<tr>
<td>Modified Time in Source</td>
<td>Specifies the time the object is modified in the source.</td>
</tr>
</tbody>
</table>

4. Click Submit.

**What to do next**
Click any of the following related lists to view additional information about objects associated with the threat notes.

<table>
<thead>
<tr>
<th>Related Links and Related Lists</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Relationships</td>
<td>Opens the STIX Visualizer where you can view the relationship of the STIX object.</td>
</tr>
</tbody>
</table>
## Related Links and Related Lists

<table>
<thead>
<tr>
<th>Related Links and Related Lists</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Relationships appears only when the object has an associated object.</td>
<td></td>
</tr>
<tr>
<td>Associated Objects</td>
<td>Lists of objects that the threat notes apply to.</td>
</tr>
<tr>
<td>Associated Indicators</td>
<td>Lists of indicators that the threat notes apply to.</td>
</tr>
<tr>
<td>Associated Observables</td>
<td>Lists observables associated with this object.</td>
</tr>
</tbody>
</table>

## Threat opinions

An Opinion is an assessment of the accuracy of the information in a STIX Object produced by a different entity. Threat opinions apply for STIX 2.x.

The opinion property captures the level of agreement or disagreement using a fixed scale. The fixed scale also supports a numeric mapping to enable consistent statistical operations across opinions.

For example, an analyst from a consuming organization might say that they "strongly disagree" with a Campaign object and provide an explanation about why.

Opinions are subjective, and the specification does not address how best to interpret them.

Human analysts create Opinions and are composed of human-oriented text, they contain an extra property to capture the author that created the Opinion.

### Define threat opinions

Define threat opinions as an assessment of the accuracy of the information in a STIX object.

#### Before you begin

Role required: sn_ti.admin

#### Procedure

1. Navigate to Threat Intelligence > IoC Repository > Threat Opinions.
2. Click New.
3. Complete the fields in the form as appropriate.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opinion</td>
<td>The producer's opinion about the STIX object.</td>
</tr>
<tr>
<td>Explanation</td>
<td>The producer's explanation about the opinion.</td>
</tr>
<tr>
<td>Authors</td>
<td>Specifies the name of the author (example, an analyst).</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies the threat source from which this record is created.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Unique identifier for this object in the threat source.</td>
</tr>
<tr>
<td>Created Time in Source</td>
<td>Specifies the time the object is created in the source.</td>
</tr>
<tr>
<td>Modified Time in Source</td>
<td>Specifies the time the object is modified in the source.</td>
</tr>
</tbody>
</table>

4. Click Submit.

What to do next

Click any of the following related lists to view additional information about objects associated with the threat opinion.

<table>
<thead>
<tr>
<th>Related Links and Related Lists</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Relationships</td>
<td>Opens the STIX Visualizer where you can view the relationship of the STIX object.</td>
</tr>
<tr>
<td>Associated Objects</td>
<td>List of objects the threat opinion applies to.</td>
</tr>
<tr>
<td>Associated Indicators</td>
<td>List of indicators the threat opinion applies to.</td>
</tr>
<tr>
<td>Associated Observables</td>
<td>Lists observables associated with this object.</td>
</tr>
</tbody>
</table>
### Threat reports

Threat Reports are collections of threat intelligence focused on one or more topics. Threat reports apply for STIX 2.x.

Threat reports include description of a threat actor, malware, attack technique, including context and related details. They are used to group-related threat intelligence together so that it can be published as a comprehensive cyber threat story.

The Threat Report SDO contains a list of references to STIX Objects along with a textual description and the name of the report.

### Define threat reports

Define threat reports that describe a threat actor, malware, attack technique, including context and related details.

**Before you begin**

Role required: sn_ti.admin

**Procedure**

1. Navigate to Threat Intelligence > IoC Repository > Threat Reports.
2. Click **New**.
3. Complete the fields in the form as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify a name to identify the threat report.</td>
</tr>
<tr>
<td>Published</td>
<td>The date that this report has been officially published by the report author.</td>
</tr>
<tr>
<td>Description</td>
<td>A description that provides additional insight and context about the report.</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies the threat source from which this record is created.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Unique identifier for this object in the threat source.</td>
</tr>
<tr>
<td>Created Time in Source</td>
<td>Specifies the time the object is created in the source.</td>
</tr>
</tbody>
</table>
### Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modified Time in Source</td>
<td>Specifies the time the object is modified in the source.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**What to do next**

Click any of the following related lists to view additional information about objects associated with the threat reports.

<table>
<thead>
<tr>
<th>Related Links and Related Lists</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Relationships</td>
<td>Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.</td>
</tr>
<tr>
<td>Associated Types</td>
<td>Lists indicator types associated with this object.</td>
</tr>
<tr>
<td>Reported Objects</td>
<td>List of objects reported in the threat report.</td>
</tr>
<tr>
<td>Reported Indicators</td>
<td>Lists of indicators reported in the threat report.</td>
</tr>
<tr>
<td>Reported Observables</td>
<td>Lists of observables reported in the threat report.</td>
</tr>
</tbody>
</table>

**Sightings**

Sightings denote that an indicator or object was seen. Objects may be a malware, tool, threat actor, and so on.

Sightings track who and what is the target, how attacks are carried out, and to track trends in attack behavior.

The Sighting relationship object contains extra properties not present in the generic relationship objects. These extra properties represent data specific to sighting relationships.

For example, a count, or representing how many times something was seen.

Sighting is captured as a relationship because you cannot have a sighting unless you have something that has been sighted.
• What was sighted, such as the malware, campaign, or other SDO
• Who sighted it and/or where it was sighted, represented as an identity
• What was seen on systems and networks, represented as observed data

Define indicator sightings
Define sightings that denote that an indicator was seen.

Before you begin
Role required: sn_ti.admin

Procedure
1. Navigate to **Threat Intelligence > IOC Repository > Indicator Sightings**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicator</td>
<td>Identifies the indicator. Search and select the indicator.</td>
</tr>
<tr>
<td>Count</td>
<td>The number of times the object was seen.</td>
</tr>
<tr>
<td>First Seen</td>
<td>The time that this object first seen performing malicious activities.</td>
</tr>
<tr>
<td>Last Seen</td>
<td>The time that this object was last seen performing malicious activities.</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies the threat source from which this record is created.</td>
</tr>
<tr>
<td>Description</td>
<td>A description that provides more details and context about the indicator sighting, potentially including its purpose and its key characteristics.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Unique identifier for this object in the threat source.</td>
</tr>
<tr>
<td>Is Summary</td>
<td>Specifies the time the object is created in the source.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Modified Time in Source
Specifications the time the object is modified in the source.

4. Click Submit.

What to do next
Click any of the following related lists to view additional information about objects associated with the indicator sighting.

<table>
<thead>
<tr>
<th>Related Lists</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External References</td>
<td>Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.</td>
</tr>
<tr>
<td>Identities</td>
<td>List of identities associated with this object.</td>
</tr>
<tr>
<td>Observed Data</td>
<td>Lists observed data associated with this object.</td>
</tr>
</tbody>
</table>

Define object sightings
Define object sighting that describes that an object (malware, tool, threat actor, and so on) was seen.

Before you begin
Role required: sn_ti.admin

Procedure
1. Navigate to Threat Intelligence > IoC Repository > Object Sightings.
2. Click New.
3. Complete the fields in the form as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object</td>
<td>Identifies the object. Search and select the object.</td>
</tr>
<tr>
<td>Count</td>
<td>The number of times the object was seen.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>First Seen</td>
<td>The time that this object first seen performing malicious activities.</td>
</tr>
<tr>
<td>Last Seen</td>
<td>The time that this object was last seen performing malicious activities.</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies the threat source from which this record is created.</td>
</tr>
<tr>
<td>Description</td>
<td>A description that provides more details and context about the object sighting, potentially including its purpose and its key characteristics.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Unique identifier for this object in the threat source.</td>
</tr>
<tr>
<td>Is Summary</td>
<td></td>
</tr>
<tr>
<td>Created Time in Source</td>
<td>Specifies the time the object is created in the source.</td>
</tr>
<tr>
<td>Modified Time in Source</td>
<td>Specifies the time the object is modified in the source.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**What to do next**
Click any of the following related lists to view additional information about objects associated with the object sighting.

<table>
<thead>
<tr>
<th>Related Lists</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External References</td>
<td>Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.</td>
</tr>
<tr>
<td>Identities</td>
<td>List of identities associated with this object.</td>
</tr>
<tr>
<td>Observed Data</td>
<td>Lists observed data associated with this object.</td>
</tr>
</tbody>
</table>
Tools

Tools are legitimate software that are used by threat actors to perform attacks. Tools apply for STIX 2.x.

Tools enable you to know how and when threat actors use them for executing campaigns. Unlike malware, these tools or software packages are often found on a system and have legitimate purposes for power users, administrators, network administrators, or even normal users.

For example, remote access tools (RDP) and network scanning tools (Nmap) are tools that a threat actor uses during an attack.

Define tools

Define tools as legitimate software that is used to perform attacks.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to Threat Intelligence > IoC Repository > Tools.
2. Click New.
3. Complete the fields in the form as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name to identify the tool.</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies the threat source from which this record is created.</td>
</tr>
</tbody>
</table>
| Description        | A description that provides more details and context about the tool, poten­
<pre><code>                 | tially including its purpose and its key characteristics.                   |
</code></pre>
<p>| Aliases            | Alternative names to identify this tool.                                    |
| Source ID          | Unique identifier for this object in the threat source.                     |
| Created Time in Source | Specifies the time the object is created in the source.                  |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Modified Time in Source</strong></td>
<td>Specifies the time the object is modified in the source.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**What to do next**
Click any of the following related lists to view additional information about objects associated with the tool object.

<table>
<thead>
<tr>
<th>Related Links and Related Lists</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External References</td>
<td>Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.</td>
</tr>
<tr>
<td>Associated Kill Chain Phases</td>
<td>Lists kill chain phases associated with this object.</td>
</tr>
<tr>
<td>Associated Types</td>
<td>Lists indicator types associated with this object.</td>
</tr>
<tr>
<td>Attack Patterns</td>
<td>Lists the attack patterns that help categorize attacks that are associated with this object.</td>
</tr>
<tr>
<td>Campaigns</td>
<td>Lists campaigns associated with this object.</td>
</tr>
<tr>
<td>Course of Actions</td>
<td>Lists the associated course of actions with this object that are technical or automated responses (applying patches, reconfiguring firewalls) to prevent an attack.</td>
</tr>
<tr>
<td>Identities</td>
<td>List of identities associated with this object.</td>
</tr>
<tr>
<td>Indicators</td>
<td>Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>Lists systems, software services, and any associated physical or virtual</td>
</tr>
<tr>
<td>Related Links and Related Lists</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>resources that are associated with this object.</td>
<td></td>
</tr>
<tr>
<td>Intrusion Set</td>
<td>Lists a set of adversarial behaviors and resources with common properties associated with this object.</td>
</tr>
<tr>
<td>Locations</td>
<td>Lists locations that provide geographic context to this object.</td>
</tr>
<tr>
<td>Malware</td>
<td>Lists malicious code associated with this object.</td>
</tr>
<tr>
<td>Threat Actors</td>
<td>Lists individuals, groups, or organizations who act with malicious intent associated with this object.</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.</td>
</tr>
<tr>
<td>Show Relationships</td>
<td>Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.</td>
</tr>
</tbody>
</table>

**Vulnerabilities**

A Vulnerability is a weakness or defect in a software or hardware component that attackers exploit. Vulnerabilities apply for STIX 2.x.

The weakness or defect is in the requirements, designs, or implementations of the code found in a software or hardware component. This weakness is directly exploited to negatively impact the confidentiality, integrity, or availability of that system.

CVE is a list of information security vulnerabilities and exposures that provides common names for publicly known problems [CVE].

For example, if a piece of malware exploits CVE-2015-12345, a Malware object could be linked to a Vulnerability object that references CVE-2015-12345.
Define vulnerabilities

Define vulnerability as a weakness or defect in a software or hardware component that attackers exploit.

Before you begin
Role required: sn_ti.admin

Procedure
1. Navigate to Threat Intelligence > IoC Repository > Vulnerabilities.
2. Click New.
3. Complete the fields in the form as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name to identify the vulnerability.</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies the threat source from which this record is created.</td>
</tr>
<tr>
<td>Description</td>
<td>A description that provides more details and context about the vulnerability, potentially including its purpose and its key characteristics.</td>
</tr>
<tr>
<td>Aliases</td>
<td>Alternative names to identify this tool.</td>
</tr>
<tr>
<td>Source ID</td>
<td>Unique identifier for this object in the threat source.</td>
</tr>
<tr>
<td>Created Time in Source</td>
<td>Specifies the time the object is created in the source.</td>
</tr>
<tr>
<td>Modified Time in Source</td>
<td>Specifies the time the object is modified in the source.</td>
</tr>
</tbody>
</table>

4. Click Submit.

What to do next
Click any of the following related lists to view additional information about objects associated with the vulnerability object.
<table>
<thead>
<tr>
<th>Related Links and Related Lists</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Relationships</td>
<td>Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.</td>
</tr>
<tr>
<td>External References</td>
<td>Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.</td>
</tr>
<tr>
<td>Attack Patterns</td>
<td>Lists the attack patterns that help categorize attacks that are associated with this object.</td>
</tr>
<tr>
<td>Campaigns</td>
<td>Lists campaigns associated with this object.</td>
</tr>
<tr>
<td>Course of Actions</td>
<td>Lists the associated course of actions with this object that are technical or automated responses (applying patches, reconfiguring firewalls) to prevent an attack.</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>Lists systems, software services, and any associated physical or virtual resources that are associated with this object.</td>
</tr>
<tr>
<td>Intrusion Set</td>
<td>Lists a set of adversarial behaviors and resources with common properties associated with this object.</td>
</tr>
<tr>
<td>Malware</td>
<td>Lists malicious code associated with this object.</td>
</tr>
<tr>
<td>Threat Actors</td>
<td>Lists individuals, groups, or organizations who act with malicious intent associated with this object.</td>
</tr>
<tr>
<td>Tools</td>
<td>Lists legitimate software that is used by threat actors to perform attacks associated with this object.</td>
</tr>
</tbody>
</table>
Relationships

Use the relationship objects to link together two SDOs or STIX Cyber-observable Objects (SCOs) to describe how they relate to each other.

STIX Relationship Objects (SROs) represent types of relationships between various STIX objects. The following relationship objects are available:

• **Object-Object Relationship**: This object defines relationships between SDOs, except the indicator object. An example of an object-object defined relationship is that an attack pattern delivers a malware.

• **Object-Indicator Relationship**: This object defines relationships between the indicator object and other SDOs. An example of an object-indicator defined relationship is that an indicator detects evidence of a campaign.

• **Object-Observable Relationship**: This object defines relationships between SDOs and the observable object (SCO). An example of an object-observable defined relationship is that an infrastructure consists of cyber observable objects which provides information of a potential attack.

<table>
<thead>
<tr>
<th>STIX Object Relationships</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relationship Object</td>
</tr>
<tr>
<td>Object-Object Relationships</td>
</tr>
<tr>
<td>Object-Indicator Relationships</td>
</tr>
</tbody>
</table>
### STIX Object Relationships (continued)

<table>
<thead>
<tr>
<th>Relationship Object</th>
<th>Example Source</th>
<th>Example Target</th>
<th>Example Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detect secondary evidence of the campaign such as malware that is commonly used by that particular campaign.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Object-Observable Relationships</td>
<td>Infrastructure</td>
<td>Observed data</td>
<td>This relationship describes that the indicator is created based on information from an observed data object. An example of an object-observable defined relationship is that an infrastructure consists of cyber observable objects which provides information of a potential attack.</td>
</tr>
</tbody>
</table>

### Define object-object relationships

Define relationships between SDOs, except the indicator object.

**Before you begin**

Role required: sn_ti.admin

**Procedure**

1. Navigate to **Threat Intelligence > IoC Repository > Object-Object-Relationships**.
2. Click **New**.
3. Complete the fields in the form as appropriate.
Define object-indicator relationships

Define relationships between the indicator object and other SDOs.

Before you begin
Role required: sn_ti.admin

Procedure
1. Navigate to Threat Intelligence > IoC Repository > Object-Indicator-Relationships.
2. Click New.
3. Complete the fields in the form as appropriate.
Define object-observable relationships

Define relationships between SDOs and the observable object (SCO).

Before you begin
Role required: sn_ti.admin

Procedure

1. Navigate to Threat Intelligence > IoC Repository > Object- Observable-Relationships.
2. Click New.
3. Complete the fields in the form as appropriate.

4. Click Submit.
**STIX Visualizer**

The STIX Visualizer visually represents the structure of the STIX object and its relationship.

You can learn more information about the selected object or relationship from the details pane.

The relationship graph shows the relationships for an object and provides context for you to investigate. You can click any node in the graph to see more details.

⚠️ **Note:** The STIX Visualizer is available for all SDOs except the Report and Observed Data objects.

**Access STIX Visualizer**
Click Show Relationships in the Related Links section for any of the SDOs to view the STIX Visualizer.
View details in STIX Visualizer
In the Visualizer, you can view the object and its relationship which provides context for you to further investigate. The Visualizer uses colors and icons to illustrate various information about the objects.

You can zoom in to an object, drag the nodes, or pin them to focus on a particular relationship.

Click any object to open the details pane. On the details pane, you can learn more information that is associated with the object.

**MITRE-ATT&CK™ framework overview**

The MITRE-ATT&CK framework is a knowledge base of common tactics, techniques, and procedures (TTP) that your organization can access to develop specific threat models and methodologies against cyberattacks.

**Overview**

The MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework documents and tracks various adversarial techniques that are used during different stages of a cyberattack.

By using the MITRE-ATT&CK framework’s knowledge base, the cyberthreat intelligence community can quickly identify threats and coordinate cyberattack responses.

**MITRE-ATT&CK and Security Operations**

See the following diagram to learn how the MITRE-ATT&CK information flows with Security Operations applications.
• The **pre-loaded TAXII client** connects to the TAXII server to ingest the **data collections** to Threat Intelligence.

• Existing **Security Information and Event Manager (SIEM) integrations** ingest their threat data (alerts and events), with relevant TTPs and are **associated with security incidents**.

• When an IoC is connected to a security incident, Threat Intelligence automatically searches threat feeds for relevant information and sends IoCs to third-party sources such as EDR, Sandbox, or TI for additional analysis.

• If any third-party source contains the MITRE-ATT&CK information, then Threat Intelligence **extracts the technique information** and enriches the data in the Threat Intelligence repository for correlation and analysis.

• MITRE-ATT&CK also shares **CVE context information** for each technique. Your security team can review the exploited techniques in Vulnerability Response to determine if your business-critical assets are threatened.

### MITRE-ATT&CK matrices, tactics, and techniques

The core of the MITRE-ATT&CK framework is a matrix of adversary tactics and techniques. The sequence of the tactics represents what an adversary is trying to accomplish at the stage of an incident. When your security team understands this sequence, you have an opportunity to anticipate an adversary’s next move and break the kill chain. ATT&CK consists of the following matrices:

• **Enterprise ATT&CK**: Describes the behaviors and actions that an adversary takes to compromise and operate in an enterprise network and cloud.

  **Note:** The Pre ATT&CK matrix has been deprecated by MITRE and is merged with the Enterprise matrix.

• **Mobile ATT&CK**: Describes the adversary behaviors and actions that focus on mobile devices.

• **ICS ATT&CK**: Describes the actions that an adversary takes while operating within an Industrial Control Systems (ICS) network.

Tactics represent the why of an ATT&CK technique. It is the adversary’s tactical objective for performing an action.

Techniques represent how an adversary achieves a tactical objective by performing an action.

Techniques may be associated with more than one tactic. For example, Access Token Manipulation is used by an adversary to achieve either the tactic of Privilege Escalation or Defense Evasion.
Using an intent-based approach for incident responses

An intent-based response uses a dynamic and contextual kill chain framework that can help your organization to correlate security incidents and to identify a large scope of attacks. Your security team can use an intent-based response to understand how the organization is being attacked and what the attacker might do next. This type of response enables you to predict an attacker's behavior so that you can focus your resources effectively.

Using Security Incident Response, your security team can manage the life cycle of each security incident from analysis to containment by focusing on indicators of compromise (IOCs) like IP addresses, file hashes, and domains.

By integrating Security Incident Response with the MITRE-ATT&CK framework, security incidents are handled as links in a larger enterprise-wide attack.

How your organization can benefit from MITRE-ATT&CK in Security Operations

Using the MITRE-ATT&CK framework can help your organization do the following:

- Equip security analysts with MITRE-ATT&CK tactics, techniques, and procedures (TTPs) to better analyze and respond to security incidents.
- Automate the incident workflows using the playbook for detecting and containing threats in the context of the MITRE-ATT&CK framework.
- Prioritize indicators of compromise and threat hunting with MITRE-ATT&CK information.
- Understand the high-level security posture of your organization in the context of the MITRE-ATT&CK framework.

MITRE-ATT&CK administration

You can set up, map data sources, map overall technique detection coverage, and maintain the MITRE-ATT&CK repository in the Now Platform.

Get started with MITRE-ATT&CK framework

Review the following information before you start setting up your MITRE-ATT&CK framework.
## Checklist

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Verify that you have assigned the required Now Platform, Threat Intelligence, and Security Incident Response roles. | The following roles are used across the MITRE-ATT&CK features:  
• The administrator (admin) installs the applications from the ServiceNow Store and assigns the security incident administrator (sn_si.admin) and threat intelligence administrator (sn_ti.admin) roles.  
  • sn_ti.admin  
  • sn_si.admin  
  • sn_si.analyst  
  • sn_ti.read  
  • sn_ti.write  
• sn_ti.mitre_analyst - The MITRE analyst role has been introduced to allow cross-navigation for the MITRE features between Security Incident Response and Threat Intelligence Support Common. With this role, you can view both the Threat Intelligence MITRE module and the Security Incident Response module in read-only mode.  
  • sn_si.read  
For more information, see [Setup Threat Intelligence](#). |
| Verify that the ServiceNow core applications that are required to support the MITRE-ATT&CK module are installed and activated. | The MITRE-ATT&CK framework is supported on Quebec, Paris, and Orlando releases.  
Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in |
Checklist (continued)

<table>
<thead>
<tr>
<th>Setup task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>the following order to ensure a smooth installation.</td>
<td>• Threat Intelligence Support Common UI Components (sn_ti_seismic) - Version 1.0 or higher</td>
</tr>
<tr>
<td>• Threat Intelligence Support Common - Version 12.0 or higher</td>
<td>• Threat Intelligence - Version 12.0 or higher</td>
</tr>
<tr>
<td>• Security Incident Response - Version 12.0 or higher</td>
<td>Domain separation</td>
</tr>
</tbody>
</table>

**Domain separation and MITRE-ATT&CK**

This domain separation overview pertains to MITRE-ATT&CK. Domain separation allows you to separate data, processes, and administrative tasks into logical groupings called domains. You can then control several aspects of this separation, including which users can see and access data.

**Support level**

Support: Basic

**How domain separation works with MITRE-ATT&CK**

Follow these steps to achieve domain separation:

• Create a user with the required sn_ti.admin roles in the respective domain.
• Replicate the following for every domain:
  ◦ TAXII Collections

⚠️ **Note:**

- Do not activate the collections in the global domain. Activate only the collections that are replicated and available in your domain.
- Change the Run as field in the collections to the user with the sn_ti.admin role in the respective domain.
Replicate TAXII Collection

1. Navigate to Threat Intelligence > Sources > TAXII Profiles.
2. In the header bar, use the domain picker to select your domain.
3. Select the TAXII collection that is relevant to your organization (Enterprise ATT&CK, Mobile ATT&CK, or ICS ATT&CK).
4. Right-click in the header bar and select Insert and Stay. The duplicate TAXII collection is created under the selected domain.
5. Navigate back to the MITRE ATT&CK TAXII Profile to view the duplicate TAXII collection.

The following illustration shows how to select the domain TOP/Initech, replicate the TAXII collection in the domain, and verify the replicated TAXII collection.

Set up the MITRE-ATT&CK™ framework

Activate the MITRE-ATT&CK profile, and set up a scheduled job so that you can set up MITRE-ATT&CK collections for threat detection in your organization.

Before you begin
Role required: sn_ti.admin
About this task
Structured Threat Information Expression (STIX™) is a language for describing cyberthreat information in a standardized and structured manner. Using STIX data and Trusted Automated Exchange of Indicator Information (TAXII™) profiles, security teams can use shared cyberthreat information to isolate threats that have been previously identified by your company and from other sources.

Procedure
1. Navigate to Threat Intelligence > Sources > TAXII Profiles.
   You see the available TAXII profiles.
2. Click the MITRE ATT&CK profile that is provided with the base system.
3. To activate the TAXII collection, set the Active option to true for the TAXII collection that is relevant to your organization (Enterprise ATT&CK, Mobile ATT&CK, or ICS ATT&CK).

<table>
<thead>
<tr>
<th>TAXII collection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise ATT&amp;CK</td>
<td>Describes the behaviors and actions that an adversary takes to compromise and operate in an enterprise network and cloud.</td>
</tr>
<tr>
<td>TAXII collection</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Note:</strong> The Pre ATT&amp;CK matrix has been deprecated by MITRE and is merged with the Enterprise matrix.</td>
<td></td>
</tr>
<tr>
<td>Mobile ATT&amp;CK</td>
<td>Describes the adversary behaviors and actions that focus on mobile devices.</td>
</tr>
<tr>
<td>ICS ATT&amp;CK</td>
<td>Describes the actions that an adversary takes while operating within an Industrial Control Systems (ICS) network.</td>
</tr>
</tbody>
</table>
4. To periodically refresh the collection, set the **Run** option as appropriate for your organization. By default this option is set to On Demand.

**Note:**

- **a.** Collections are packaged as part of Threat Intelligence Core plugin. Installing or updating the Threat Intelligence Support Common - Version 12.0 or higher, and Threat Intelligence - Version 12.0 or higher ensures that your collections data is auto-populated.

- **b.** Activate the TAXII collection only for the collection that you intend to use in your organization and disable the other collections. For example, if you intend to use Enterprise ATT&CK matrix, then activate Enterprise ATT&CK at the TAXII collection level and at the Matrices level. Disable the other Mobile ATT&CK and ICS ATT&CK matrices at the TAXII collection and at the Matrices level.

- **c.** In the TAXII Collections related lists, if you select the Run option as Daily, then an error occurs and the option defaults to On Demand. This error occurs as scheduling the MITRE-ATT&CK data refresh daily is restricted to optimize the load on the MITRE servers. Also, MITRE updates the ATT&CK data only twice a year.

- **d.** The TAXII collections are not refreshed unless you activate the TAXII collection.

- **e.** Updates to existing collections can be retrieved from the MITRE server by scheduling the ‘run’ frequency in each collection.

- **f.** The customizations that you make to the MITRE-ATT&CK repository data (Malware, Group, Mitigation, and Tool objects to a technique) are saved during scheduled updates.

- **g.** MITRE updates the MITRE-ATT&CK knowledge base where some objects are identified as revoked or deprecated, new objects are added, or existing objects are modified. If MITRE revokes any tactic or technique, then these objects are marked as revoked in the Now Platform. The revoked objects are kept in the repository but are not available for use in the Now Platform.

**What to do next**

After the TAXII profile setup is complete, the MITRE-ATT&CK repository data is imported at regular intervals to the Now Platform®. You can see this data by navigating to **MITRE ATT&CK Repository > Matrices** and **MITRE ATT&CK Repository > Techniques**.
Manage matrices

Manage the matrices that have been imported from the MITRE TAXII collections. Matrices are a collection of tactics and techniques. You can view the matrices to review if your collections are available in the MITRE-ATT&CK repository.

Before you begin

Note: Review and verify that only the matrix you intend to use in your organization is set to active and disable the other matrices. For example, if you intend to use the Enterprise ATT&CK matrix, then the Enterprise ATT&CK matrix is activated at the TAXII collection level and in the Matrices level. Disable the other Mobile ATT&CK and ICS ATT&CK matrices at the TAXII collection and at the Matrices level.

Role required:

• sn_ti.admin: delete access
• sn_ti.read: read access
• sn_ti.write: create, write access

Procedure

1. Navigate to Threat Intelligence > MITRE ATT&CK Repository > Matrices.
   All matrices are disabled by default.

2. To activate a matrix, point to Active, double-click, and select true.

3. To view all the associated information, click a matrix.

4. To view all the tactics that are associated with this collection, click the MITRE Tactics tab.

5. To view additional details and the techniques that are associated with a selected tactic, click a tactic.

6. Under the MITRE ATT&CK Techniques tab, select a technique.

7. Under the related lists, view the associations that are available for the technique that you selected.

In the following illustration, you can see the navigational path from the Enterprise ATT&CK matrix, to the Initial Access (TA0001) tactic, and then to the Phishing (T1566) technique. On the Attack Pattern - Phishing technique page, you can view the related list - Tactic, Sub Technique, Group, Mitigation, External References, Malware, and Tools.
What to do next

You can extend the information in some of these related list objects based on the technique that you selected. For example, you can add new information for Group, Mitigation, External References, Malware, and Tools.

Manage techniques

Manage the techniques that have been imported from the MITRE TAXII collections. The techniques contain various ways attackers have developed to employ a given tactic. You can review and deactivate techniques that are not relevant to your organization.

Before you begin

Role required:

- sn_ti.admin: delete access
- sn_si.admin: create, write, delete access
- sn_ti.read: read access
- sn_ti.write: create, write access
Procedure

1. Navigate to Threat Intelligence > MITRE ATT&CK Repository > Techniques.

The list of techniques and sub-techniques are now listed.

2. To review and deactivate techniques that are not relevant to your organization, go to the list view for the selected technique, and under the Active column, update the setting to false, and save the setting.

You want to deactivate the techniques so that aren’t used by the other objects in the MITRE-ATT&CK repository.

3. Click a technique to view all the associated information with this technique.

In the following illustration, you can view the details for each Access Notification technique, its ID, source, and other related information.

4. To view how these objects are related, click Show Relationships.
What to do next
You can extend the information in some of these related list objects. For example, you can add new information for Group, Mitigation, and External References.

Extend the MITRE-ATT&CK data
Extend the MITRE-ATT&CK repository data in the Now Platform by enriching it.

Before you begin
Role required:
• sn_ti.admin: delete access
• sn_ti.read: read access
• sn_ti.write: create, write access

About this task
You can extend the Malware, Group, Mitigation, and Tool objects to a technique in the MITRE-ATT&CK repository.

You can create a new object and establish a relationship between a technique and the new object in the MITRE ATT&CK Repository module, but you can't define the relationship type in this module. For more information about defining relationship types, see object to object relationships. To define a relationship type, navigate to the Threat Intelligence > IoC Repository > Object-Object Relationships module.

If you map the relationship type between an existing technique and an existing object, then you must define the technique as the target object and the object as the source object. To do so, navigate to the IoC Repository > Object-Object Relationships module.

You can create a new group and associate it with an attack pattern, but in the MITRE ATT&CK Repository, you can only establish the relationship between the group and the attack pattern. To define the object-to-object relationship type, you must do so in the IoC Repository.
Note:

- Any customizations that you make to the objects are saved during scheduled updates.

- If you are extending the MITRE-ATT&CK data with custom information, do not mark the source as MITRE collection sources (Enterprise ATT&CK, Mobile ATT&CK, or ICS ATT&CK). This is because you are already customizing the information in the MITRE collections. If you mark the source with any of the existing MITRE collection sources (Enterprise ATT&CK, Mobile ATT&CK, or ICS ATT&CK) in the customized objects, then your object may be marked as revoked after a scheduled update.

Procedure

1. Navigate to Threat Intelligence > MITRE ATT&CK Repository > Techniques.

2. Click a techniques or sub-technique to view all the associated information with this technique.

   In the following illustration, you can see that the Botnet (T1584.005) technique is not associated with any group. If you have additional information about a technique or sub-technique, you can enrich it by adding or modifying the information.

3. Click a related list to enrich its data to associate it with a new group.
In the following illustration, a group, Custom1, has been associated with the Botnet sub-technique.

Define the data source and detection tool mapping

Define the data source and detection tool mapping for MITRE-ATT&CK tactics and techniques. The data source mapping provides you with insight into the relevance and availability of the data sources and the detection tools for monitoring the data sources in your environment.

Before you begin
Role required:

- sn_ti.admin, sn_si.admin: write access
- sn_ti.read: read access

About this task
You can identify the data sources and the detection tools that your organization needs to detect the techniques effectively.

For example, if your organization focuses on 5 techniques, you may need 10 data sources and 10 detection tools to monitor those sources. Let’s say that you identify that your organization does not have two data sources and five detection tools. This exercise gives you visibility into the data sources, their relevance to your organization, and to identify gaps in the coverage. You can also focus on enhancing your environment with the right data sources and detection tools.

All the active tactics, techniques, ID, and data sources are automatically populated based on your TAXII profile.
Procedure

1. Navigate to Threat Intelligence > MITRE ATT&CK Administration > Data Source Mapping.

The following illustration shows the list of tactics, techniques, and their IDs that have been populated based on your collection updates.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tactic</td>
<td>Adversary’s objective or the reason for performing an action.</td>
</tr>
<tr>
<td>ID</td>
<td>Technique’s unique identity.</td>
</tr>
<tr>
<td>Technique</td>
<td>How an adversary achieves a tactical objective by performing an action.</td>
</tr>
<tr>
<td>Data Source</td>
<td>Data source that is associated with the technique.</td>
</tr>
<tr>
<td>Data Source Available</td>
<td>Availability of the data source.</td>
</tr>
<tr>
<td>Detection Tool</td>
<td>Tool that supplements the data source by detecting the techniques that are used. The detection tool is mapped with the alert sensor in SIR.</td>
</tr>
</tbody>
</table>
2. Review the listed data sources and modify the value in the **Data Source Available** field based on your environment.

3. **Note:** You cannot edit this entry from the list view.

   In the **Detection Tool** field, do the following steps:
   
   a. Click the information icon, and click **Open Record**.
   
   b. Unlock **Detection Tool** entry.
   
   c. Use the lookup list to select a detection tool. You can multi-select detection tools.
   
   d. Click **Update**.

   In the following illustration, you see how to add detection tools to monitor the data source.

   ![Detection Tool Illustration]

   **Define the technique detection coverage**

   Define the technique detection coverage that your organization must measure and detect specific adversary techniques.

   **Before you begin**

   - sn_ti.admin, sn_si.admin: write access
   - sn_ti.read: read access
About this task
The technique coverage definitions are used in the overall technique detection mapping. You can use the base system technique coverage. The base system technique coverage consists of coverage types None, Poor, Fair, Good, Very Good, and Excellent. The base system technique coverage is also associated with pre-defined colors. You can customize the coverage type entries and colors, or create your own entries. For example, you can modify the base system coverage types to Not Applicable, Partial Coverage, and Complete Coverage. Alternatively, you can also create numerical measures for the coverage types such as 0-25 percent, 25–50 percent, and 50–100 percent. The type of modifications done to the base system coverage are not limited to the examples shared.

The customizations that you make to the coverage type and color are used in the overall technique detection mapping and also in the heat map.

Note: If you modify the base system coverage definition, the Coverage Type icons do not display with the techniques in the heat map. The heat map works as expected when you modify the same fields as the base system’s-defined technique detection coverage and coverage colors. However, if you delete existing fields from the overall technique detection coverage, the heat map does not display the coverage type icons.

Procedure
1. Navigate to Threat Intelligence > MITRE ATT&CK Administration > Technique Coverage Definition.
2. Review the overall technique detection entries and customize the entries for your environment.
### Technique Detection Coverage Definition

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Technique Detection Coverage</td>
<td>Name of the overall technique detection coverage. The base system technique coverage consists of None, Poor, Fair, Good, Very Good, or Excellent.</td>
</tr>
<tr>
<td>Coverage Color</td>
<td>Color that is assigned to the detection coverage score. The color that you define is used for the technique detection coverage in the heat map. You can customize the colors using HEX codes and RGB(A) values.</td>
</tr>
<tr>
<td>Description</td>
<td>Overall technique detection coverage. See the base system definition in the Scoring Definition.</td>
</tr>
</tbody>
</table>

The following illustration shows the Technique Detection Coverage Definition list.

3. To add an entry, click **New**, complete the entries, and click **Submit**.

**MITRE-ATT&CK Scoring definition**

Define your organization’s MITRE-ATT&CK scoring system so that you can measure how effectively your organization can detect specific adversary techniques.
<table>
<thead>
<tr>
<th>Score</th>
<th>Score mapping</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>0</td>
<td>Insufficient data to detect a specific adversary technique.</td>
</tr>
<tr>
<td>Poor</td>
<td>1</td>
<td>Basic signatures and correlation rules are in place to detect specific adversary techniques. Threat detection is not in real time and covers only a minimal number of aspects of a technique. For example, hunting occurs only on one endpoint at a time. Your organization might still have thousands or hundreds of events that hunters must review and correlate with other events to find outliers. The number of false positives is high.</td>
</tr>
<tr>
<td>Fair</td>
<td>2</td>
<td>Collecting the right data to a great extent and the data quality is fair. For example, your organization might be starting to add Sysmon Logs, ETW, PowerShell logs, and the like. However, the threat detection is still not in real time. Your organization may not have all the right tools to effectively aggregate and analyze the data. Hunters must manually run queries and correlate to accurately analyze the data. The number of false positives is high.</td>
</tr>
<tr>
<td>Good</td>
<td>3</td>
<td>Real-time detection that correlates and integrates multiple data across your endpoints. Threat detection covers many aspects of a technique’s procedures. Your adversaries could possibly bypass detection with evasion and obfuscation. Your organization can easily identify false positives and filter them out. Your organization uses basic data science techniques to analyze the data in the central repository.</td>
</tr>
<tr>
<td>Very Good</td>
<td>4</td>
<td>Effectively detect malicious techniques in real time and cover most aspects of a technique’s procedures. The possibility of</td>
</tr>
</tbody>
</table>
### Scoring definition (continued)

<table>
<thead>
<tr>
<th>Score</th>
<th>Score mapping</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>your adversaries bypassing detection with evasion and obfuscation methods is harder than at the Good level. Your organization can easily identify false positives and filter them out. Your organization uses advanced data science techniques to detect the adversary techniques.</td>
</tr>
<tr>
<td>Excellent</td>
<td>5</td>
<td>Effectively detect malicious techniques in real time and cover all aspects of a technique’s procedures. Your organization has a good understanding of your environment with the right automation and quality of data. The possibility of your adversaries bypassing detection with evasion and obfuscation methods is not possible at this level. The number of false negatives is low.</td>
</tr>
</tbody>
</table>

### Map your technique detection coverage to a technique

Map your overall technique detection coverage with the technique that enables your organization to detect specific adversary techniques.

**Before you begin**

- sn_ti.admin, sn_si.admin: write access
- sn_ti.read: read access

**About this task**

You can use the technique detection coverage to get an overview into your organization’s overall technique detection coverage. For example, if an adversary is attacking your organization, you see the kind of coverage that you have to detect the attacker’s techniques.

The technique and ID are automatically populated for all the collections and techniques that you have activated. The coverage type and scoring definition that you have defined are available for as an option that you can select in the overall technique detection coverage.

You can map the overall technique detection coverage with the technique to complete the mapping. You can associate a technique with only one overall technique detection coverage.
The technique detection coverage mapping that you define is used in the coverage visualization in the heatmap.

**Note:** You can arrive at the overall technique detection coverage using your organization-specific calculations. You may use any Breach & Attack Simulation (BAS) products, the Cyber Analytics Repository (CAR), or any other methods as necessary to define the scoring definition, and use it in this procedure for the overall technique detection coverage mapping.

**Procedure**

1. Navigate to Threat Intelligence > MITRE ATT&CK Administration > Technique Coverage Mapping.

In this illustration, you see that the Cloud Accounts (T1078.004) sub-technique has excellent coverage in the organization and that the Overall Technique Detection Coverage is mapped to **Excellent**.

2. Review each technique and map your overall technique detection coverage based on your technique coverage definition and your organization’s coverage availability.

**Create and map detection rules**

Create detection rules and map them against the tactics and techniques. With this mapping, you can see the coverage for the detection rules in your organization.

**Before you begin**

Role required:
- `sn_ti.admin`, `sn_si.admin`: create, write, delete access
- `sn_ti.read`: read access

© 2021 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
About this task
Detection rule mapping enables your organization to see which detection rules are available to identify specific techniques.

The primary purpose of the mapping is to provide visibility if your organization has the necessary detection rules to identify when an alert or event is triggered as a result of an attack by an adversary using a specific technique.

For example, view the following illustration that shows a list of the detection rules mapped to various techniques. You can also view this information in the MITRE-ATT&CK navigator.

If your organization does not intend to use the base system SIEM auto-extraction rules, then you should customize or create a custom logic to monitor the alerts and events that are ingested to the security incident and create a custom business rule to map the tactics and techniques to the security incident.

For example, an alert ID or event ID is ingested into Security Incident Response. Now, write a custom logic to detect the correlation rule that triggered the alert or event. After fetching the information, you need to correlate the detection rule with the tactics and techniques. Once this is done, write another custom logic to map the techniques and tactics automatically to the security incident.

Procedure

1. Navigate to Threat Intelligence > MITRE ATT&CK Administration > Detection Rules - MITRE ATT&CK Mappings.

2. Use one of the following methods to create your detection rule:
   Method 1: Manually create detection rules.
   a. Click New and on the form, fill in the fields.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MITRE-ATT&amp;CK Tactic</td>
<td>Relevant MITRE-ATT&amp;CK tactic.</td>
</tr>
<tr>
<td>MITRE-ATT&amp;CK Technique</td>
<td>Relevant MITRE-ATT&amp;CK technique.</td>
</tr>
<tr>
<td>Source</td>
<td>Source of the security incident, such as email, firewall, network monitoring, and so on.</td>
</tr>
<tr>
<td>Alert Sensor</td>
<td>Security integration through which you ingest the alert or event data such as CarbonBlack, CrowdStrike, McAfee, and so on.</td>
</tr>
<tr>
<td>Created</td>
<td>Creation date of the rule.</td>
</tr>
<tr>
<td>Updated</td>
<td>Date that the rule is updated.</td>
</tr>
<tr>
<td>Category</td>
<td>Category that identifies the type of security issue.</td>
</tr>
<tr>
<td>Subcategory</td>
<td>Subcategory that further defines the issue.</td>
</tr>
</tbody>
</table>

b. Click **Submit**.

Method 2: Import and create detection rules.

a. Right-click the Rule Name column header.

b. From the list, click **Import**.

c. Click **Create Excel template**.

d. Click **Download** after the export completes. An excel template with the filename sn_ti_alert_rules_mitre_attack_technique_mapping is downloaded to your computer.

In the following illustration, you see how to export the excel template, fill the details in the spreadsheet, upload the file, preview the fields, and import it back to the Now Platform.
e. Open the spreadsheet, select the second sheet tab, and review what you entered. On the form, fill in the fields and then, save your file.

### Import template

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Sensor</td>
<td>Security integration through which you ingest the alert or event data such as CarbonBlack, CrowdStrike, McAfee, and so on.</td>
</tr>
<tr>
<td>Category</td>
<td>Category that identifies the type of security issue.</td>
</tr>
<tr>
<td>MITRE-ATT&amp;CK Technique ID</td>
<td>MITRE-ATT&amp;CK technique ID, such as T1546.008, for Accessibility Features.</td>
</tr>
<tr>
<td>MITRE-ATT&amp;CK Tactic ID</td>
<td>MITRE-ATT&amp;CK tactic ID, such as TA0003, for Persistence.</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Detection rule name.</td>
</tr>
<tr>
<td>Source</td>
<td>Source of the security incident, such as email, firewall, network monitoring, and so on.</td>
</tr>
<tr>
<td>Subcategory</td>
<td>Subcategory that further defines the issue.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>MITRE-ATT&amp;CK Tactic</td>
<td>Relevant MITRE-ATT&amp;CK tactic.</td>
</tr>
<tr>
<td>MITRE-ATT&amp;CK Technique</td>
<td>Relevant MITRE-ATT&amp;CK technique.</td>
</tr>
</tbody>
</table>

The following illustration shows the spreadsheet template. The required fields are highlighted in red - Rule Name, MITRE-ATT&CK Tactic ID, and MITRE-ATT&CK Technique ID.

f. Click Choose file and select the spreadsheet on your computer.

h. Click Upload.

i. Preview the mappings and click Complete Import.

The following illustration shows how to upload the spreadsheet, preview the data, review any errors, and complete the detection rule mapping import process.
Auto-extract technique rules for importing MITRE-ATT&CK information

Use the base system auto-extraction rules to import the MITRE-ATT&CK information from any existing third-party integrations.

Use threat-lookup auto-extraction rules

Use the threat lookup auto-extraction rules to import the MITRE-ATT&CK information from any existing Threat Intelligence third-party integrations.

Before you begin
Role required:

- sn_ti.admin, sn_si.admin: create, write, delete access
- sn_ti.read: read access

About this task
When any Threat Intelligence integration, such as Sandbox or a TIP, supports the MITRE-ATT&CK framework and if the MITRE-ATT&CK information is parsed at each integration level, then the information is displayed in each threat lookup result record. However, not all Threat Intelligence integrations parse the MITRE-ATT&CK information. The threat lookup global auto-extraction rule can extract MITRE-ATT&CK information from all Threat Intelligence integrations.

You can choose to roll up the MITRE-ATT&CK information automatically from the threat lookup results to a security incident. For automatic rollup of threat lookup results to security incidents, enable the system property. Alternatively, you can rollup the information manually for each individual threat lookup.

The base system Threat Intelligence automatically extracts the MITRE-ATT&CK information from the third-party integrations raw payload to the threat lookup result record, if the Threat Intelligence integration provides you with MITRE-ATT&CK information like the technique ID.

If the MITRE-ATT&CK information is not available in the raw payload field of the threat lookup record, or if the technique ID information is not available in the raw payload, then you must define your own rule for auto-extraction from the third-party integration.

Procedure

1. Navigate to Threat Intelligence > MITRE ATT&CK Administration > Technique Extraction Rule.
2. Click New.
3. On the form, fill in the fields.
Technique Extraction Rule form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Auto-extraction rule name.</td>
</tr>
<tr>
<td>Rule Type</td>
<td>Auto-extraction rule type. Select <strong>Threat Lookup</strong>.</td>
</tr>
<tr>
<td>Ignore Auto-Extraction</td>
<td>Setting that by default, is cleared. This setting enables automatic extraction of MITRE-ATT&amp;CK techniques.</td>
</tr>
<tr>
<td>Source Engine</td>
<td>Source engine.</td>
</tr>
<tr>
<td>Global</td>
<td>Source engine setting. When you set the source engine to <strong>Global</strong>, the extraction runs on all threat lookup integration results.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the auto-extraction rule.</td>
</tr>
<tr>
<td>Process Method</td>
<td>Regex or a script method that you specify to link the technique information from the raw payload.</td>
</tr>
<tr>
<td>Regex Extraction</td>
<td>Option that you specify for the <strong>Target Field</strong> when using the regex extraction method. Regex is the default.</td>
</tr>
<tr>
<td>Script Extraction</td>
<td>Process that you select when running a script. The script reviews the following:</td>
</tr>
<tr>
<td></td>
<td>• threatLookupResultSysId:sys_id of the threat lookup result record</td>
</tr>
<tr>
<td></td>
<td>• sourceName: Name of the threat lookup source.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**Use SIEM auto-extraction rules**

Use the SIEM auto-extraction rules to import the MITRE-ATT&CK information from any existing Security Operations SIEM third-party integrations.
Before you begin
Role required:
- sn_ti.admin, sn_si.admin: create, write, delete access
- sn_ti.read: read access

About this task
The technique extraction rule is available for all base system Security Operations SIEM integrations such as Splunk, IBM QRadar, and ArcSight integrations. When the Now Platform ingests alert or event data from these SIEM integrations and they contain MITRE-ATT&CK information, the Now Platform processes the raw payload and auto-extracts the MITRE-ATT&CK information.

If your Now Platform contains base system SIEM integrations, that means that the technique extraction rules are already created in the MITRE-ATT&CK module. You should review and modify the rules as needed.

Procedure
1. Navigate to Threat Intelligence > MITRE ATT&CK Administration > Technique Extraction Rule.
2. Click New.
3. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Auto-extraction rule name.</td>
</tr>
<tr>
<td>Rule Type</td>
<td>Auto-extraction rule type. Select SIEM.</td>
</tr>
<tr>
<td>Ignore Auto-Extraction</td>
<td>Setting that by default is cleared. This setting enables automatic extraction of MITRE-ATT&amp;CK techniques.</td>
</tr>
<tr>
<td>Import Table</td>
<td>Import table that is automatically mapped for base system SIEM integrations. Review this field for other SIEM integrations for the MITRE-ATT&amp;CK information and map accordingly.</td>
</tr>
<tr>
<td>Import Field</td>
<td>Import field that is automatically mapped for base system SIEM integrations. Review this field for</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Description</td>
<td>Auto-extraction rule.</td>
</tr>
<tr>
<td>Process Method</td>
<td>Regex or a script method that you specify to link the technique information from the raw payload.</td>
</tr>
<tr>
<td>Regex Extraction</td>
<td>Option that you specify for the <strong>Target Field</strong> when using the regex method. Regex extraction is the default process method.</td>
</tr>
<tr>
<td>Script Extraction</td>
<td>Script process method that you use if you want to customize how the MITRE-ATT&amp;CK information is extracted.</td>
</tr>
</tbody>
</table>

In the following illustration, you see an example of the Splunk Enterprise SIEM technique extraction rule in the form view. This rule is similar to all the other SIEM technique extraction rules.

4. Click **Submit**.
Review the MITRE-ATT&CK system properties

Review the MITRE-ATT&CK system property values.

Before you begin
Role required: sn_ti.admin, sn_si.admin

Procedure
1. Navigate to Threat Intelligence > MITRE ATT&CK Administration > Properties.
2. On the form, fill in the fields.

MITRE-ATT&CK Properties form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roll up MITRE ATT&amp;CK information automatically from Observables to security incident [sn_ti.rollup_mitre_att&amp;ck_technique_observable_si]</td>
<td>Rollup of MITRE-ATT&amp;CK information from observables to the security incident. For more information, see Associate MITRE ATT&amp;CK information with observables. Default value: Yes</td>
</tr>
<tr>
<td>Roll up MITRE ATT&amp;CK information automatically from Threat Lookup results to security incident [sn_ti.rollup_mitre_att&amp;ck_technique_threat_lookup_si]</td>
<td>Rollup of MITRE-ATT&amp;CK information from threat lookup results to the security incident. For more information, see Threat lookup auto-extraction. Default value: Yes</td>
</tr>
<tr>
<td>Enabling this property allows mapping of Security Incident Fields like category and sub category with Detection Rules in &quot;Detection Rules - MITRE ATT&amp;CK mapping&quot; table [sn_ti.enable_category_mapping_with_alert_rule]</td>
<td>Category and sub-category in the Detection Rules - MITRE ATT&amp;CK mapping page. Default value: No</td>
</tr>
</tbody>
</table>

3. Click Save.

Using MITRE-ATT&CK to detect and analyze threats

Use the MITRE-ATT&CK framework across the Threat Intelligence and the SIR module to detect and analyze threats to your organization.
**Associate MITRE-ATT&CK™ information with security incidents**

Associate the MITRE-ATT&CK tactics and techniques to the security incident for better security incident and threat analysis.

**Before you begin**

Role required: sn_si.analyst

**About this task**

Add the MITRE-ATT&CK tactics and techniques information to the security incident so that you can correlate your security incident and threat information for better analysis. For example, your organization may be receiving tactics, techniques, and procedures (TTP)-related information from your third-party sources, such as Threat Intelligence reports or other sources outside of the Security Incident Response. You then add this information back to SIR for better correlation and threat analysis.

You can choose to roll up the MITRE-ATT&CK information automatically from the threat lookup auto-extraction results or from observables to a security incident. For automatic roll up to security incidents, enable the system property. Alternatively, you can roll up the information manually for each individual threat lookup or observable.

**Procedure**

1. Navigate to **Security Incidents > Show All Incidents**.
2. Select the security incident that you want to enrich with the MITRE-ATT&CK information.
3. Click the **Associate MITRE ATT&CK Technique** related link.
   The Associate MITRE ATT&CK Technique pane appears.
   This illustration shows how to navigate to the related list and look for Associate MITRE-ATT&CK Technique, review the source Enterprise ATT&CK, add a tactic Impact, and add a technique System Shutdown/Reboot.
4. Select **Source**.

*Note:* Only the **collections** and **matrices** that have been activated appear in the source list.

The tactics and techniques that are associated with the source are available for selection. You can also associate multiple sources.

5. Select the **Tactic** and **Techniques**.

6. Optional: Review the information based on the relevance with the security incident and do the following:

   - To completely remove the association, click the bin icon. Clicking this icon deletes the source and its associated tactics and techniques.
   - To remove a tactic, click the minus icon next to the tactic.
   - To remove a technique, click the x icon next to the technique.
7. Click **Save**.

**Results**
The MITRE-ATT&CK information is associated with the security incident. You can now view the associated information in the **MITRE ATT&CK Card**.

**Using the MITRE-ATT&CK Card to see related information in a security incident**

You can use the MITRE-ATT&CK card to see the MITRE-ATT&CK related information in a security incident.

After the information is rolled up from a threat lookup, an observable, or a SIEM integration, it is added to the security incident. Then, the aggregated information is presented in the MITRE-ATT&CK Card. The **MITRE ATT&CK Card** provides two views:

- **Navigator view:** This view, which is similar to the MITRE-ATT&CK navigator, shows all the techniques that have been manually added or rolled up from the observable or threat lookup tables. **Show origin of techniques** displays the source of the technique if it has been manually rolled up or through a Source. **Show ID** displays the technique ID.
The following illustration shows how to navigate to the **MITRE ATT&CK Card** navigator view. By clicking any of the available links, the information opens in the Threat Intelligence module.
• List view: This view shows the data in a list or table format. You can see all the data that is spread across different tables and groups in this view.

The following illustration shows how to navigate to the MITRE ATT&CK Card list view. By clicking any of the available links, the information opens in the Threat Intelligence module.

Associate MITRE-ATT&CK information with observables

Associate MITRE-ATT&CK tactics and techniques to an observable for better security incident and threat analysis at a granular level.

Before you begin

Role required: sn_si.analyst

About this task

Some SIEMs may provide MITRE-ATT&CK information with events, alerts, or observables. To associate the MITRE-ATT&CK information at a granular level, you can add the information with an observable.

You can choose to roll up the MITRE-ATT&CK information automatically from the observables to a security incident. For automatic rollup of observables to security incidents, enable the system property. Alternatively, you can roll up the information manually for each observable.
Procedure

1. Navigate to **Security Incidents > Show All Incidents**.

2. Select the security incident that you want to enrich with the MITRE-ATT&CK information.

3. Click **Show All Related Lists** and the **Associated Observables** tab.

4. Point to the observable that you want to associate, right-click, and select **Associate MITRE ATT&CK Technique**.

   In the following illustration, you can see how to navigate from the related list to **Associate MITRE ATT&CK Technique**, review the source, and add a tactic and technique.

5. In the source lists, review the **Source**.

   - **Note**: Only the **collections** and **matrices** that have been activated appear in the source list.

6. Review the **Tactic** and **Techniques**, and add or remove them based on the relevance with the observable.

7. Click **Save**.

   The tactics and techniques that you have added appear in the MITRE-ATT&CK Information column in the observables related list.

8. Select the observable and then from the Actions menu, click **Roll up MITRE ATT&CK Information to SI**.
If you have enabled automatic roll up of MITRE-ATT&CK information from observables to security incident, then the information is automatically rolled up. If you have not enabled automatic rollup, you need to do this manually.

The following illustration shows how to select an observable and roll up the MITRE-ATT&CK information to a security incident.

9. To see an aggregated view of the techniques that are associated with the observables, select two or more observables from the list and then from the Actions menu on the selected rows list, click the Show MITRE ATT&CK Information.

Results
An aggregated view of the MITRE ATT&CK information for the selected observables is displayed.

Rollup MITRE-ATT&CK information using Threat Lookup results
If you have not enabled automatic rollup of MITRE-ATT&CK information, you can do this manually.

Before you begin
Role required: sn_si.analyst

About this task
If you have enabled automatic roll up of MITRE-ATT&CK information from Threat Lookup results to security incident, then the information is automatically rolled up. If you have not enabled automatic rollup, you can do this manually.
Procedure

1. Navigate to Security Incidents > Show All Incidents.

2. Select the security incident that you want to enrich with the MITRE-ATT&CK information.

3. Click Show All Related Lists and the Threat Lookup Results tab.

4. Select the observable and then from the Actions menu, click Roll up MITRE ATT&CK Information to SI.
   You can select multiple observables and rollup the information.

5. Click Reload to confirm the changes.

   The following illustration shows how to select an observable and roll up the Threat Lookup results to the security incident.
   You can view the MITRE-ATT&CK Card to confirm that the Threat Lookup results have been rolledup to the security incident.

Perform link analysis and threat hunting using MITRE-ATT&CK specific filters

Correlate and perform link analysis of observables, security incidents, and MITRE-ATT&CK related information so that your organization can start hunting for threats.

Before you begin

Role required: sn_ti.mitre_analyst, sn_si.read
About this task
After you associate the security incidents with MITRE-ATT&CK information, you can use the MITRE-ATT&CK specific filters for threat hunting. Use the MITRE-ATT&CK filters with the existing Security Incident Response filters to correlate and perform link analysis.

Procedure
1. Navigate to Security Incidents > Show All Incidents.
2. Click Update Personalized List to add the MITRE columns.
3. Select a filter condition so that you can view MITRE-related information and associations with security incidents or observables:
   - MITRE-ATT&CK Adversary Group
   - MITRE-ATT&CK Data Source
   - MITRE-ATT&CK Procedure (Malware)
   - MITRE-ATT&CK Procedure (Tools)
   - MITRE-ATT&CK Tactic
   - MITRE-ATT&CK Technique
4. Create a filter condition that is based on the above criteria and click Run to perform a link analysis or correlation between security incidents, observables, and MITRE-ATT&CK related information.

   Note: The MITRE-ATT&CK data is stored as a string and you can only use contains as the operator for filter conditions.

   For example, if you want to review that a configuration item (CI) is compromised, you select a CI. You then correlate the CI with techniques that
are present by adding a MITRE-ATT&CK Technique ID. You can then continue to build your filter criteria to correlate the information and for threat hunting.

MITRE-ATT&CK heat map and navigator
You can use the MITRE-ATT&CK heat map and navigator for basic navigation and to visualize your overall technique detection coverage.

Overview of the MITRE-ATT&CK heat map and navigator
You can use the navigator with the primary filters for basic navigation and observation of ATT&CK matrices. The heat map highlights the spectrum of the detection coverage including the blind spots where your organization does not have any coverage. This is available once you map the technique detection coverage.

With the heat map and navigator, you can:

• Quickly and efficiently identify your organization's detection capabilities and highlight gaps in the technique detection coverage.
• Hunt for threats and perform correlation of threats using associated features.

Access the MITRE-ATT&CK heat map and navigator
Access the MITRE-ATT&CK heat map and navigator so that you can visualize the matrix that enables you to use ATT&CK.

Before you begin
Role required: sn_ti.read, sn_ti.mitre_analyst

About this task
You can review the heat map, use the filters to correlate, and perform link analysis of MITRE-ATT&CK information, the observables, and the security incidents in your organization.
Procedure

1. Navigate to Threat Intelligence > MITRE ATT&CK Repository > Heatmap and Navigator.
   The heat map and navigator open in a new tab.

2. Select the source to populate the heat map.

   Note: Only the collections and matrices that have been activated appear in the source list.

In the following illustration, you see how to navigate to the heat map and navigator, and how to select the source, which is Enterprise ATT&CK in this example.

3. Use the search box to quickly find a particular tactic or technique by using its name or ID.
   The following illustration shows how to search for a tactic, technique, or any information that is contained in them.
4. Click **Filters** and select a filter from the **Primary** or **Advanced** filters.

5. Click **Apply** and control the filters as follows:

   - To save your filters, click **Make this as default view** to directly load this view the next time that you land on the heat map.

   - To remove the selected filters, click **Restore Default Filters** to load your default saved view.

   - To clear all filters and your default saved view, click **Clear all filters**.

   **Note:** The views that you save are specific for a user.

**Navigator with primary filters**

Use the primary filters to filter techniques in the MITRE-ATT&CK navigator. The information in the MITRE-ATT&CK repository is available for selection.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adversary Group</td>
<td>Sets of related intrusion activity that are tracked by a common name in the security community. Groups can mean various threat groups, activity groups, threat actors, intrusion sets, and campaigns. You can add multiple groups to the <strong>Adversary Group</strong> filter. For example, you add APT1 and AT12 as both are threat groups that are attributed to China. While both groups...</td>
</tr>
<tr>
<td>Filter</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>might target different sources, they could use similar techniques.</td>
</tr>
<tr>
<td>Tool</td>
<td>Legitimate software that is used by threat actors to perform attacks. You can understand how threat actors execute campaigns if you know how and what tools are used by threat actors. Tools includes both software that is not found on an enterprise system and software that is available as part of an operating system that is already present in an environment such as Microsoft Windows utilities. For example, gsecdump is a publicly available credential dumper that the APT1 adversary group uses to obtain password hashes and LSA secrets (Local Security Authority) from Microsoft Windows operating systems.</td>
</tr>
<tr>
<td>Malware</td>
<td>Commercial, custom closed source, or open-source software that is intended to be used for malicious purposes by adversaries. Examples are PlugX, CHOPSTICK, and so on</td>
</tr>
<tr>
<td>Platform</td>
<td>Tactics and techniques that represent MITRE-ATT&amp;CK in a particular platform. For example, MITRE-ATT&amp;CK supports these platforms in the Enterprise ATT&amp;CK matrix: Microsoft Windows, macOS, Linux, PRE, AWS, GCP, Azure, Azure AD, Office 365, SaaS, Network.</td>
</tr>
<tr>
<td>Data source</td>
<td>Data sources that you are collecting in your environment and using to detect MITRE-ATT&amp;CK techniques. Examples are DLL monitoring, and browser extensions.</td>
</tr>
</tbody>
</table>
The following illustration shows all the primary filters available in the MITRE-ATT&CK navigator.

Using a heat map with primary and advanced features

You can use a heat map with advanced filters to perform an analysis by correlating security incidents with MITRE-ATT&CK information.

View technique IDs

You can view the MITRE-ATT&CK technique IDs with the technique names when you select the **Display technique IDs** filter.
View technique detection coverage

To view the overall technique detection coverage in the heat map, select the **Display technique detection coverage** filter. The heat map highlights the visual spectrum of the detection coverage including the blind spots where you do not have any coverage. The base system scoring definition and the colors have been defined in the technique detection coverage. The information has been auto-extracted from the overall technique detection coverage.

For example, areas of the heat map that are marked in red indicate a lack of detection. Areas that are marked in blue indicate the presence of full detection capabilities. Areas that are marked in orange, yellow, and light blue reflect partial detection capabilities.

- The color visualization is based on the technique definition and color coding that you define.
- The coverage visualization is based on the technique detection coverage mapping that you define.
- If you modify the base system coverage definition, the Coverage Type icons do not display with the techniques in the heat map.
Note: The heat map works as expected when you modify the same fields as the base system's-defined technique detection coverage and coverage colors. However, if you delete existing fields from the overall technique detection coverage, the heat map does not display the coverage type icons.

In this illustration, you see the technique detection coverage for all the techniques and sub-techniques and the coverage type with their colors and icons.

View Security incidents associated with technique
To view the techniques that are frequently exploited in your organization and that have resulted in security incidents, click Display security incident associated
with technique. You can view more information about each of the associated security incidents when you click the link that open in a new window for analysis.

- Priority: Select **Security Incident Priority** to filter by the security incident priority.
- Date range: Select the **Security Incident Date Range** to filter security issues by the date range.
- False positives: Select **Filter false positives security incident** to remove false positive issues. Selecting this filter reduces the number of security incidents you see in the heatmap.

When you use this filter with the **Display technique detection coverage** filter, it provides you with an insight into the relevance of the technique detection coverage for your organization until the selected date.

For example, when you turn on both filters, you can see that under the Defense Evasion tactic, the Masquerading technique has no coverage. When you look further, the Masquerading technique is related to the Masquerade Task or Service, which also has a security incident that is associated with it. This shows that there is a gap in the technique detection coverage for the Masquerading technique and you may want to revise the overall technique detection coverage.
View detection rules

To view if you have the detection rules defined for a particular technique, click **Display detection rules**. You can also see each associated detection rule with their definition.
This information is based on the detection rules mapping that you have defined.

View CVEs associated with technique
To view the Common Vulnerabilities and Exposures (CVE) information that is associated with each of the techniques, click Display CVEs associated with technique. The CVE information is mapped to the techniques and shared by MITRE. This provides you insight into known vulnerabilities and lets you know if adversaries can potentially exploit your organization.

Note: The Display CVEs associated with technique is available only when the Vulnerability Response product is installed in your environment.

When you use this filter with the Display security incident associated with technique filter, you can learn if the known vulnerabilities have caused security incidents in your organization.

You can view more information about each CVE to analyze if the CVE is relevant to your organization. To do so, view the vulnerability items. If vulnerability items are created, you can view more information about any associated CI information in the Vulnerability Response module. You
can also review the severity and priority to make informed decisions.

Analyze Security Incidents

To analyze security incidents and review the techniques that are used by an adversary for an attack, click **Analyze Security Incidents**. You can add multiple security incidents for analysis by using comma-separated strings.

This filter helps you to analyze a security incident. You can learn why the incident occurred, what techniques were exploited, if any known threat actors were involved, if the threat actors used a particular sequence for an attack, and so on. Because you can analyze multiple security incidents at the same time, you can correlate the information to see if they are related or if they are an isolated incident. If the security incidents are related and you observe a pattern, you can review their progress on the kill chain to stop the attack or to form a defense strategy for your organization.

When you use the **Analyze Security Incidents** filter with primary filters, such as an **Adversary Group**, you can correlate if known adversaries are involved. For example, when multiple security incidents are being analyzed, the techniques that are associated with the security incidents are present in the form of a kill chain. As you overlap the information with the adversary, you will notice an overlap between the techniques that are associated with the security incident and the techniques that are associated with the adversary. Only the overlapped technique information is shown if both filters are enabled.
Using the MITRE-ATT&CK dashboard

The MITRE-ATT&CK dashboard provides an executive view of the data source coverage, tactics, and techniques that are used in your organization.

The MITRE-ATT&CK Overview module displays MITRE-ATT&CK information about security incidents including trends and reports. You can click any part of a widget (bar, data point, table, and so on) to view data that is specific to that part.
Use the MITRE-ATT&CK dashboard to see your security-related data

Use the MITRE-ATT&CK dashboard to get an overview of the data source coverage, tactics, and techniques that are used in your organization.

**Before you begin**

Role required: sn_si.ciso, sn_si.analyst, sn_si.manager, sn_ti.read

**Procedure**

1. Navigate to Threat Intelligence > MITRE ATT&CK Repository > Overview.
2. Click any of the following widgets to see additional details:
   - Security Incidents by MITRE-ATT&CK Technique
   - Security Incidents by MITRE-ATT&CK Tactic
   - Critical Assets with MITRE-ATT&CK Techniques
   - Security Incident Close Codes Vs MITRE-ATT&CK Techniques

**MITRE-ATT&CK widgets**

The MITRE-ATT&CK Overview module consists of four widgets which enable you to correlate the MITRE-ATT&CK information with the security incident information in your environment.

**Example of Security Incidents by MITRE-ATT&CK Technique**

In this example, the Security Incidents by MITRE ATT&CK Technique widget displays the techniques by security incident in an organization's environment in the last 90 days.
Example of Security Incidents by MITRE-ATT&CK Tactic

In this example, the Security Incidents by MITRE ATT&CK Tactic widget displays the top tactics by security incident in an organization’s environment in the last 90 days.

![Security Incidents by MITRE ATT&CK Tactic](chart)

Example of Critical Assets with MITRE-ATT&CK Techniques

In this example, the Critical Assets with MITRE ATT&CK Techniques widget displays the top 10 critical assets that are associated with the MITRE-ATT&CK techniques. The assets have a business criticality of either 1 (most critical) or 2 (somewhat critical).

This report enables an organization to see the types and number of techniques that are used in carrying attacks against the critical assets.
Example of Security Incident Close Codes Vs MITRE ATT&CK Techniques

In this example, the Security Incident Close Codes Vs MITRE ATT&CK Techniques widget displays the security incident close codes that were mapped against the identified top techniques in an organization's environment.

The x-axis displays the top techniques that were used to carry attacks against the enterprise, and the y-axis displays the closed codes.

Threat Intelligence administration

The Threat Intelligence base system is ready to use on activation. You can add records to certain modules in the Administration application menu, but most are already populated with industry-standard information.
The following applications are available under the **Administration** module of the Threat Intelligence navigation bar:

### Threat Intelligence administration applications

<table>
<thead>
<tr>
<th>Application</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Properties</td>
<td>Threat Intelligence properties allow you to control how different aspects of the system function, including the setting of API keys.</td>
</tr>
<tr>
<td>Attack Mechanism</td>
<td>This module organizes attack patterns hierarchically, based on mechanisms that are frequently employed when exploiting a vulnerability.</td>
</tr>
<tr>
<td>Discovery Method</td>
<td>This module describes how security incidents are discovered.</td>
</tr>
<tr>
<td>Feeds</td>
<td>This feature has been deprecated.</td>
</tr>
<tr>
<td>Indicator Types</td>
<td>This module is used to characterize cyber threat indicators made up of patterns that identify certain observable conditions, as well as contextual information about the meaning of the patterns, and how and when they are acted on.</td>
</tr>
<tr>
<td>Intended Effect</td>
<td>This application is used for expressing the intended effect of a threat actor.</td>
</tr>
<tr>
<td>Notifications</td>
<td>This module is used for creating email notifications. This involves specifying when they are sent, who receives them, and what they contain.</td>
</tr>
<tr>
<td>Observable Types</td>
<td>This module lists the possible classifications of an observable, such as an IP address or file hash.</td>
</tr>
<tr>
<td>Threat Actor Type</td>
<td>This module characterizes malicious actors (or adversaries) representing a cyber attack threat, including presumed intent and historically observed behavior.</td>
</tr>
<tr>
<td>Attack motivations</td>
<td>This module lists the possible attack motivations that shape intensity of an attack by a threat actor or intrusion set.</td>
</tr>
<tr>
<td>Infrastructure types</td>
<td>This module lists the possible classifications of infrastructure.</td>
</tr>
<tr>
<td>Malware capabilities</td>
<td>This module lists the possible capabilities of malware.</td>
</tr>
<tr>
<td>Malware types</td>
<td>This module lists the possible classifications of malware.</td>
</tr>
</tbody>
</table>
Threat Intelligence administration applications (continued)

<table>
<thead>
<tr>
<th>Application</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report types</td>
<td>This module lists the possible classifications of threat reports.</td>
</tr>
<tr>
<td>Threat actor roles</td>
<td>This module lists the roles the threat actors play.</td>
</tr>
<tr>
<td>Tool types</td>
<td>This module lists the possible classification of tools.</td>
</tr>
</tbody>
</table>

Threat Intelligence integrations

The Threat Intelligence base system includes integrations to third-party malware-detection software packages. This section provides instructions for activating the plugins and configuring both ServiceNow and third-party integrations. Also included are some basic guidelines for developing your own integrations, as well as details on specific integrations included in the base system.

Integration Configurations

The base system includes a series of "cards" for each of the integration implementations you can activate and use. Also, cards are displayed for any integrations posted on the ServiceNow Store that have dependencies on Security Operations plugins. The integration cards can be viewed by selecting Security Operations > Integration Configurations.
You can filter the visible integrations using the **Category** drop-down menu. The **Show Configurations** drop-down menu lets you see multiple instances of implementations that allow their creation.

**Buttons on integration cards**
Integration cards display different buttons depending on the current state of the integration and the source of the card.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Plugin</td>
<td>Click this button to install the applicable plugin to activate the integration. After the plugin is installed, the button changes to <strong>Configure</strong>.</td>
</tr>
<tr>
<td>Button</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Configure</td>
<td>Click this button to enter information for configuring the integration. For some integrations, you may need to enter API keys or URLs acquired from the website of the third-party integration.</td>
</tr>
<tr>
<td>New</td>
<td>Certain integrations, such as Carbon Black and IBM QRadar, allow you to define multiple implementations of the same integration. For those integrations, click <strong>New</strong> after the plugin is activated. The cards allow you to install plugins (where applicable) and configure the implementations for use.</td>
</tr>
<tr>
<td>Open Page</td>
<td>In the base system, your instance performs a query to the ServiceNow Store for any applications that have dependencies on Security Operations plugins. When those applications are found, and the associated application plugins are activated, integration cards for them are displayed with the other security integration cards. Click <strong>Open Page</strong> to access the website of the third-party application to configure the integration. After you have completed the configuration, the <strong>Open Page</strong> button changes to <strong>Configure</strong>.</td>
</tr>
</tbody>
</table>

**CrowdStrike Falcon Intelligence integration**

CrowdStrike Falcon Intelligence enriches Threat Intelligence with data for security incidents and associated observables.

<table>
<thead>
<tr>
<th>Explore</th>
<th>Set up</th>
</tr>
</thead>
<tbody>
<tr>
<td>- CrowdStrike Falcon Intelligence integration overview</td>
<td>- Activate and configure the CrowdStrike Falcon Intelligence integration</td>
</tr>
<tr>
<td>- Security Incident Response integrations</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use</th>
<th>Develop</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Perform lookups on observables</td>
<td>- ServiceNow Security Operations integration development guidelines</td>
</tr>
<tr>
<td>- Threat Lookup - CrowdStrike Falcon Intelligence workflow</td>
<td>- Tips for writing integrations</td>
</tr>
<tr>
<td></td>
<td>- Developer training</td>
</tr>
<tr>
<td></td>
<td>- Developer documentation</td>
</tr>
<tr>
<td></td>
<td>- Find components installed with an application</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
Integration troubleshooting
Ask or answer questions in the Security Operations community
Search the Known Error Portal for known error articles
Contact Customer Service and Support

CrowdStrike Falcon Intelligence integration overview
CrowdStrike Falcon Intelligence provides cyber security intelligence that easily integrating with Security Operations.

⚠️ Note: The Threat Intelligence plugin is required to implement the CrowdStrike Falcon Intelligence integration.

Activate and configure the CrowdStrike Falcon Intelligence integration
The Integration Configuration feature allows you to quickly activate and set up third-party security integrations, including the CrowdStrike Falcon Intelligence integration. Before you can use the CrowdStrike Falcon Intelligence integration, you must download it from the ServiceNow Store and add the appropriate API key and ID.

Before you begin
Role required: admin

• The Threat Intelligence plugin must be installed and activated before you can use the CrowdStrike Falcon Intelligence integration.

• Obtain the API Client ID and API Client Secret under your CrowdStrike Falcon Intelligence profile.

• If you are upgrading CrowdStrike Falcon Intelligence integration from a previous version, then you must delete the existing configuration and set up a new configuration. The integration supports OAUTH2 authentication. This update requires you to enter the API Client ID and the API Client Secret to authenticate and complete the configuration.

• In the CrowdStrike Falcon Intelligence portal API Scopes, enable the Read setting for Indicators (Falcon X).
Procedure

1. Download the integration from the ServiceNow Store.
3. In the CrowdStrike Falcon Intelligence card, click Configure.
4. On the form, fill in the fields to complete the configuration:

   **CrowdStrike Falcon Intelligence Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the integration, for example, demo-1.</td>
</tr>
<tr>
<td>API Client ID</td>
<td>The client ID that you obtain from the settings section of your account profile in CrowdStrike Falcon Intelligence portal.</td>
</tr>
<tr>
<td>API Client Secret</td>
<td>The client secret key that you obtain from the settings section of your account profile in CrowdStrike Falcon Intelligence portal.</td>
</tr>
</tbody>
</table>

5. Click Submit.

Results
After it is configured, CrowdStrike Falcon Intelligence can be selected for performing lookups on observables in Threat Intelligence and on observables in security incidents.

Related information
Perform lookups on observables

Threat Lookup - CrowdStrike Falcon Intelligence workflow
The Threat Lookup - CrowdStrike Falcon Intelligence workflow performs a lookup on selected observables. If the observables are of a type recognized by CrowdStrike Falcon Intelligence, the observables are scanned for malware, and the results are returned.

About this task
This workflow is triggered by the Security Operations Integration - Threat Lookup capability when you publish one or more observables to a watchlist, and
the CrowdStrike Falcon Intelligence implementation is selected. After they are published, the watchlists can be viewed in the CrowdStrike Falcon Host software. For more information, see

For information on the activities used by this workflow, see Common integration workflow activities.

**Have I been pwned? integration**

The Security Operations Have I been pwned? integration enables you to submit lookups on domain names and email addresses to determine whether user personal data has been compromised by data breaches.

<table>
<thead>
<tr>
<th>Explore</th>
<th>Set up</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Security Incident Response integrations</td>
<td>• Security Operations Have I been pwned? integration setup</td>
</tr>
<tr>
<td>• Threat Lookup - Have I been pwned? workflow</td>
<td>• Activate the Security Operations Have I been pwned? integration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use</th>
<th>Develop</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Perform lookups on observables</td>
<td>• ServiceNow Security Operations integration development guidelines</td>
</tr>
<tr>
<td>• Threat Lookup - Have I been pwned? workflow</td>
<td>• Tips for writing integrations</td>
</tr>
<tr>
<td></td>
<td>• Developer training</td>
</tr>
</tbody>
</table>
Security Operations Have I been pwned? integration setup

Have I been pwned? is a free resource used to assess if someone may have been put at risk due to their online account being compromised or "pwned" in a data breach. It easily integrates with Security Operations.

Before you can use the Have I been pwned? integration, you must activate the plugin. If necessary, you can also update your X509 SSL certification.

The Security Incident Response, Threat Intelligence, and Security Operations Have I been pwned? plugins are required to implement the Security Operations Have I been pwned? integration.

Activate the Security Operations Have I been pwned? integration

The Integration Configuration feature allows you to quickly activate and set up third-party security integrations, including the Security Operations Have I been pwned? integration. Before you can use the Have I been pwned? integration, you must download it from the ServiceNow Store.

Before you begin
The Threat Intelligence plugin must be installed and activated before you can use the Security Operations Have I been pwned? Integration.

Role required: sn_si_admin

Procedure
Download the integration from the ServiceNow Store.
This integration supports an open API and does not require further configuration. Have I been pwned? can now be selected for performing lookups on observables in Threat Intelligence and on observables in security incidents.
Related information

Perform lookups on observables

Update your X.509 certificate

If you require an SSL connection for the integration, there are circumstances when the certificate provided by the third-party vendor is either not yet trusted in ServiceNow or has expired. This task is optional.

Before you begin
Role required: admin

Procedure

1. Acquire the SSL certificate from the third-party vendor. For example, you can import an X.509 Certificate (PEM) from an SSL endpoint in the Firefox browser, as follows.
   a. Enter the endpoint URL into the browser address bar. For example: https://<3rdparty>/.
   b. Click the lock icon in the address line.
   c. Click More Information and click the Security tab.
   d. Click View Certificate and click the Detail tab.
   e. Click Export to save the PEM into your local file system.
   f. Open the saved file in any text editor tool and copy the content to the clipboard. It must begin with -----BEGIN CERTIFICATE----- and end with -----END CERTIFICATE-----.

2. Navigate to System Definition > Certificates.

3. Click New and create a new record for the integration.

4. In PEM Certificate, paste in the certificate you downloaded and copied into the clipboard earlier.

5. Click Save.
   The other fields in the record are generated automatically.

Threat Lookup - Have I been pwned? workflow

The Threat Lookup - Have I been pwned? workflow performs a lookup on selected observables. If the observables are of a type recognized by Have I been pwned?, the observables are scanned for malware, and the results are returned.
About this task
This workflow is triggered by the Security Operations Integration - Threat Lookup capability when you perform a threat lookup on one or more observables, and the Have I been pwned? implementation is selected. For more information, see Perform lookups on observables.

For information on the activities used by this workflow, see Common integration workflow activities.

OPSWAT Metadefender Integration
OPSWAT Metadefender allows threat data, detected by the third-party Metadefender scanner, to be downloaded to the Threat Intelligence application for tracking, prioritization, and resolution.

<table>
<thead>
<tr>
<th>Explore</th>
<th>Set up</th>
</tr>
</thead>
<tbody>
<tr>
<td>• OPSWAT Metadefender integration overview</td>
<td>• Activate and configure the OPSWAT Metadefender integration</td>
</tr>
<tr>
<td>• Threat Intelligence integrations</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use</th>
<th>Develop</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Perform lookups on observables</td>
<td>• ServiceNow Security Operations integration development guidelines</td>
</tr>
<tr>
<td>• Threat Lookup - OPSWAT Metadefender workflow</td>
<td>• Tips for writing integrations</td>
</tr>
<tr>
<td></td>
<td>• Developer training</td>
</tr>
<tr>
<td></td>
<td>• Developer documentation</td>
</tr>
<tr>
<td></td>
<td>• Find components installed with an application</td>
</tr>
</tbody>
</table>

Troubleshoot and get help
OPSWAT Metadefender integration overview

OPSWAT Metadefender is a security solution that provides access to multiple anti-malware machines and easily integrates with Security Operations.

Before you can use the OPSWAT Metadefender integration, you must activate the plugin and configure the integration. If necessary, you can also update your X509 SSL certification.

Activate and configure the OPSWAT Metadefender integration

Before you can use the OPSWAT Metadefender integration, you must download it from the ServiceNow Store.

Before you begin
Role required: admin

Procedure
1. Download the integration from the ServiceNow Store.
2. When the integration is complete, access the OPSWAT portal and obtain the Metadefender Cloud API Key
4. In the OPSWAT Metadefender card, click Configure.
5. Enter (or paste) the API Key you acquired from the OPSWAT portal.
6. Click Submit.

Results
After it is configured, OPSWAT Metadefender can be selected for performing lookups on observables in Threat Intelligence and on observables in security incidents.
Related information

Perform lookups on observables

Update your X.509 certificate

If you require an SSL connection for the integration, there are circumstances when the certificate provided by the third-party vendor is either not yet trusted in ServiceNow or has expired. This task is optional.

Before you begin
Role required: admin

Procedure

1. Acquire the SSL certificate from the third-party vendor. For example, you can import an X.509 Certificate (PEM) from an SSL endpoint in the Firefox browser, as follows.
   a. Enter the endpoint URL into the browser address bar. For example: https://<3rdparty>/.
   b. Click the lock icon in the address line.
   c. Click More Information and click the Security tab.
   d. Click View Certificate and click the Detail tab.
   e. Click Export to save the PEM into your local file system.
   f. Open the saved file in any text editor tool and copy the content to the clipboard. It must begin with -----BEGIN CERTIFICATE----- and end with -----END CERTIFICATE-----.

2. Navigate to System Definition > Certificates.

3. Click New and create a new record for the integration.

4. In PEM Certificate, paste in the certificate you downloaded and copied into the clipboard earlier.

5. Click Save.
   The other fields in the record are generated automatically.

Threat Lookup - OPSWAT Metadefender workflow

The Threat Lookup - OPSWAT Metadefender workflow performs a lookup on selected observables. If the observables are of a type recognized by OPSWAT Metadefender, the observables are scanned for malware, and the results are returned.
About this task
This workflow is triggered by the Security Operations Integration - Threat Lookup capability when you perform a threat lookup on one or more observables, and the OPSWAT Metadefender implementation is selected. For more information, see Perform lookups on observables.

For information on the activities used by this workflow, see Common integration workflow activities.

Recorded Future integration
Recorded Future enriches security incidents with valuable threat data.

<table>
<thead>
<tr>
<th>Explore</th>
<th>Set up</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Threat Intelligence integrations</td>
<td>• Activate and Configure Recorded Future integration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use</th>
<th>Develop</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Perform lookups on observables</td>
<td>• ServiceNow Security Operations integration development guidelines</td>
</tr>
<tr>
<td>• Threat Lookup - Recorded Future workflow</td>
<td>• Tips for writing integrations</td>
</tr>
<tr>
<td></td>
<td>• Developer training</td>
</tr>
</tbody>
</table>
Activate and Configure Recorded Future integration

The Integration Configuration feature allows you to quickly activate and set up third-party security integrations, including the Recorded Future integration. Before you can use the Recorded Future integration, you must download it from the ServiceNow Store and add the appropriate API token.

**Before you begin**

Role required: admin

Threat Intelligence must be installed and activated before you can use the Recorded Future integration.

**Procedure**

1. Download the integration from the ServiceNow Store.
2. When the installation is complete, access your Recorded Future account and obtain the API Token under the user settings of your profile.
4. In the Recorded Future card, click Configure.
5. Enter (or paste) the API Token you acquired from the Recorded Future site.
6. Click Submit.

**Results**

After it is configured, Recorded Future can be selected for performing lookups on observables in Threat Intelligence and on observables in security incidents.
Related information

Perform lookups on observables

Threat Lookup - Recorded Future workflow
The Threat Lookup - Recorded Future workflow performs a lookup on selected observables. If the observables are of a type recognized by Recorded Future, the observables are scanned for malware, and the results are returned.

About this task
This workflow is triggered by the Security Operations Integration - Threat Lookup capability when you perform a threat lookup on one or more observables, and the Recorded Future implementation is selected. For more information, see Perform lookups on observables.

For information on the activities used by this workflow, see Common integration workflow activities.

VirusTotal integration
The Virus Total integration enables you to request the analysis of suspicious IP addresses, hashes, and URL addresses to aid in your investigation to determine if they are malicious.

<table>
<thead>
<tr>
<th>Explore</th>
<th>Set up</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Threat Intelligence integrations</td>
<td>• Virus Total integration setup</td>
</tr>
<tr>
<td></td>
<td>• Activate and configure the VirusTotal inte-</td>
</tr>
<tr>
<td></td>
<td>gration</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Virus Total integration setup

Virus Total is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware. It integrates easily with Security Operations.

Before you can use the Virus Total integration, you must activate the plugin and add the appropriate API key. If necessary, you can also update your X509 SSL certification.

If the Virus Total lookup source is used and malware is encountered, an observable is created. For IP lookups, an additional list of URLs that share the IP address is created, and observables are created for each of the URLs.

Note: The Threat Intelligence plugin is required in order to implement Virus Total integration.

Activate and configure the VirusTotal integration

Before you can use the VirusTotal integration, you must download it from the ServiceNow Store.

Before you begin
Role required: admin
Threat Intelligence must be installed and activated before you can use VirusTotal.
**Procedure**

1. **Download the integration from the ServiceNow Store.**
2. When the installation is complete, access VirusTotal and obtain the API Key under your VirusTotal profile.
3. In your instance, navigate to **Security Operations > Integration Configuration.** The available security integrations appear as a series of cards.
4. In the VirusTotal card, click **Configure.**
5. Enter (or paste) the **API Key** you acquired from the VirusTotal site.
6. Click **Submit.**

**Results**
After it is configured, VirusTotal can be selected for performing lookups on observables in Threat Intelligence and on observables in security incidents.

**Related information**
- **Perform lookups on observables**

**Threat Lookup - VirusTotal workflow**
The Threat Lookup - VirusTotal workflow performs a lookup on selected observables. If the observables are of a type recognized by VirusTotal, the observables are scanned for malware, and the results are returned.

**About this task**
This workflow is triggered by the **Security Operations Integration - Threat Lookup capability** when you perform a threat lookup on one or more observables, and the VirusTotal implementation is selected. For more information, see **Perform lookups on observables.**
For information on the activities used by this workflow, see Common integration workflow activities.

**WhoisXML API integration**

The WhoisXML API integration enables you to submit Whois lookups on domain names and URLs to obtain context on URL observables, and to make better determination on threats.

---

**Explore**

- Threat Intelligence integrations

**Set up**

- WhoisXML API integration setup
- Activate and configure the Security Operations Whois integration

**Use**

- Threat Intelligence - Run IoC Lookup workflow

**Develop**

- ServiceNow Security Operations integration development guidelines
- Tips for writing integrations
- Developer training
- Developer documentation
- Find components installed with an application

**Troubleshoot and get help**

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
WhoisXML API integration setup

Before you can use the Whois integration, you must activate the plugin and add the credentials. If necessary, you can also update your X509 SSL certification. The Threat Intelligence and WhoisXML API Integration plugins are required to implement the WhoisXML API integration.

Activate and configure the Security Operations Whois integration

The Integration Configuration feature allows you to quickly activate and set up third-party security integrations, including the Security Operations Whois integration. Before you can use the Security Operations Whois integration, you must download it from the ServiceNow Store, and you must have a valid account from WhoisXML API.

Before you begin
Threat Intelligence must be installed and activated before you can use the Security Operations Whois Integration.

Role required: admin

Procedure
1. Download the integration from the ServiceNow Store.

2. When the installation is complete, navigate to Security Operations > Integration Configuration. The available security integrations appear as a series of cards.

3. In the Whois API card, click Configure.

4. Enter the Username and Password from your WhoisXML API account.

5. Click Submit.
Update your X.509 certificate

If you require an SSL connection for the integration, there are circumstances when the certificate provided by the third-party vendor is either not yet trusted in ServiceNow or has expired. This task is optional.

Before you begin
Role required: admin

Procedure
1. Acquire the SSL certificate from the third-party vendor. For example, you can import an X.509 Certificate (PEM) from an SSL endpoint in the Firefox browser, as follows.
   a. Enter the endpoint URL into the browser address bar. For example: https://<3rdparty>/.
   b. Click the lock icon in the address line.
   c. Click More Information and click the Security tab.
   d. Click View Certificate and click the Detail tab.
   e. Click Export to save the PEM into your local file system.
   f. Open the saved file in any text editor tool and copy the content to the clipboard. It must begin with -----BEGIN CERTIFICATE----- and end with -----END CERTIFICATE-----.

2. Navigate to System Definition > Certificates.

3. Click New and create a new record for the integration.

4. In PEM Certificate, paste in the certificate you downloaded and copied into the clipboard earlier.

5. Click Save.
   The other fields in the record are generated automatically.

Enrich Observable Whols workflow

The Enrich Observable Whols workflow performs enrichment on selected observables. If the observables are of a type recognized by the WhoisXML API Integration, the observables are enriched.

About this task
This workflow is triggered by the Security Operations Integration - Enrich Observable capability when you perform enrichment on one or more observables, and the Whols implementation is selected.
Activities specific to this integration are described here. For more information on other activities, see Common integration workflow activities.

**Observable Enrichment Lookup activity**

The **Observable Enrichment Lookup** workflow activity initiates the observable enrichment process.

The **Observable Enrichment Lookup** activity can be used with any observables workflow to begin enrichment.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The lookup is successful.</td>
</tr>
<tr>
<td>Fail</td>
<td>An error occurred while attempting to perform the lookup. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>implementation_id</td>
<td>System identifier of the implementation used to perform the lookup.</td>
</tr>
</tbody>
</table>
Variable | Description
--- | ---
**domain_id** | The domain identifier for the domain within which the lookup is being performed.

**observable_ids** | One or more observables to perform the desired action against. The IDs are used as a workflow input.

**capabilityExecutionId** | System identifier of the capability that launched the implementation workflow. Only required for Integration Capability implementation workflows such as Splunk, Elasticsearch.

**task_sys_id** | System identifier for any task associated with the workflow.

**Output variables**
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>response_data</strong></td>
<td>Raw data returned by the implementation’s API endpoint for the given domain.</td>
</tr>
<tr>
<td><strong>mapping_id</strong></td>
<td>The identifier for the enrichment mapping. For example, the WhoIs integration returns data in two different format, IP and URL, with a mapping id for each.</td>
</tr>
</tbody>
</table>

**Threat Intelligence Orchestration**

Threat Intelligence Orchestration activities allow users to determine whether a threat has been seen before in other security incidents or on other systems using workflow orchestration.

For more information on editing Security Incident Response Orchestration workflows or creating custom workflows, see Getting started with workflows and Workflow editor.

**Set up Threat Intelligence Orchestration**

Prior to using Threat Intelligence Orchestration, perform steps to set up various parts of the system, including populating the CMDB, configuring the MID Server, and configuring credentials.
Before you begin
Role required: admin
To use Threat Intelligence Orchestration you need a fully populated CMDB with domain names. For more information, see .

About this task

Procedure
1. Activate the Threat Intelligence plugin.
2. Configure the MID Server
3. Configure MID Server service credentials
   You are now ready to use Threat Intelligence Orchestration activities within a workflow.

Threat Intelligence Orchestration workflows and activities
The base system includes workflows and workflow activities you can use to automate actions on your instance.

Threat Intelligence - Run IoC Lookup workflow
The Threat Intelligence - Run IoC Lookup workflow checks whether there is an unexpired observable and if so, the lookup is set to Complete and updated with the data from the observable.

Before you begin
Role required: sn_si.basic

Note: This workflow replaces Threat Intelligence Orchestration business rules (Populate with existing IoC tables, Queue the lookup, and Update observable) with activities.

If a lookup is inserted or updated and meets the conditions, the Lookup business rule triggers this workflow.

About this task
The Threat Intelligence - Run IoC Lookup workflow checks whether there is an unexpired observable and if so, the lookup is set to Complete and updated with the data from the observable. Any indicators associated with the observable are reactivated.

If the observable is expired, the workflow runs the lookups and increments the Sighting count in the existing, expired observable.

If no correlating observable exists, a new observable with indicator is created.
Workflow process activities include:

- Populate lookup with observable activity
- Perform IoC Lookup activity
- Wait for lookup (core activity)
- Update observable with lookup result activity

Populate lookup with observable activity

If an unexpired observable is found, the Threat Intelligence Orchestration - Populate lookup with observable workflow activity supplies data from an existing observable to a lookup. This activity can accelerate the investigation and remediation process.

When triggered by a workflow Populate lookup with observable attempts to find an existing observable for a lookup that matches the value and type of the lookup provided to the activity as input.

If the observable exists and is not expired, this activity:

- Updates the lookup with the information found in the observable
- Reactivates an indicator if it is inactive, increments the Encountered count, and updates the Last seen date
- Sets State to Complete.
**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Input variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scanID[string]</td>
<td>lookup identifier</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Output variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>True</td>
<td>Found valid observable and updated lookup.</td>
</tr>
<tr>
<td>False</td>
<td>Did not find valid observable. Observable is either missing or expired.</td>
</tr>
</tbody>
</table>

**Perform IoC Lookup activity**

The **Threat Intelligence Orchestration - Perform IoC Lookup** workflow activity performs a given lookup. This activity can accelerate the investigation and remediation process.

When triggered by a workflow, **Perform IoC Lookup** takes a scanID, looks up the lookup record, and adds the lookup to the queue by creating a lookup queue entry.

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scanID[string]</td>
<td>lookup identifier</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.
Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>True</td>
<td>Triggered the lookup.</td>
</tr>
<tr>
<td>False</td>
<td>Did not trigger the lookup.</td>
</tr>
</tbody>
</table>

Update observable with lookup result activity

The **Threat Intelligence Orchestration - Update observable with lookup result** workflow activity updates the observable record. If one does not exist, it creates a new observable. This activity is useful for logging information.

When triggered by a workflow **Update observable with lookup result** updates an existing observable to include the new **Sighting count**, adds a note, and, if inactive, reactivates any indicators. The **Encountered count** and **Last seen** date in the indicator are also updated.

If no correlating observable exists, the workflow creates a new observable with indicator as follows:

- Runs the IoC lookups
- Creates a new observable
- Creates an indicator for the observable
- Adds a **Sighting count** to the observable
- Adds an **Encountered count** and **Last seen** date to the indicator
- Adds a message indicating from which lookup it was created

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scanID[string]</td>
<td>Lookup identifier.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.
Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>True</td>
<td>Update or creation of observable is successful.</td>
</tr>
<tr>
<td>False</td>
<td>Update or creation of observable failed.</td>
</tr>
</tbody>
</table>

Run Default IoC Lookup Sources activity

When triggered by a workflow, Threat Intelligence - Run Default IoC Lookup Sources takes in a lookup request ID and creates multiple lookups depending on the entered data values.

For each data type, the include_in_bulk scan column of the supported lookup type table of each lookup source is evaluated. If true, a lookup is added to the lookup request.

Input variables

Input variables determine the initial behavior of the activity.

Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scan_request_id</td>
<td>Lookup request system identifier</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of scans created</td>
<td>Integer</td>
</tr>
</tbody>
</table>

Security Case Management

Security Case Management provides a means for security analysts who are engaged in threat hunting to gather information on suspicious activity in their environment. Case-related records, such as security incidents, observables, CIs, and affected users can be added to cases to accommodate broad and specific analysis.
With the ability to easily pivot through the records and related information, analysts can assess whether they are facing a targeted campaign, advanced persistent threat, and so forth.

Security cases can be created from various sources on your instance, including Security Case Management, Security Incident Response, and Threat Intelligence. You can also create cases from configuration items and affected users in the Configuration Items [cmdb.ci] and Users [sys.user] tables, respectively. After cases have been created, each of these sources can be also used to add valuable analysis resources to existing cases.

Each security case consists of three main sections, a header section, a section with additional case details, and a case artifacts section containing a collection of records that aid in building an argument for identifying and dealing with particular threats.

**Case header**

**Case header section**

<table>
<thead>
<tr>
<th>Number</th>
<th>SECC0001001</th>
<th>Case type</th>
<th>Adversary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Password attack</td>
<td>Rating</td>
<td>Critical</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated</td>
<td>2017-04-05 15:35:40</td>
</tr>
</tbody>
</table>

The case header provides basic information used to identify and classify the security case. The case number uses the SCA prefix.
The **Additional Case Details** section provides information specific to the analysis that has already been performed on the case, including its current state, and work notes and activities recorded for the case.
The **Case Artifacts** section provides a series of tabs of information contained in the security case.

You can perform searches within the contents of each tab. You can also exclude specific records you have already evaluated as being safe or which are of no value in your investigation. The excluded records are not deleted, but are hidden from view. If needed, you can view excluded records and add them back.

Within each tab, you can click the Additional Details ( ) icon to show related information for the selected record. For example, if you click the **Configuration Items** tab to view the Configuration Items Explorer, and click ( ) for a specific CI, you can view incidents, vulnerable items, and annotations associated with that CI.
You can also select a record and click the **Annotate** button for a case-related artifact to add annotations to the record. Annotations are simply notes that each analyst can make on a particular artifact.

**Security Annotations**

Add Security Annotation

Security Annotation

A password attack was reported on this CI on 2017-04-05 15:15:49.

Other tools the analyst can use for examining cases include:

- Run a sightings search on observables in a case
- Search for security artifacts
Create cases in Security Case Management

Cases are used to track information about a campaign or state actor threatening your organization. After a case is created, you can add artifacts that allow you to review and analyze all related information within a single case record.

Before you begin
Role required: sn_ti.case_user

Procedure
1. Navigate to Threat Intelligence > Case Management > All Cases.
   The Security Cases list opens.
2. Click New.
   The Security Cases screen opens.
3. Fill in the fields as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case Number</td>
<td>[Read only] The case number.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>Case Name</td>
<td>Enter a descriptive name for the case.</td>
</tr>
<tr>
<td>Case Type</td>
<td>Select the type of case being investigated.</td>
</tr>
<tr>
<td>Rating</td>
<td>Select the importance of this case (from Critical to Low).</td>
</tr>
<tr>
<td>Last Updated</td>
<td>[Read only] The date and time the case was last updated.</td>
</tr>
<tr>
<td>Short Description</td>
<td>A brief description of the case.</td>
</tr>
</tbody>
</table>

4. Click the **Additional Case Details** tab.

5. Fill in the fields as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created by</td>
<td>[Read only] The name of the user who created this case.</td>
</tr>
<tr>
<td>State</td>
<td>The current state of the case. At case creation, the State defaults to Draft.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>Click the lookup icon and assign the case to an analyst.</td>
</tr>
<tr>
<td>Work notes list</td>
<td>Click the lock icon and add internal users who can view work notes.</td>
</tr>
<tr>
<td>Additional comments</td>
<td>As needed, enter notes on the case that will be visible to the customer.</td>
</tr>
<tr>
<td>Work Notes</td>
<td>If needed, type a work note for the case.</td>
</tr>
</tbody>
</table>
6. Click **Submit**. After the record has been saved, you can click the **Case Artifacts** tab and add artifacts to the case.

### Add artifacts to a case
After you have created a case, you can add artifacts, such as security incidents, CIs, and indicators of compromise, to the case. These artifacts act as clues in solving the case.

### Before you begin
The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

### Procedure
1. Open a case to which you want to add artifacts.
2. Click the **Case Artifacts** related list.

3. Click the tab associated with the type of artifact you want to add to the case. For example, click **Configuration Items** to add one or more CIs to the case.
4. Click **Edit**.

![Configuration Items Explorer](image)

**Related Details of selected Configuration Items**

- **Add Filter**
- **Run filter**

---

**Collection**

- "*ANNE-IBM"
- "*BETH-IBM"
- "*BOW-IBM"
- "*BUD-IBM"
- "*CAROL-IBM"
- "*CAROL3-GATEWAY"
- "*CHUCK-IBM"
- "*DAVID-IBM"
- "*DENNIS-IBM"
- "*DUDE-IBM"
- "*JEMPLOYEE-IBM"
- "*RON-IBM"
- "*NET Framework"
- "*NET SDK"
- "*3Com DMI Agent"

**List**

- "*ASSET-IBM"
- "*CAROL-IBM"
- "*DAVID-IBM"
- "*WAYNE-IBM"
5. Using the slushbucket and filters, locate the artifact records you want to add to the case and move them from the Collection bucket to the List bucket, and click **Save**. The list appears in the selected tab and the selected artifacts are added to the list.

**Related information**
- Add IoCs and observables to an existing case
- Add security incidents to an existing case
- Add CIs to existing cases
- Add affected users to existing cases

**Case creation from security artifacts**
In addition to creating cases manually from Security Case Management, you can also create cases from security artifacts, such as security incidents, indicators of compromise, affected users, and configuration items.

**IoCs and observables in cases**
In Threat Intelligence, you can create cases from IoCs and observables, as well as add IoCs and observables to existing cases. You can also create observables directly from a case.

**Create a case from IoCs or observables**
In Threat Intelligence, you can create a case from artifacts (IoCs or observables). After the IoCs or observables have been used to create a case, you can use Security Case Management to analyze the data.

**Before you begin**
The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

**Procedure**
1. Navigate to the artifacts (IoCs or observables) you want to use to create a case.
   - To create a case from IoCs, navigate to **Threat Intelligence > IoC Repository > Indicators**.
   - To create a case from observables, navigate to **Threat Intelligence > IoC Repository > Observables**.
2. In the list, select the artifacts you want added to a new case.

   **Note:** If you select multiple IoCs or observables, they are all added to the case.

3. From the Actions on selected items drop-down list, select Add to Security Case.

   ![Image of Add to Security Case dialog box]

The Add to Security Case dialog box opens. If you already have cases assigned to you, they display in the list.

<table>
<thead>
<tr>
<th>Number</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECC0011903</td>
<td>Password attack</td>
<td>Brute force password attack</td>
</tr>
<tr>
<td>SECC0011901</td>
<td>Possible Spear phishing attack</td>
<td>Possible Spear phishing attack</td>
</tr>
</tbody>
</table>

4. Click Create New Case.

5. Fill in the fields.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case Name</td>
<td>Enter a name for this case.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that would be of value to the case analyst.</td>
</tr>
</tbody>
</table>

6. **Click Submit.**
   
   A message at the top of the list indicates that a new case has been created, along with a link to the case in Security Case Management.

7. **Click the link to view the new case.**

**Add IoCs and observables to an existing case**

You can add IoCs and observables to existing cases. After the security incidents have been added to cases, you can use Security Case Management to analyze the data.

**Before you begin**
The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

**Procedure**

1. **Navigate to the artifacts (IoCs or observables) you want to add to existing cases.**
   
   • To add IoCs to one or more cases, navigate to **Threat Intelligence > IoC Repository > Indicators.**
   
   • To add observables to one or more cases, navigate to **Threat Intelligence > IoC Repository > Observables.**

2. **In the list, select the artifact records you want added to existing cases.**

   **Note:** If you select multiple cases, the selected IoCs or observables are added to each of the selected cases.

3. **From the Actions on selected items drop-down list, select Add to Security Case.**
   
   The **Add to Security Case** dialog box opens. If you already have cases assigned to you, they display in the list.

4. **Select the cases into which you want to add the selected IoCs or observables.**
5. Click **Add**.
   A message indicates that the selected records have been added to the cases, along with a link to the cases in Security Case Management.

**Create an observable from a case**

New observables can be created from cases in Security Case Management.

**Before you begin**
Role required: sn_ti.case_user

**Procedure**

1. Navigate to **Threat Intelligence > Case Management > All Cases**. The Security Cases list opens.
2. Either open an existing case or click **New** to create a new case.
3. Click the **Case Artifacts** related link and click the **Observables** tab.
4. Click **New** and enter the requested information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>[Read only] The case number.</td>
</tr>
<tr>
<td>Observable type</td>
<td>Enter a descriptive name for the case.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observable type category</td>
<td>Select the type of case being investigated.</td>
</tr>
<tr>
<td>Incident count</td>
<td>Select the importance of this case (from Critical to Low).</td>
</tr>
<tr>
<td>Finding</td>
<td>[Read only] The date and time the case was last updated.</td>
</tr>
<tr>
<td>Notes</td>
<td>A brief description of the case.</td>
</tr>
</tbody>
</table>

5. Click the **Additional Case Details** tab.

6. Fill in the fields as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created by</td>
<td>[Read only] The name of the user who created this case.</td>
</tr>
<tr>
<td>State</td>
<td>The current state of the case. At case creation, the State defaults to Draft.</td>
</tr>
<tr>
<td>Work notes list</td>
<td>Click the check box to display the work notes in the Additional Case Details section of the case record.</td>
</tr>
<tr>
<td>Work Notes</td>
<td>If needed, type a work note for the case. If the Work notes list is selected, the work note appears in the Additional Case Details section of the case record.</td>
</tr>
</tbody>
</table>

7. Click **Submit**.
   
   As needed, you can click the **Case Artifacts** tab and add artifacts to the case.

**Run a sightings search on observables in a case**

You can search for observables using the Sighting Search feature to determine how often they occur. Each occurrence is considered a sighting. You can limit the search to the number of sightings within a selected number of days or within a date range.

**Before you begin**

The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write
**Procedure**

1. Navigate to **Threat Intelligence > Case Management > All Cases**.
2. Open the case that contains observables for which you want to run a sightings search.
3. Click the **Case Artifacts** related link.
4. Click the **Observables** tab.
5. Select one or more observables for which you want to search for sightings.

6. From the **Actions on selected items** drop-down list, select **Run sightings search**. The **Run Sighting Search** dialog box appears.
7. Either enter the number of days or hours you want to search for sightings of the selected observables, or select a date range.

8. Click **Search**.

**Security incidents in cases**

In Security Incident Response, you can create cases from security incidents, CIs, and affected users, as well as add those artifacts to existing cases.

**Create a case from security incidents**

In Security Incident Response, you can create cases from security incidents. After the security incidents have been used to create a new case, you can use Security Case Management to analyze the data.

**Before you begin**

The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

**Procedure**

1. Navigate to the security incidents you want to use to create cases. For example, navigate to **Security Incident > Incidents > Show Open Incidents**. The Security Incidents list opens. From the list, you can create a new case from one or more security incidents, or you can select a specific security incident and create a new case from the form.

2. To create a case from the list, select the artifacts you want added to a new case.

3. From the **Actions on selected items** drop-down list, select **Add to Security Case**.

The **Add to Security Case** dialog box opens. If you already have cases assigned to you, they display in the list.
4. Click **Create New Case**.
5. Fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case Name</td>
<td>Enter a name for this case.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that would be of value to the case analyst.</td>
</tr>
</tbody>
</table>

6. Click **Submit**.  
   A message at the top of the list indicates that a new case has been created, along with a link to the case in Security Case Management.

7. Click the link to view the new case.

**Add security incidents to an existing case**

You can add security incidents to one or more existing cases. After the security incidents have been added to cases, you can use Security Case Management to analyze the data.

**Before you begin**

The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write
Procedure

1. Navigate to the security incidents you want to add to existing cases. For example, navigate to Security Incident > Incidents > Show Open Incidents. The Security Incidents list opens.

2. In the list, select one or more security incidents that you want to add to existing cases.

   Note: If you select multiple security incidents, the selected security incidents are added to each of the selected cases.

3. From the Actions on selected items drop-down list, select Add to Security Case. The Add to Security Case dialog box opens and displays the cases assigned to you.

4. Select the cases into which you want to add the selected security incidents.

5. Click Add.
   A message indicates that the selected records have been added to the cases, along with a link to the cases in Security Case Management.

Configuration items in cases

You can create a new case from one or more configuration items (CI) in the Configuration Item [cmdb_ci] table. You can also add CIs to existing cases.
Create a case from CIs

You can create a security case from configuration items in the Configuration Item [cmdb_ci] table. After the CIs have been used to create a new case, you can use Security Case Management to analyze the data.

Before you begin
The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

Procedure
1. Navigate to the configuration items you want to use to create a case. For example, you can navigate to Configuration > Base Items > Computers to view CIs for computers.
   The list for the selected CI type opens. From the list, you can create a new case from one or more CIs, or you can select a specific CI and create a new case from the form.

2. From the list, select the CIs you want added to a new case.

3. From the Actions on selected items drop-down list, select Add to Security Case.

   The Add to Security Case dialog box opens. If you already have cases assigned to you, they display in the list.
4. Click **Create New Case**.

5. Fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case Name</td>
<td>Enter a name for this case.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that would be of value to the case analyst.</td>
</tr>
</tbody>
</table>

6. Click **Submit**.
   
   A message at the top of the list indicates that a new case has been created, along with a link to the case in Security Case Management.

7. Click the link to view the new case.

**Add CIs to existing cases**

You can add configuration items to one or more existing cases. After the CIs have been added to cases, you can use Security Case Management to analyze the data.

**Before you begin**

The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write
Procedure

1. Navigate to the CIs you want to add to existing cases. For example, you can navigate to Configuration > Base Items > Computers to view CIs for computers. The list of the selected CIs opens.

2. In the list, select one or more CIs that you want to add to existing cases.

   Note: If you select multiple CIs, the selected CIs are added to each of the selected cases.

3. From the Actions on selected items drop-down list, select Add to Security Case. The Add to Security Case dialog box opens and displays the cases assigned to you.

4. Select the cases into which you want to add the selected CIs.
5. Click Add.
   A message indicates that the selected records have been added to the cases, along with a link to the cases in Security Case Management.

**Affected users in cases**

You can create a new case from one or more affected users in the User [sys_user] table. You can also add users to existing cases.

**Create a case from affected users**

You can create a security case from affected users in the User [sys_user] table. After the affected users have been used to create a new case, you can use Security Case Management to analyze the data.

**Before you begin**

The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write
Procedure

1. Navigate to the users you want to use to create a case. For example, you can navigate to User Administration > Users. The list for the selected users opens. From the list, you can create a new case from one or more user records, or you can select a specific user record and create a new case from the form.

2. From the list, select the users you want added to a new case.

3. From the Actions on selected items drop-down list, select Add to Security Case.

The Add to Security Case dialog box opens. If you already have cases assigned to you, they display in the list.

4. Click Create New Case.

5. Fill in the fields.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case Name</td>
<td>Enter a name for this case.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that would be of value to the case analyst.</td>
</tr>
</tbody>
</table>

6. Click **Submit**.  
A message at the top of the list indicates that a new case has been created, along with a link to the case in Security Case Management.

7. Click the link to view the new case.

**Add affected users to existing cases**

You can add affected users to one or more existing cases. After the user records have been added to cases, you can use Security Case Management to analyze the data.

**Before you begin**

The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

**Procedure**

1. Navigate to the user records you want to add to existing cases. For example, you can navigate to **User Administration > Users**.  
The list of user records opens.

2. In the list, select one or more users that you want to add to existing cases.  

   ✪ **Note:** If you select multiple users, the selected user records are added to each of the selected cases.

3. From the **Actions on selected items** drop-down list, select **Add to Security Case**.  
The **Add to Security Case** dialog box opens and displays the cases assigned to you.
4. Select the cases into which you want to add the selected users.

5. Click **Add**.

A message indicates that the selected records have been added to the cases, along with a link to the cases in Security Case Management.

**Security artifact analysis**

After you have created cases, either using Security Case Management, or from artifacts such as IoCs, observables, security incidents, and so forth, you can continue to add artifacts to aid in analysis of the threats identified.

**Related details for case artifacts**

As you add artifacts to a case, additional related details for each artifact may also be automatically added. For example, if you add a security incident, it may contain affected CIs and user records. You can quickly view the related details for a selected artifact without leaving the list of artifacts.

**View related details for a security incident artifact**

If your case includes security incident artifacts, you can view any related details contained in each security incident referenced by the case.

**Before you begin**

The Threat Intelligence plugin must be activated to use Security Case Management.
Role required: sn_ti.case_user_write

Procedure
1. Open a case that contains security incident artifacts.
2. Click the Incidents tab.
3. Click the Additional Details ( ) icon for the security incident you want to view related details for.
4. Click any of the tabs to view specific types of details for the selected artifact.
5. You can also click Security Annotation tab to view annotations for the selected artifact.

View related details for a configuration item artifact
If your case includes configuration item artifacts, you can view any related details contained in each CI referenced by the case.

Before you begin
The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write
Procedure

1. Open a case that contains CI artifacts.
2. Click the Configuration Items tab.
3. Click for the CI artifact you want to view related details for.
4. Click any of the tabs to view specific types of details for the selected artifact.
5. You can also click the Security Annotation tab to view annotations for the selected artifact.

View related details for an IoC artifact

If your case includes indicators of compromise (IoC) artifacts, you can view any related details contained in each IoC referenced by the case.

Before you begin

The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write
Procedure

1. Open a case that contains IoC artifacts.
2. Click the **Indicators of Compromise** tab.
3. Click for the IoC artifact you want to view related details for.

4. Click any of the tabs to view specific types of details for the selected artifact.
5. You can also click **Security Annotation** tab to view annotations for the selected artifact.

View related details for an affected user artifact

If your case includes affected user artifacts, you can view any related details contained in each affected user referenced by the case.

**Before you begin**

The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

Procedure

1. Open a case that contains affected user artifacts.
2. Click the **Users** tab.
3. Click for the affected user artifact you want to view related details for.

4. Click any of the tabs to view specific types of details for the selected artifact.

5. You can also click Security Annotation tab to view annotations for the selected artifact.

View related details for an observable artifact

If your case includes observable artifacts, you can view any related details contained in each observable referenced by the case.

Before you begin

The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

Procedure

1. Open a case that contains observable artifacts.
2. Click the Observables tab.
3. Click for the observable artifact you want to view related details for.
4. Click any of the tabs to view specific types of details for the selected artifact.

5. You can also click **Security Annotation** tab to view annotations for the selected artifact.

**Security artifact exclusion and inclusion**

The lists of supporting artifacts assigned to a case can sometimes get long and there may be instances where you want to remove particular artifacts from a list. Rather than permanently remove the artifacts, you can exclude them from the list and, as needed, return them to the list at a later time.

**Exclude security artifacts from a case**

You can remove artifacts from the lists of supporting artifacts. They are not permanently removed and can be returned to the case as needed.

**Before you begin**

The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

**Procedure**

1. Open a case that contains artifacts that you want to exclude from a list.

2. Click the **Case Artifacts** related list.
3. Click the tab associated with the artifacts you want to exclude. For example, click **Incidents** to exclude security incidents from the list.

4. Select one or more artifact records that you want to exclude.

5. From the **Actions on selected items** drop-down list, select **Exclude**.

6. Click **Exclude** in the confirmation box. The selected artifacts are removed from the list.

**Return excluded security artifacts to a case**

After you have excluded artifacts from a list in a case, you can return them to the case you can continue to work on them.

**Before you begin**

The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

**Procedure**

1. Open a case that contains artifacts that you previous excluded from a list that you want to return to the list.

2. Click the **Case Artifacts** related list.

3. Click the tab associated with the artifacts you want to return to the list.

4. Click the Artifact Filter drop-down list and select **Excluded Artifacts**.
5. Select one or more artifact records that you want to return to the Include list.

6. From the **Actions on selected items** drop-down list, select **Include**.

7. Click **Include** in the confirmation box.
   The selected artifacts are removed from the list of excluded artifacts and returned to the list of artifacts included in the case.

**Annotate security artifacts**

As you are analyzing a case, you can add annotations to any artifact.

**Before you begin**

The Threat Intelligence plugin must be activated to use Security Case Management.
Role required:

• sn_ti.case_user_write for adding annotations
• sn_ti.case_user_read to view annotations

Procedure

1. Open a case that contains artifacts that you want to annotate.
2. Click the Case Artifacts related list.
3. Click the tab associated with the artifacts you want to annotate. For example, click Indicators of Compromise to add annotations to IoCs.
4. To add an annotation to one or more artifacts, perform the following steps:
   a. Select the artifacts to which you want to add an annotation.
   b. Click Annotate.
   c. Type the annotation and click Annotate.
      The annotation is added to the selected artifacts.
5. To view annotations for an artifact, click the View annotations () icon.
   The existing annotations appear in the Annotations dialog box.
6. You can also enter a new annotation for the artifact in the Security Annotation box, and click Annotate.

**Search for security artifacts**
You can perform a keyword search on any security artifact list.

**Before you begin**
The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

**Procedure**
1. Open a case that contains security artifacts.
2. Click the tab for the security artifacts you want to perform a keyword search on.
3. In the **Keyword search** box, begin to type the name of the artifact you want to locate.
   When artifacts that match your entry are found, they are displayed.

**Trusted Security Circles**
The Trusted Security Circles application allows you and other users to generate and receive community-sourced observables (in the form of IP addresses, hashes, domains, URLs, and so forth) with the goal of improving threat prioritization and to shorten the time to identify and remediate threats.
<table>
<thead>
<tr>
<th>Explore</th>
<th>Set up</th>
<th>Administer</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Trusted Security Circles overview</td>
<td>• Activate the Trusted Security Circle Client</td>
<td>• Set Trusted Security Circle properties</td>
</tr>
<tr>
<td>• Domain separation and Trusted Security Circle</td>
<td>• Create a Trusted Security Circle profile</td>
<td>• Trusted Security Circles overview</td>
</tr>
<tr>
<td>• Upgrade to Paris.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Security Operations videos</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Use</strong></td>
<td><strong>Develop</strong></td>
<td><strong>Integrate</strong></td>
</tr>
<tr>
<td>• Trusted Security Circles overview</td>
<td>• Developer training</td>
<td>• ServiceNow Security Operations integration development guidelines</td>
</tr>
<tr>
<td>• Trusted Security Circles and Threat Intelligence sharing guidelines</td>
<td>• Developer documentation</td>
<td>• Tips for writing integrations</td>
</tr>
<tr>
<td>• Trusted Security Circles messages</td>
<td>• Components installed with Threat Intelligence Sharing</td>
<td></td>
</tr>
<tr>
<td><strong>Troubleshoot and get help</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Ask or answer questions in the Security Operations community</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Search the Known Error Portal for known error articles</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Contact Customer Service and Support</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Trusted Security Circles overview

With the Trusted Security Circles application, your security team can identify suspicious network activity, and inquire to other members of the circle if it has been observed. An anonymous query goes to the other members of the circle, and a sightings search is performed using the suspicious observables.

With these tools, your team can immediately determine if a security incident they are investigating is affecting your peers, suppliers, or partners. This detection capability, in turn, not only protects the IT assets of other Trusted Security Circle members, but also guards your supply chain.

Trusted Security Circle are communication channels that connect sets of Trusted Security Circle customers who have some kind of underlying relationship, such as:

- Trusted Security Circle (all users)
- Financial Services
- Healthcare
- Chicago area
- Suppliers for ACME corp.

A Trusted Security Circle can consist of groups of organizations within the same line of business, divisions of the same corporation or corporate hierarchy, or groups of organizations that want to share threat intelligence. The only requirements for organizations to belong to a circle are that they have a valid organizational profile.

When messages or observables are shared between members of the Trusted Security Circle, notifications are sent to each member.

Trusted Security Circles profiles

Members of a circle are called profiles. A profile identifies a customer or customer domain (if domain separation is used). Profiles define how you, or more exactly, your Trusted Security Circle instance, is identified to other members of the circle. By default, a profile labeled "anonymous" is created automatically when either a basic or advanced Trusted Security Circle plugin is first installed. This profile also is automatically enrolled as a member of the Trusted Security Circle global trusted security circle, referred to as the central instance.

Trusted Security Circles central instance

The Trusted Security Circle central instance is a ServiceNow-hosted, scoped application that protects the identities of the participants and manages the
behavior of Trusted Security Circle profiles. It is responsible for managing such processes as:

- Registering a Threat Intelligence Sharing profile
- Updating and deactivating a profile
- Creating a circle
- Listing circles

The central instance authenticates any requests to ensure that only valid ServiceNow customer profiles can access it. All access to the central instance is restricted. You can access the central instance only through the application and modules installed by the Threat Intelligence Sharing plugin.

**Note:** Non-production Threat Intelligence Sharing instances register with a different, non-production central instance. You cannot register a non-production Threat Intelligence Sharing profile with the production central instance. You also cannot register instances that are not registered with Customer Service and Support. So you cannot register local development instances.

Threat information shared through the circles is routed through the central instance and the messages are distributed to all the intended participants. The central instance also tracks the circles to which each profile belongs, and queues up messages that the profiles retrieve when they poll for them.

The following diagram illustrates the manual and automatic steps involved in sharing observable information from a sender to a recipient via the central instance.

**Trusted Circles ecosystem**

**Sender**
- Select observable to share: manual
- Add name and description: manual
- Share: manual

**Recipient**
- Results sent back to the circle: automatic
- Local sightings search performed: manual or automatic as configured
- Security incident created: automatic

**Central Instance**

**Trusted Security Circle messages**

Messages destined for Trusted Circles are sent to the central instance. Messages are then queued up for each of the recipient profiles. Each customer instance
with a Trusted Security Circle plugin installed sends a request for messages every 30 seconds. Messages not picked up within the specified time limit (currently 48 hours) are removed from the message table.

**Trusted Security Circle terminology**
The following terms are used in Trusted Security Circle.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observable</td>
<td>A suspicious change to your computers or network. An observable can be a change to a stateful property (such as the MD5 hash of a file or the value of a registry key), or a measurable event (such as the creation of a registry key or the deletion of a file).</td>
</tr>
<tr>
<td>Registration</td>
<td>The process of enrolling a basic or advanced client with the Trusted Security Circle central instance. The registration process happens automatically after you install a basic or advanced Trusted Security Circle plugin.</td>
</tr>
<tr>
<td>Sighting</td>
<td>The detection of an observable.</td>
</tr>
<tr>
<td>Sightings search</td>
<td>A computer search to find instances of observables. Sighting searches can be conducted automatically as part of a workflow, or manually from an observable.</td>
</tr>
<tr>
<td>Trusted Security Circle</td>
<td>A channel that facilitates the sharing of observables data between member profiles.</td>
</tr>
<tr>
<td>Trusted Security Circle messages</td>
<td>The packets of information exchanged by Trusted Security Circle that describe suspected malicious observables.</td>
</tr>
<tr>
<td>Trusted Security Circle profile</td>
<td>An entity that identifies a customer instance that has joined a Trusted Security Circle.</td>
</tr>
<tr>
<td>Trusted Security Circle advanced client</td>
<td>This plugin provides complete access to Trusted Security Circle. It gives Trusted Security Circle customers the ability to join any public or private circle and share an unlimited number of observables. The license for this plugin must be purchased separately.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Trusted Security Circle basic client</td>
<td>The plugin that provides limited access to Trusted Security Circle. Five observables can be shared per day and customers can join only the default global Trusted Security Circle. This plugin is included in any purchase of the Threat Intelligence application. However, it must be installed separately.</td>
</tr>
</tbody>
</table>

**Request apps on the Store**

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

**Related information**

Activate the Trusted Security Circle Client

**Trusted Security Circles and Threat Intelligence sharing guidelines**

Adversaries continue to gain access to more sophisticated tools and techniques, which in turn has led to an increase in the frequency and, in some cases, effectiveness of cyber-attacks.

As threat actors have collaborated to increase the effectiveness of their attacks, there is increasing awareness of the need for collaboration among those defending against such attacks (see the NIST Guide to Cyber Threat Information Sharing http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf).

The ServiceNow® Trusted Security Circles provides ServiceNow customers with the ability to collaborate by facilitating the sharing of observables, their frequency, and context for sharing (collectively, “Threat Intelligence”) among peers and partners. By enabling these peers and partners to share Threat Intelligence instance-to-instance, ServiceNow customers benefit from relevant, timely, and actionable data.

These Trusted Security Circle Guidelines (“Guidelines”) are intended to assist members of the Trusted Security Circles community in deriving the greatest benefit while preventing the accidental or incidental disclosure or dissemination of information that, if improperly disclosed, may have adverse consequences for member’s organization. These Guidelines are not exhaustive and are not intended to replace your information security practices or established threat information sharing program.
Guidelines specific to the Trusted Security Circles

Members of the Trusted Security Circles are encouraged to:

- Create internal policies that define when members will share threat intelligence and what members will do with threat intelligence that a member receives from others. Members typically share observables, including their frequency in a member environment, name, and description.
- Identify those individuals that can configure the Trusted Security Circle application ("Application"), including joining Trusted Security Circles. Make sure only those individuals have administrative rights to the Application.
- Identify those individuals who will have access to the Threat Intelligence that has been shared with your organization.
- Identify those individuals that will have the ability to send Threat Intelligence. Make sure that only those individuals have the appropriate roles.
- Review all configuration relevant to sharing including relevant system properties, security tags for filtering of observables, Trusted Security Circle membership, and profile configuration. Understand that within certain configurations automated sharing and automated responses are enabled.
- Understand how the Application works with Sighting Search to provide all members of a Trusted Security Circle prevalence information for other members.

General guidelines for Threat Intelligence sharing

- You are solely responsible for complying with all applicable legal, regulatory, and contractual requirements pertaining to information sharing, including without limitation, applicable data privacy laws and laws governing classified information.
- You are encouraged to establish threat information sharing agreements and policies governing the protection and handling of personal data.
- You should also implement safeguards to protect intellectual property, trade secrets, and other proprietary information from unauthorized disclosure.
- To help ensure the protection of personal data, you should:
  - Perform, when possible, automated analyses and technical mitigations to delete personal data that is not directly related to a cyber threat.
  - Minimize the amount of data included in the shared threat intelligence to information that is directly related to a cyber threat.
Retain only information needed to address cyber threats.

Ensure any information collected is used only for network defense or limited law enforcement purposes.

**Keys to successful Threat Intelligence sharing using Trusted Security Circles**

A successful threat sharing community depends on trust. It is incumbent on the members of the Trusted Security Circles community to promote this trust by participating appropriately, including without limitation, by:

- Joining Trusted Security Circles that are targeted at organizations like yours (e.g., focused on your vertical or a related vertical).
- Sharing information that is accurate, relevant and timely to the members of the Trusted Security Circle.
- Responding to information that is shared from other members of the Trusted Security Circle using the automatic Sighting Search and response feature.

**Trusted Security Circles messages**

The members of Threat Intelligence Sharing share threat intelligence information with other Threat Intelligence Sharing member profiles by means of anonymous, encrypted messages.

Trusted Security Circles profiles share threat intelligence information with other profiles in the circle using anonymous, encrypted messages. The messages are stored in a shared intelligence table with the content of the messages shared by other profiles. The central instance contains a remote message broker that is responsible for receiving threat intelligence sharing requests and sending the encrypted messages to participants in the Trusted Security Circle. It also brokers response messages to all participants using various REST web services. Supporting tables store messages pulled to customer instances via a REST endpoint. Similarly, customer instances can post information/messages. All communication is performed asynchronously. When messages are sent to a trusted circle, they are exploded into multiple messages, each targeted at the individual members of the circle. Messages that are not picked up within the specified time limit (48 hours) are removed from the message table. Messages use a compressed data type to reduce storage size. Each customer instance with Trusted Security Circles installed sends a stateless RESTful GET request to the central instance for messages every 30 seconds for each profile created. The central instance returns an empty response unless a message has been sent to the user. When messages are sent, the message payloads are relatively small. The message data is stored based on sightings for a specific observable. As these messages are processed, they reside in local memory.
have been split into specific records, however, the message data contained in the client tables is cached to the central instance to keep the data up to date. A scheduled job called Refresh Central Data runs once per day to refresh all table data from the central instance to the local profiles. Users can manually update the table data by clicking a Refresh button on list views in the client instance.

**Remote message broker**

Trusted Circle messages are encrypted. In ServiceNow this can be accomplished with various REST web services. Supporting tables can store messages for customer instances which those instances can pull via a REST endpoint. Similarly, customer instances can post information/messages. The Trusted Security Circles plugins are responsible for initiating messages to the central instance and for receiving messages from this instance. All communication is performed asynchronously.

Messages sent to Trusted Circles are exploded into multiple messages, targeted at the circle members existing at the time of message sending. Messages not picked up within the specified time limit (currently 48 hours) are removed from the message table. Additionally, messages use a compressed data type to reduce storage size.

Each customer instance with a Trusted Security Circle plugin installed sends a request for messages every 30 seconds for each profile created. This is a stateless RESTful GET request to the central instance. This request returns an empty response unless a message has been sent to the user.

On the central instance, getting any messages for a profile is a single query in addition to the REST authentication. Since this table is cleaned regularly, this should not be an expensive query. Additionally, these messages are stored in compressed data fields.

When a message is sent, the message payloads are relatively small. In order to load test we are using a maximum message size of about 1.4MB. This data is stored based on sightings for a specific observable. This leads to a sightings record with a maximum size of about 4,500 bytes.

During message processing they reside in memory but once they have been split into specific records the message are not be persisted in the customer’s instance. The downloaded payload is not encrypted (except for SSL encryption in transport).

**Data caching**

Data caching is a term we are using to describe the logic of keeping the client tables (sometimes referred to as “local tables”) up to date with the data stored
on central. This is accomplished via REST APIs to central. There are different ways to trigger updating the local "cache". They are:

- **Scheduled job - "Refresh Central Data"** which runs once a day and refreshes all table data.
- **Navigating to a List View -** navigating to a list view such as viewing a list of circles. If the table supports data caching, there is a "Refresh" button at the top of the list. Pressing this button refreshes all data for this table.
- **Navigating to a single record -** navigating to a form refreshes that record and all its visible related lists. This is accomplished via client script onload of the record form.
- **Programmatically -** any arbitrary script can call the logic to get the latest data from central. Any "get" operation also updates the local cache.
- **Attachments** - Central must accept and host files shared between components.

Each message is a new item in the table, keyed by recipient. The Trusted Security Circles should also make sure we don't explode table if customers stop to check for messages, since this table is the one that has potential to grow rapidly. When messages are checked, they are removed from database. We should be able to send message to a trusted circle or individual profile, so we might have 2 different fields in message json, that is sent to API, but in messages table we only store id of recipient profile. This table includes these fields:

- **id** – sys_id provided by platform.
- **profile_id** - id of recipient, this should be indexed, since we're mostly going to perform selects based on it.
- **message** – message itself, JSON string.
- **encrypted** – boolean, to specify if message would have been encrypted if possible.

**Domain separation and Trusted Security Circle**

This is an overview of domain separation in Trusted Security Circle. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can then control several aspects of this separation, including which users can see and access data.
Support level: Standard

- Includes Basic level support.
- Business logic: Processes can be created or modified per customer by the service provider (SP). The use cases reflect proper use of the application by multiple SP customers in a single instance.
- The owner of the instance needs to be able to configure the minimum viable product (MVP) business logic and data parameters per tenant as expected for the specific application.

Use case: An admin needs to be able to make comments mandatory when a record closes for one tenant, but not for another.

How domain separation works in Trusted Security Circle

Domain separation enables service providers (SPs) to standardize Trusted Security Circle procedures across the customer base they serve with lowered operational costs and a higher quality of service.

Separate customer workspaces for workflows, dashboards, reports, and so forth ensures that customer data is separated and never exposed to other clients.

Domain separation support in Trusted Security Circle by version releases

<table>
<thead>
<tr>
<th>Release</th>
<th>Support level</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jakarta</td>
<td>Level 2 (Data, Requestor, Fulfiller)</td>
<td>All integrations reside across multiple domains.</td>
</tr>
<tr>
<td>Kingston</td>
<td>Level 2 (Data, Requestor, Fulfiller)</td>
<td>All integrations reside across multiple domains.</td>
</tr>
<tr>
<td>London</td>
<td></td>
<td>All integrations reside across multiple domains.</td>
</tr>
<tr>
<td>Madrid</td>
<td>Level 2 (Data, Requestor, Fulfiller)</td>
<td>All integrations reside across multiple domains.</td>
</tr>
<tr>
<td>New York</td>
<td>Level 2 (Data, Requestor, Fulfiller)</td>
<td>All integrations reside across multiple domains.</td>
</tr>
<tr>
<td>Orlando</td>
<td>Standard</td>
<td>All integrations reside across multiple domains.</td>
</tr>
<tr>
<td>Paris</td>
<td>Standard</td>
<td>All integrations reside across multiple domains.</td>
</tr>
</tbody>
</table>
Domain separation setup
Setting up domain separation for Trusted Security Circle requires that you request domain separation, register the central instance for each domain, and configure the job queue.

**Important:** If you are using domain separation, you must activate the Domain Support - Domain Extensions plugin before activating Trusted Security Circle. Several of the setup steps are also different for domain separation setup.

Related information
- Domain separation for service providers

Request domain separation
All domain support features are activated with a plugin called Domain Support - Domain Extensions Installer. Administrators can request activation of this plugin.

Before you begin
To purchase a subscription, contact your ServiceNow account manager. The account manager can arrange to have the plugin activated on your organization’s production and sub-production instances, generally within a few days.

If you do not have an account manager, decide to delay activation after purchase, or want to evaluate the product on a sub-production instance without charge, follow these steps.

Role required: admin

About this task
If the Domain Support - Domain Extensions Installer plugin is already active, content in the Domain Support - Domain Extensions Installer plugin will not be installed to avoid potential conflict with an existing implementation.

Domain separation replaces Company Separation. Starting with the Helsinki release, the Company Separation plugin can no longer be activated. However, if company separation is already active when you activate domain separation, both plugins are active at the same time. You can control the company separation activation status with the `glide.db.separation.field` property.

**Note:** Domain paths are used for all customers on Helsinki and later. Domain numbering is no longer used. Customer Service and Support can assist in the upgrade.
Procedure

1. Navigate to System Applications > All Available Applications > All.

2. On the All Applications page, click Request Plugin to open the request form on HI.

3. On HI, select to be redirected to the HI Service Portal Service Catalog.

4. On the Activate Plugin request form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Instance</td>
<td>Instance on which to activate the plugin.</td>
</tr>
<tr>
<td>Plugin Name</td>
<td>Name of the plugin to activate.</td>
</tr>
<tr>
<td>Specify the date and time you would like this plugin to be enabled</td>
<td>The date and time must be at least two business days from the current time.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Reason/Comments</td>
<td>Information that would be helpful for the ServiceNow personnel who are activating the plugin. For example, if you need the plugin activated at a specific time instead of during one of the default activation windows, specify it in the comments.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

**Results**
Activating the Domain Extension Installer plugin enables these features:

- Domain separation is based on the Domain `[sys_domain]` table.
- Delegated administration lets each domain have separate policy.
- All records are part of the global domain.
- The current user's domain determines the domain to use when viewing or operating on a record in a different domain.

**Related information**

**Register the Trusted Security Circles central instance for each domain**

If domain separation is not installed, registration to the global domain occurs automatically. If you have installed domain separation, manually register the Trusted Security Circle central instance for each of your domains.

**Before you begin**
If you are using the basic level of Trusted Security Circle, it is activated automatically when you activate Security Incident Response. Trusted Security Circles Client (Advanced) is available as a separate subscription. When domain separation is activated, two additional modules appear in the Trusted Security Circles navigation bar:
• Job Queue Entries
• Registration

Role required: sn_tis_admin

Procedure
1. If it is not already activated, active the appropriate level of Trusted Security Circles.
2. Navigate to Trusted Security Circles > Registration.
3. From the Domain (△) drop-down list, select the domain you want to register to the Trusted Security Circles central instance.
4. Click Register.
5. You can verify that the domain registration completed successfully by navigating to Trusted Security Circles > Circles.

Configure the job queue
The job queue is used to execute scheduled jobs for getting messages from the central instance, processing records in the central instance, and refreshing records from central for your domain or for each of your domains (if you are using domain separation).

Before you begin
Role required: admin

Procedure
1. Navigate to Trusted Security Circles > Job Queue Entries.
2. In the Job Queue Entries screen, click New.
3. From the Domain (△) drop-down list, select the domain for which you want to configure the job queue.
4. Fill in the fields as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job</td>
<td>Click the lookup icon and select the scheduled job executer you want to use for the selected domain.</td>
</tr>
<tr>
<td>Last Run</td>
<td>Displays the date and time when the job was last run. The oldest job will be the next one to run.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Domain User</td>
<td>Select the user in this domain who is identified as the person running this job.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

6. Repeat these steps as needed to select other jobs for this domain and for other domains (if you are using domain separation).

**Related information**

**Domain separation and Trusted Security Circle**

**Set up Trusted Security Circle**

Before using Trusted Security Circle, you must set up the application. This process includes identifying the location of the Trusted Security Circle Central instance, setting parameters for communicating with this instance, and defining sightings thresholds for observables derived from both internally- and externally-generated threat intelligence.

The setup you perform depends on whether you intend to use domain separation.

**Activate the Trusted Security Circle Client**

Two versions of Trusted Security Circle are available. The basic level of Trusted Security Circle is activated automatically when you activate Security Incident Response. Trusted Security Circles Client (Advanced) is available as a separate subscription. It provides the capabilities of the basic level, along with the ability to join any available trusted circle and initiate an unlimited number of threat shares per day.

**Before you begin**

If you are installing either version of Trusted Security Circle on an instance other than prod or subprod (for example, on a demo instance), you must manually activate the appropriate Trusted Circles plugins and register the client to the central instance.

**Important:** If you are using domain separation, it is important that you request the Domain Support - Domain Extensions plugin from the Service Catalog and activate it **before** activating Trusted Security Circle.

Role required: admin
About this task
Trusted Security Circles Client (Advanced) activates the following plugins if they are not already active. Additionally, it registers the instance running the client with the central instance. This includes creating both the instance administrator and an anonymous profile. It also adds the client instance as a member of the default public Trusted Security Circle (named ServiceNow).

Plugins for Trusted Security Circles Client (Advanced)

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted Security Circle Client [com.snc.intel_sharing.client]</td>
<td>Integrates Trusted Security Circle with Threat Intelligence. This plugin is responsible for displaying group membership within the ServiceNow platform and for keeping Trusted Security Circle membership information up-to-date. It is also responsible for sending messages to the central instance and receiving messages from this instance.</td>
</tr>
<tr>
<td>Threat Core [com.snc.threat]</td>
<td>Integrates Trusted Security Circle with Threat Intelligence and other Security Operations applications.</td>
</tr>
</tbody>
</table>

To purchase a subscription, contact your ServiceNow account manager. After purchasing the subscription, activate the plugin within the production instance.

Procedure
1. Navigate to System Applications > All Available Applications > All.
2. Find the plugin using the filter criteria and search bar.
   
   You can search for the plugin by its name or ID. If you cannot find a plugin, you may have to request it from ServiceNow personnel. To request a plugin, follow the steps in Request a plugin.

3. Click Install, and then in the Activate Plugin dialog box, click Activate.

   Note: When domain separation and delegated admin are enabled in an instance, the administrative user must be in the global domain. Otherwise, they will receive the following error: Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.
Register the Trusted Security Circles client to the central instance

After either the Basic or Advanced versions of Trusted Security Circle has been activated, you must register the Trusted Security Circle client to the central instance.

Before you begin
If you have installed domain separation, you must manually register the Trusted Security Circle central instance for each of your domains.

Role required: sn_tis_admin

Procedure
1. If it is not already activated, activate the appropriate level of Trusted Security Circles.
2. Navigate to Trusted Security Circles > Registration.
3. Click Register.
4. You can verify that the registration completed successfully by navigating to Trusted Security Circles > Circles. You should see a list of available Trusted Security Circles.

Set Trusted Security Circle properties

Trusted Security Circle properties allow you to set the URL to the ServiceNow instance the application uses as the central repository for sharing threat information with other trusted security circle customers.

Before you begin
Role required: sn_tis.admin

Procedure
1. Type `sys_properties.list` in the navigation filter and press Return.
2. Set the following properties, as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically share the results of a sightings search to the default ServiceNow trusted circle</td>
<td>Set to <code>true</code> to automatically share the results of a sighting search to the default ServiceNow trusted circle. [sn_tis.auto_share_sighting_searches]</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Include observables with no local sightings when automatically sharing sighting search results</td>
<td>Set to true to include observables with no local sightings when automatically sharing sighting search results.</td>
</tr>
<tr>
<td>sn_tis.auto_share_zero_sightings</td>
<td></td>
</tr>
<tr>
<td>Respond with local sightings whenever a threat share is received from a trusted circle</td>
<td>Set to true to respond with local sightings whenever a threat share is received from a trusted circle.</td>
</tr>
<tr>
<td>sn_tis.threat_share_responses</td>
<td></td>
</tr>
</tbody>
</table>

Join a Trusted Security Circle

A user with the Advanced client can join a trusted security circle by selecting a circle from a list and specifying a profile.

**Before you begin**
Role required: sn_tis.admin

**Procedure**
1. Navigate to **Trusted Security Circles > Circles**.
2. Select the circle you want to join.
3. Click **Join**.

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
4. In the **Profile** field, select the profile that belongs to the trusted circle.

5. Click **Submit**.

**Create a Trusted Security Circle profile**

When you first register a Trusted Security Circle to the central instance, two profiles are automatically created: Instance Admin and Anonymous. Instance Admin is used for administrative interactions with central. The Anonymous profile is automatically joined to the global ServiceNow Trusted Security Circle. If needed, you can create additional profiles and give them whatever names you want.

**Before you begin**

Role required: sn_tis_admin

**Procedure**

1. Navigate to **Trusted Circles > Profiles**.
2. Click **New**.
3. Fill in the fields, as needed.

### Profiles

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the profile.</td>
</tr>
<tr>
<td>Anonymous</td>
<td>This field determines whether the profile is associated with the instance name at central. If a profile is marked as anonymous, there is no linkage to identify the instance it came from.</td>
</tr>
<tr>
<td>Automatic Sighting</td>
<td>Indicates whether shared threat intelligence is automatically queried against your internal SIEMs for every circle for which the profile is a member.</td>
</tr>
<tr>
<td>Active</td>
<td>Displays whether the profile is active.</td>
</tr>
<tr>
<td>Instance Admin</td>
<td>This field identifies this profile as an Instance Admin profile, which is automatically created by the system. It is used for administrative access to the central system. This field cannot be modified.</td>
</tr>
<tr>
<td>Internal</td>
<td>Denotes whether this profile belongs to this instance. This field is set by the system and cannot be modified.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.
Configure the sightings threshold

Sightings thresholds are used to determine whether a set of observables from a threat intelligence source merit being shared with a Trusted Security Circle. Only sightings whose counts exceed the specified threshold value are used to create automatic security incidents for the indicated circle.

Before you begin
Role required: sn_tis.admin

Procedure

1. Navigate to Trusted Security Circles > Sightings Thresholds.
   The Sightings Thresholds list opens.

2. Click New.
   The Sightings Threshold screen opens.

3. Fill in the fields as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sightings Search Source</td>
<td>Select the threat intelligence source to be analyzed.</td>
</tr>
<tr>
<td>Circle</td>
<td>Select the Trusted Security Circle with which you want to share the threat sightings.</td>
</tr>
<tr>
<td>Threshold</td>
<td>Enter the maximum number of sightings of a suspicious observable that are tolerated in your environment. Only observables with a sighting count greater than this value are used to create automatic security incidents for the specified circle.</td>
</tr>
</tbody>
</table>

4. Click Submit.

Trusted Security Circles threat data sharing

Observables are artifacts found on a network or operating system that are likely to indicate an intrusion. Typical observables are IP addresses, MD5 hashes.
of malware files, URLs, or domain names. Users in a trusted circle can share observables to other users in the same circle of trust. When you share an observable, all local sightings of that observable are shared.

There are several options available for sharing observables, including:

- **Share Sightings Search results** on individual or multiple observables in a security incident for a selected date range.
- **Share observables from a security incident**.
- **Share observables from Threat Intelligence**.

When observables are shared, the tags associated with the observables are not shared to the trusted circle. So, for example, if a member shares observables that are tagged as **Denylist**, they are not necessarily deny listed on the instances of the shared members. Records that are tagged with **Block from Sharing**, however, are excluded.

Additionally, whenever observables are shared, a notification is sent to all members in the circle to whom the observables are shared.

### Run a Sightings Search

Determine the prevalence of a threat over time or test remediation or eradication efforts. You can select individual or multiple observables and the date range for your search from a security incident. Results are included in the **Security Incident Observables** related list.

**Before you begin**

Role required: sn_si.analyst

**About this task**

The Sightings Search capability has a workflow, **Security Operations Integration - Sightings Search workflow**, that executes the sightings search. This workflow accepts a list of observables, finds any implementing capabilities, creates the queries based on Sightings Search Configurations, and executes the searches based on the configured workflow.

**Note:** An active implementation must be configured. Sightings Search supports Elasticsearch, Splunk, McAfee ESM, HPE ArcSight Logger, and QRadar incident enrichment. If no implementations are available, capability actions, such as **Run Sightings Search**, are not displayed in product menus.
Procedure
1. Navigate to a security incident.
2. Click the **Show IoC** related link.
3. Select **Observables** from the Related List tab.
4. Select the observables you want to perform a sightings search on.
5. Click **Run Sightings Search** in the **Actions on selected rows...** drop-down menu.

The Run Sightings Search dialog box opens.

**Note:** Values entered in the dialog box overwrite capability configuration values for this run.

6. Choose the number of days or a date range to search for data.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last</td>
<td>The number of hours or days prior to the creation of the incident to search. The default is 7 days. The limit is 99 hours or days.</td>
</tr>
<tr>
<td>between</td>
<td>Range of dates to search. Default dates are:</td>
</tr>
<tr>
<td></td>
<td>The date and time the incident was opened.</td>
</tr>
<tr>
<td></td>
<td>The date and time seven days prior to the opening of the incident.</td>
</tr>
</tbody>
</table>

**Note:** Last is the number of hours or days prior to the creation of the incident to search. The default is 7 days. The limit is 99 hours or days.

7. Click Search.
A Sightings Search record is created. Aggregate and associated sightings data are displayed in the security incident under the Sightings Search Results and Sightings Search Details tabs.

**Note:** Sightings search results data can be shared with Trusted Security Circle, with the exception of raw data in the case of implementations configured to include raw data.

### Sightings Search Results

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>The identifier for the sightings search.</td>
</tr>
<tr>
<td>Observable count</td>
<td>Number of observables searched for by query.</td>
</tr>
<tr>
<td>Internal sightings</td>
<td>Count of internal sightings.</td>
</tr>
<tr>
<td>External sightings</td>
<td>Count of external sightings. (Received from threat sharing.)</td>
</tr>
<tr>
<td>Matched configuration items</td>
<td>Count of configuration items that matched an existing record in your cmdb for each observable found in your environment.</td>
</tr>
</tbody>
</table>
### Sighting Search Details

<table>
<thead>
<tr>
<th>Detail</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sighting search</td>
<td>The identifier for the sightings search.</td>
</tr>
<tr>
<td>Observable</td>
<td>Observable searched for by query.</td>
</tr>
<tr>
<td>Observable type</td>
<td>Type of observable searched for by query.</td>
</tr>
<tr>
<td>Internal sightings</td>
<td>Aggregated count of internal sightings.</td>
</tr>
<tr>
<td>External sightings</td>
<td>Aggregated count of external sightings. (Received from threat sharing.)</td>
</tr>
<tr>
<td>Updated</td>
<td>Date and time of the last modification.</td>
</tr>
</tbody>
</table>

#### Note:
If the implementation used for the sightings search is configured to include raw data, and at least one sighting is found, an attachment containing raw data samples appears at the top of the security incident.

### Share Sighting Search results

You can share local sightings details or results that are associated with a particular search with your Trusted Security Circle.

**Before you begin**

Role required: sn_si.analyst

**About this task**

Sharing can be automated using the following Security Incident Response Properties.
• Automatically share the results of a sightings search to the default ServiceNow trusted circle
• Include observables with no local sightings when automatically sharing sightings search results
• Respond with local sightings whenever a threat share is received from a trusted circle

Procedure
1. Navigate to a security incident.
2. Click the Show IoC related list and select the Sightings Search Results tab to view the list of sightings searches.
3. Click on a sightings search result.
4. On the **Sightings Search Result** form, click the **Share sighting search result** related link. The Sighting Search Result Share dialog box appears.

5. Enter a **Name** for this observable share record.

6. Enter a **Description** of the observables to share.

7. Choose **Circles** to share the observables with.

8. Click **Submit**.

   The observable(s) are shared with the specified Trusted Circle.

**Share observables from Threat Intelligence**

Observables can be shared from Threat Intelligence to members in your trusted circle.
Before you begin
Threat Intelligence must be activated.
Role required: sn_ti.analyst

Procedure
1. Navigate to Threat Intelligence > loc Repository > Observables.
2. Select the check boxes for observables you want to share to your trusted security circle.
3. From the Actions on selected rows drop-down list, select Share observable. The Observable Share dialog box appears.

4. Enter a Name for this threat share record.
5. Enter a Description of the observables to share.
6. Choose Circles to share the observables with.
7. Click Submit.

The observable(s) are shared with the specified Trusted Circle.

Create a security incident from shared observables

Automatically create Security Incidents from threat intelligence shared with you, if the sighting count after a sightings search exceeds your preset threshold.

Before you begin
Role required: sn_si.analyst

Procedure
1. Configure the sightings threshold.

2. Define a threshold for each Sightings Search Source for which you want to automatically create security incidents when the defined threshold is exceeded.
   When the sighting count of any observable searched in your environment exceeds the threshold, a security incident is created and all the observables in the search are added to that security incident. If a security incident already exists with the same list of observables, the new incident is made a child incident.

Components installed with Threat Intelligence Sharing

Several types of components are installed with Threat Intelligence Sharing.

⚠️ Note: The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

Tables installed with Threat Intelligence Sharing

Tables are added with activation of Threat Intelligence Sharing.

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comm State [sn_tis_comm_state]</td>
<td>Provides asynchronous processing capabilities with central. This is the parent table for cached central tables (sn_tis_profile, sn_tis_member, sn_tis_trusted_circle, and sn_tis_sic).</td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Job Queue Entry</td>
<td>Scheduled Jobs are queued up to run in each configured domain.</td>
</tr>
<tr>
<td>[sn_tis_job_q_entry]</td>
<td></td>
</tr>
<tr>
<td>Member</td>
<td>Holds the membership records for profiles in circles.</td>
</tr>
<tr>
<td>[sn_tis_member]</td>
<td></td>
</tr>
<tr>
<td>Observables</td>
<td>Contains a record of any Observable found on both your network and on the network of a Profile of belonging to one of your Trusted Circles.</td>
</tr>
<tr>
<td>[sn_tis_m2m_share_observable]</td>
<td></td>
</tr>
<tr>
<td>Processor</td>
<td>Defines the script handler for an asynchronous record operation to central.</td>
</tr>
<tr>
<td>[sn_tis_processor]</td>
<td></td>
</tr>
<tr>
<td>Profile</td>
<td>Represents an organization that can join a Trusted Circle</td>
</tr>
<tr>
<td>[sn_tis_profile]</td>
<td></td>
</tr>
<tr>
<td>Standard Industrial Classification</td>
<td>Contains the Standard Industrial Classification (SIC) codes of Profiles belonging to Trusted Circles.</td>
</tr>
<tr>
<td>[sn_tis_sic]</td>
<td></td>
</tr>
<tr>
<td>Share Response</td>
<td>A response to sharing that is sent back to the trusted security circle.</td>
</tr>
<tr>
<td>[sn_tis_share_response]</td>
<td></td>
</tr>
<tr>
<td>Sighting Threshold</td>
<td>Identifies when an observable or group of observables has sightings that exceed this threshold.</td>
</tr>
<tr>
<td>[sn_tis_sighting_threshold]</td>
<td></td>
</tr>
<tr>
<td>Sightings</td>
<td>The number of times the Observable has been encountered at both yours and the profile.</td>
</tr>
<tr>
<td>[sn_tis_m2m_share_sighting]</td>
<td></td>
</tr>
<tr>
<td>Threat Share</td>
<td>Stores messages shared to a trusted security circle.</td>
</tr>
<tr>
<td>[sn_tis_share]</td>
<td></td>
</tr>
<tr>
<td>Threat Sharing Message Type</td>
<td>Type of message being shared to a trusted security circle.</td>
</tr>
<tr>
<td>[sn_tis_message_type]</td>
<td></td>
</tr>
<tr>
<td>Trusted Circle</td>
<td>Contains a list of the Profiles that are members of a Trusted Circle.</td>
</tr>
<tr>
<td>[sn_tis_trusted_circle]</td>
<td></td>
</tr>
</tbody>
</table>
Roles installed with Threat Intelligence Sharing

Roles are added with activation of Threat Intelligence Sharing.

<table>
<thead>
<tr>
<th>Role title [name]</th>
<th>Description                                                                                                                                                                                                --------------------</th>
<th>Contains roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted Security Circles Administrator [sn_tis.admin]</td>
<td>This is the administrative role for the Trusted Security Circle application. The Trusted Security Circles Client plugin creates this role when you install it. The Trusted Security Circle administrator has full control over the Trusted Security Circle Properties module, and the Sighting Thresholds [sn_tis_sighting_threshold] and Central Sync [sn_tis_async_state_handler] tables.</td>
<td>• sn_ti_admin • sn_tis.write</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role title [name]</th>
<th>Description</th>
<th>Contains roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted Security Circles Read [sn_tis.read]</td>
<td>Allows viewing shared intelligence.</td>
<td>sn.ti.read</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role title [name]</th>
<th>Description</th>
<th>Contains roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted Security Circles Write [sn_tis.write]</td>
<td>Allows performing sharing operations as well as reading shared intelligence.</td>
<td>• sn.tis.read • sn.ti.write</td>
</tr>
</tbody>
</table>

**Related information**

Activate the Trusted Security Circle Client

**Security Operations common functionality**

Whenever any of the plugins for the main Security Operations applications (Security Incident Response, Vulnerability Response, Threat Intelligence, or Configuration Compliance) are activated, the Security Support Common plugin is activated. This plugin loads various modules that provide functionality that is common across all Security Operations applications.
Note: Only users with the [sn_sec_cmn.admin] can view and use the Security Operations module. This role is inherited when you are assigned an administrative role in any of the Security Operations applications.

Security Operations Modules

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Operations Integration Reference, Threat Intelligence integrations, Vulnerability Response integrations</strong></td>
<td>Several integrations are included with the Security Operations applications (Security Incident Response, Threat Intelligence, and Vulnerability Response). This section provides instructions for activating the plugins and configuring both ServiceNow and third-party integrations. Also included are some basic guidelines for developing your own integrations, as well as details on specific integrations included in the base system.</td>
</tr>
<tr>
<td><strong>Security Operations email processing</strong></td>
<td>You can set up the integration of information from external detection systems, provide granularity in processing security operations records, handle unmatched emails, and prevent duplication of records using Email Processing.</td>
</tr>
<tr>
<td><strong>Groups</strong></td>
<td><strong>Filter Groups</strong> Create and use filter groups to locate records from any table on your instance. For example, you can create a group of all computers by the same manufacturer. You can also filter configuration items (CIs) that have similar vulnerabilities or that fall within a particular subnet IP address range. <strong>Escalations</strong> You can create an escalation path for security incidents for issues requiring more</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>attention or expertise. Once an escalation group exists, a button appears</td>
</tr>
<tr>
<td></td>
<td>on any security incident in that group.</td>
</tr>
<tr>
<td>Security Tags</td>
<td>Tags</td>
</tr>
<tr>
<td></td>
<td>Security tag rules provide filtering for security tag access.</td>
</tr>
<tr>
<td>Workflows</td>
<td>View Security Workflows</td>
</tr>
<tr>
<td></td>
<td>You can view the many workflows included with the Security Operations</td>
</tr>
<tr>
<td></td>
<td>applications. You can create workflows from templates and in the Workflow</td>
</tr>
<tr>
<td></td>
<td>Editor.</td>
</tr>
<tr>
<td>Workflow Triggers</td>
<td>Security Operations workflow triggers contain a condition on a table. All</td>
</tr>
<tr>
<td></td>
<td>workflows attached to the workflow trigger record run when the condition</td>
</tr>
<tr>
<td></td>
<td>is met.</td>
</tr>
<tr>
<td>Utilities</td>
<td>Enrichment Data Mapping</td>
</tr>
<tr>
<td></td>
<td>Enrichment Data Mapping transforms data from XML, JSON, or Properties files</td>
</tr>
<tr>
<td></td>
<td>to ServiceNow records. Security Operations workflows use enrichment data</td>
</tr>
<tr>
<td></td>
<td>maps and provide output data to security incidents.</td>
</tr>
<tr>
<td></td>
<td>Field Value Transforms</td>
</tr>
<tr>
<td></td>
<td>Transforms unique customer field values into field values recognized by</td>
</tr>
<tr>
<td></td>
<td>Security Operations email parsing, data enrichment or tables using field</td>
</tr>
<tr>
<td></td>
<td>maps. Supports choice fields, references, and</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>aligns external data into the standard terminology and format for your new record.</td>
</tr>
<tr>
<td><strong>Field Mapping</strong></td>
<td>Security Operations tables can be mapped to and from other tables, linking a security incident to a customer service case or a problem to other parts of the Security Operations system. For example, you can integrate a plugin to a Security Incident Response task.</td>
</tr>
<tr>
<td><strong>On-Demand Orchestration</strong></td>
<td>During Security Incident Response analysis, a security analyst may want to perform a task that is driven by a security incident workflow. For example, run a process dump on a particular CI. This can be accomplished with on-demand orchestration.</td>
</tr>
<tr>
<td><strong>Operating Systems Groups</strong></td>
<td>NA</td>
</tr>
<tr>
<td><strong>SecOps Application Registry</strong></td>
<td>NA</td>
</tr>
<tr>
<td><strong>CMDB</strong></td>
<td>CI identifiers are rules used to lookup a configuration item (CI) in the CMDB that contains matching information from a third-party integration. These rules define the fields that contain matching data and the order of precedence by which they are evaluated.</td>
</tr>
</tbody>
</table>
Create and define filter groups in Security Operations

Create and use filter groups to locate records from any table on your instance. For example, you can create a group of all computers by the same manufacturer. You can also filter configuration items (CIs) that have similar vulnerabilities or that fall within a particular subnet IP address range.

Before you begin
Role required: sn_sec_cmn.write

About this task
Filter groups can contain dynamically updated records, a series of static records that are not filtered using conditions, or a combination of dynamically updated and static records. Some filter groups are included in the base system, for example, CI exclusions.

Procedure
2. Click New.
3. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The lowest Order value is evaluated first.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the filter group.</td>
</tr>
<tr>
<td>Active</td>
<td>Box to activate the group.</td>
</tr>
<tr>
<td>Description</td>
<td>Description for the filter group.</td>
</tr>
<tr>
<td>Network IP Address</td>
<td>The network IP address that contains the IP addresses of the CIs you want to add to the group.</td>
</tr>
<tr>
<td></td>
<td>This field appears only if you selected Configuration Item [cmdb_ci] or a table that extends configuration item in the Table field.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>The subnet that contains the IP addresses of the CIs you want to add to the group, for example, 255.255.255.0.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>This field appears only if you selected Configuration Item [cmdb_ci] or a table that extends configuration item in the Table field.</td>
</tr>
<tr>
<td>Table</td>
<td>The table to be filtered on.</td>
</tr>
<tr>
<td>Condition</td>
<td>Use the condition builder to define the criteria to be filtered.</td>
</tr>
</tbody>
</table>

4. Right-click the form header and select **Save**. An **Advanced Conditions** tab appears.

More tabs appear depending on the type of table you specified in the **Table** field, as follows:

<table>
<thead>
<tr>
<th>Table</th>
<th>Tabs Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Item [cmdb_ci] or a table that extends the configuration item table</td>
<td>Manually Added CIs and Matching CIs</td>
</tr>
<tr>
<td>Task [task] or a table that extends the task table</td>
<td>Manually Added Tasks and Matching Tasks</td>
</tr>
<tr>
<td>A table not related to a CI or task</td>
<td>Manually Added Record</td>
</tr>
</tbody>
</table>

5. To define more conditions for your filter group:

a. Click **Advanced Conditions**.

b. Insert a new row into the **Additional Filter Group Conditions** embedded list to select other prebuilt filter groups that you want to combine with the filter group being updated. If you want the selected filter group to filter records based on a reference field, a mapped field is automatically selected when the current record is saved.

   🔄 **Note:** The **Mapped field** value cannot be edited from the **Additional Filter Group Conditions** embedded list. To change the field, click the information icon 🔄 to open the record.

c. Click **Update**.

6. To manually add more CIs or tasks to the filter group:

a. Click the **Manually Added CIs** or **Manually Added Tasks** tab.

b. Click **Edit**.
c. Select the CIs or tasks you want to add.

d. Click Save.

7. To view the CIs or tasks that match your selection criteria:

   a. Click the Matching CIs or Matching Tasks tab.

   b. If you changed the criteria, refresh the list by right-clicking in the form header and selecting Refresh List.

Shared data transformation

The Security Incident Response, Vulnerability Response, and Threat Intelligence plugins share common features, for relationship data and duplication rules, used to import external and internal information into Security Operations.

Email Parsing, Duplication Rules, and Field Mapping take input data (an email, JSON or XML file, or a record) and transform that data into the correct format to create a new record. Each of these features pulls data in their own way but, it is transformed into the new record using many of the same processes.

Relationship data

When you add information to a related list (such as an associated observable in a security incident), you can create a relationship record consisting of an m2m table. Sometimes, there is additional data on that relationship record to set. For example, an observable being a Source IP (as opposed to a destination IP). That information goes in the Relationship data field in the Field Transform form used by Email Parsing or a Field Mapping Fields related list in the Field Mapping form.

The Relationship data field is usually empty. It is most commonly used for IP addresses on observables in Email Parsing.

You can transform data from any ServiceNow record to any other ServiceNow record using Field Mapping Fields in the Field Mapping feature. For example, to transform data from an incident to a security incident, or a security incident to a PRB.

Security Operations duplication rules

Use Duplication Rules to handle duplicate records for security, vulnerability, IoCs, and so on.

Duplication rules have two purposes. They prevent too many duplicate records from being created and, when a duplicate is detected, they specify which fields in the record are updated. Only active duplicates are looked for. If the record is not active, for example, if the incident is closed, then any new identical problem becomes a new incident.
Duplication rules are used by **Email Parsing**, **Field Mapping**, and **Enrichment Data Mapping**.

**Related information**
- Create email parsers in Security Operations
- Map tables to tables with Security Operations field mapping

**Create duplication rules in Security Operations**
You can use Duplication Rules to identify new email, enrichment data, or field maps with active duplicate records and process them appropriately.

**Before you begin**
Role required: sn_sec_cmn.write

**Procedure**
1. Navigate to **Security Operations > Duplication Rules**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the duplication rule.</td>
</tr>
<tr>
<td>Table</td>
<td>Table where records are created and used to determine duplication.</td>
</tr>
<tr>
<td>Identifying fields</td>
<td>Select a set of fields that indicate a duplicate security incident, observable, vulnerability, and so on, when the values in these fields are identical.</td>
</tr>
<tr>
<td>Duplicate action</td>
<td>Governs how to handle duplicate emails. Choices are:</td>
</tr>
<tr>
<td></td>
<td><strong>Create as child</strong></td>
</tr>
<tr>
<td></td>
<td>Creates a record as a child of the original. The field linking the child to the parent is the <strong>Parent</strong> field.</td>
</tr>
<tr>
<td></td>
<td><strong>Do not create nor update records</strong></td>
</tr>
<tr>
<td></td>
<td>(default) Does nothing. Ignores duplicates.</td>
</tr>
<tr>
<td></td>
<td><strong>Update duplicate record</strong></td>
</tr>
<tr>
<td></td>
<td>Updates the fields in the existing record as specified in <strong>Duplication Actions</strong>.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to activate the rule.</td>
</tr>
<tr>
<td>Description</td>
<td>Describes the purpose and application of this duplication rule; when it should be used, for example a rule designed for IP-based observable, or security incidents from the firewall.</td>
</tr>
</tbody>
</table>

4. Right-click in the record header and select **Save** or click **Update**.

5. To set duplication actions, if you have chosen **Update duplicate record**, click **New** to create duplication actions for each field you want to update in the incident.

6. Fill in or edit the fields on the form, to describe how to update the field:

<table>
<thead>
<tr>
<th>Duplication actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
</tr>
<tr>
<td>--------</td>
</tr>
<tr>
<td>Field</td>
</tr>
</tbody>
</table>
| Action | The actions supported vary by field type. Choices are:

  **Update this field with the new value**
  Replaces the previous value in the existing record with this value.

  **Append the new value to a comma separated list, if unique**
  Treats the value as an entry in a comma-separated list and adds the new data (if any) as a new entry in that list. If the data is already in the list, it is not added twice.

  **Append the new value to this field**
  Appends the new value to the end of the existing text in the field.

  **Add one to a counter field**
  Adds one to the numeric field.

  **Set the field to today**
  Sets the field to the current date and time. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Append to related list</strong></td>
<td>Adds the related record with this value to the related list of the current record. Appears when there is a many-to-many table, with a column of the same type, linked to the table being updated. For example, <strong>Affected CI</strong> or <strong>Affected User</strong>.</td>
</tr>
<tr>
<td>Relationship</td>
<td>[Optional] This field appears only when the <strong>Append to related list</strong> action is chosen. It is the name of the related list you want to associate with this rule.</td>
</tr>
<tr>
<td>Duplication rule</td>
<td>Rule that this action is part of.</td>
</tr>
<tr>
<td>Table</td>
<td>Table where records are created. Displays as information only.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to activate the action.</td>
</tr>
</tbody>
</table>
7. Click **Submit**.

---

**Security Operations email processing**

You can set up the integration of information from external detection systems, provide granularity in processing security operations records, handle unmatched emails, and prevent duplication of records using Email Processing.

Email Processing consists of these features:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Parsing</td>
<td>Generate new Security Operations records from external system emails.</td>
</tr>
<tr>
<td>Duplication Rules</td>
<td>Identifies new email with known incidents and processes them appropriately.</td>
</tr>
<tr>
<td>Properties</td>
<td>Specifies accounts used as input in Email Parsing for security, vulnerability, and IoCs. Provides for granularity in processing Security Operations records.</td>
</tr>
<tr>
<td>Unmatched Emails</td>
<td>Lists emails that do not match any Security Operations record.</td>
</tr>
</tbody>
</table>
Security Operations email properties

Email Properties specify which inboxes are used as input in Email Parsing to import information from external detection systems to create records for security, vulnerability, and IoCs. You can set up a general account for all external detection systems to use, or individual email accounts for Security Incident Response, Threat Intelligence, or Vulnerability Response.

Create Security Operations email properties

You can specify email addresses for reports and control automatic email behaviors using email Properties.

Before you begin
Role required: sn_sec_cmn.admin
Set up external detection tools to send emails to your email parsing inbox.

Procedure

2. Enter your recipient mailboxes as appropriate:
   These are inbound email addresses to be processed by Email Parsing, rather than Inbound Actions.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbox for Security Operations tools</td>
<td>Full email address for Security Operations. For example, <a href="mailto:secops_support@yourcompany.com">secops_support@yourcompany.com</a>.</td>
</tr>
<tr>
<td>Inbox for Security Incident tools</td>
<td>Full email address for Security Incident Response. For example, <a href="mailto:sir_support@your.company.com">sir_support@your.company.com</a>.</td>
</tr>
<tr>
<td>Inbox for Vulnerability Response tools</td>
<td>Full email address for Vulnerability Response. For example, <a href="mailto:vuln_resp@yourcompany.com">vuln_resp@yourcompany.com</a>.</td>
</tr>
<tr>
<td>Inbox for Threat Intelligence tools</td>
<td>Full email address for Threat Intelligence. For example, <a href="mailto:threat_intel@yourcompany.com">threat_intel@yourcompany.com</a>.</td>
</tr>
</tbody>
</table>

3. Click Save.
Security Operations email parsing

Generate new Security Operations records from external detection systems using Email Parsing. This feature provides a method for integrating information from external tools such as malware detection, vulnerability detection, firewalls, threat intelligence, and more.

How emails are parsed

Any system that can send an email, can create Security Operations records, for example, security incidents, requests, vulnerable items, vulnerabilities, security incident observables, attack methods, and more.

All Security Operations plugins (Security Incident Response, Threat Intelligence, and Vulnerability Response) have a property (email_to) that defines the email address where external integrations should send emails to, to be parsed by the email parsers. See Email Processing > Properties for more information.

Email sent to any of the Security Operations email addresses is stored in an email events table. These emails are processed to determine whether they match any email parser.

Emails that have a match are flagged and the transform and duplication rules create or update a Security Operations record. The email is linked to that record and flagged as matched.

Emails that do not match are listed in Unmatched Emails as a Security Operations record. They can be reviewed to help build email parsers to handle these emails. A Reprocess action allows you to run the unmatched email through the parsers again. The original email log is linked to that record.

The duplication rules for the email transform manage multiple emails relating to the same issue. These rules define what makes a duplicate record and can prevent duplicate records from being created. When a duplicate is detected, the rule specifies what action to take: no action (do not create a new record), create the new record as a child record of the existing record, or update the existing record. When updating the duplicate rule specifies which fields in the existing record are updated.

Note: A Security Operations email parser works in conjunction with platform inbound actions and does not replace them. It does not support setting values on indirect fields for example, sys_journal_field entries.

By default, email events are deleted after 30 days.

Multiple records
External detection systems (malware detectors, vulnerability, and so on) can send emails that report on multiple items at one time. The email parser supports separators within the email.

For example, a malware detector could send you an email report about all systems within your network infected by one particular malware with information about the malware first, followed by a list of the systems affected.

In this example, when the Record Separator is set within your Email Transform as ===============, it splits the email into four sections that are evaluated separately. This creates a Security Incident for each of the three affected systems.

Note: The header section is detected but does not have any affected systems so, it is used in all three records and does not create a fourth record.

Field Transforms pull in data from each section. If something in the header or footer of the email applies to all records, such as Malware Hash, Malware Name, and Type in this example, the field transform for them should set Search for value to a value that searches within the email body either At the start of a line in the email body or Anywhere in the email body.

Field Transforms must be set to search At the start of a line within the record section or Sec for data that is defined within each section, such as System, IP address, or Status. The record section options are only available when there is a record separator defined within the email transform.

When parsing an email with a separator defined, records are only created for sections with at least one piece of section-specific data.

In this example, three records are created, even though there are four sections defined. The first section is a header, and it lacks anything specific to only one
system. If any of the fields within the first section were filled in (System, IP, or Status), then a record would be created for that section, as well.

Related information
- Create email parsers in Security Operations
- Security Operations enrichment data mapping
- Security Operations field mapping

Create email parsers in Security Operations
Email Parsing creates Security Operations records from your email for security, vulnerability, and observables to expedite threat response and remediation.

Before you begin
Role required: sn_sec_cmn.admin
- Set up external detection tools to send emails to a central email address.
- Set the email address in Security Operations Properties. For more information, see Create Security Operations email properties.
- Assign a user account to this email address and give that user security access controls to create and update the email event records.
- Have a copy of the relevant email from your external detection tool in front of you.
- Decide what type of record you want to create, a security incident, vulnerability record, task and so on. This choice determines the table you select.

Procedure
1. Navigate to Security Operations > Email Parsing.
2. Click New.
3. Fill in the fields on the form, as appropriate.

Note: If more than one field is specified, all fields must match the email to create a record.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the email parser.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Email is from</td>
<td>If filled in, only emails from this address are transformed by this email parser.</td>
</tr>
<tr>
<td>Email is to</td>
<td>If filled in, only emails from this address are transformed by this email parser.</td>
</tr>
<tr>
<td>Email subject contains</td>
<td>If filled in, only emails where the subject contains this phrase are transformed by this email parser.</td>
</tr>
<tr>
<td>Dupslication rule</td>
<td>Governs how to handle duplicate emails for any email this transform handles. For more information, see <a href="#">Shared data transformation</a>.</td>
</tr>
<tr>
<td>Order</td>
<td>In what order to consider the transforms. The first matching email transform is used. Typically, you want to set up the most specific email parsers in the lower numbers, with some fallback. Give catchall email parsers higher Order numbers so they run if nothing else matches. Default is 100. When everything matches, the most specific email parser (matches from, to, and subject) is used.</td>
</tr>
<tr>
<td>Destination table</td>
<td>The table where you want to create records.</td>
</tr>
<tr>
<td>Active</td>
<td>Whether this transform is active, in use, or not active. If unchecked, no emails are transformed with this code.</td>
</tr>
<tr>
<td>Record Separator</td>
<td>When emails handled by this email parser create multiple records, this field contains the separator between the information for those records. See <a href="#">Security Operations email parsing</a> for more information.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of this email parser, which tool it works with, the purpose, and so on.</td>
</tr>
</tbody>
</table>

4. When you have completed your entries, right-click in the form header and select **Save**.

A Field Transforms tab appears. This tab shows how individual fields within the destination table are set based on the email contents.
5. To add Field Transforms, perform these steps.
   a. In the Field Transforms tab, click New.
   b. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>Store value in a field or a related list</td>
<td>Select where to find the value. Choices include:</td>
</tr>
<tr>
<td></td>
<td>• Store the value into a field in the new record</td>
</tr>
<tr>
<td></td>
<td>• Link to this value in a related list</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Field</td>
<td>Select the field to fill in with this value.</td>
</tr>
<tr>
<td>Note:</td>
<td>For choice fields, matches are made to existing choices using the underlying choice label or value. If no match is found, the field is set, but no new entry is added to the choice list. For more information, see Choice lists. For reference fields, an entry is set only when a value matching the display name of the record or a valid sys_id is found. For more information, see Reference fields.</td>
</tr>
<tr>
<td>Related list</td>
<td>When Store value in a field or related list is set to Link to this value in a related list or Link to this value, creating a new record if a matching record does not exist, this field specifies the related list to add information to.</td>
</tr>
<tr>
<td>Value field</td>
<td>When Store value in a field or related list is set to Link to this value in a related list or Link to this value, creating a new record if a matching record does not exist, this field specifies the field within the table displayed in the related list. It is used to look up and find an existing record. For example, if your related list is Affected CIs, this field can contain Name or Fully Qual-</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Relationship data</strong></td>
<td>When <em>Store value in a field or related list</em> is set to <em>Link to this value in a related list</em>, a record is created to link that record (such as a security incident) to the value (a CI, an Observable, and so on.). This field specifies any additional information (field and value pairs) that should be added to the linking record. For example, adding an Observable for a source IP, specify that this IP is the source, rather than destination IP. For multiple values, use a ^ separator, for example, type=Source IP^Active=true.</td>
</tr>
<tr>
<td><strong>New record data</strong></td>
<td>When <em>Store value in a field or related list</em> is set to <em>Link to this value</em>, creating a new record if a matching record does not exist, if no related record matching the parsed value is found, a record is created. This field specifies the static data to add to that record. For <em>Affected CIs</em>, if no matching CIs are found a CI record is created. When that happens, the value found in the email, is set to the <em>Value</em> field in the CI record. You can set additional data – a note indicating why the CI was created, some information about what type of CIs you are working with and, so on. A sample would be: description=Created by Malware Scanner email parser^type=autodetect.</td>
</tr>
</tbody>
</table>
| **Search for value** | Select the location in the email to search. Choices include:  
  - At the start of a line in the email body  
  - Anywhere in the email body |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• In the email subject line</td>
<td>When you have defined a <strong>Record Separator</strong>, more options (Anywhere within the record section and At the start of a line within the record section) enable you to search only within the current section instead of in the entire email body (See Security Operations email parsing for more information. Information that is in a header or footer, applying to all records, is searched for in the entire email body. The information that differs between records is searched for only within the section.</td>
</tr>
<tr>
<td>Value separator</td>
<td>When <strong>Store value in a field or related list</strong> is set to <strong>Link to this value in a related list</strong> or <strong>Link to this value</strong>, creating a new record if a matching record does not exist, this field specifies the separator to use for lists of items. For example a comma or semicolon when the data from the email is a list of IP addresses.</td>
</tr>
<tr>
<td>Value prefix</td>
<td>The text that always precedes the value placed within this field to extract.</td>
</tr>
<tr>
<td>End of value</td>
<td>Select what indicates the end of the value. Choices include: <strong>End of line</strong>, <strong>End of email</strong> (brings in all remaining text in the email), or <strong>Until</strong> (stops when it finds the specified text), or <strong>Until</strong> (stops when it finds the specified text).</td>
</tr>
<tr>
<td>Value suffix</td>
<td>When the <strong>End of Value</strong> is set to <strong>Until</strong>, this field specifies what text always</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Value transform</td>
<td>Choose the field transformation entry to apply. Converts the value found in the email into a different value, used to fill in choice fields, occasionally reference, and other fields.</td>
</tr>
<tr>
<td>Order</td>
<td>The order in which the field transforms run, from lowest to highest. A field transform with an order entry of 100 is attempted first. Only if that field transform fails to find a value will a field transform with a higher order (200) on the same field run.</td>
</tr>
<tr>
<td>Email transform</td>
<td>The transform this field transform belongs to.</td>
</tr>
<tr>
<td>Destination table</td>
<td>Destination table of the email transform. It contains informational data from the email transform.</td>
</tr>
<tr>
<td>Active</td>
<td>The default is checked. When checked, the field transform is activated. Uncheck this box to deactivate the field transform.</td>
</tr>
</tbody>
</table>

a. Click **Submit**. The new record is used to parse the information in the email into a new record.
Related information

- Create duplication rules in Security Operations
- Create Security Operations field value transforms
- Define Vulnerability Response email notifications

Edit email records in Security Operations

Add or create transforms in your existing email event records.

Before you begin

Role required: sn_sec_cmn.admin

Procedure

1. Navigate to **Security Operations > Email Parsing**.
2. Click the email parser to edit.
   - If the record is read-only, click the here link in the header message.
   - You are taken to the editable form of the transform.
3. Edit fields as appropriate.

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
4. To edit **Field Transforms**, click in the field and change as appropriate.

5. Click **Update**.

**Unmatched Security Operations email events**

Email events that do not match an email parser have their "matched" flag unset. You can view these email event records from the Unmatched Emails list, to reveal external detection systems whose emails are not yet parsed.

As you create email parsers, you can attempt to reprocess the email event (from the form or the list) to validate a new email parser.

**View and reprocess unmatched Security Operations emails**

You can review Unmatched Emails for discontinued filters or as candidates for a new filter to maintain or improve the rate at which you catch email threats.

**Before you begin**

Role required: sn_sec_cmn.read

**Procedure**

1. Navigate to **Security Operations > Unmatched Emails**.
   - If any unmatched emails have been found, they are listed.

2. The fields on the form are as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>Email address of the sender.</td>
</tr>
<tr>
<td>To</td>
<td>Email address of the recipients.</td>
</tr>
<tr>
<td>Subject</td>
<td>Subject line in the email.</td>
</tr>
<tr>
<td>Body</td>
<td>Contents of the body of the email.</td>
</tr>
<tr>
<td>Matched</td>
<td>Indicates if this email event was matched.</td>
</tr>
</tbody>
</table>

3. To reprocess this email, create an email record or edit an existing email record to match the information in this email. See [Create email parsers in Security Operations](#).
4. Navigate back to **Security Operations > Unmatched Emails**.

5. Click **Reprocess Email Event** to attempt to process this email. It returns you to the Unmatched Emails main list. If the new email record matches, the email event is no longer in the list. A message indicates if it was matched or not.

### Security Operations field mapping

Security Operations tables can be mapped to and from other tables, linking a security incident to a customer service case or a problem to other parts of the Security Operations system.

**Field Mapping** defines the mapping used when a record from the source table is used to create a new record in the destination table. Typically used to create a security incident from another record, these maps define which fields in a security incident are inserted into a new problem or which fields from an existing customer incident populate a new security incident.

### Map tables to tables with Security Operations field mapping

Security Operations provides you with finer field mapping granularity so you can map a Security Operations table to any other table.

**Before you begin**

Role required: sec_cmn.write

**Procedure**

1. Navigate to **Security Operations > Utilities > Field Mapping**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the field map.</td>
</tr>
<tr>
<td>Source table</td>
<td>The table that provides the data to use to create a record in the destination table.</td>
</tr>
<tr>
<td>Duplication rule</td>
<td>Governs how to handle source records that would generate a duplicate record. For more information, see <a href="#">Shared data transformation</a>.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Destination table</td>
<td>The table where new records are created.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to activate the mapping.</td>
</tr>
<tr>
<td>Description</td>
<td>Description for the field map.</td>
</tr>
</tbody>
</table>

Note: Only one mapping between tables can be active at a time. If two maps contain the same tables, then the older version is automatically deactivated.

4. When you have completed your entries, right-click in the form header and select **Save**. **Field Mapping Fields** tab appears. This record defines what data is placed in the target field, in records created by this field transform.

5. Click **New**.

6. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Select where to find the value. Choices include:</td>
</tr>
<tr>
<td></td>
<td>• Add new value into a field in the record</td>
</tr>
<tr>
<td></td>
<td>• Link to this value in a related list</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Related list</td>
<td>When Store value in a field or related list is set to Link to this value in a related list or Link to this value, creating a new record if a matching record does not exist, this field specifies the related list to add information to.</td>
</tr>
<tr>
<td>Value field</td>
<td>When Store value in a field or related list is set to Link to this value in a related list or Link to this value, creating a new record if a matching record does not exist, this field specifies the field within the table displayed in the related list, that is used to look up and create a new record if a matching record does not exist.</td>
</tr>
</tbody>
</table>
| Field                        | When Store value in a field or related list is set to Add new value into a field in the record, this field specifies the field to fill in. \n
| Note:                        | \n
© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Relationship data</strong></td>
<td>When Store value in a field or related list is set to Link to this value in a related list, a new record is created to link that record (such as a security incident) to the value (a CI, an observable, and so on). This field specifies any additional information (field and value pairs) that should be added to that linking record. For example, adding an observable for a source IP, you can specify that this IP is the source, rather than destination IP. For multiple values, use a ^ separator, for example, type= Source IP^active=true.</td>
</tr>
<tr>
<td><strong>New record data</strong></td>
<td>When Store value in a field or related list is set to Link to this value, creating a new record if a matching record does not exist, if a related record matching the parsed value is not found, a new record is created. This field specifies the static data to add to that record. For example, for Affected CIs, if we cannot find the CI, this setting indicates that a new CI is created). The value found in the source record is set to the Value field in the CI record. You can set additional data – a note indicating why this CI was created, some information about what type of CIs you are working with. A sample would be:</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Value separator</td>
<td>When <strong>Store value in a field or related list</strong> is set to <strong>Link to this value in a related list</strong> or <strong>Link to this value</strong>, creating a new record if a matching record does not exist, this field specifies the separator to use for lists of items, commonly a comma or semicolon.</td>
</tr>
<tr>
<td>Value type</td>
<td>When <strong>Store value in a field or related list</strong> is set to <strong>Add new value into a field in the record</strong> this field specifies the type of value. Choices include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Source field record</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Append to the field as a new line</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Static value</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Static value plus source record field value</strong></td>
</tr>
<tr>
<td>Source field</td>
<td>Choose the source field that contains the value to be placed within the destination field or the selected related list.</td>
</tr>
<tr>
<td>Static field</td>
<td>Static value for the field.</td>
</tr>
<tr>
<td>Value transform</td>
<td>Choose the field value transformation entry to apply. It is used to map choice fields between records, for example, converting the set of <strong>Category</strong> choices for a security incident into the appropriate <strong>Type</strong> field for a Change Request.</td>
</tr>
<tr>
<td>Destination table</td>
<td>Auto-populated with the destination table.</td>
</tr>
<tr>
<td>Field Mapping</td>
<td>Auto-populated with the parent field map.</td>
</tr>
</tbody>
</table>
Security Operations field value transforms

Transforms unique customer field values into field values recognized by Security Operations email parsing, data enrichment or tables using field maps. Supports choice fields, references, and aligns external data into the standard terminology and format for your new record.

You can map data for fields such as Category, State, or Assignment Group into the values used within the Security Operations table. For example, map "In Analysis" to "Work in progress."

Create Security Operations field value transforms

Field Value Transforms defines one transformation between provided source data, and the replacement value to use.

Before you begin
Role required: sn_sec_cmn.basic or sn_si.basic

About this task
Define each transformation entry to apply either when there is a match to the search value, or when the search value is contained within the provided source data, or when no matches are found. Set a default value for when no match is found. If no default value is set, and no matches are found, the original source data is used.

Procedure
2. Click New.
3. Fill in the fields on the form, as appropriate.

Field value transforms

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the field value transform.</td>
</tr>
<tr>
<td>Description</td>
<td>Description for the field map.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Field Value Transform</td>
<td>The table list of entries.</td>
</tr>
<tr>
<td>Transform Entries</td>
<td></td>
</tr>
<tr>
<td>a. Under <strong>Replace data</strong></td>
<td>double-click 'Insert a new row.'</td>
</tr>
<tr>
<td>b. Choose one of the following:</td>
<td></td>
</tr>
<tr>
<td>When the date for this field matches</td>
<td></td>
</tr>
<tr>
<td>When the data for this field contains</td>
<td></td>
</tr>
<tr>
<td>When no other transform entry matches the data</td>
<td>(default)</td>
</tr>
<tr>
<td>c. Click the green check mark.</td>
<td></td>
</tr>
<tr>
<td>d. Double-click under <strong>Search value</strong>, add your search value.</td>
<td></td>
</tr>
<tr>
<td>e. Click the green check mark.</td>
<td></td>
</tr>
<tr>
<td>f. Double-click under <strong>Replacement value</strong> add the ServiceNow corresponding value.</td>
<td></td>
</tr>
<tr>
<td>g. Repeat if necessary.</td>
<td></td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to activate the transform.</td>
</tr>
<tr>
<td>Application</td>
<td>Scope of the application.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**Security Operations enrichment data mapping**

Enrichment Data Mapping transforms data from XML, JSON, or Properties files to ServiceNow records. Security Operations workflows use enrichment data maps and provide output data to security incidents.

Security Operations includes several enrichment data maps, triggered by various workflows, for example, **Security Operations Integrations - Get Network Statistics workflow** and **Security Operations System Command Integration - Get Running Processes workflow**. Enrichment data map output from Security Operations workflows is displayed in the **Enrichment Data** tab on the security incident form.

**Create a Security Operations enrichment data map**

Transform data from JSON, XML, or Properties file format to ServiceNow records using enrichment data maps.

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Before you begin
Role required: sn_sec_cmn.write

About this task
Existing enrichment data maps are used by workflows provided within Security Operations. You can view the list under Enrichment Data Mapping. To use a map, you need a trigger, either a business rule or workflow.

Procedure
2. Click New.
3. Fill in the fields, as appropriate.

Creating an enrichment data map

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of this enrichment data map.</td>
</tr>
<tr>
<td>Input format</td>
<td>Choose a format from the list:</td>
</tr>
<tr>
<td></td>
<td>JSON (default)</td>
</tr>
<tr>
<td></td>
<td>XML</td>
</tr>
<tr>
<td></td>
<td>Properties File format</td>
</tr>
<tr>
<td>Prefix key</td>
<td>Use to limit the input data set to a specified key. The root of the input</td>
</tr>
<tr>
<td></td>
<td>data set is set to this key. In this example, if you entered file_info,</td>
</tr>
<tr>
<td></td>
<td>then the input values would be limited to those values within file_info.</td>
</tr>
</tbody>
</table>

```xml
<?xml version="1.0" encoding="UTF-8"?>
<malware>
  <version>2.0</version>
  <file_info>
    <malware>yes</malware>
    <sha1>24c051142583e10451a53893fed3aa5d80bfb1f6</sha1>
    <filetype>PE</filetype>
    <sha256>be9bd96808173e2d967feef8c8c5b8c4d73b621584fb11eb68434da1e6a0a930</sha256>
  </file_info>
</malware>
```
Application | Scope of the application.
---|---
Duplication rule | Rule defining when a record is considered a duplicate and what actions to take with duplicate records.
Destination table | Choose a table from the list.
Active | Select this check box to activate the map.
Description | Enter a description of the enrichment data map.

4. Click **Submit**. The Enrichment Data Mapping Fields tab appears.

5. Click **New**.

6. Fill in the fields on the form, as appropriate.

### Enrichment data mapping fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Name of the enrichment data map.</td>
</tr>
<tr>
<td>Value type</td>
<td>Choose from the list:</td>
</tr>
<tr>
<td></td>
<td>Lookup data using property key</td>
</tr>
<tr>
<td></td>
<td>Static value</td>
</tr>
<tr>
<td></td>
<td>Static value plus data from the property key</td>
</tr>
<tr>
<td></td>
<td>Field is an array or object (raw data nesting)</td>
</tr>
<tr>
<td></td>
<td>Each choice has different entries. Field values and arrays or objects require a Property key.</td>
</tr>
<tr>
<td>Property key</td>
<td>Determines the key for the input data search and the value written to the target field.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Value transform</td>
<td>The field value transform that maps one value to another.</td>
</tr>
<tr>
<td>Application</td>
<td>Scope of the application.</td>
</tr>
<tr>
<td>Order</td>
<td>In what order to consider the mapping. The first match is used. Default is 100.</td>
</tr>
<tr>
<td>Mapping</td>
<td>Name of the enrichment data map.</td>
</tr>
<tr>
<td>Destination table</td>
<td>The table to which the fields to map are going.</td>
</tr>
</tbody>
</table>

7. Click **Submit**. The following is an example of an enrichment data map.
Security Operations user-defined escalation

You can create an escalation path for security incidents for issues requiring more attention or expertise. Once an escalation group exists, a button appears on any security incident in that group.

Create a Security Operations user-defined escalation group

Escalate a security incident to any group associated with the incident using Escalations.

Before you begin
Role required: sn_si.admin

Procedure

2. Click New.
3. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Escalation incident number (field is auto-generated).</td>
</tr>
<tr>
<td>Initial group</td>
<td>Select group this security incident belongs to.</td>
</tr>
<tr>
<td>Escalation group</td>
<td>Select group to escalate the security incident to.</td>
</tr>
</tbody>
</table>

4. Click Submit.
An escalation group is available for all security incidents in the initial group. You can create multiple groups.

Create domain-separated property overrides

When you use domain separation, you can create overrides to existing Security Operations properties that allow you to customize the functions of the applications in each of your domains.

Before you begin
Requires that Domain Support - Domain Extensions Installer be activated.
Role required: admin

Procedure
2. Click New.
   The Domain Separated Property form opens.
3. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Override existing</td>
<td>Select this check box to create a domain-specific value for an existing property.</td>
</tr>
<tr>
<td>Application</td>
<td>Select the application that contains the property you want to override.</td>
</tr>
<tr>
<td>Property</td>
<td>Select the property for the selected application for which you want to create a domain-specific override.</td>
</tr>
<tr>
<td>Domain</td>
<td>Select the domain for which you are creating this property override.</td>
</tr>
<tr>
<td>Active</td>
<td>Turn the override on or off.</td>
</tr>
<tr>
<td>Suffix</td>
<td>Displays the property suffix.</td>
</tr>
<tr>
<td>Name</td>
<td>Displays the property name.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays the property type.</td>
</tr>
<tr>
<td>Value</td>
<td>Displays the current value set for the property.</td>
</tr>
<tr>
<td>New value</td>
<td>Enter a new value for the property to be applied to this domain.</td>
</tr>
</tbody>
</table>
4. Click **Submit**.
   The property override is applied to the selected property in the specified domain. When the logic for this property is triggered, the system checks for domain-separated property overrides. If an override for the domain is found, the new value is used. Otherwise, the value for the default domain is used.

**Related information**

**Create an operating system group**

Operating system groups are used to map an operating system to specific process types and scripts in Security Incident Response workflows. The scripts define how running processes for the defined operating system groups are retrieved. New operating systems can be added as needed.

**Before you begin**

Role required: sn_sec_cmn.admin

**Procedure**

1. Navigate to **Security Operations > Utilities > Operating System Groups**.
   The base system includes scripts for three operating systems:
   - BSD-based OS
   - POSIX-based OS
   - Windows OS

2. Click **New**.

3. Fill in the fields, as needed.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the operating system group.</td>
</tr>
<tr>
<td>Description</td>
<td>A description for the operating system group.</td>
</tr>
<tr>
<td>Table</td>
<td>The affected table.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to activate the operating system group.</td>
</tr>
<tr>
<td>Use filter group</td>
<td>Select this check box to use a filter group for locating matching records in the selected table.</td>
</tr>
<tr>
<td>Filter group</td>
<td>Select the filter group for locating matching records in the selected table. This field displays only if you selected the <strong>Use filter group</strong> check box.</td>
</tr>
<tr>
<td>Condition</td>
<td>The condition builder fields display only if you did not select the <strong>Use filter group</strong> check box.</td>
</tr>
</tbody>
</table>

4. Right-click in the form header and select **Save**. The Operating System Related Scripts related list opens.

5. Click **New**.

6. Select scripts that correspond with the workflows you are using to get running processes, services, and/or network statistics.

7. Click **Submit**.

**Related information**

**Set up security tag groups and tags**

You can assign tags to security incidents, response tasks, vulnerable items, observables, IoCs, and security cases to create metadata on the responding record and define who should have access to specific types of security content. The tags can be added to security groups to organize them.
Before you begin
Role required: sn_si.admin

Procedure

1. Navigate to **Security Operations** > **Security Tags** > **Groups**.
   Three default classification groups are included in the base system.
   - **Enrichment allow list/deny list**: This group defines whether a record is to be treated as a allow list or deny list record. Allow list records are generally of less significance, so they can be ignored. Deny list records are generally of higher interest.
   - **Metatag**: This group is provided as demo data. You can use it to create custom classification tags that are used by security operations applications.
   - **Traffic Light Protocol**: This group is used to ensure that sensitive information is shared with the correct audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity. For each color, you can assign the appropriate read/write access roles. When sharing observables to a trusted security circle, the tag assigned to the trusted security circle profile determines which TLP-tagged observables can be shared to the circle, as follows:
     - **TLP: WHITE**: Only observables with TLP: WHITE can be shared to a TLP: WHITE profile.
     - **TLP: GREEN**: Observables with TLP: GREEN and TLP: WHITE can be shared to a TLP: GREEN profile.
     - **TLP: AMBER**: Observables with TLP: AMBER, TLP: GREEN, and TLP: WHITE can be shared to a TLP: AMBER profile.
     - **TLP: RED**: All observables, regardless of their TLP tag, can be shared with a TLP: RED profile since TLP: RED is the highest ranked TLP tag.
   
   **Note**: You can add other TLP colors, but any in addition to the four colors included are considered not valid by the Forum for Incident Response and Security Teams (FIRST).

2. Click **New**.

3. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter name of the security group.</td>
</tr>
<tr>
<td>Allow multi-selection</td>
<td>Check this box if you want to be able to assign multiple security tags to a record that shares a group.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Active</td>
<td>Turn the group on or off.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of this group.</td>
</tr>
</tbody>
</table>

4. Right-click the form header and select **Save**. The Security Tags related list appears.

5. In the Security Tags related list, click **New**.

6. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the classification tag.</td>
</tr>
<tr>
<td>Security Tag Group</td>
<td>If the tag was created using the <strong>New</strong> button in the group related list, this field defaults to the current group. If needed, you can add the tag to a different group, but this is optional.</td>
</tr>
<tr>
<td>Order</td>
<td>Specify the order the tag appears on forms or within a list.</td>
</tr>
<tr>
<td>Color</td>
<td>Select the color for this tag.</td>
</tr>
<tr>
<td>Enforce restricted access</td>
<td>Select this check box to assign read and/or write roles needed by users to read or write to records that have this security tag.</td>
</tr>
<tr>
<td>Active</td>
<td>Turn the tag on or off.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of this tag.</td>
</tr>
<tr>
<td>Roles (read access)</td>
<td>To assign read access to a security tag, click the lock icon, select the appropriate access roles, and click the lock icon again. This field appears only if you selected the <strong>Enforce restricted access</strong> check box.</td>
</tr>
<tr>
<td>Roles (write access)</td>
<td>To assign write access to a security tag, click the lock icon, select the appropriate access roles, and click the lock icon again. This field appears only if you selected the <strong>Enforce restricted access</strong> check box.</td>
</tr>
</tbody>
</table>

7. Repeat as needed to create more security tags.

8. Click **Update**.

**Note:** You can also create new tags by navigating to **Security Operations > Security Tags > Tags**. The procedure is the same.
Related information

Security Case Management

Create security tag rules

Security tag rules provide filtering for security tag access.

Before you begin

Role required: admin

Procedure

2. Choose or create a security tag.
4. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the security tag rule.</td>
</tr>
<tr>
<td>Security Tag</td>
<td>The security tag to attach to the rule.</td>
</tr>
<tr>
<td>Active</td>
<td>Turn the security tag on or off.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of this rule.</td>
</tr>
</tbody>
</table>

5. Determine Record Filtering.

6. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use filter group</td>
<td>Associates filter group to the rule.</td>
</tr>
<tr>
<td>Table</td>
<td>The table to contain the rule.</td>
</tr>
<tr>
<td>Condition</td>
<td>Add one or more filter conditions.</td>
</tr>
</tbody>
</table>

7. Click Submit

Import security tag rules

You can import security tag rules from other tables in your deployment.

Before you begin

Role required: admin
Procedure

2. Choose or create a security tag.
3. Click the Import security tag rules related link.

4. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target table</td>
<td>Choose the table to use to import rules.</td>
</tr>
<tr>
<td>Target field</td>
<td>Choose the field to use to import rules.</td>
</tr>
<tr>
<td>Type of Match</td>
<td>Choose how to match the imported rules to Security Tags from:</td>
</tr>
<tr>
<td></td>
<td>Exact match (default)</td>
</tr>
<tr>
<td></td>
<td>Contains</td>
</tr>
<tr>
<td></td>
<td>Starts with</td>
</tr>
<tr>
<td></td>
<td>Ends with</td>
</tr>
<tr>
<td></td>
<td>Regular Expression</td>
</tr>
<tr>
<td>Import type</td>
<td>Choose:</td>
</tr>
<tr>
<td></td>
<td>From clipboard</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>Copy a list of delimited values into the text area. The values are parsed into security tags.</td>
</tr>
<tr>
<td></td>
<td><strong>From file upload</strong></td>
</tr>
<tr>
<td></td>
<td>Upload a file with delimited values. The values are parsed into security tags.</td>
</tr>
<tr>
<td></td>
<td>Add values for the security tag rules using new line, or pipe delimiters.</td>
</tr>
</tbody>
</table>

5. Click Submit

Security annotations

A security annotation is a note of explanation or comments added to a configuration item, observable, or use on a security incident.

Multiple security annotations are available for users and observables (requires the Threat Intelligence plugin). Reports on security annotations are also available.

Create security annotations for CIs

Annotations on CIs allow you to track activity across incidents. You can add annotations to a single or multiple CIs.

**Before you begin**

Role required: admin

**Procedure**

1. From a security incident or the Configuration Item table, open a CI.
2. Right click in the header and choose View > Security.
3. In the **Security Annotations** related list tab, click **New**.

4. Enter an annotation. Annotations can be in any text format.

5. Click **Submit**.

   ![Image of security annotations](image.png)

   **Note:** You can add the same annotation to multiple CIs by selecting CIs on the list, choose **Add security annotation**, enter an annotation in any text format, and click **Submit**.

### Create security annotations for observables

You can select a single or multiple observables and apply security annotations to them using the **Actions on selected rows** choice menu.

**Before you begin**

Requires the Threat Intelligence plugin and activation. The Threat Intelligence plugin is available as a separate subscription.

**Role required:** admin

**Procedure**

1. Navigate to **Threat Intelligence > Observables**
2. Select one or more observables in the list.
3. From the **Actions on selected rows** drop-down menu, choose **Add security annotation**.

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
4. Enter an annotation. Annotations can be in any text format.

5. Click Submit.

**Create security annotations for users**

You can select a single or multiple users and apply security annotations to them using the **Actions on selected rows** choice menu.

**Before you begin**

Requires the Threat Intelligence plugin and activation. The Threat Intelligence plugin is available as a separate subscription.

Role required: admin

**Procedure**

1. Navigate to **User Administration > Users**
2. Select one or more users in the list.
3. From the **Actions on selected rows** drop-down menu, choose **Add security annotation**.
4. Enter an annotation. Annotations can be in any text format.
5. Click **Submit**.

**View security annotations reports**

The Security Annotations report presents details stored in the Security Annotations [sn_sec_cmn_security_annotations] table. You can customize the columns in the report and group the data in any way that suits you.
Before you begin
Role required: admin

Procedure

1. Navigate to Reports > View/Run.
2. Search for Security Annotations under My reports or All.

Related information

Components installed with Security Support Common
Several types of components are installed with Security Support Common. They provide common functionality for use across the various security applications, such as Security Incident Response.

Search Security Operations
You can find information quickly in any Security Operations application using the search icon in the screen header. Zing is the text indexing and search engine that performs all text searches in your instance.

Before you begin
Role required: sn_si.read or higher

Procedure

1. Click the search icon (🔍) in the upper right-hand corner of the screen.
2. Type in the criteria you want to search by, and press Enter.
   If you have the Security Incident Response plugin activated, the search criteria you entered present any matching short description text, CIs, IP addresses, or URLs in your security incidents, Security Incident Response tasks, or security requests. If you have the Vulnerability Response or Threat
Intelligence plugins activated, the search results include vulnerabilities, vulnerable items, vulnerable entries, observables, IoCs, and attack mode/methods.

Related information
Introduction to searching
Zing text search

Security Operations Integration Reference

Developers and ServiceNow partners can use the information in this section to gain understanding of the under-the-hood functionality of third-party integrations, including development guidelines, integration capabilities, and workflows.

ServiceNow Security Operations integration development guidelines

The ServiceNow platform provides several mechanisms for developing integrations with external systems. The ServiceNow Security Operations product suite adds integration capabilities intended to streamline the process of integrating with security-focused external systems.

Most of the concepts in this guide assume some familiarity with standard ServiceNow functionality. To integrate with the Security Operations suite, at a minimum, knowledge of the following ServiceNow concepts is required:

- Script includes
- Inbound/outbound web services
- Data sources
- Import sets
- Transform maps

Technology Partner Program

Any requirements for application certification or guidelines given in the Technology Partner Program literature supersede any information in this guide. This guide is not a replacement for the Technology Partner Program literature and serves only as a supplement to existing documentation.

For more information, see Technology Partner Program training course blog post.
Types of ServiceNow integrations provided

The Security Operations applications (Security Incident Response, Threat Intelligence, and Vulnerability Response) can be seamlessly integrated with other ServiceNow applications to enhance their functionality.

The following integrations are provided in the Security Operations base system.

Security Incident Response – Event Management integration

The capabilities of the Event Management application have been expanded to support Security Incident Response. The Security Incident Response Event Management support plugin automatically parses the contents of events in Event Management to populate fields in security incidents.

Use case covered:

• Creation of security events in the Event Management system from Security Information and Event Management (SIEM) tools

Useful capabilities provided:

• Event management functionality – event correlation, event rules, and alert rules
• Automatic mapping of additional_information values to resulting security incident

Resources:

Security Incident event management support documentation
Event Management documentation

Security Incident Response - Import Set API integration

In addition to using Event Management to push security-related events, the Security Incident Response application provides an Import Set API that allows direct creation of security incidents. The REST endpoint for the Security Incident Import Set is http://localhost:8080/api/now/import/sn_si_incident_import.

This integration technique is useful when a) Event Management is not installed, or b) it is desired to simply create Security Incidents without going through the event > alert > Security Incident flow that is required when using Event Management.

Use case covered:

• Creation of security incidents directly from SIEM tools

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Useful capabilities provided:

- Automatic CI matching on Security Incident creation based on IP, NetBIOS, or fully qualified domain name

Resources:

Platform Import Set API documentation
Security Incident Web Service Import Set documentation

**Threat Intelligence - lookup source integration**

Lookup sources provide the ability to send data to external lookup sources to determine if that data is malicious. Generally, that data is an IP address, URL, file, or file hash.

Use case covered:

- Lookup an IP address, URL, file, or hash with an external lookup service

Useful capabilities provided:

- Consistent way to request lookups from catalog items and security incidents
- Rate limiting and throttling capabilities provided with little/no coding
- Automatic creation of Indicators of Compromise (IoC) observable entries for any issues found by lookup sources

**Threat Intelligence - threat source integration**

Threat Sources provide the ability to pull in data from external threat intelligence repositories. This data is then imported into the various Indicators of Compromise tables that exist within the system. TAXII collections and simple blocklists are supported natively. To add new TAXII collections (or profiles based on a discovery or collection management service), it is as simple as adding an entry. Similarly, adding a new simple, single column blocklist is a matter of entering a new record and providing the URL of the blocklist. For more complicated sets of data, a custom integration can be provided to make a call to a URL and parse the response.

Use case covered:

- Retrieve data from a threat intelligence source to load into IoC tables

Useful capabilities provided:
• Support for simple blocklists and TAXII collections with no coding
• Simple mechanism for executing REST messages for retrieving data
• Decoupled data retrieval/processing for integration component reusability
• Native support for processing passing data returned to data sources (and import sets/transform maps)
• Supports multiple data requests per integration (for paginated calls) with the ability to pass context to subsequent calls

Resources:
Define a threat source

**Vulnerability Response - scanner invocation integration**

Vulnerability Scanner Invocation is a lightweight integration entry point that supports invoking vulnerability scans from the instance. A third-party vulnerability scanner is called asynchronously to schedule a scan for configuration items or IP addresses.

Use case covered:

• Make request to third-party scanner to scan a CI (using host information derived from CI) or IP address/IP addresses

Useful capabilities provided:

• Simple framework for defining scanner implementations
• Consistent way to request scans from catalog items, security incidents, and vulnerable items
• Automatic updating of tasks with result of scan invocation

Resources:

**Vulnerability Response - data integration**

Vulnerability data integrations are intended to retrieve vulnerability data from third-party vulnerability systems. The expected outputs from these integrations are vulnerability entries and vulnerable items. This integration allows third-party vulnerability scanners to function independently, with the expectation that vulnerabilities can be worked and tracked within the instance.

Use cases covered:
• Retrieve vulnerability libraries
• Retrieve vulnerability/CI pairings
• Synchronize CIs with vulnerability management system

Useful capabilities provided:

• Decoupled data retrieval/processing for integration component reusability
• Native support for processing passing data returned to data sources (and import sets/transform maps)
• Supports multiple data requests per integration (for paginated calls) with the ability to pass context to subsequent calls

Resources:
Vulnerability data integration documentation

Security Operations Integration Configurations

Many of the integrations included in the base system require little or no setup, and operate in the same way. Certain integrations, such as the Qualys Cloud Platform, however, require separate steps for setting up the integration. Others support different sets of scan and lookup types and different rate limits.

This section describes the differences between the supported integrations and points you to more documentation, as needed.

• **Carbon Black integration**: allows you to investigate and respond to security incidents by using the Carbon Black APIs to query and interact with endpoints associated with security incidents.

• **Check Point Anti-bot - Email Parser integration**: uses an email parser that consumes email notifications from Check Point Anti-bot to create security incidents.

• **Elasticsearch Incident Enrichment integration**: searches your logs and adds relevant sighting information to your security incidents.

• **Have I been pwned? integration**: allows the list of breached accounts (email addresses and usernames) to be quickly searched via a RESTful service.

• **HPE Security ArcSight ESM - Email Parser integration**: uses an email parser that consumes email notifications from HPE ArcSight ESM to create security incidents.

• **HPE ArcSight Logger - Incident Enrichment integration**: searches your logs and adds relevant sighting information to your security incidents.
• **IBM QRadar - Incident Enrichment Integration**: searches your logs and adds relevant sighting information to your security incidents.

• **McAfee ESM - Email Parser integration**: uses an email parser that consumes email notifications from McAfee ESM to create security incidents.

• **McAfee ESM - Incident Enrichment Integration**: searches your logs and adds relevant sighting information to your security incidents.

• **OPSWAT Metadefender integration overview**: allows threat data, detected by the third-party Metadefender scanner, to be downloaded to the Threat Intelligence application for tracking, prioritization, and resolution.

• **Palo Alto Networks - AutoFocus integration**: Palo Alto Networks AutoFocus, a threat intelligence cloud service, allows you to search for session information related to security incident observables.

• **Palo Alto Networks - Firewall integration**: Palo Alto Networks Firewall allows you to set up and maintain firewalls for preventing known and unknown threats across the network, cloud, and endpoints.

• **Palo Alto Networks - WildFire integration**: Wildfire integration allows you to programmatically query analysis jobs on Wildfire and retrieve historical results through a simple XML API interface.

• **Understanding the Qualys Vulnerability Integration**: Qualys Cloud Platform is used in Vulnerability Response.

• **Recorded Future integration**: enriches security incidents with valuable threat data.

• **Splunk - Incident Enrichment integration**: searches your logs and adds relevant sighting information to your security incidents.

• **Tanium Endpoint Platform integration**: Security Operations Tanium integration uses a workflow and workflow activities to return running processes for affected CIs.

• **VirusTotal integration**: used in Threat Intelligence. To use this lookup source, you must activate the VirusTotal Integration plugin.

• **WhoisXML API integration setup**: provides consistent, well-structured data from a Whois lookup. Keeps accurate Whois data accessible 24/7.

---

**Activate and configure third-party integrations**

You can activate the plugins for third-party integrations and configure them for use from the same screen.

**Before you begin**

Role required: sn_sec_cmn.admin
Procedure

1. Navigate to **Security Operations > Integration Configuration**.
   The available security integrations appear as a series of cards, similar to the following group of cards. You can point to any card to get a description of the integration.

   ![Integration Cards](image)

   2. To install the plugin for a given integration, click **Install Plugin**.
      
      a. On the System Plugin form, review the plugin details and click the **Activate/Upgrade** related link.
      
      b. Click **Activate**.
      
      When the activation is complete, the Security Integration screen reopens and the button for the integration you activated is labeled **Configure**.

   3. Click **Configure**.
      
      **Note:** If you are configuring the Qualys Vulnerability Integration, see **Installation of Vulnerability Response and supported applications**.

   4. Enter the **API Key**.
   
   5. Click **Submit**.
Create an integration

You can create an integration and add the associated integration card to the Security Integrations screen. This procedure is intended for partners who create third-party integrations.

Before you begin
Role required: sn_sec_cmn.admin
Audience: Partners who create third-party integrations.

Procedure
1. In the navigation filter, type sn_sec_core_integration_item.list and press the Enter key.
2. Click New.
3. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the integration.</td>
</tr>
<tr>
<td>Plugin ID</td>
<td>The plugin that must be activated to use the integration.</td>
</tr>
<tr>
<td>Order</td>
<td>Indicates the order that this integration card appears.</td>
</tr>
<tr>
<td>Banner Text</td>
<td>Click the link, select an image or logo to appear in the integration card, and click OK.</td>
</tr>
<tr>
<td>Installed</td>
<td>Read-only field that indicates whether the plugin has already been installed.</td>
</tr>
<tr>
<td>Configurable</td>
<td>Indicates whether you can configure the integration.</td>
</tr>
<tr>
<td>Categories</td>
<td>Used for filtering the integration cards.</td>
</tr>
<tr>
<td>Short description</td>
<td>A description of the integration that appears in the tooltip hint for the card.</td>
</tr>
<tr>
<td>Description</td>
<td>A longer description of the integration.</td>
</tr>
</tbody>
</table>

4. Right-click the form header and select Save. The Integration and Configurations related list appears. You can use this related list to define configuration options for the integration. These options appear when you click the Configuration button on the associated integration card.
5. Click New.
6. Fill in the fields on the form, as appropriate.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>The name of the integration item.</td>
</tr>
<tr>
<td>Name</td>
<td>The plugin that must be activated to use the integration.</td>
</tr>
<tr>
<td>Integration</td>
<td>Displays the integration for which you are defining integration items</td>
</tr>
<tr>
<td>Order</td>
<td>Indicates the order in which this integration item appears.</td>
</tr>
<tr>
<td>Type</td>
<td>From the list, select the type of field:</td>
</tr>
<tr>
<td></td>
<td>• String</td>
</tr>
<tr>
<td></td>
<td>• Integer</td>
</tr>
<tr>
<td></td>
<td>• Decimal</td>
</tr>
<tr>
<td></td>
<td>• Date</td>
</tr>
<tr>
<td></td>
<td>• Boolean</td>
</tr>
<tr>
<td></td>
<td>• Password</td>
</tr>
<tr>
<td></td>
<td>• IPv4</td>
</tr>
<tr>
<td></td>
<td>• IPv6</td>
</tr>
<tr>
<td></td>
<td>• URL</td>
</tr>
<tr>
<td>Value</td>
<td>Enter the value associated with the Type selected. If a value that is invalid for the selected Type is entered, no records are retrieved when the integration is run. For example, if you select the URL type and enter a value of 12.32.23.10, no records are retrieved.</td>
</tr>
</tbody>
</table>

7. Click **Submit**.

**Tips for writing integrations**

Avoid some of the pitfalls you can encounter when writing your own integrations by following these guidelines.

**Use ServiceNow platform functionality whenever possible**

Mostly, the integration capabilities built into Security Operations applications (Security Incident Response, Threat Intelligence, and Vulnerability Response) are intended to enhance or streamline existing ServiceNow platform integration functionality. When writing integrations, always make sure to use platform
functionality when it exists. Here are some common ServiceNow functionalities that can be used rather than “rolling-your-own.”

- Outbound web services – for most interactions with third-party systems, communication are through web services. In those cases, utilize platform outbound web services (REST and SOAP are supported).
- A data sources/import sets/transform map – for processing data and inserting into ServiceNow tables, the preferred mechanism is to use data sources and associated components.

Use Security Operations integration frameworks whenever possible

Because Security Operations integration mechanisms have solved many common problems, it is not necessary to reimplement basic functionalities for every integration. For example, the vulnerability data and threat source frameworks support handling multiple pages and passing that data to data sources/transforms/import sets. Similarly, the scan or lookup source framework provides configurable rate limiting functionality. As a rule, when implementing a feature or set of features, check to see if the existing Security Operations integration framework covers your use case. If so, use that framework.

Extend the existing Security Operations integration frameworks as needed

Most of the tables and scripts used by Security Operations integration frameworks were intended to be extended to suit future needs. If a use case is encountered while you are writing an integration, extend an integration table or script to better suit that use case.

Provide feedback to ServiceNow for issues encountered during integration

As an integration is being developed or tested, be sure to provide feedback when issues are encountered. Even if a workaround is required, Customer Service and Support personnel can provide an improvement in future releases that could alleviate the issue for future integrations.

Test under reasonable load

A common issue with integrations is that they are not equipped to handle realistic loads. Because each integration is a scoped application, there are more limitations imposed by the platform to ensure system stability. These limitations may result in long running jobs or API calls being terminated. You can ensure that long running processes or processes that process lots of data are handled gracefully by reducing the time each call or process takes (usually by providing a means of paginating API requests or chunking large sets of data).
Integration troubleshooting

These troubleshooting suggestions can help you resolve common issues you can encounter when setting up or running integrations.

Replace an untrusted or expired third-party SSL certificate

When an SSL connection is required in an integration, there are circumstances when the certificate provided by the third-party vendor is either not yet trusted in ServiceNow or has expired. You can replace it or add a new certificate.

Before you begin
Role required: sn_ti.write

Procedure

1. Acquire the SSL certificate from the third-party vendor. For example, you can import an X.509 Certificate (PEM) from an SSL endpoint in the Firefox browser, as follows.
   a. Enter the endpoint URL into the browser address bar. For example: https://<3rdparty>/.
   b. Click the lock icon in the address line.
   c. Click More Information and click the Security tab.
   d. Click View Certificate and click the Detail tab.
   e. Click Export to save the PEM into your local file system.
   f. Open the saved file in any text editor tool and copy the content into the clipboard. It must begin with -----BEGIN CERTIFICATE----- and end with -----END CERTIFICATE-----.

2. Navigate to System Definition > Certificates.

3. Click New and create a new record for the integration.

4. In PEM Certificate, paste in the certificate you downloaded and copied into the clipboard earlier.

5. Click Save.
   The other fields in the record are generated automatically.

Integrations Capabilities framework 2.0

The new Integration Capabilities Framework 2.0 has been redesigned to enable implementation of integrations in a simple and consistent manner. This ensures a consistent experience for similar types of integrations (for example: observable
reputation lookup). The new framework has capabilities implemented using Flows.

Benefits from the enhanced framework implementation include:

• The capability flows that include only business level components without any implementation specific logic.

• The capability flows now accept a broad array of inputs and formats for maximum flexibility (For example, observable references, CI references, tasks, any table or sys_id combinations).

• Rate limiting or throttling on integration executions are now easy to configure (removing the need to do this using custom code or changes to implementation workflows).

• Enhanced auditing and execution tracking capabilities now enable better reporting and easier troubleshooting.

• Robust error handling functions are built into the capability flows to avoid duplicating implementation routines.

• Ability to configure conditional triggering of the capabilities or the integrations. This provides flexibility to automatically launch automations based on incident category.

• A default filter condition has been introduced on all capabilities to filter allow listed observables before inputs are provided to the integrations.

**Note:** This new capability framework does not upgrade the current capability framework. Both frameworks can work in parallel. For instructions on how to leverage the new capability framework, see Using the new Capability Framework with an installed integration and Using the new Capability Framework with a Flow.

**Supported integrations and components**

The Security Incident Response plugin includes all the capability flows listed in Integrations Capabilities framework 2.0 and standard high-level filters that you can enable or disable depending on your requirement.

**Note:** If you want to use the new Capability Integration Framework with the New York release, you must install the ServiceNow IntegrationHub Starter Pack Installer plugin. Contact Customer Support for assistance with the installation.

**Supported application versions**

Starting with Security Incident Response 10.0, the following integrations are supported:
<table>
<thead>
<tr>
<th>Application</th>
<th>Minimum version required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Operations Hybrid Analysis Integration</td>
<td>10.0.0</td>
</tr>
<tr>
<td>Security Operations PhishTank Integration</td>
<td>10.0.0</td>
</tr>
<tr>
<td>Security Operations ThreatCrowd Integration</td>
<td>10.0.0</td>
</tr>
<tr>
<td>Security Operations CrowdStrike Intelligence Integration</td>
<td>10.0.0</td>
</tr>
<tr>
<td>Security Operations 'Have I been pwned?' Integration</td>
<td>10.0.0</td>
</tr>
<tr>
<td>Security Operations Metadefender Integration</td>
<td>10.0.0</td>
</tr>
<tr>
<td>Security Operations Recorded Future Integration</td>
<td>10.0.0</td>
</tr>
<tr>
<td>Security Operations VirusTotal Integration</td>
<td>10.0.0</td>
</tr>
<tr>
<td>Security Operations Reverse Whols Integration</td>
<td>10.0.0</td>
</tr>
</tbody>
</table>

Starting with Security Incident Response 10.4, the following integrations are supported:

<table>
<thead>
<tr>
<th>Application</th>
<th>Minimum version required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Operations RiskIQ Integration</td>
<td>10.0.0</td>
</tr>
<tr>
<td>Security Operations Shodan Integration</td>
<td>10.0.0</td>
</tr>
<tr>
<td>Security Operations Whols Integration</td>
<td>10.0.0</td>
</tr>
<tr>
<td>Security Operations Carbon Black Integration</td>
<td>10.3.1</td>
</tr>
<tr>
<td>Security Operations Splunk Search Integration</td>
<td>10.3.0</td>
</tr>
<tr>
<td>Application</td>
<td>Minimum version required</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Security Operations ArcSight Logger Integration</td>
<td>10.3.0</td>
</tr>
<tr>
<td>Security Operations McAfee ESM Integration</td>
<td>10.3.0</td>
</tr>
<tr>
<td>Security Operations Elasticsearch Integration</td>
<td>10.3.0</td>
</tr>
<tr>
<td>Security Operations IBM QRadar Integration</td>
<td>10.3.1</td>
</tr>
<tr>
<td>Security Operations CrowdStrike Falcon Host</td>
<td>10.3.0</td>
</tr>
</tbody>
</table>

**Components included**

The new Capability Integration Framework includes the following components:

- **Capabilities**: All of the following capabilities that exist in the product today as workflows have been redesigned using Flows:
  - **Block Request**: Provides a way to block observables associated with a security incident on a firewall, web proxy, or some other control point. This capability is used during incident response investigations to contain an identified threat.
  - **Email Search and Delete**: Provides a way to search an email server during a security investigation and if necessary, delete emails from the server.
  - **Enrich Configuration Item**: Provides a general way to enrich configuration items with additional information from a variety of sources. This capability is used during incident response investigations to enrich data associated with a security incident.
  - **Enrich Observable**: Provides a general way to enrich observables with additional information from a variety of sources. This capability is used during incident response investigations to contain an identified threat.
  - **Event Ingestion**: Provides a general way to create a security incident by mapping events from an integration source to a security incident.
  - **Get Network Statistics**: Retrieves a list of active network connections from an endpoint or host. This capability is used for incident enrichment during investigations.
  - **Get Running Processes**: Retrieves a list of running processes from an endpoint or host. This capability is used for incident enrichment during investigations.
- **Isolate Host**: Provides a way to isolate an endpoint or a host associated with a security incident. Isolate host is executed against a configuration item (CI).

- **Publish to Watchlist**: Provides a way to add observables associated with a security incident to a watchlist that monitors for security events and generates alerts. This capability is used as part of incident response during investigations.

- **Sightings Search**: Searches various SIEMs or other log stores for instances of observables. This capability is used to determine the presence of malicious IoCs in your environment.

- **Threat Lookup**: Performs threat intelligence lookups to determine whether a certain observable is associated with a known security threat. This capability is used as part of incident response during investigations.

**New tables:**

- `sn_sec_cmn_capability`: Capability and flow that implements the capability.

- `sn_sec_cmn_capability_implementation`: The actual implementation flow that provides the services of the capability.

- `sn_sec_cmn_capability_execution`: The execution record for a capability at runtime.

- `sn_sec_cmn_capability_implementation_execution`: The execution record for a capability implementation at runtime.

- `sn_sec_cmn_filter_condition`: The filter conditions that can be applied at runtime to the capability or a capability implementation.

**Include script**: CapabilityProcessor: Handles all the processing code for the framework.

**Rate limit**: Capability Max Concurrent Req Per Period: Defines how many integrations can be executed in parallel.

**Scheduled job process capability implementation**: Runs every 15 seconds and can be disabled in the Security Administration Properties page (Security Incident > Administration > Properties).

- Enables or Disables the scheduled job, Process Capability Implementations: This job automatically schedules and manages capability implementation execution flows.

- Enables or Disables Automated Lookups or Enrichments: Setting that activates or deactivates the scheduled job that performs automated threat
lookup or enrichment of observables when observables are added to security incidents in the current capability framework.

- Enables or Disables the scheduled job, Lookup Security Incident Observables: This job automatically schedules a Threat Lookup or Enrich Observables job when observables are added to a security incident.

Configurations in the new Capability Framework
This section describes the configurations available in the new framework.

Procedure
1. Navigate to **Security Operations > Integrations > Capabilities**.

   - **Note:** Version 10.4: Starting with Security Incident Response 10.4, the menu name **Capabilities** has been changed to **Integration Capabilities** (Flows).

2. The capabilities available with the base system are displayed.

   - **Note:** These are the capabilities provided with the base system. You can use the capabilities, or you can customize them as required. The following steps describe how to configure a capability and the integrations implemented for the capability.

3. Click the link in the Name column to configure a capability. The Capability Implementations page is displayed.
4. The Name, Application, Description, and the Flow that the Capability implements is displayed. Select the **Active** check box to activate the capability.

- **Filter conditions at the capability level**: When an integration capability implements a flow, the filter conditions associated with the flow will be executed before the capability flow is launched. For example, the Threat Lookup capability includes the Filter Whitelisted Observables condition as shown above. Click on the Name link to edit the filter condition.

  **Note**: Select the **Add worknote to task** checkbox to add worknotes to include information on the filter conditions used.

You can either define filter conditions or a script, or a combination of both. In the above example, a script is used to define the filter conditions.
When the capability flow is executed, the script searches for whitelisted observables and removes them from the table.

ℹ️ Note: The filter conditions set here are applicable to all active integrations defined in the Capability Implementations tab.

- **Capability implementations**: Click the Capability Implementations tab. The implementations (integrations) that have been configured for the capability are displayed. The example below shows the integrations configured for the Threat Lookup capability:

![Capability Implementations Example]

5. Click the Name link to view the Capability Implementation. The Name, Application, Description, and the Flow that the capability implements is displayed. Click the Active checkbox to activate the capability.
You can specify the following details:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Select this check box to enable disable this integration. <strong>Note</strong>: If you configure this integration using the integration tile in the Security Operations &gt; Integrations &gt; Integrations Configurations page, this flag is automatically set to Active.</td>
</tr>
<tr>
<td>Order</td>
<td>Indicates the order in which the integrations are executed.</td>
</tr>
<tr>
<td>Capability</td>
<td>The capability implemented by this integration.</td>
</tr>
<tr>
<td>Flow</td>
<td>The subflow that implements the capability.</td>
</tr>
<tr>
<td>Configuration</td>
<td>The integration configuration for this capability. <strong>Note</strong>: This is initially set to the default configuration provided with the base system. When an integration is configuring using the integration tile in the Integration Configurations page, this value is automatically reset to the new configuration created.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Rate Limit</td>
<td>Indicates the number of integrations that can be executed at run-time (in parallel or per unit of time).</td>
</tr>
<tr>
<td>Batch Inputs Size</td>
<td>The batch input size for each execution. For example, for a Sighting Search integration you may want to group the observables into batches of 50 so that the queries generated do not become too large. 0 indicates that there is no limit.</td>
</tr>
<tr>
<td>Timeout Period</td>
<td>The maximum duration before the capability implementation flow is cancelled. 0 indicates that there is no timeout period.</td>
</tr>
<tr>
<td>Total Requests</td>
<td>The total number of implementation execution requests. This field in conjunction with the Total Reqs Period field, can be used to limit the number of requests to the service. For example, you can limit the number to 4 requests per minute.</td>
</tr>
<tr>
<td>Total Reqs Period</td>
<td>The total number of execution requests allowed per period.</td>
</tr>
<tr>
<td>Retry Limit</td>
<td>The number of retries allowed for a failed execution request. This limit will be applicable if the <strong>Retry</strong> flag is set in your integration to retry an execution request when a condition is met. For example, a retry request is made when you have exceeded your license limit for that service for a time period or the service is down.</td>
</tr>
<tr>
<td>Retry After</td>
<td>The period after which an attempt is made to retry a failed execution request.</td>
</tr>
<tr>
<td>Max Concurrent Reqs</td>
<td>The maximum number of concurrent implementation execution requests. 0 indicates no limit.</td>
</tr>
<tr>
<td>Sighting Search Configurations</td>
<td>The default sighting search queries that can be executed.</td>
</tr>
</tbody>
</table>

Click the Name link in the Filter Conditions section to configure the conditions defined for the implementation. Add or delete filter conditions, modify the script if required and update the record.
Using the new Capability Framework with an installed integration

This section describes how to use the new framework for an existing integration.

Use the steps below to enable an already installed and configured integration (see supported list of Integrations in Supported integrations and components) to use the new capability framework.

⚠️ Note: Integration Capability Framework 2.0 available with Security Incident Response 10.0.2 supports implementations for the Threat Lookup and Enrich Observable capabilities. Implementations for other capabilities will be made available in a future release.

Before you begin

- Role required: sn_si.admin
- Security Incident Response 10.0.2

2. Click on Threat Lookup capability.
3. Click the Capabilities Implementation tab.
4. View the Capability Implementation record for the integration of interest (example: Crowdstrike Falcon Intelligence). The **Active** column should have the value as **False**.

5. Click the **Name** link to view the implementation record.

6. Select the **Active** check box.

7. Ensure the implementation record is pointing to the right configuration record (the tile name for the integration in **Integration Configurations > Show Configurations (Yes)**).

---

© 2021 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
8. The implementation is enabled for use with the new framework.

⚠️ Note: All supported Integrations when installed with Security Incident Response 10.0.2 will automatically be enabled under the new Integration Capability framework.

Using the new Capability Framework with a Flow

Use the steps below to create a flow and call the subflow provided by the new capability framework.

Before you begin

- Role required: sn_si.admin, flow_designer, action_designer
- Install one of the supported integrations (see Supported integrations and components)

The steps below describe how to create a sample flow and call one of the subflows provided with the new capability framework.

Procedure

1. Navigate to Flow Designer > Designer.
2. Click New to create a new flow and provide the necessary information for the properties.
Note: Select **System User** in the Run As choice list as shown in the above image.

3. Select a Trigger condition for the flow (a common trigger is the creation of a security incident record for a certain incident category).

4. In step 1 of the flow, select an action to get inputs from the security incident (for example, observables). You can select an action from the actions provided with the base system with the Security Support Common Spoke.
5. In step 2, select a subflow (for example, Threat Lookup).

6. Configure the subflow you have selected as shown below:

7. Save and publish the flow.

Troubleshooting Integration Capability flows
The Capability Executions option provides detailed information on each capability that has been executed.

Note: Completed executions are archived after 30 days.

Navigate to Security Operations > Integrations > Capability Executions..
Click on the Capability Executions link to view additional details.

**Security Incident Record Worknotes**

When observables have been added to a security incident and the trigger condition for the flow is met, the Threat Lookup and Enrich Observable subflows are initiated and the following work notes are added to the security incident:

- Flow execution started: Security Operations Integration - Enrich Observable V1
- Flow execution completed: Security Operations Integration - Enrich Observable V1
- Flow execution started: Security Operations Integration – Threat Lookup V1
- Flow execution completed: Security Operations Integration – Threat Lookup V1

To view these worknotes, login as a user with the `sn_si.admin` or `sn_si.analyst`, and `flow_designer`, and `action_designer` roles.

Navigate to the security incident record page and click on these worknotes to view the flow execution details.
REST APIs for third-party integration with Security Operations

The Security Operations base system includes a series of scripted REST APIs that allow customers and partners to easily integrate with an existing Security Operations deployment. The APIs allow you to gather data from outside of your system (for example, a Python script is used to receive data from VirusTotal) and send it back to your instance.

Scripts written in almost any language (Python, for example) can be used with the APIs to perform customer-specific processes. The scripts must be written in a language able to make an outside-facing HTTP Post call. For example, if you have a Java application, you must use a library, such as the java.net.HttpURLConnection package, to construct an HTTP call and pass in a JSON string as Body for the message.

the API is solely used to add data that was gathered outside of our system, e.g. if you wrote VT python script and receive data from VT, you could send that data back to the SN instance

Authentication
All operations within the API definitions use platform authentication provided by the Scripted REST API operation feature. To access, navigate to System Web Services > Scripted Web Services > Scripted REST APIs and locate the SecOps Integration Capabilities API.
The user and the user’s domain are readily available within the context of the API. Records can be tied to a user, an audit path to be established, and domain separation accomplished. Also, since you are authenticated as a specific user, you can use GlideRecordSecure to prevent any unauthorized access to data.

**Authorization**

To protect the record creation process from users outside of the Security Operations application, you must have the `sn_sec_cmn.api_write` role. Only users with this role can access the APIs.

**Configuration request parameters**

The following request parameters are available.

<table>
<thead>
<tr>
<th>Name</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ignore_mandatory_fields</td>
<td>false</td>
<td>If set to true, the record persists even if mandatory fields are not filled in.</td>
</tr>
<tr>
<td>include_wrap</td>
<td>false</td>
<td>If set to true, the response includes the instance-provided standard wrapper for Scripted REST APIs.</td>
</tr>
<tr>
<td>Name</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>simple_response</td>
<td>false</td>
<td>If set to true, the response includes only whether the operation was successful.</td>
</tr>
</tbody>
</table>

**Error responses**
The following error responses may occur.

<table>
<thead>
<tr>
<th>Error message</th>
<th>When does it occur?</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insufficient access</td>
<td>User does not have the sn_sec_cmn.api_write role.</td>
<td>Add the role to the user.</td>
</tr>
<tr>
<td>Invalid post body</td>
<td>Request body is empty or an empty object.</td>
<td>Conform to the API definition.</td>
</tr>
<tr>
<td>No fields supplied</td>
<td>Data fields provided to persist are empty.</td>
<td>Conform to the API definition.</td>
</tr>
<tr>
<td>Mandatory fields missing: x,y,z</td>
<td>Mandatory fields are missing.</td>
<td>Conform to the table definition of the target table or set ignore_mandatory_fields to true.</td>
</tr>
<tr>
<td>Unable to persist record</td>
<td>Unable to persist parsed record.</td>
<td>GlideRecord insert() failed, further analysis is required.</td>
</tr>
<tr>
<td>Unknown error</td>
<td>Occurs if no known error path has been followed.</td>
<td>Further analysis is required.</td>
</tr>
</tbody>
</table>

**CI enrichment use case**
Using your third-party scripts, you can write to the Configuration Item Enrichment [sn_sec_cmn_ci_enrichment_result] table for CI enrichment. The enrichment records are based on existing capabilities that provide detailed information about a record from a third-party source.

Sample request and responses for the CI enrichment use case are shown here.
Example: Create-Request for CI enrichment

```json
{
    "ignore_mandatory_fields": true,
    "payload": {
        "configuration_item_id": "2df7c8437201000deeabf8bcbe5d56",
        "data": {
            "external_link": "http://www.servicenow.com",
            "vendor": "aafbf46ad72212007a6de294de6103a2",
            "data_type": null,
            "source": null,
            "name": null,
            "parent": null,
            "summary": "Found 1000 open vulnerabilities on the specified configuration item",
            "retrieval_date": "2017-09-05 08:56:28"
        }
    }
}
```

Example: Create-Response for CI enrichment

```json
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [{
            "sys_id": "2df7c8437201000deeabf8bcbe5d56",
            "results": [
                {
                    "sys_id": "4a8b92fb0b410300263a809b37673a33",
                    "reference_url": "http://10.0.214.15:8000/nav_to.do?uri=sn_sec_cmp_ci_enrichment_result.do?sys_id=4a8b92fb0b410300263a809b37673a33"
                }
            ],
            "domain": "global",
            "configuration_item_ids": ["2df7c8437201000deeabf8bcbe5d56"]
        }
    }
}
```

Observable enrichment use case

Using your third-party scripts, you can write to the Observable Enrichment Result [sn_ti_observable_enrichment_result] table for observable enrichment. The enrichment records are based on existing capabilities that provide detailed information about a record from a third-party source.
Sample request and responses for the observable enrichment use case are shown here.

**Example: Create-Request for observable enrichment**

```
"ignore_mandatory_fields": true,
"payload": {
  "observable_value": "http://www.google.com",
  "security_incident_ids": ["9424d4e10b11038263a089b37673a21"],
  "enrichment_mapping_id": "9fa7d4590b622200623a089b37673a1d",
  "data": {
    "vendor": "f15a46140b622200623a089b37673a7e",
    "summary": "Registrar:MarkMonitor, Inc., Registration Date:1997-09-15, Expiration Date:2020-09-14, Registrant country:UNITED STATES",
    "data_type": "json",
    "retrieval_date": "2017-08-30 10:35:02",
    "raw_data": "{"WhoisRecord":{"administrativeContact":{"city":\"Mountain View\",\"country\":\"UNITED STATES\",\"email\":\"dns-admin@google.com\",\"fax\":\"16506188571\",\"name\":\"DNS Admin\",\"organization\":\"Google Inc.\"}}}
  }
}
```

**Example: Create-Response for observable enrichment**

```
{
  "success": true,
  "status": "success",
  "payload": {
    "results": [
      {
        "sys_id": "43bd3f210b510380263a089b37673ac6",
        "reference_url": "http://10.0.65.185:8080/sn_tti_observable.do?sys_id=43bd3f210b510380263a089b37673ac6&sys_target=XML",
        "results": {
          "sys_id": "0bbd3f210b510380263a089b37673acc",
          "reference_url": "http://10.0.65.185:8080/sn_tti_observable_enrichment_result.do?sys_id=0bbd3f210b510380263a089b37673acc&sys_target=XML"
        }
      }
    ],
    "domain": "global",
    "observable_ids": {
      "43bd3f210b510380263a089b37673ac6"
    }
  }
}
```
Note: In addition to enriching existing records, you can also use Security Operations enrichment data mapping to add new records to tables by passing in an enrichment_mapping_id for an existing enrichment mapping and a corresponding raw_data string that can be parsed by the mapping process.

Threat lookup use case

Using your third-party scripts, you can write to the Threat Lookup Result [sn_ti_lookup_result] table for threat lookup results. The lookup records are based on existing capabilities that provide detailed information about a record from a third-party source.

Sample request and responses for the threat lookup use case are shown here.

Example: Create-Request for threat lookups

```json
{
  "simple_response": false,
  "include_wrapper": true,
  "ignore_mandatory_fields": false,
  "payload": [
    {
      "request_element_correlation_id": "1",
      "observable_value": "128.214.67.80",
      "date": [
        {
          "request_element_correlation_id": "2",
          "finding": "Malicious6",
          "source_engine": "VirusTotal API",
          "vendor": "aabf45ad72212007a9de294de6103a2",
          "data_type": null,
          "source": null,
          "name": null,
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/information/
        },
        {
          "finding": "Malicious8",
          "source_engine": "VirusTotal API",
          "source_engine_version": "v2",
          "first_found": "2000-09-05 15:56:28",
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/information/
        }
      ]
    }
  ]
}
```
Example: Create-Response for threat lookups

```json
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "a0bdaaf0b04a10300263a089b37673a93",
                "reference_url":
                    a0bdaaf0b0410300263a089b37673a93",
                "request_element_correlation_id": "1",
                "results": [
                    {
                        "sys_id": "24bdaaf0b0418300263a089b37673a95",
                        "reference_url":
                            "http://10.0.214.15:8080/nav_to.do?uri=sn_ti_observable.do?sys_id=24bdaaf0b0418300263a089b37673a95",
                        "request_element_correlation_id": "2",
                    },
                    {
                        "sys_id": "e8bdaaf0b0418030263a089b37673a96",
                        "reference_url":
                            "http://10.0.214.15:8080/nav_to.do?uri=sn_ti_observable.do?sys_id=e8bdaaf0b0418030263a089b37673a96"
                    }
                ],
                "domain": "global",
                "observable_ids": [
                    "a0bdaaf0b0410300263a089b37673a93"
                ]
            }
        ]
    }
}
```

Integration capabilities

The Integration Capabilities framework provides a consistent architecture to support interoperability with third-party integrations. This abstracted interface and data model insulates integrations from changes to the core application and ensures a consistent experience for similar types of integrations.

Each integration capability persists in the Integration Capability [sn_sec_cmn_integration_capability] table. Integration capability workflows cannot be executed alone, and require the launch of an implementation workflow. Any plugin that provides an implementation of the capability adds their implementation to the child table: Integration Capability Implementation [sn_sec_cmn_integration_capability_implementation].

The implementation specifies the workflow to be executed, the related integration (plugin id), and the capability it implements. These workflows can be executed in parallel using the parallel workflow launcher; however, sequential execution is the default in the base system. If needed, you can change the order of execution.
Note: If no implementations are available, capability actions are not displayed in product menus.

Security Operations Integration - Block Request capability

The Block Action capability blocks observables associated with a security incident on a firewall, web proxy, or other control point using implementation workflows. This capability is used during incident response investigations to contain an identified threat.

The Block Request capability has a workflow, Security Operations Integration - Block Request workflow, that executes the request to block. This workflow accepts a list of observables, finds any implementing capabilities, and executes the request based on the configured workflow.

The capability also uses other implementations:

- Security Operations Integration Palo Alto Networks Firewall Launcher workflow
- Security Operations Palo Alto Networks - Check and Block Value workflow

Note: If no implementations are available, capability actions are not displayed in product menus.

Run Block Request

Blocks communication with observables associated with a security incident.

Before you begin
Role required: sn_si.analyst

About this task

Note: If no implementations are available, capability actions are not displayed in product menus.

The Security Operations Integration - Block Request workflow can be triggered from an observable form, or from the Security Incident Observables related list on a security incident.

This example shows a Block Request from a security incident.

Procedure

1. Navigate to a security incident.
2. Select observables from the Related List tab.
3. Click Block Request in the Actions on selected rows... drop-down menu.
The dialog box appears.

4. Choose the implementation.

5. Click **Block**.

The workflow execution audit is displayed in the work notes section.
Security Operations Integration - Block Request workflow

The **Security Operations Integration - Block Request** workflow is a high-level workflow independent of integrations. It blocks observables associated with a security incident. Use it to fulfill an integration such as Palo Alto Networks - Firewall.

**Before you begin**
Role required: sn_si.analyst

**About this task**
The **Security Operations Integration - Block Request** workflow can be triggered on an observable form, or from the **Security Incident Observables** related list on a security incident. On a list, it is in the drop-down action menu. On a form, it is a related link. Blocking a request is available only when you have an implementation installed for the block request capability.

Activities specific to this workflow are described here. For more information on other activities, see Common integration workflow activities.

**Filter Allowlisted Observables activity**
The **Filtered Allowlisted Observables** workflow activity removes observables that can be ignored from the list of observables. This activity can accelerate the investigation and remediation process.

The **Filter Allowlisted Observables** activity can be used with any workflow to filter observables prior to taking any action.

**Results**
Possible results for this activity are:
Results

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Filter list created.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to filter the observables. More error</td>
</tr>
<tr>
<td></td>
<td>information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>observables</td>
<td>List of available observables.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filteredObservables</td>
<td>Filtered observables.</td>
</tr>
</tbody>
</table>

Security Operations Integration - Email Search and Delete capability

The Email Search and Delete capability returns the number of threat emails from an email server search and, optionally, returns details for each email found. After the email search is completed, you can delete the emails.

The Email Search and Delete capability has one workflow that executes the email search and delete processes.

Note: If no implementations are available, capability actions are not displayed in product menus. Additionally, if none of the Email Search and Delete capability implementations are active, the Email Search related link on a security incident is not displayed.

Security Operations Integration - Email Search and Delete workflow

The Security Operations Integration - Email Search and Delete workflow returns the number of threat emails from an email server search and, optionally, return details for each email found. After the email search is completed, you can delete the emails.
About this task
The search query can take some time to complete. After the count is received, approval is required to delete emails from an email server.

This workflow is triggered by the **Delete from Email Server(s)** and **Search on Email Server(s)** buttons on the **Email Search** form in a security incident. For more information, see [Search for and delete phishing emails](#).

Activities specific to this workflow are described here. For more information on other activities, see [Common integration workflow activities](#).

**Execution Tracking Begin (Mail Search) activity**

The **Execution Tracking - Begin (Mail Search)** capability execution activity creates an execution tracking record and marks the record state as Started. This activity is used by all capability and implementation workflows to keep track of their state.

**Results**

Possible results for this activity are:
Results

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Execution tracking record has been created.</td>
</tr>
<tr>
<td>Failure</td>
<td>Could not create execution tracking record.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityId</td>
<td>System identifier of the Integration Capability being executed.</td>
</tr>
<tr>
<td>implementationId</td>
<td>System identifier of the integration capability implementation being executed.</td>
</tr>
<tr>
<td>taskId</td>
<td>System identifier for any task associated with the workflow.</td>
</tr>
<tr>
<td>workflowContextId</td>
<td>System identifier of the associated workflow context record. Supplied by the system.</td>
</tr>
<tr>
<td>workflowName</td>
<td>Name of the workflow. Supplied by the system.</td>
</tr>
<tr>
<td>parentCapabilityExecutionId</td>
<td>System identifier of the audit record that launched the implementation workflow. Only required for Integration Capability implementation workflows, such as Splunk, Elasticsearch.</td>
</tr>
<tr>
<td>emailsearchId</td>
<td>The sysid of the email search record in the Email Search [sn_sec_cmn_email_search] table.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityExecutionId</td>
<td>System identifier of the execution tracking record.</td>
</tr>
</tbody>
</table>
Get Supported Security Capabilities activity

The Get Supported Capabilities workflow activity retrieves the name and number of integrations that are active and support the requested capability.

The Get Supported Capabilities activity can be used with any workflow to determine which capabilities are supported.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Integration that supports the capability found.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to find an active integration that supports the capability. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityName</td>
<td>Name of the capability.</td>
</tr>
<tr>
<td>taskId</td>
<td>System identifier for any task associated with the workflow.</td>
</tr>
<tr>
<td>domainId</td>
<td>System identifier for any domain associated with the workflow.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>supportedCapabilities</td>
<td>List of integrations that support the capability.</td>
</tr>
<tr>
<td>capabilityCount</td>
<td>Number of integrations that support the capability.</td>
</tr>
</tbody>
</table>
**Capability Execution Tracking - No Impls activity**

The **Capability Execution Tracking - No Impls** workflow activity creates an error record when no integration capability implementation is found.

The **Capability Execution Tracking - No Impls** activity can be used with any abstract integration capability workflow to handle the error condition when no configured capability implementation is available.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The execution tracking record state is set to <strong>Error</strong> and a message indicating the error is recorded.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityExecutionId</td>
<td>System identifier for the audit record. Output from the activity used to begin execution tracking.</td>
</tr>
<tr>
<td>workflowName</td>
<td>Name of the workflow. Supplied by the system.</td>
</tr>
</tbody>
</table>

**Output variables**

There are no output variables.

**Security Operations Integration - Enrich CI capability**

The **Enrich CI** capability allows you to enrich data for configuration items associated with a security incident.

The **Enrich CI** capability has a workflow, **Security Operations Integration - CI Enrichment workflow**. When the capability workflow runs, it executes additional workflows for the activated implementations. You can specify an implementation to use to perform enrichment on the selected CIs, or you can perform the enrichment using all implementations.
Note: This enriched data is not the type of data you would want to store in your CMDB as it is forensic data that is specific to a given investigation—for example, performing a memdump from a CI. Instead, the data is stored in the Configuration Item Enrichment [sn_sec_cmn_ci_enrichment_result] table.

Note: If no implementations are available, capability actions are not displayed in product menus.

Security Operations Integration - CI Enrichment workflow

The Security Operations Integration - CI Enrichment workflow allows you to enrich data in configuration items (CI) associated with a security incident.

About this task

This workflow is triggered from Security Incident Response in two ways.

• by selecting one or more CIs from the Configuration Items tab (under the Affected Items related link) and selecting Run CI enrichment from the Actions on selected rows choice list.

• by opening a CI record and clicking the Run CI enrichment related link.

Either method then allows you to specify which implementations to be used to enrich the selected CIs. The associated implementation workflows are executed to perform the enrichment.

Note: The base system does not include an implementation workflow for this capability. To enrich CIs, you must create your own implementation workflow.
Activities specific to this workflow are described here. For more information on other activities, see Common integration workflow activities.

**Execution Tracking - Begin activity**

The **Execution Tracking - Begin** workflow activity starts the auditing process for a Security Operations Integration workflow that operates on observables.

The **Execution Tracking - Begin** activity can be used with any workflow to begin recording the progress of the workflow in an audit.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>An audit record is created.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityId</td>
<td>System identifier of the Integration Capability being executed.</td>
</tr>
</tbody>
</table>
| isImpl                        | Flag that specifies whether auditing is done for an Integration Capability workflow or an Integration Capability implementation workflow. Possible values are:  
  • false - denotes auditing on an abstract Integration Capability workflow such as Sightings Search. (default.)  
  • true - denotes auditing on an Integration Capability implementation workflow. For example, Splunk or Elasticsearch. |
| taskId                       | System identifier for any task associated with the workflow.                |
| observableList               | One or more observable SyslDs to perform the desired action. Used as a workflow input. |
| workflowContextId            | System identifier of the associated workflow context record. Supplied by the system. |
| workflowName                 | Name of the workflow. Supplied by the system.                              |
| parentCapabilityExcutionId    | System identifier of the audit record that launched the implementation workflow. Only required for Integration Capability implementation workflows such as Splunk, Elasticsearch, and VirusTotal. |

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityExecutionId</td>
<td>System identifier of the audit record.</td>
</tr>
</tbody>
</table>
Get Supported Security Capabilities activity

The Get Supported Capabilities workflow activity retrieves the name and number of integrations that are active and support the requested capability.

The Get Supported Capabilities activity can be used with any workflow to determine which capabilities are supported.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Integration that supports the capability found.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to find an active integration that supports the capability. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityName</td>
<td>Name of the capability.</td>
</tr>
<tr>
<td>taskId</td>
<td>System identifier for any task associated with the workflow.</td>
</tr>
<tr>
<td>domainId</td>
<td>System identifier for any domain associated with the workflow.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>supportedCapabilities</td>
<td>List of integrations that support the capability.</td>
</tr>
<tr>
<td>capabilityCount</td>
<td>Number of integrations that support the capability.</td>
</tr>
</tbody>
</table>
Capability Execution Tracking - No Impls activity

The Capability Execution Tracking - No Impls workflow activity creates an error record when no integration capability implementation is found.

The Capability Execution Tracking - No Impls activity can be used with any abstract integration capability workflow to handle the error condition when no configured capability implementation is available.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The execution tracking record state is set to <strong>Error</strong> and a message indicating the error is recorded.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityExecutionId</td>
<td>System identifier for the audit record. Output from the activity used to begin execution tracking.</td>
</tr>
<tr>
<td>workflowName</td>
<td>Name of the workflow. Supplied by the system.</td>
</tr>
</tbody>
</table>

Output variables

There are no output variables.

Security Operations Integration - Enrich Observable capability

The Enrich Observable capability allows you to enrich observables with additional information from a variety of sources using implementation workflows. This capability is used during incident response investigations to contain an identified threat.

The Enrich Observable capability has a workflow, Security Operations Integration - Enrich Observable workflow. When the capability workflow runs, it executes additional workflows for the activated implementations. You can specify an implementation to use to perform enrichment on the selected observables, or you can perform the enrichment using all implementations that match the supported observable types.
Note: If no implementations are available, capability actions are not displayed in product menus.

Security Operations Integration - Enrich Observable workflow

The Security Operations Integration - Enrich Observable workflow allows you to enrich observables with additional information from a variety of sources using implementation workflows.

About this task

This workflow can be triggered from either Security Incident Response or Threat Intelligence in two ways.

- by selecting one or more observables from the Observables list and selecting Run observable enrichment from the Actions on selected rows choice list.
- by opening an observable record and clicking the Run observable enrichment related link.

Either method then allows you to specify which implementations to be used to enrich the selected observables. The associated implementation workflows are executed to perform the enrichment.

Activities specific to this workflow are described here. For more information on other activities, see Common integration workflow activities.

Get Supported Security Capabilities activity

The Get Supported Capabilities workflow activity retrieves the name and number of integrations that are active and support the requested capability.
The **Get Supported Capabilities** activity can be used with any workflow to determine which capabilities are supported.

### Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Integration that supports the capability found.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to find an active integration that supports the capability. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

### Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityName</td>
<td>Name of the capability.</td>
</tr>
<tr>
<td>taskId</td>
<td>System identifier for any task associated with the workflow.</td>
</tr>
<tr>
<td>domainId</td>
<td>System identifier for any domain associated with the workflow.</td>
</tr>
</tbody>
</table>

### Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>supportedCapabilities</td>
<td>List of integrations that support the capability.</td>
</tr>
<tr>
<td>capabilityCount</td>
<td>Number of integrations that support the capability.</td>
</tr>
</tbody>
</table>

### Capability Execution Tracking - No Impls activity

The **Capability Execution Tracking - No Impls** workflow activity creates an error record when no integration capability implementation is found.
The **Capability Execution Tracking - No Impls** activity can be used with any abstract integration capability workflow to handle the error condition when no configured capability implementation is available.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The execution tracking record state is set to <strong>Error</strong> and a message indicating the error is recorded.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityExecutionId</td>
<td>System identifier for the audit record. Output from the activity used to begin execution tracking.</td>
</tr>
<tr>
<td>workflowName</td>
<td>Name of the workflow. Supplied by the system.</td>
</tr>
</tbody>
</table>

**Output variables**

There are no output variables.

**Security Operations Integration - Get Network Statistics capability**

The **Get Network Statistics** capability retrieves a list of active network connections from a host or endpoint. It can be used for incident enrichment during investigations. This capability is triggered automatically when a configuration item is added to a security incident.

The **Get Network Statistics** capability has a workflow, **Security Operations Integrations - Get Network Statistics workflow** that accepts one or more CIs and tasks. The workflow iterates over each implementation and each CI and re-invokes the implementation workflow.

**Note:** If no implementations are available, capability actions are not displayed in product menus.
Security Operations Integrations - Get Network Statistics workflow

The **Security Operations Integrations - Get Network Statistics** workflow retrieves a list of active network connections from a host or endpoint.

**Before you begin**
Role required: sn_si.analyst

**About this task**
This workflow runs automatically when a configuration item is added to a security incident.

Activities specific to this workflow are described here. For more information on other activities, see [Common integration workflow activities](#).

**Capability - Determine CIs activity**

The **Capability - Determine CIs** workflow activity determines which configuration items (CIs) to include in the workflow.

The **Capability - Determine CIs** activity can be used with any workflow to determine which CIs to include in the workflow.

**Results**
Possible results for this activity are:
### Results

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Found configuration items.</td>
</tr>
<tr>
<td>Failure</td>
<td>No CIs found. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

### Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>task_sys_id</td>
<td>Task identifier (maps security incident to CIs).</td>
</tr>
<tr>
<td>cis_affected</td>
<td>Configuration items.</td>
</tr>
</tbody>
</table>

### Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Output variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variable</td>
</tr>
<tr>
<td>cis_affected</td>
</tr>
<tr>
<td>task_sys_id</td>
</tr>
</tbody>
</table>

### Execution Tracking - Begin (CIs) activity

The **Execution Tracking - Begin (CIs)** workflow activity starts the auditing process for a Security Operations Integration workflow that operates on configuration items (CIs).

The **Execution Tracking - Begin (CIs)** activity can be used with any CI workflow to begin recording the progress of the workflow in an audit.

### Results

Possible results for this activity are:
### Results

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>An audit record is created.</td>
</tr>
</tbody>
</table>

### Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityId</td>
<td>System identifier of the Integration Capability being executed.</td>
</tr>
</tbody>
</table>
| isImpl               | Flag that specifies whether auditing is done for an Integration Capability workflow or an Integration Capability implementation workflow. Possible values are:  
  • false - denotes auditing on an abstract Integration Capability workflow such as Sightings Search. (default.)  
  • true - denotes auditing on an Integration Capability implementation workflow. For example, Splunk or Elasticsearch. |
| taskId               | System identifier for any task associated with the workflow.                |
| ciList               | One or more Configuration Items (CI)s to perform the desired action against in the following format:  
  
```plaintext  
["sysId", "sysId"]  
```

  or

```plaintext  
"sysId"  
```

Used as a workflow input. |
| workflowContextId    | System identifier of the associated workflow context record. Supplied by the system. |
| workflowName         | Name of the workflow. Supplied by the system.                                 |
| parentCapabilityExcutionId | System identifier of the audit record that launched the implementation workflow. Only required for Integration Capability |
### Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityExecutionId</td>
<td>System identifier of the audit record.</td>
</tr>
</tbody>
</table>

### Get Supported Security Capabilities activity

The **Get Supported Capabilities** workflow activity retrieves the name and number of integrations that are active and support the requested capability.

The **Get Supported Capabilities** activity can be used with any workflow to determine which capabilities are supported.

### Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Integration that supports the capability found.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to find an active integration that supports the capability. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

### Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityName</td>
<td>Name of the capability.</td>
</tr>
<tr>
<td>taskId</td>
<td>System identifier for any task associated with the workflow.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>domainId</td>
<td>System identifier for any domain associated with the workflow.</td>
</tr>
</tbody>
</table>

**Output variables**
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>supportedCapabilities</td>
<td>List of integrations that support the capability.</td>
</tr>
<tr>
<td>capabilityCount</td>
<td>Number of integrations that support the capability.</td>
</tr>
</tbody>
</table>

**Capability Execution Tracking - No Impls activity**
The **Capability Execution Tracking - No Impls** workflow activity creates an error record when no integration capability implementation is found.

The **Capability Execution Tracking - No Impls** activity can be used with any abstract integration capability workflow to handle the error condition when no configured capability implementation is available.

**Results**
Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The execution tracking record state is set to <strong>Error</strong> and a message indicating the error is recorded.</td>
</tr>
</tbody>
</table>

**Input variables**
Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityExecutionId</td>
<td>System identifier for the audit record. Output from the activity used to begin execution tracking.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>workflowName</td>
<td>Name of the workflow. Supplied by the system.</td>
</tr>
</tbody>
</table>

**Output variables**

There are no output variables.

**Security Incident Response - Get Network Statistics workflow**

The **Security Incident Response > Get Network Statistics** workflow retrieves the network statistics for an affected Windows-based resource when added to a security incident in the **Analysis** state.

**Before you begin**

Role required: sn_si.analyst

**About this task**

For new security incidents that contain configuration items, the workflow runs automatically when the state changes to Analysis.

Existing security incidents are automatically updated when you are in the Analysis state and you add a new configuration item.

Workflow process activities include:

- Get Configuration Item FQDN activity
- Determine Shell Script by OS
- If statement is executed by Powershell
- Execution Tracking - Begin activity
- Get Network Statistics via netstat activity
- Capability Execution Tracking - Failure activity
Create Enrichment Data records activity
Capability Execution Tracking - Failure activity - Returns enrichmentID.
Capability Execution Tracking - Complete activity

Procedure
1. Open a security incident.
2. Update the State to Analysis, if necessary.
3. Add a configuration item (computer, server, or similar).
4. Click Update.
   Security Incident Response Orchestration provides network statistics information in the Related Links > Security Incident Enrichments tab. For more information see, Security Operations enrichment data mapping.

Activities specific to this workflow are described here. For more information on other activities, see Common integration workflow activities.

Get Configuration Item FQDN activity

The Security Common Orchestration > Get Configuration Item FQDN workflow activity retrieves the fully qualified domain name (FQDN) of a configuration item. This activity can accelerate the investigation and remediation process.

The Get Configuration Item FQDN activity can be used with any workflow to retrieve the fully qualified domain name (FQDN) of a configuration item.

Input variables
Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cmdb_ci.id</td>
<td>The system identifier (sys_id) of a configuration item record.</td>
</tr>
</tbody>
</table>

Output variables
The output variables contain data that can be used in subsequent activities.
Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fqdn</td>
<td>The fully qualified domain name (FQDN) of the configuration item.</td>
</tr>
</tbody>
</table>

Additional Notes

The fqdn field on the configuration item must be populated.

Get Network Statistics via netstat activity

The Security Common Orchestration - Get Network Statistics via netstat workflow activity retrieves the network statistics for an affected resource on a Windows-based system. This activity can accelerate the investigation and remediation process.

The Get Network Statistics via netstat activity can be used with any workflow to retrieve network statistics from a Windows-based system. The machine is queried with the `netstat` command including the `-a` and `-o` parameters. To enhance the output data, `get-process` command is also invoked.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Network statistics were retrieved in JSON format.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to retrieve network statistics. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>The fully qualified domain name (FQDN) or IP address of the target system.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.
### Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
</table>
| response [string] | A JSON string representing the current running processes on the target machine. JSON data includes:
  - **pid**
    - Process identifier
  - **local_port**
    - Local port for the network transaction
  - **state**
    - Status of the TCP connection.
    - **Note:** This field is null for UDP connections.
  - **local_address**
    - Local fully qualified domain name (FQDN) or IP address
  - **remote_address**
    - Remote fully qualified domain name (FQDN) or IP address
  - **protocol**
    - TCP or UDP
  - **remote_port**
    - Remote port of the network transaction
  - **path**
    - The file path of the process executable
  - **hash**
    - The hash value of the process executable. The hash is in SHA-256 for PowerShell V4 or higher. Otherwise, the hash is in MD5. |

### Restrictions

The MID Server must support **PowerShell**.

SHA-256 hash requires PowerShell V4.
**Capability Execution Tracking - Failure activity**

The **Capability Execution Tracking - Failure** workflow activity records a failure to the audit record.

The **Capability Execution Tracking - Failure** activity can be used with any workflow to record a failure condition.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The audit record state is set to <strong>Error</strong> and a message indicating the error is recorded.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityExecutionId</td>
<td>System identifier for the audit record. This is the output from any of the Begin auditing activities.</td>
</tr>
<tr>
<td>errorMessage</td>
<td>Message indicating the reason for the failure.</td>
</tr>
<tr>
<td>workflowName</td>
<td>Name of the workflow. Supplied by the system.</td>
</tr>
</tbody>
</table>

**Output variables**

There are no output variables.

**Security Operations Integration - Get Running Processes capability**

The **Get Running Processes** capability retrieves a list of running processes on a configuration item (CI) from a host or endpoint. This capability is used for incident enrichment during investigations.

The **Get Running Processes** capability has three implementation workflows:
• Security Operations Carbon Black Integration - Get Running Processes workflow
• Security Operations System Command Integration - Get Running Processes workflow
• Security Operations Tanium Integration - Get Running Processes workflow

Note: If no implementations are available, capability actions are not displayed in product menus.

Activities specific to this workflow are described here. For more information on other activities, see Common integration workflow activities.

Security Operations - Get Running Processes workflow

The Security Operations - Get Running Processes workflow is a high-level workflow independent of integrations. It retrieves a list of running processes on a configuration item (CI) from a host. Use it to fulfill an integration, such as Carbon Black, or for a Windows-based security incident.

Before you begin
Role required: sn_si.analyst

About this task

Workflow process activities include:
• Capability - Determine CIs activity
• Execution Tracking - Begin (CIs) activity
• Get Supported Security Capabilities activity
• Capability Execution Tracking - No Impls activity
• Parallel Flow Launcher - returns search results in an array.
• Capability Execution Tracking - Complete activity
Activities specific to this workflow are described here. For more information on other activities, see Common integration workflow activities.

**Capability - Determine CIs activity**

The **Capability - Determine CIs** workflow activity determines which configuration items (CIs) to include in the workflow.

The **Capability - Determine CIs** activity can be used with any workflow to determine which CIs to include in the workflow.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Found configuration items.</td>
</tr>
<tr>
<td>Failure</td>
<td>No CIs found. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.
### Variable Description

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>task_sys_id</td>
<td>Task identifier (maps security incident to CIs).</td>
</tr>
<tr>
<td>cis_affected</td>
<td>Configuration items.</td>
</tr>
</tbody>
</table>

### Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cis_affected</td>
<td>Filtered CIs</td>
</tr>
<tr>
<td>task_sys_id</td>
<td>Task identifier (maps security incident to CIs).</td>
</tr>
</tbody>
</table>

### Get Supported Security Capabilities activity

The Get Supported Capabilities workflow activity retrieves the name and number of integrations that are active and support the requested capability.

The Get Supported Capabilities activity can be used with any workflow to determine which capabilities are supported.

### Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Integration that supports the capability found.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to find an active integration that supports the capability. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

### Input variables

Input variables determine the initial behavior of the activity.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityName</td>
<td>Name of the capability.</td>
</tr>
<tr>
<td>taskId</td>
<td>System identifier for any task associated with the workflow.</td>
</tr>
<tr>
<td>domainId</td>
<td>System identifier for any domain associated with the workflow.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>supportedCapabilities</td>
<td>List of integrations that support the capability.</td>
</tr>
<tr>
<td>capabilityCount</td>
<td>Number of integrations that support the capability.</td>
</tr>
</tbody>
</table>

**Capability Execution Tracking - No Impls activity**

The Capability Execution Tracking - No Impls workflow activity creates an error record when no integration capability implementation is found.

The Capability Execution Tracking- No Impls activity can be used with any abstract integration capability workflow to handle the error condition when no configured capability implementation is available.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The execution tracking record state is set to Error and a message indicating the error is recorded.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.
### Variable Description

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityExecutionId</td>
<td>System identifier for the audit record. Output from the activity used to begin execution tracking.</td>
</tr>
<tr>
<td>workflowName</td>
<td>Name of the workflow. Supplied by the system.</td>
</tr>
</tbody>
</table>

### Output variables

There are no output variables.

### Security Operations Carbon Black Integration - Get Running Processes workflow

The **Security Operations Carbon Black Integration - Get Running Processes** is the implementation for the Carbon Black integration launched by the **Security Operations Integration - Get Running Process** workflow.

### Before you begin

Role required: sn_si.analyst

### About this task

Workflow process activities include:

- Get IP from CI activity
- Collect Carbon Black Configurations activity
- Get Sensor ID activity
- Execution Tracking - Begin (CIs) activity
- Create Session
- Capability Execution Tracking - Failure activity
- Check Session Status activity
- Timer workflow activity - Waits for 1 second
- Turnstile workflow activity - Check Session ready 30 times
- Create Command Process activity
- Check Command Status and Get Process activity
- Map Processes Data activity and return process list
- Create Enrichment Data records activity
- Capability Execution Tracking - Complete activity
- Close Session activity
Activities specific to this workflow are described here. For more information on other activities, see Common integration workflow activities.

Get IP from CI activity

The **Get IP from CI** workflow activity gathers the IP address from configuration items (CIs) to use in the workflow.

The **Get IP from CI** activity can be used with any workflow to gather configuration item (CI) IP addresses to use in the workflow.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Found IP addresses.</td>
</tr>
<tr>
<td>Failure</td>
<td>No IP addresses found. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.
### Output variables
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ci_sys_id</td>
<td>Configuration item identifier.</td>
</tr>
</tbody>
</table>

### Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_addr</td>
<td>IP addresses.</td>
</tr>
</tbody>
</table>

### Collect Carbon Black Configurations activity

The **Collect Carbon Black Configurations** workflow activity gathers configuration information to use in the workflow.

The **Collect Carbon Black Configurations** activity gathers Carbon Black configuration information to use in the workflow.

### Results
Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Configuration succeeded.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to verify the configuration. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

### Input variables
There are no input variables for this activity.

### Output variables
The output variables contain data that can be used in subsequent activities.
Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpoint_base</td>
<td>Base URL of the third-party integration API.</td>
</tr>
<tr>
<td>use_mid_server</td>
<td>Determines whether the REST activity uses the MID server to interact with Carbon Black or not.</td>
</tr>
<tr>
<td>api_token</td>
<td>Third-party integration API key.</td>
</tr>
</tbody>
</table>

Check MID Server Status

Determines whether the MID Server identified in the **MID Server Host** field of the integration's configuration is up and running. If the field is set to **Any**, the activity verifies that any MID Server is up and running.

The **Check MID Server Status** activity can be used with any workflow to check for the presence of a running MID Server within the workflow.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Session status returned.</td>
</tr>
<tr>
<td>Failure</td>
<td>Session status error. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityExecutionId</td>
<td>The ID of the capability being executed.</td>
</tr>
<tr>
<td>workflowName</td>
<td>The name of the workflow being executed.</td>
</tr>
<tr>
<td>mid_server_host</td>
<td>The MID Server identified in the integration's configuration i</td>
</tr>
</tbody>
</table>
Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mid_server_live</td>
<td>Identifies whether the MID Server identified in the MID Server Host field of the integration's configuration is up and running. If the field is set to Any, the activity verifies that any MID Server is up and running.</td>
</tr>
</tbody>
</table>

Get Sensor ID activity

The Get Sensor ID workflow activity gathers sensor identifiers to use in the workflow.

The Get Sensor ID activity can be used with any workflow to gather sensor information to use in the workflow.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Found sensor identifiers.</td>
</tr>
<tr>
<td>Failure</td>
<td>No sensors found. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>api_token</td>
<td>Carbon Black API key.</td>
</tr>
<tr>
<td>use_mid_server</td>
<td>Determines whether the REST activity uses the MID server to interact with Carbon Black or not.</td>
</tr>
<tr>
<td>endpoint_base</td>
<td>Base URL of the Carbon Black API.</td>
</tr>
</tbody>
</table>
### Variable Description

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ci_ip_address</td>
<td>Configuration item IP address.</td>
</tr>
</tbody>
</table>

### Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_code</td>
<td>Determines if the request was successful. If not, displays an HTTP error code and message.</td>
</tr>
<tr>
<td>Array</td>
<td>Element type: API variables.</td>
</tr>
<tr>
<td>sensor_detail</td>
<td>Description of the Carbon Black sensor in JSON format.</td>
</tr>
</tbody>
</table>

### Execution Tracking - Begin activity

The **Execution Tracking - Begin** workflow activity starts the auditing process for a Security Operations Integration workflow that operates on observables.

The **Execution Tracking - Begin** activity can be used with any workflow to begin recording the progress of the workflow in an audit.

### Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>An audit record is created.</td>
</tr>
</tbody>
</table>

### Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityId</td>
<td>System identifier of the Integration Capability being executed.</td>
</tr>
</tbody>
</table>
### Variable Description

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>isImpl</td>
<td>Flag that specifies whether auditing is done for an Integration Capability workflow or an Integration Capability implementation workflow. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• false - denotes auditing on an abstract Integration Capability workflow such as Sightings Search. (default.)</td>
</tr>
<tr>
<td></td>
<td>• true - denotes auditing on an Integration Capability implementation workflow. For example, Splunk or Elasticsearch.</td>
</tr>
<tr>
<td>taskId</td>
<td>System identifier for any task associated with the workflow.</td>
</tr>
<tr>
<td>observableList</td>
<td>One or more observable SysIDs to perform the desired action. Used as a workflow input.</td>
</tr>
<tr>
<td>workflowContextId</td>
<td>System identifier of the associated workflow context record. Supplied by the system.</td>
</tr>
<tr>
<td>workflowName</td>
<td>Name of the workflow. Supplied by the system.</td>
</tr>
<tr>
<td>parentCapabilityExecutionId</td>
<td>System identifier of the audit record that launched the implementation workflow. Only required for Integration Capability implementation workflows such as Splunk, Elasticsearch, and VirusTotal.</td>
</tr>
</tbody>
</table>

### Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityExecutionId</td>
<td>System identifier of the audit record.</td>
</tr>
</tbody>
</table>

### Create Session activity

The **Create Session** workflow activity establishes a Carbon Black session to use in the workflow.
The **Create Session** activity can be used with any workflow to create a Carbon Black session within the workflow.

### Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Session created.</td>
</tr>
<tr>
<td>Failure</td>
<td>Session not created. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

### Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>api_token</td>
<td>Carbon Black API key.</td>
</tr>
<tr>
<td>endpoint_base</td>
<td>Base URL of the Carbon Black API.</td>
</tr>
<tr>
<td>sensor_id</td>
<td>Sensor identifier.</td>
</tr>
<tr>
<td>use_mid_server</td>
<td>Determines whether the REST activity uses the MID server to interact with Carbon Black or not.</td>
</tr>
</tbody>
</table>

### Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_code</td>
<td>Determines if the request was successful. If not, displays an HTTP error code and message.</td>
</tr>
<tr>
<td>output</td>
<td>API variables</td>
</tr>
</tbody>
</table>

### Check Session Status activity

Determines the status of a Carbon Black session within the workflow.
The **Check Session Status** activity can be used with any workflow to check Carbon Black session status within the workflow.

### Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Session status returned.</td>
</tr>
<tr>
<td>Failure</td>
<td>Session status error. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

### Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>api_token</td>
<td>Carbon Black API key.</td>
</tr>
<tr>
<td>endpoint_base</td>
<td>Base URL of the Carbon Black API.</td>
</tr>
<tr>
<td>session_id</td>
<td>Session identifier.</td>
</tr>
<tr>
<td>use_mid_server</td>
<td>Determines whether the REST activity uses the MID server to interact with Carbon Black or not.</td>
</tr>
</tbody>
</table>

### Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_code</td>
<td>Determines if the request was successful. If not, displays an HTTP error code and message.</td>
</tr>
<tr>
<td>output</td>
<td>Information on Carbon Black running processes.</td>
</tr>
</tbody>
</table>

### Create Command Process activity

The **Create Command Process** workflow activity create a Carbon Black command process to use in the workflow.
The **Create Command Process** activity can be used with any workflow to create a Carbon Black command process within the workflow.

### Results
Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Command process created.</td>
</tr>
<tr>
<td>Failure</td>
<td>Command process not created. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

### Input variables
Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>api_token</td>
<td>Carbon Black API key.</td>
</tr>
<tr>
<td>endpoint_base</td>
<td>Base URL of the Carbon Black API.</td>
</tr>
<tr>
<td>session_id</td>
<td>Session identifier.</td>
</tr>
<tr>
<td>command_id</td>
<td>Command identifier.</td>
</tr>
<tr>
<td>use_mid_server</td>
<td>Determines whether the REST activity uses the MID server to interact with Carbon Black or not.</td>
</tr>
</tbody>
</table>

### Output variables
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_code</td>
<td>Determines if the request was successful. If not, displays an HTTP error code and message.</td>
</tr>
<tr>
<td>output</td>
<td>API variables</td>
</tr>
</tbody>
</table>
Check Command Status and Get Process activity

Checks the Carbon Black command status and retrieves processes to use in the workflow.

The Check Command Status and Get Process activity can be used with any workflow to check a Carbon Black command status and get processes within the workflow.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Command status returned and processes created.</td>
</tr>
<tr>
<td>Failure</td>
<td>Command status or process error. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>api_token</td>
<td>Carbon Black API key.</td>
</tr>
<tr>
<td>endpoint_base</td>
<td>Base URL of the Carbon Black API.</td>
</tr>
<tr>
<td>session_id</td>
<td>Session identifier.</td>
</tr>
<tr>
<td>command_id</td>
<td>Command identifier.</td>
</tr>
<tr>
<td>use_mid_server</td>
<td>Determines whether the REST activity uses the MID server to interact with Carbon Black or not.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.
**Output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_code</td>
<td>Determines if the request was successful. If not, displays an HTTP error code and message.</td>
</tr>
<tr>
<td>output</td>
<td>API variables</td>
</tr>
</tbody>
</table>

**Map Processes Data activity**

The **Map Processes Data** workflow activity maps Carbon Black process data within the workflow.

The **Map Processes Data** activity can be used with any workflow to map Carbon Black processes.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Processes mapped</td>
</tr>
<tr>
<td>Failure</td>
<td>Processes not mapped. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>affected_ci</td>
<td>Configuration item affected.</td>
</tr>
<tr>
<td>implementation_id</td>
<td>Implementation identifier.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.
Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>output</td>
<td>Formatted return data on running processes used by the abstract workflow.</td>
</tr>
<tr>
<td>processes</td>
<td>List of processes in an array.</td>
</tr>
</tbody>
</table>

**Capability Execution Tracking - Complete activity**

The Capability Execution Tracking - Complete workflow activity updates the audit record when the workflow is complete.

The Capability Execution Tracking - Complete activity can be used with any workflow to record the completion of the workflow.

ℹ️ **Note:** The Return Value array from the Parallel Launcher core activity contains an array of results from all integration workflows run and prompts the successful completion of execution tracking.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The audit record state is updated to Complete.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityExecutionId</td>
<td>System identifier for the audit record. This field was the output from any of the Begin auditing activities.</td>
</tr>
<tr>
<td>workflowName</td>
<td>Name of the workflow. Supplied by the system.</td>
</tr>
<tr>
<td>message</td>
<td>Completion message.</td>
</tr>
</tbody>
</table>

**Output variables**

There are no output variables.
Close Session activity
Closes a Carbon Black session within the workflow.

The **Close Session** activity can be used with any workflow to close a Carbon Black session.

**Results**
Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Session closed.</td>
</tr>
<tr>
<td>Failure</td>
<td>Session not closed. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

**Input variables**
Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>api_token</td>
<td>Carbon Black API key.</td>
</tr>
<tr>
<td>endpoint_base</td>
<td>Base URL of the Carbon Black API.</td>
</tr>
<tr>
<td>session_id</td>
<td>Session identifier.</td>
</tr>
<tr>
<td>use_mid_server</td>
<td>Determines whether the REST activity uses the MID server to interact with Carbon Black or not.</td>
</tr>
</tbody>
</table>

**Output variables**
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_code</td>
<td>Determines if the request was successful. If not, displays an HTTP error code and message.</td>
</tr>
<tr>
<td>output</td>
<td>API variables</td>
</tr>
</tbody>
</table>
Security Operations Tanium Integration - Get Running Processes workflow


Before you begin
Role required: sn_si.analyst

About this task
Workflow process activities include:

• Get IP from CI activity
• Capability Execution Tracking - Failure activity
• Tanium: Execute Request activity
• Tanium: Get Question ID from Response activity
• Execution Tracking - Begin (CIs) activity
• Turnstile workflow activity - wait for data
• Tanium: Build Check if Done Request activity
• Tanium: Determine if done from Response activity
• Tanium: Build Get Result Data Request activity
• Tanium: Get Result Data from Response activity - return process list
• Create Enrichment Data records activity
• Timer workflow activity - Timer workflow activity - Waits for 1 second
• Create Enrichment Data records activity
• Capability Execution Tracking - Complete activity
Activities specific to this workflow are described here. For more information on other activities, see Common integration workflow activities.

Get IP from CI activity

The Get IP from CI workflow activity gathers the IP address from configuration items (CIs) to use in the workflow.

The Get IP from CI activity can be used with any workflow to gather configuration item (CI) IP addresses to use in the workflow.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Found IP addresses.</td>
</tr>
<tr>
<td>Failure</td>
<td>No IP addresses found. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ci_sys_id</td>
<td>Configuration item identifier.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_addr</td>
<td>IP addresses.</td>
</tr>
</tbody>
</table>

**Tanium: Build Get Processes Request activity**

The **Tanium: Get Result Data from Response** workflow activity builds a request for processes to use in the workflow.

The **Tanium: Build Get Processes Request** activity can be used with any workflow to build a process request to use in the workflow.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Process request built.</td>
</tr>
<tr>
<td>Failure</td>
<td>Process request failed. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ci_ip_address</td>
<td>Configuration item IP address.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.
**Output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpoint</td>
<td>Specifies the encrypted SOAP endpoint to use.</td>
</tr>
<tr>
<td>request_body</td>
<td>Encrypted SOAP request contents.</td>
</tr>
<tr>
<td>http_timeout</td>
<td>Integer in seconds.</td>
</tr>
<tr>
<td>use_mid</td>
<td>Determines whether to use the MID server.</td>
</tr>
</tbody>
</table>

**Tanium: Execute Request activity**

This workflow activity executes an HTTP request. The inputs define the endpoint and the expected request body. The request body itself is the encrypted SOAP envelope.

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Input variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>request_body [Encrypted]</td>
</tr>
<tr>
<td>use_mid [Boolean]</td>
</tr>
<tr>
<td>endpoint [string]</td>
</tr>
<tr>
<td>http_timeout [integer]</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Output variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_code [integer]</td>
</tr>
<tr>
<td>header [string]</td>
</tr>
<tr>
<td>body [string]</td>
</tr>
</tbody>
</table>
Output variables (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error [string]</td>
<td>Any errors provided by the server.</td>
</tr>
</tbody>
</table>

**Tanium: Get Question ID from Response activity**
This workflow activity processes the response body to obtain the Question ID.

**Input variables**
Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
</table>

**Output variables**
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>question_id [integer]</td>
<td>The Question ID returned from the Tanium server.</td>
</tr>
</tbody>
</table>

**Tanium: Build Check if Done Request activity**
This workflow activity builds a request of the Tanium server to check if data collection for the question is complete. It returns the encrypted request and other components necessary to execute the request.

**Input variables**
Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>question_id [integer]</td>
<td>The Question ID returned from the Tanium server.</td>
</tr>
</tbody>
</table>
Output variables
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpoint [string]</td>
<td>The encrypted endpoint from the database.</td>
</tr>
<tr>
<td>request_body [Encrypted]</td>
<td>The SOAP request body.</td>
</tr>
<tr>
<td>http_timeout [Integer]</td>
<td>The HTTP timeout value, in seconds.</td>
</tr>
<tr>
<td>use_mid [Boolean]</td>
<td>A boolean flag indicating whether to use the MID Server.</td>
</tr>
</tbody>
</table>

Tanium: Execute Request activity
This workflow activity executes an HTTP request. The inputs define the endpoint and the expected request body. The request body itself is the encrypted SOAP envelope.

Input variables
Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>request_body</td>
<td>The SOAP request body. This input field is mandatory.</td>
</tr>
<tr>
<td>use_mid [Boolean]</td>
<td>A boolean flag indicating whether to use the MID Server.</td>
</tr>
<tr>
<td>endpoint [string]</td>
<td>The encrypted endpoint from the database. This input field is mandatory.</td>
</tr>
<tr>
<td>http_timeout [integer]</td>
<td>The HTTP timeout value, in seconds.</td>
</tr>
</tbody>
</table>

Output variables
The output variables contain data that can be used in subsequent activities.
### Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_code</td>
<td>Standard HTTP status codes.</td>
</tr>
<tr>
<td>header</td>
<td>The SOAP header.</td>
</tr>
<tr>
<td>body</td>
<td>The SOAP body.</td>
</tr>
<tr>
<td>error</td>
<td>Any errors provided by the server.</td>
</tr>
</tbody>
</table>

**Tanium: Determine if done from Response activity**

This workflow activity determines if a request has completed based on the response body.

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>response_body</td>
<td>The SOAP request body returned from Tanium.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>done</td>
<td>Returns true if the request processing is done.</td>
</tr>
</tbody>
</table>

**Tanium: Build Get Result Data Request activity**

This workflow builds a request to collect all the data returned from Tanium in answer to a question. It takes a Question ID as input and provides the output to execute the request, including an encrypted SOAP envelope payload.

**Input variables**

Input variables determine the initial behavior of the activity.
### Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>question_id [string]</td>
<td>The question ID of the question posed to Tanium.</td>
</tr>
</tbody>
</table>

### Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpoint [string]</td>
<td>The encrypted endpoint from the database.</td>
</tr>
<tr>
<td>request_body [Encrypted]</td>
<td>The SOAP request body.</td>
</tr>
<tr>
<td>http_timeout [Integer]</td>
<td>The HTTP timeout value, in seconds.</td>
</tr>
<tr>
<td>use_mid [Boolean]</td>
<td>A boolean flag indicating whether to use the MID Server.</td>
</tr>
</tbody>
</table>

### Tanium: Execute Request activity

This workflow activity executes an HTTP request. The inputs define the endpoint and the expected request body. The request body itself is the encrypted SOAP envelope.

### Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>request_body [Encrypted]</td>
<td>The SOAP request body. This input field is mandatory.</td>
</tr>
<tr>
<td>use_mid [Boolean]</td>
<td>A boolean flag indicating whether to use the MID Server.</td>
</tr>
<tr>
<td>endpoint [string]</td>
<td>The encrypted endpoint from the database. This input field is mandatory.</td>
</tr>
<tr>
<td>http_timeout [integer]</td>
<td>The HTTP timeout value, in seconds.</td>
</tr>
</tbody>
</table>
Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_code [integer]</td>
<td>Standard HTTP status codes.</td>
</tr>
<tr>
<td>header [string]</td>
<td>The SOAP header.</td>
</tr>
<tr>
<td>body [string]</td>
<td>The SOAP body.</td>
</tr>
<tr>
<td>error [string]</td>
<td>Any errors provided by the server.</td>
</tr>
</tbody>
</table>

Tanium: Get Result Data from Response activity

The `Tanium: Get Result Data from Response` workflow activity processes the response body from the result data and outputs an array of JSON objects representing the results from Tanium.

The `Tanium: Get Result Data from Response` activity can be used with any workflow to retrieve result data to use in the workflow.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Retrieved result data.</td>
</tr>
<tr>
<td>Failure</td>
<td>No data retrieved. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>response_body</td>
<td>Encrypted SOAP response contents</td>
</tr>
<tr>
<td>implementation_id</td>
<td>Implementation identifier.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>affected_ci</td>
<td>Configuration item affected.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result_data</td>
<td>Array Element type of API variables. Each array contains key-value pairs composed of the column and values returned from the server. If no data is received from the server, the output is an empty array.</td>
</tr>
<tr>
<td>output</td>
<td>Formatted return data on running processes used by the abstract workflow.</td>
</tr>
</tbody>
</table>

**Security Operations System Command Integration - Get Running Processes workflow**

The Security Operations System Command Integration - Get Running Processes workflow retrieves the running processes of a configuration item when added or updated to a Windows or Unix-based security incident in the Analysis state.

**Before you begin**

Role required: sn_si.analyst

**About this task**

For new security incidents, the workflow runs automatically when you submit the incident with a selected configuration item, when the state automatically changes to Analysis. If it remains in the Draft state, then it does not run.

Existing security incidents are automatically updated when you are in the Analysis state and you add a new configuration item.

Workflow process activities include:

- Get Configuration Item FQDN activity
- Determine Shell Script by OS activity
- Execution Tracking - Begin activity
- Get Running Processes via PowerShell
- Execute Shell Script activity
- Capability Execution Tracking - Failure activity
- Extract Shell Script from MID Script activity
- Combine Results and return values in an array
- Create Enrichment Data records activity
- Capability Execution Tracking - Complete activity

**Procedure**

1. Open a security incident.
2. Update the **State** to **Analysis**, if necessary.
3. Add a configuration item (computer, server, or similar).
4. Click **Update**.

   Security Incident Response Orchestration provides running process information in the Related Link > Security Incident Enrichments tab. For more information, see Security Operations enrichment data mapping.

   Activities specific to this workflow are described here. For more information on other activities, see Common integration workflow activities.

**Get Configuration Item FQDN activity**

The **Security Common Orchestration > Get Configuration Item FQDN** workflow activity retrieves the fully qualified domain name (FQDN) of a configuration item. This activity can accelerate the investigation and remediation process.

The **Get Configuration Item FQDN** activity can be used with any workflow to retrieve the fully qualified domain name (FQDN) of a configuration item.
**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cmdb_ci.id</td>
<td>The system identifier (sys_id) of a configuration item record.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fqdn</td>
<td>The fully qualified domain name (FQDN) of the configuration item.</td>
</tr>
</tbody>
</table>

**Additional Notes**

The fqdn field on the configuration item must be populated.

**Determine Shell Script by OS activity**

The Determine Shell Script by OS workflow activity determines which operating system to use in the workflow.

The Determine Shell Script by OS activity can be used with any workflow to determine which shell script to run based on the operating system running on the system containing the configuration item.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Found operating system.</td>
</tr>
<tr>
<td>Failure</td>
<td>No operating system found. More error information is available in the</td>
</tr>
<tr>
<td></td>
<td>activity output error.</td>
</tr>
</tbody>
</table>
**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ciSysId</td>
<td>System identifier of the configuration item.</td>
</tr>
<tr>
<td>processType</td>
<td>Internal identifier that defines which script to pull from the table.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>processScript</td>
<td>ECC agent that gathers the running process.</td>
</tr>
<tr>
<td>executionTemplate</td>
<td>Determines whether the script is run through a probe or using PowerShell.</td>
</tr>
<tr>
<td>enrichmentMappingId</td>
<td>System identifier of the enrichment mapping used to transform the response data.</td>
</tr>
</tbody>
</table>

**Get Running Processes via PowerShell activity**

The **Get Sensor ID** workflow activity gathers running processes using PowerShell to use in the workflow.

The **Get Running Processes via PowerShell** workflow activity can be used with any workflow to retrieve processes to include in the workflow.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Found processes</td>
</tr>
<tr>
<td>Failure</td>
<td>No processes found. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>
**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>IP or fully-qualified domain name (FQDN) of the target CI.</td>
</tr>
<tr>
<td>processingScript</td>
<td>ECC script run on a Windows-based system.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>response</td>
<td>Raw output. Running processes data.</td>
</tr>
</tbody>
</table>

**Extract Shell Script from MID Script activity**

The *Extract Shell Script from MID Script* workflow activity pulls a MID server shell script to use with in the workflow.

The *Extract Shell Script from MID Script* activity can be used with any workflow to extract a MID server shell script to include in the workflow.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Found shell script</td>
</tr>
<tr>
<td>Failure</td>
<td>No shell script found. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.
Variable | Description
---------|------------
sysId    | System identifier

**Output variables**
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scriptValue</td>
<td>Script, as a string value, executed on a Unix system.</td>
</tr>
</tbody>
</table>

**Execute Shell Script activity**
The **Execute Shell Script** workflow activity runs a MID server shell script within the workflow.

The **Execute Shell Script** activity can be used with any workflow to execute a MID server shell script in the workflow.

**Results**
Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Found shell script</td>
</tr>
<tr>
<td>Failure</td>
<td>No shell script found. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

**Input variables**
Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>IP or fully-qualified domain name (FQDN) of the target CI.</td>
</tr>
<tr>
<td>scriptValue</td>
<td>Script, as a string value, executed on a Unix system.</td>
</tr>
</tbody>
</table>
Output variables
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>response</td>
<td>Raw output. Running processes data.</td>
</tr>
</tbody>
</table>

Combine results activity
The **Combine results** workflow activity merges the results from third-party integrations to use in the workflow.

The **Combine results** activity can be used with any workflow to execute a MID server shell script in the workflow.

Results
Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Results combined.</td>
</tr>
<tr>
<td>Failure</td>
<td>Combination failed. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables
Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>inputA</td>
<td>Result set A</td>
</tr>
<tr>
<td>inputB</td>
<td>Result set B</td>
</tr>
<tr>
<td>implementation_id</td>
<td>Implementation identifier.</td>
</tr>
<tr>
<td>affected_ci</td>
<td>Configuration item</td>
</tr>
</tbody>
</table>

Output variables
The output variables contain data that can be used in subsequent activities.
Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Result set A or Result set B based on which one is filled.</td>
</tr>
</tbody>
</table>

**Security Operations Integration - Isolate Host capability**

The **Isolate Host** capability restricts system connections to other devices. Isolate host is executed against a configuration item (CI).

The **Isolate Host** capability has a workflow, **Security Operations - Isolate Host workflow** that accepts one or more CIs and optionally an implementation. You can specify an implementation to use to isolate the host or for the workflow to attempt to isolate the host using all implementations.

**Note:** While not integrated with a capability, a workflow, **Security Operations Carbon Black Integration - Remove Host Isolation workflow** is available for orchestration to restore communication with an isolated host.

**Note:** If no implementations are available, capability actions are not displayed in product menus.

**Run Isolate Host**

**Isolate Host** restricts system connections to other devices.

**Before you begin**

Role required: sn_si.analyst

**About this task**

**Note:** If no implementations are available, capability actions are not displayed in product menus.

The **Security Operations Integration - Isolate Host or Endpoint** workflow can be triggered from the related list on a security incident.

**Procedure**

1. Navigate to a security incident.
2. Select **Configuration Items** from the **Related List** tab.
3. Click **Isolate Host** in the **Actions on selected rows...** drop-down menu.
The dialog box appears.

4. Choose the implementation.

5. Click **Isolate Host**.

The workflow execution audit is displayed in the work notes section.

**Security Operations - Isolate Host workflow**

The **Security Operations - Isolate Host** workflow is a high-level workflow independent of integrations. It uses the configured queries to search for a set of configuration items. Use it to fulfill an integration, such as Carbon Black.
Before you begin
Role required: sn_si.analyst

About this task
This workflow is triggered from the Configuration Items tab on a security incident related list.

Workflow process activities include:
- Capability - Determine CIs activity
- Execution Tracking - Begin (CIs) activity
- Get Supported Security Capabilities activity
- Parallel Flow Launcher - launch the appropriate workflow. Store the results in an array.
- Capability Execution Tracking - No Impls activity
- Capability Execution Tracking - Failure activity

Activities specific to this workflow are described here. For more information on other activities, see Common integration workflow activities.

Capability - Determine CIs activity
The Capability - Determine CIs workflow activity determines which configuration items (CIs) to include in the workflow.

The Capability - Determine CIs activity can be used with any workflow to determine which CIs to include in the workflow.
Results
Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Found configuration items.</td>
</tr>
<tr>
<td>Failure</td>
<td>No CIs found. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables
Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>task_sys_id</td>
<td>Task identifier (maps security incident to CIs).</td>
</tr>
<tr>
<td>cis_affected</td>
<td>Configuration items.</td>
</tr>
</tbody>
</table>

Output variables
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cis_affected</td>
<td>Filtered CIs</td>
</tr>
<tr>
<td>task_sys_id</td>
<td>Task identifier (maps security incident to CIs).</td>
</tr>
</tbody>
</table>

Get Supported Security Capabilities activity
The Get Supported Capabilities workflow activity retrieves the name and number of integrations that are active and support the requested capability.

The Get Supported Capabilities activity can be used with any workflow to determine which capabilities are supported.

Results
Possible results for this activity are:
### Results

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Integration that supports the capability found.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to find an active integration that supports the capability. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

### Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityName</td>
<td>Name of the capability.</td>
</tr>
<tr>
<td>taskId</td>
<td>System identifier for any task associated with the workflow.</td>
</tr>
<tr>
<td>domainId</td>
<td>System identifier for any domain associated with the workflow.</td>
</tr>
</tbody>
</table>

### Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>supportedCapabilities</td>
<td>List of integrations that support the capability.</td>
</tr>
<tr>
<td>capabilityCount</td>
<td>Number of integrations that support the capability.</td>
</tr>
</tbody>
</table>

### Capability Execution Tracking - No Impls activity

The **Capability Execution Tracking - No Impls** workflow activity creates an error record when no integration capability implementation is found.

The **Capability Execution Tracking- No Impls** activity can be used with any abstract integration capability workflow to handle the error condition when no configured capability implementation is available.

### Results

Possible results for this activity are:
Results

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The execution tracking record state is set to <strong>Error</strong> and a message indicating the error is recorded.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityExecutionId</td>
<td>System identifier for the audit record. Output from the activity used to begin execution tracking.</td>
</tr>
<tr>
<td>workflowName</td>
<td>Name of the workflow. Supplied by the system.</td>
</tr>
</tbody>
</table>

Output variables

There are no output variables.

Security Operations Carbon Black Integration - Isolate Host workflow

The **Security Operations Carbon Black Integration - Isolate Host** is the implementation for the Carbon Black integration launched by the **Security Operations Integration - Isolate Host** workflow.

Before you begin

Role required: sn_si.analyst

About this task

Workflow process activities include:

- Execution Tracking - Begin (CIs) activity
- Get IP from CI
- Collect Carbon Black configurations
- Capability Execution Tracking - Failure activity
- Get Sensor ID
- Set Network Isolation Enabled
- Update Sensor - returns Isolate Host result.
- Capability Execution Tracking - Complete activity
Activities specific to this workflow are described here. For more information on other activities, see Common integration workflow activities.

Get IP from CI activity

The Get IP from CI workflow activity gathers the IP address from configuration items (CIs) to use in the workflow.

The Get IP from CI activity can be used with any workflow to gather configuration item (CI) IP addresses to use in the workflow.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Found IP addresses.</td>
</tr>
<tr>
<td>Failure</td>
<td>No IP addresses found. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ci_sys_id</td>
<td>Configuration item identifier.</td>
</tr>
</tbody>
</table>
**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_addr</td>
<td>IP addresses.</td>
</tr>
</tbody>
</table>

**Collect Carbon Black Configurations activity**

The **Collect Carbon Black Configurations** workflow activity gathers configuration information to use in the workflow.

The **Collect Carbon Black Configurations** activity gathers Carbon Black configuration information to use in the workflow.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Configuration succeeded.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to verify the configuration. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

**Input variables**

There are no input variables for this activity.

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpoint_base</td>
<td>Base URL of the third-party integration API.</td>
</tr>
<tr>
<td>use_mid_server</td>
<td>Determines whether the REST activity uses the MID server to interact with Carbon Black or not.</td>
</tr>
</tbody>
</table>
Output variables (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>api_token</td>
<td>Third-party integration API key.</td>
</tr>
</tbody>
</table>

Get Sensor ID activity

The Get Sensor ID workflow activity gathers sensor identifiers to use in the workflow.

The Get Sensor ID activity can be used with any workflow to gather sensor information to use in the workflow.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Found sensor identifiers.</td>
</tr>
<tr>
<td>Failure</td>
<td>No sensors found. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>api_token</td>
<td>Carbon Black API key.</td>
</tr>
<tr>
<td>use_mid_server</td>
<td>Determines whether the REST activity uses the MID server to interact with Carbon Black or not.</td>
</tr>
<tr>
<td>endpoint_base</td>
<td>Base URL of the Carbon Black API.</td>
</tr>
<tr>
<td>ci_ip_address</td>
<td>Configuration item IP address.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.
### Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_code</td>
<td>Determines if the request was successful. If not, displays an HTTP error code and message.</td>
</tr>
<tr>
<td>Array</td>
<td>API variables.</td>
</tr>
<tr>
<td>Element type</td>
<td></td>
</tr>
<tr>
<td>sensor_detail</td>
<td>Description of the Carbon Black sensor in JSON format.</td>
</tr>
</tbody>
</table>

### Set Network Isolation Enabled activity

The **Set Network Isolation Enabled** workflow activity enables network isolation.

The **Set Network Isolation Enabled** activity can be used with any workflow to enable network isolation.

### Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Network isolation enabled.</td>
</tr>
<tr>
<td>Failure</td>
<td>Network isolation cannot be enabled. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

### Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sensor_detail</td>
<td>Description of the Carbon Black sensor in JSON format.</td>
</tr>
<tr>
<td>disable</td>
<td>Determines whether the host is isolated or removes host isolation. True = disable isolation False = isolation remains enabled</td>
</tr>
</tbody>
</table>
Output variables
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sensor_detail</td>
<td>Description of the Carbon Black sensor in JSON format.</td>
</tr>
</tbody>
</table>

Update Sensor activity
The **Update Sensor** workflow activity updates the sensor to isolate hosts or endpoints.

The **Update Sensor** activity can be used with any workflow to isolate hosts or endpoints.

Results
Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Updated sensor.</td>
</tr>
<tr>
<td>Failure</td>
<td>Unable to update sensor. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables
Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>api_token</td>
<td>Carbon Black API key.</td>
</tr>
<tr>
<td>use_mid_server</td>
<td>Determines whether the REST activity uses the MID server to interact with Carbon Black or not.</td>
</tr>
<tr>
<td>endpoint_base</td>
<td>Base URL of the Carbon Black API.</td>
</tr>
<tr>
<td>sensor_id</td>
<td>Sensor identifier.</td>
</tr>
<tr>
<td>sensor_detail</td>
<td>Description of the Carbon Black sensor in JSON format.</td>
</tr>
</tbody>
</table>
Output variables
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_code</td>
<td>Determines if the request was successful. If not, displays an HTTP error code and message.</td>
</tr>
</tbody>
</table>

Security Operations Carbon Black Integration - Remove Host Isolation workflow

The Security Operations Carbon Black Integration - Remove Host Isolation workflow unblocks communication with a specified host or endpoint in a Carbon Black system.

Before you begin
Role required: sn_si.analyst

About this task
This workflow is not part of a capability and needs a custom orchestration in order to run.
Workflow process activities include:

- Get IP from CI
- If successful - Collect Carbon Black configurations
- Get Sensor ID
- If - Device supports isolation - and device is not isolated - Set Network Isolation Enabled to disabled.
- Update Sensor - returns Isolate Host result.
Get IP from CI activity

The Get IP from CI workflow activity gathers the IP address from configuration items (CIs) to use in the workflow.

The Get IP from CI activity can be used with any workflow to gather configuration item (CI) IP addresses to use in the workflow.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Found IP addresses.</td>
</tr>
<tr>
<td>Failure</td>
<td>No IP addresses found. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ci_sys_id</td>
<td>Configuration item identifier.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_addr</td>
<td>IP addresses.</td>
</tr>
</tbody>
</table>

Collect Carbon Black Configurations activity

The Collect Carbon Black Configurations workflow activity gathers configuration information to use in the workflow.

The Collect Carbon Black Configurations activity gathers Carbon Black configuration information to use in the workflow.
Results
Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Configuration succeeded.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to verify the configuration. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables
There are no input variables for this activity.

Output variables
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpoint_base</td>
<td>Base URL of the third-party integration API.</td>
</tr>
<tr>
<td>use_mid_server</td>
<td>Determines whether the REST activity uses the MID server to interact with Carbon Black or not.</td>
</tr>
<tr>
<td>api_token</td>
<td>Third-party integration API key.</td>
</tr>
</tbody>
</table>

Get Sensor ID activity
The Get Sensor ID workflow activity gathers sensor identifiers to use in the workflow.

The Get Sensor ID activity can be used with any workflow to gather sensor information to use in the workflow.

Results
Possible results for this activity are:
Results

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Found sensor identifiers.</td>
</tr>
<tr>
<td>Failure</td>
<td>No sensors found. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>api_token</td>
<td>Carbon Black API key.</td>
</tr>
<tr>
<td>use_mid_server</td>
<td>Determines whether the REST activity uses the MID server to interact with Carbon Black or not.</td>
</tr>
<tr>
<td>endpoint_base</td>
<td>Base URL of the Carbon Black API.</td>
</tr>
<tr>
<td>ci_ip_address</td>
<td>Configuration item IP address.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_code</td>
<td>Determines if the request was successful. If not, displays an HTTP error code and message.</td>
</tr>
<tr>
<td>Array Element type</td>
<td>API variables.</td>
</tr>
<tr>
<td>sensor_detail</td>
<td>Description of the Carbon Black sensor in JSON format.</td>
</tr>
</tbody>
</table>

Set Network Isolation Enabled activity

The Set Network Isolation Enabled workflow activity enables network isolation.

The Set Network Isolation Enabled activity can be used with any workflow to enable network isolation.
Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Network isolation enabled.</td>
</tr>
<tr>
<td>Failure</td>
<td>Network isolation cannot be enabled. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sensor_detail</td>
<td>Description of the Carbon Black sensor in JSON format.</td>
</tr>
</tbody>
</table>
| disable      | Determines whether the host is isolated or removes host isolation.  
               | True = disable isolation  
               | False = isolation remains enabled |

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sensor_detail</td>
<td>Description of the Carbon Black sensor in JSON format.</td>
</tr>
</tbody>
</table>

Update Sensor activity

The **Update Sensor** workflow activity updates the sensor to isolate hosts or endpoints.

The **Update Sensor** activity can be used with any workflow to isolate hosts or endpoints.

Results

Possible results for this activity are:
### Results

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Updated sensor.</td>
</tr>
<tr>
<td>Failure</td>
<td>Unable to update sensor. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

### Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>api_token</td>
<td>Carbon Black API key.</td>
</tr>
<tr>
<td>use_mid_server</td>
<td>Determines whether the REST activity uses the MID server to interact with Carbon Black or not.</td>
</tr>
<tr>
<td>endpoint_base</td>
<td>Base URL of the Carbon Black API.</td>
</tr>
<tr>
<td>sensor_id</td>
<td>Sensor identifier.</td>
</tr>
<tr>
<td>sensor_detail</td>
<td>Description of the Carbon Black sensor in JSON format.</td>
</tr>
</tbody>
</table>

### Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_code</td>
<td>Determines if the request was successful. If not, displays an HTTP error code and message.</td>
</tr>
</tbody>
</table>

### Security Operations Integration - Publish to Watchlist capability

The **Publish to Watchlist** capability adds observables and indicators associated with a security incident to a third-party watchlist that monitors for security events and generates alerts. This capability is used as part of incident response during investigations.

**Note:** If no implementations are available, capability actions are not displayed in product menus.
Security Operations Integration - Publish to Watchlist workflow

The Security Operations Integrations - Publish to Watchlist workflow is a high-level workflow independent of integrations. It adds observables to third-party watchlists that support the capability. Use it to fulfill an integration.

Before you begin
Role required: sn_si.analyst

About this task
This workflow is visible and runs only when an integration is available. It is triggered from the Observables or Associated Indicators tab on a security incident.

Activities specific to this workflow are described here. For more information on other activities, see Common integration workflow activities.

Determine Observables activity
The Determine Observables workflow activity determines which observable to include in the workflow.

The Determine Observables activity can be used with any workflow to determine which observables to include in the workflow.

Results
Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Found observables</td>
</tr>
</tbody>
</table>
Results (continued)

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure</td>
<td>No observables found. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>task_sys_id</td>
<td>Task identifier (maps security incident to observables).</td>
</tr>
<tr>
<td>observables</td>
<td>IP addresses, hash, URLs, domain names.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>observables</td>
<td>Filtered observables</td>
</tr>
</tbody>
</table>

**Filter Allowlisted Observables activity**

The **Filter Allowlisted Observables** workflow activity removes observables that can be ignored from the list of observables. This activity can accelerate the investigation and remediation process.

The **Filter Allowlisted Observables** activity can be used with any workflow to filter observables prior to taking any action.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Filter list created.</td>
</tr>
</tbody>
</table>
Results (continued)

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to filter the observables. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>observables</td>
<td>List of available observables.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filteredObservables</td>
<td>Filtered observables.</td>
</tr>
</tbody>
</table>

Get Supported Security Capabilities activity

The Get Supported Capabilities workflow activity retrieves the name and number of integrations that are active and support the requested capability.

The Get Supported Capabilities activity can be used with any workflow to determine which capabilities are supported.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Integration that supports the capability found.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to find an active integration that supports the capability. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>
Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityName</td>
<td>Name of the capability.</td>
</tr>
<tr>
<td>taskId</td>
<td>System identifier for any task associated with the workflow.</td>
</tr>
<tr>
<td>domainId</td>
<td>System identifier for any domain associated with the workflow.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>supportedCapabilities</td>
<td>List of integrations that support the capability.</td>
</tr>
<tr>
<td>capabilityCount</td>
<td>Number of integrations that support the capability.</td>
</tr>
</tbody>
</table>

Capability Execution Tracking - No Impls activity

The **Capability Execution Tracking - No Impls** workflow activity creates an error record when no integration capability implementation is found.

The **Capability Execution Tracking - No Impls** activity can be used with any abstract integration capability workflow to handle the error condition when no configured capability implementation is available.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The execution tracking record state is set to <strong>Error</strong> and a message indicating the error is recorded.</td>
</tr>
</tbody>
</table>
Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityExecutionId</td>
<td>System identifier for the audit record. Output from the activity used to begin execution tracking.</td>
</tr>
<tr>
<td>workflowName</td>
<td>Name of the workflow. Supplied by the system.</td>
</tr>
</tbody>
</table>

Output variables

There are no output variables.

Security Operations Integration - Sightings Search capability

The **Sightings Search** capability accepts a set of observables, finds any integrations that support a Sightings Search, then executes these searches.

The Sightings Search capability has a workflow, **Security Operations Integration - Sightings Search workflow**, that executes the sightings search. This workflow accepts a list of observables, finds any implementing capabilities, creates the queries based on Sightings Search Configurations, and executes the searches based on the configured workflow. Once the search is complete, a note is added to the incident Work notes including whether any sightings were found and if so, how many.

ℹ️ Note: To view Sightings Search Configurations, navigate to Security Operations > Integrations > Sightings Search Configurations.

ℹ️ Note: If no implementations are available, capability actions are not displayed in product menus.

Create sightings search configuration records

Create multiple sightings search configuration records and use them while querying multiple log stores or varying the search parameters.

Before you begin

- The CIM add-on must be installed on the Splunk instance
- Saved Searches and Inplace queries are supported for Splunk Integration only.
- Role required: sn_si.admin
About this task
You can also create sightings search configuration records to invoke saved searches on the Splunk enterprise log store.

Note: The search configuration queries rely on Splunk log data to be Splunk Common Information Model (CIM) compliant.

With saved search configurations, you can:
• Create custom searches that combine multiple event records.
• Design-efficient and effective searches.
• Use parameterized inputs in the Splunk saved search.

The base system includes the sample configurations as shown in this image:

<table>
<thead>
<tr>
<th>Name</th>
<th>Observable type</th>
<th>Search</th>
<th>Is saved search</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Point Inplace Search - Emails</td>
<td>Email</td>
<td>tag=email</td>
<td></td>
</tr>
<tr>
<td>Default Saved Search - Emails</td>
<td>Email</td>
<td>args.email.subject=$[email.subject]&amp;args...</td>
<td>true</td>
</tr>
<tr>
<td>Default PAN Inplace Search - URLs</td>
<td>URL</td>
<td>tag=network.url=$[observable]</td>
<td>table us...</td>
</tr>
</tbody>
</table>

The saved search and inplace configuration queries are example queries and can be substituted with appropriate parameters for your environment. Create additional saved search configurations as required. When you define a saved search configuration, the name and the parameters in the search query must match the saved configuration defined on your Splunk instance. If the name and parameters are not the same, you may not see accurate results when you perform a sightings search.

Note: On your Splunk instance, navigate to the Searches, Reports, and Alerts page and locate your saved search query. Click the Permissions link to navigate to the Permissions page. Select the All Apps radio button and enable the Read Permission option for Everyone. This will change the Sharing column value from Private to App for your saved search query. If this is not set, saved search query may not return any results.

To verify if the saved search configuration matches the configuration defined on your Splunk instance:
1. Navigate to **Settings > Searches, Reports, and Alerts**.

2. Change **App Context** to **All**.
   
   A list of search reports is displayed.

3. Confirm that the saved search query is present in the list.

For example, the Sightings Search Configuration form contains the email address and email sender as search parameters:

![Sightings Search Configuration form](image)

In your Splunk instance, define the saved search with the same name, Default Saved Search - Emails, and the same search parameters for the email address and email subject. If the name and search parameters are not the same, sightings search does not generate accurate result.
Procedure

1. Navigate to **Security Operations > Integrations > Sightings Search Configuration** and create a new record (see table for field descriptions).

### Sightings Search Configuration form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the configuration.</td>
</tr>
<tr>
<td>Is saved search</td>
<td>Saved search configuration is created if you select this option.</td>
</tr>
<tr>
<td>Sightings search source</td>
<td>The source for the sightings search. Select the Splunk log store as the source.</td>
</tr>
<tr>
<td>Active</td>
<td>Option for the saved search status. Only active search configurations can be used to perform a sightings search.</td>
</tr>
<tr>
<td>Observable type</td>
<td>Observable type can be any observable type such as IP, hash value, URL, domain name, and so on.</td>
</tr>
<tr>
<td>Maximum observables per search</td>
<td>Maximum number of observables to be returned from the search.</td>
</tr>
<tr>
<td>Search</td>
<td>The default search string is $(observable), but you can define your own search query by specifying parameters that are supported by the Splunk log store.</td>
</tr>
</tbody>
</table>

2. Click **Submit**.

Results

You have created a sightings search configuration record.

What to do next

After defining the search query, click **Generate Sightings Search Test Query**, and specify a list of observable values to generate a test query based on this saved search configuration.

Run a Sightings Search

Determine the prevalence of a threat over time or test remediation or eradication efforts. You can select individual or multiple observables and the date range for your search from a security incident. Results are included in the **Security Incident Observables** related list.
Before you begin
Role required: sn_si.analyst

About this task
The Sightings Search capability has a workflow, Security Operations Integration - Sightings Search workflow, that executes the sightings search. This workflow accepts a list of observables, finds any implementing capabilities, creates the queries based on Sightings Search Configurations, and executes the searches based on the configured workflow.

Note: An active implementation must be configured. Sightings Search supports Elasticsearch, Splunk, McAfee ESM, HPE ArcSight Logger, and QRadar incident enrichment. If no implementations are available, capability actions, such as Run Sightings Search, are not displayed in product menus.

Procedure
1. Navigate to a security incident.
2. Click the Show IoC related link.
3. Select Observables from the Related List tab.
4. Select the observables you want to perform a sightings search on.
5. Click Run Sightings Search in the Actions on selected rows... drop-down menu.

The Run Sightings Search dialog box opens.
Note: Values entered in the dialog box overwrite capability configuration values for this run.

6. Choose the number of days or a date range to search for data.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last</td>
<td>The number of hours or days prior to the creation of the incident to search.</td>
</tr>
<tr>
<td></td>
<td>The default is 7 days. The limit is 99 hours or days.</td>
</tr>
<tr>
<td>between</td>
<td>Range of dates to search. Default dates are:</td>
</tr>
<tr>
<td></td>
<td>The date and time the incident was opened.</td>
</tr>
<tr>
<td></td>
<td>The date and time seven days prior to the opening of the incident.</td>
</tr>
</tbody>
</table>

Note: Last is the number of hours or days prior to the creation of the incident to search. The default is 7 days. The limit is 99 hours or days.

7. Click Search.
A Sightings Search record is created. Aggregate and associated sightings data are displayed in the security incident under the Sightings Search Results and Sightings Search Details tabs.

Note: Sightings search results data can be shared with Trusted Security Circle, with the exception of raw data in the case of implementations configured to include raw data.
### Sightings Search Results

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>The identifier for the sightings search.</td>
</tr>
<tr>
<td>Observable count</td>
<td>Number of observables searched for by query.</td>
</tr>
<tr>
<td>Internal sightings</td>
<td>Count of internal sightings.</td>
</tr>
<tr>
<td>External sightings</td>
<td>Count of external sightings. (Received from threat sharing.)</td>
</tr>
<tr>
<td>Matched configuration items</td>
<td>Count of configuration items that matched an existing record in your cmdb for each observable found in your environment.</td>
</tr>
<tr>
<td>Start date range</td>
<td>Time to start looking for sightings.</td>
</tr>
<tr>
<td>End date range</td>
<td>Time to stop looking for sightings.</td>
</tr>
<tr>
<td>Updated</td>
<td>Date and time of the last modification.</td>
</tr>
</tbody>
</table>

**Note:** If the implementation used for the sightings search is configured to include raw data, and at least one sighting is found, an attachment containing raw data samples appears at the top of the security incident.

### Sighting Search Details

<table>
<thead>
<tr>
<th>Detail</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sighting search</td>
<td>The identifier for the sightings search.</td>
</tr>
<tr>
<td>Observable</td>
<td>Observable searched for by query.</td>
</tr>
<tr>
<td>Observable type</td>
<td>Type of observable searched for by query.</td>
</tr>
<tr>
<td>Internal sightings</td>
<td>Aggregated count of internal sightings.</td>
</tr>
<tr>
<td>Detail</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>External</td>
<td>Aggregated count of external sightings. (Received from threat sharing.)</td>
</tr>
<tr>
<td>sightings</td>
<td></td>
</tr>
<tr>
<td>Updated</td>
<td>Date and time of the last modification.</td>
</tr>
</tbody>
</table>

**Security Operations Integration - Sightings Search workflow**

**Security Operations Integration - Sightings Search** workflow is a high-level workflow independent of integrations. It uses the configured queries to search for a set of observables based on the configured integrations which support the capability. Use it to fulfill an integration such as Splunk or Elasticsearch.

**Before you begin**
Role required: sn_si.analyst

**About this task**
If a security incident has an observable attached to it, this workflow is triggered when you click on **Run Sighting Search** in the **Actions on selected rows...** drop-down menu in the **Security Incident Observables** tab.

Workflow process activities include:

- **Determine Observables activity**
- **Execution Tracking - Begin activity**
- **Timer workflow activity** - Timer workflow activity - Waits one second to get a lock.
- **Lock workflow activity**
- **Filter Allowlisted Observables**
- **Get Supported Security Capabilities activity**
- **Capability Execution Tracking - No Impls activity**
- **Unlock Sightings Search workflow**
- **Get Observable Sightings Queries activity**
- **Capability Execution Tracking - Failure activity**
- **Parallel Flow Launcher**
- **If workflow activity** - If workflow activity - Iterate until all the appropriate workflows have run and store the results in an array.
- **Capability Execution Tracking - Complete activity**
Activities specific to this workflow are described here. For more information on other activities, see Common integration workflow activities.

Sightings Search - Determine Observables activity

The **Sightings Search - Determine Observables** workflow activity determines which observables to include in the workflow.

The **Sightings Search - Determine Observables** activity can be used with any workflow to determine which observables to include in the workflow.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Found observables</td>
</tr>
<tr>
<td>Failure</td>
<td>No observables found. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.
### Variable Description

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>task_sys_id</td>
<td>Task identifier (maps security incident to observables).</td>
</tr>
<tr>
<td>observables</td>
<td>IP addresses, hash, URLs, domain names.</td>
</tr>
<tr>
<td>workflow_current_sys_id</td>
<td>System identifier of the current record. (Used only if task_sys_id, observable inputs are not available.</td>
</tr>
</tbody>
</table>

### Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>observables</td>
<td>Filtered observables</td>
</tr>
</tbody>
</table>

### Filter Allowlisted Observables activity

The **Filter Allowlisted Observables** workflow activity removes observables that can be ignored from the list of observables. This activity can accelerate the investigation and remediation process.

The **Filter Allowlisted Observables** activity can be used with any workflow to filter observables prior to taking any action.

### Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Filter list created.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to filter the observables. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

### Input variables

Input variables determine the initial behavior of the activity.
### Output variables
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>observables</td>
<td>List of available observables.</td>
</tr>
</tbody>
</table>

### Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filteredObservables</td>
<td>Filtered observables.</td>
</tr>
</tbody>
</table>

### Get Supported Security Capabilities activity
The Get Supported Capabilities workflow activity retrieves the name and number of integrations that are active and support the requested capability.

The Get Supported Capabilities activity can be used with any workflow to determine which capabilities are supported.

### Results
Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Integration that supports the capability found.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to find an active integration that supports the capability. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

### Input variables
Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityName</td>
<td>Name of the capability.</td>
</tr>
<tr>
<td>taskId</td>
<td>System identifier for any task associated with the workflow.</td>
</tr>
</tbody>
</table>
Variable | Description
---|---
domainId | System identifier for any domain associated with the workflow.

### Output variables
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
</table>
supportedCapabilities | List of integrations that support the capability. |
capabilityCount | Number of integrations that support the capability. |

### Capability Execution Tracking - No Impls activity
The **Capability Execution Tracking - No Impls** workflow activity creates an error record when no integration capability implementation is found.

The **Capability Execution Tracking - No Impls** activity can be used with any abstract integration capability workflow to handle the error condition when no configured capability implementation is available.

### Results
Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
</table>
Success | The execution tracking record state is set to **Error** and a message indicating the error is recorded. |

### Input variables
Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
</table>
capabilityExecutionId | System identifier for the audit record. Output from the activity used to begin execution tracking. |
<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>workflowName</td>
<td>Name of the workflow. Supplied by the system.</td>
</tr>
</tbody>
</table>

Output variables
There are no output variables.

Get Observable Sightings Queries activity
The Get Observable Sightings Queries workflow activity retrieves queries from the integration configuration.

The Get Observable Sightings Queries activity can be used with any workflow to get queries to send to the specified implementation using the Parallel Flow Launcher.

Results
Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Queries found.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to get queries. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables
Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>observables</td>
<td>List of filtered observables.</td>
</tr>
<tr>
<td>capabilities</td>
<td>List of supported capabilities.</td>
</tr>
</tbody>
</table>

Output variables
The output variables contain data that can be used in subsequent activities.
Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>queries</td>
<td>Search string.</td>
</tr>
<tr>
<td>queryCount</td>
<td>Number of queries to run.</td>
</tr>
</tbody>
</table>

Security Operations - ArcSight Logger Sightings Search workflow

The **Security Operations - ArcSight Logger Sightings Search** workflow is the implementation for the Splunk integration launched by the **Security Operations Integration - Sightings Search workflow**.

**Before you begin**
Role required: sn_si_analyst

**About this task**
Workflow process activities include:
- Execution Tracking - Begin activity
- Collect ArcSight Configurations activity
- Capability Execution Tracking - Failure activity
- ArcSight Event Query activity
- Checks to see if the MID Server is running or not.
- ArcSight Event Query activity
- Persist Observable Sightings activity - returns search results in an array.
- Capability Execution Tracking - Complete activity
Activities specific to this workflow are described here. For more information on other activities, see Common integration workflow activities.

**Collect ArcSight Configurations activity**

The **Collect ArcSight Configurations** workflow activity gathers configuration information to use in the workflow.

The **Collect ArcSight Configurations** activity can be used with any workflow to gather the HPE Security ArcSight Logger configuration settings.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Configuration succeeded.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to verify the configuration. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>Source of the request to run the workflow. Supported inputs are: Trusted Security Circles or security incident task.</td>
</tr>
<tr>
<td>days_to_search</td>
<td>Days to search from the current day backwards. Default is 7.</td>
</tr>
<tr>
<td>max_rows</td>
<td>Maximum rows to return from the query. The limit depends on the third-party integration.</td>
</tr>
<tr>
<td>observables</td>
<td>The list of observables from Trusted Security Circle or the security incident task to search for. Returned in JSON format.</td>
</tr>
<tr>
<td>query</td>
<td>Search syntax. $(observable) is the default.</td>
</tr>
</tbody>
</table>

### Output variables
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpoint_base</td>
<td>Base URL of the third-party integration API.</td>
</tr>
<tr>
<td>link_endpoint_base</td>
<td>Link to an ArcSight Logger search interface, when available.</td>
</tr>
<tr>
<td>use_default_workflows</td>
<td>Determines use of the workflow that was installed with the plugin. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• true - use the workflow</td>
</tr>
<tr>
<td></td>
<td>• false - do not use the workflow</td>
</tr>
<tr>
<td>arcsight_username</td>
<td>HPE Security ArcSight Logger user name</td>
</tr>
<tr>
<td>arcsight_password</td>
<td>HPE Security ArcSight Logger password</td>
</tr>
<tr>
<td>source</td>
<td>Source of the request to run the workflow. Supported inputs are: Trusted Security Circles or security incident task.</td>
</tr>
<tr>
<td>max_rows</td>
<td>Maximum rows to return from the query. The limit depends on the third-party integration.</td>
</tr>
<tr>
<td>days_to_search</td>
<td>Days to search from the current day backwards. Default is 7.</td>
</tr>
<tr>
<td>query</td>
<td>Search syntax. $(observable) is the default.</td>
</tr>
</tbody>
</table>
Output variables (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all_peers</td>
<td>Determines whether to search all other loggers connected on the network.</td>
</tr>
</tbody>
</table>

**ArcSight Event Query activity**

The **ArcSight Event Query** workflow activity searches the ArcSight event logs for malicious indicators.

The **ArcSight Event Query** activity can be used with any workflow to search the HPE Security ArcSight Logger event logs.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Query succeeded.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to verify the query. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>User name for the HPE Security ArcSight Logger system.</td>
</tr>
<tr>
<td>password</td>
<td>Password for the HPE Security ArcSight Logger system.</td>
</tr>
<tr>
<td>observables</td>
<td>The list of observables from Trusted Security Circles or the security incident task to search for. Returned in JSON format.</td>
</tr>
<tr>
<td>base_url</td>
<td>Base URL of the third-party integration API.</td>
</tr>
<tr>
<td>link_base_url</td>
<td>Link to an ArcSight Logger search interface, when available.</td>
</tr>
<tr>
<td>source</td>
<td>Source of the request to run the workflow. Supported inputs are: Trusted Security Circles or security incident task.</td>
</tr>
</tbody>
</table>
### Variable Description

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>max_rows</td>
<td>Maximum rows to return from the query. The limit depends on the third-party integration.</td>
</tr>
<tr>
<td>days_to_search</td>
<td>Days to search from the current day backwards. Default is 7.</td>
</tr>
<tr>
<td>query</td>
<td>Search syntax. ${observable} is the default.</td>
</tr>
<tr>
<td>all_peers</td>
<td>Determines whether to search all other loggers connected on the network.</td>
</tr>
</tbody>
</table>

### Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>output</td>
<td>Output of the query in JSON format.</td>
</tr>
</tbody>
</table>

### Persist Observable Sightings activity

The **Persistent Observable Sightings** workflow activity retrieves observables from the third-party integration.

The **Persistent Observable Sightings** activity can be used with any workflow to record observables found in the third-party integration.

### Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Observables retrieved.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to gather observables. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

### Input variables

Input variables determine the initial behavior of the activity.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sightingsResponse</td>
<td></td>
</tr>
<tr>
<td>taskId</td>
<td>Task identifier.</td>
</tr>
</tbody>
</table>

### Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>response</td>
<td></td>
</tr>
</tbody>
</table>

### Security Operations - Elasticsearch Sightings Search workflow

**Security Operations - Elasticsearch Sightings Search** workflow is the Elasticsearch implementation launched by the **Security Operations Integration - Sightings Search** workflow.

### Before you begin

Role required: sn_si.analyst

### About this task

Workflow process activities include:

- Execution Tracking - Begin activity
- Collect Elasticsearch Configurations activity
- Checks to see if the MID Server is running or not.
- Capability Execution Tracking - Failure activity
- Elasticsearch Event QueryActivity activity
- Persist Observable Sightings activity - returns search results in an array.
- Capability Execution Tracking - Complete activity
Activities specific to this workflow are described here. For more information on other activities, see Common integration workflow activities.

**Collect Elasticsearch Configurations activity**

The *Collect Elasticsearch Configurations* workflow activity gathers configuration information to use in the workflow.

The *Collect Elasticsearch Configurations* activity can be used with any workflow to gather the Elasticsearch configuration settings.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Configuration succeeded.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to verify the configuration. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>Source of the request to run the workflow. Supported inputs are: Trusted Security Circles or security incident task.</td>
</tr>
<tr>
<td>days_to_search</td>
<td>Days to search from the current day backwards. Default is 7.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>max_rows</td>
<td>Maximum rows to return from the query. The limit depends on the third-party integration.</td>
</tr>
<tr>
<td>observables</td>
<td>The list of observables from Trusted Security Circles or the security incident task to search for. Returned in JSON format.</td>
</tr>
<tr>
<td>query</td>
<td>Search syntax. $(observable) is the default.</td>
</tr>
</tbody>
</table>

### Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpoint_base</td>
<td>Base URL of the third-party integration API.</td>
</tr>
<tr>
<td>link_endpoint_base</td>
<td>[Optional] Link to a Kibana instance, when available.</td>
</tr>
</tbody>
</table>
| use_default_workflows | Determines use of the workflow that was installed with the plugin. Possible values are:  
  • true - use the workflow  
  • false - do not use the workflow  |
| elastic_username | Elasticsearch user name                                                      |
| elastic_password  | Elasticsearch password                                                       |
| source         | Source of the request to run the workflow. Supported inputs are: Trusted Security Circles or security incident task. |
| max_rows       | Maximum rows to return from the query. The limit depends on the third-party integration. |
| days_to_search | Days to search from the current day backwards. Default is 7.                |
| query          | Search syntax. $(observable) is the default.                                 |

### Capability Execution Tracking - No Impls activity

The **Capability Execution Tracking - No Impls** workflow activity creates an error record when no integration capability implementation is found.
The **Capability Execution Tracking- No Impls** activity can be used with any abstract integration capability workflow to handle the error condition when no configured capability implementation is available.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The execution tracking record state is set to <strong>Error</strong> and a message indicating the error is recorded.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityExecutionId</td>
<td>System identifier for the audit record. Output from the activity used to begin execution tracking.</td>
</tr>
<tr>
<td>workflowName</td>
<td>Name of the workflow. Supplied by the system.</td>
</tr>
</tbody>
</table>

**Output variables**

There are no output variables.

**Elasticsearch Event QueryActivity activity**

The **Elasticsearch Event Query** workflow activity searches the Elasticsearch event logs for malicious indicators.

The **Elasticsearch Event QueryActivity** activity can be used with any workflow to search the Elasticsearch event logs.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Query succeeded.</td>
</tr>
</tbody>
</table>
Results (continued)

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to verify the query. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>User name for the Elasticsearch system.</td>
</tr>
<tr>
<td>password</td>
<td>Password for the Elasticsearch system.</td>
</tr>
<tr>
<td>observables</td>
<td>The list of observables from Trusted Security Circles or the security incident task to search for. Returned in JSON format.</td>
</tr>
<tr>
<td>base_url</td>
<td>Base URL of the third-party integration API.</td>
</tr>
<tr>
<td>link_base_url</td>
<td>[Optional] Link to a Kibana instance, when available.</td>
</tr>
<tr>
<td>source</td>
<td>Source of the request to run the workflow. Supported inputs are: Trusted Security Circles or security incident task.</td>
</tr>
<tr>
<td>max_rows</td>
<td>Maximum rows to return from the query. The limit depends on the third-party integration.</td>
</tr>
<tr>
<td>days_to_search</td>
<td>Days to search from the current day backwards. Default is 7.</td>
</tr>
<tr>
<td>query</td>
<td>Search syntax. $(observable) is the default.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>output</td>
<td>Output of the query in JSON format.</td>
</tr>
</tbody>
</table>

**Persist Observable Sightings activity**

The Persistent Observable Sightings workflow activity retrieves observables from the third-party integration.
The **Persistent Observable Sightings** activity can be used with any workflow to record observables found in the third-party integration.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Observables retrieved.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to gather observables. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sightingsResponse</td>
<td></td>
</tr>
<tr>
<td>taskId</td>
<td>Task identifier.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>response</td>
<td></td>
</tr>
</tbody>
</table>

**Security Operations - McAfee ESM Sightings Search workflow**

The **Security Operations - McAfee ESM Sightings Search workflow** is the implementation for the Splunk integration launched by the **Security Operations Integration - Sightings Search workflow**.

**Before you begin**

Role required: sn_si_analyst

**About this task**

Workflow process activities include:
Activities specific to this workflow are described here. For more information on other activities, see Common integration workflow activities.

**Collect McAfee Configurations activity**

The **Collect McAfee Configurations** workflow activity gathers configuration information to use in the workflow.

The **Collect McAfee Configurations** activity can be used with any workflow to gather the McAfee ESM configuration settings.

**Results**

Possible results for this activity are:
### Results

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Configuration succeeded.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to verify the configuration. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

### Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>Source of the request to run the workflow. Supported inputs are: Trusted Security Circles or security incident task.</td>
</tr>
<tr>
<td>days_to_search</td>
<td>Days to search from the current day backwards. Default is 7.</td>
</tr>
<tr>
<td>max_rows</td>
<td>Maximum rows to return from the query. The limit depends on the third-party integration.</td>
</tr>
<tr>
<td>observables</td>
<td>The list of observables from Trusted Security Circles or the security incident task to search for. Returned in JSON format.</td>
</tr>
<tr>
<td>query</td>
<td>Search syntax. $(observable) is the default.</td>
</tr>
</tbody>
</table>

### Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpoint_base</td>
<td>Base URL of the third-party integration API.</td>
</tr>
<tr>
<td>link_endpoint_base</td>
<td>Link to a McAfee web interface, when available.</td>
</tr>
<tr>
<td>use_default_workflows</td>
<td>Determines use of the workflow that was installed with the plugin. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• true - use the workflow</td>
</tr>
<tr>
<td></td>
<td>• false - do not use the workflow</td>
</tr>
<tr>
<td>elastic_username</td>
<td>McAfee user name</td>
</tr>
<tr>
<td>elastic_password</td>
<td>McAfee password</td>
</tr>
</tbody>
</table>
Output variables (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>Source of the request to run the workflow. Supported inputs are: Trusted Security Circles or security incident task.</td>
</tr>
<tr>
<td>max_rows</td>
<td>Maximum rows to return from the query. The limit depends on the third-party integration.</td>
</tr>
<tr>
<td>days_to_search</td>
<td>Days to search from the current day backwards. Default is 7.</td>
</tr>
<tr>
<td>query</td>
<td>Search syntax. $(observable) is the default.</td>
</tr>
</tbody>
</table>

McAfee ESM Event Query activity

The *McAfee ESM Event Query* workflow activity searches the McAfee ESM event logs for malicious indicators.

The *McAfee ESM Event Query* activity can be used with any workflow to search the HPE Security ArcSight Logger event logs.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Query succeeded.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to verify the query. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>User name for the McAfee ESM system.</td>
</tr>
<tr>
<td>password</td>
<td>Password for the McAfee ESM system.</td>
</tr>
</tbody>
</table>
## Output variables

The output variables contain data that can be used in subsequent activities.

### Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>output</td>
<td>Output of the query in JSON format.</td>
</tr>
</tbody>
</table>

## Persist Observable Sightings activity

The **Persistent Observable Sightings** workflow activity retrieves observables from the third-party integration.

The **Persistent Observable Sightings** activity can be used with any workflow to record observables found in the third-party integration.

## Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Observables retrieved.</td>
</tr>
</tbody>
</table>
Results (continued)

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to gather observables. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sightingsResponse</td>
<td></td>
</tr>
<tr>
<td>taskId</td>
<td>Task identifier.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>response</td>
<td></td>
</tr>
</tbody>
</table>

Security Operations - QRadar Sightings Search workflow

Security Operations - QRadar Sightings Search workflow is the implementation for the IBM QRadar integration launched by the Security Operations Integration - Sightings Search workflow.

Before you begin
Role required: sn_si_analyst

About this task
Workflow process activities include:
• Execution Tracking - Begin activity
• Collect QRadar Configurations activity
• Capability Execution Tracking - Failure activity
• Checks to see if the MID Server is running.
• QRadar Event QueryActivity activity
• **Persist Observable Sightings activity** - returns search results in an array.
• **Capability Execution Tracking - Complete activity**

Activities specific to this workflow are described here. For more information on other activities, see [Common integration workflow activities](#).

**Collect QRadar Configurations activity**

The **Collect QRadar Configurations** workflow activity gathers configuration information to use in the workflow.

The **Collect QRadar Configurations** activity can be used with any workflow to gather the IBM QRadar configuration settings.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Configuration succeeded.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to verify the configuration. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>Source of the request to run the workflow. Supported inputs are: Trusted Security Circles or security incident task.</td>
</tr>
<tr>
<td>days_to_search</td>
<td>Days to search from the current day backwards. Default is 7.</td>
</tr>
<tr>
<td>max_rows</td>
<td>Maximum rows to return from the query. The limit depends on the third-party integration.</td>
</tr>
<tr>
<td>observables</td>
<td>The list of observables from Trusted Security Circles or the security incident task to search for. Returned in JSON format.</td>
</tr>
<tr>
<td>query</td>
<td>Search syntax. $(observable) is the default.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpoint_base</td>
<td>Base URL of the third-party integration API.</td>
</tr>
<tr>
<td>link_endpoint_base</td>
<td>Link to an IBM QRadar instance, when available.</td>
</tr>
<tr>
<td>use_default_workflows</td>
<td>Determines whether to use the workflow that was installed with the plugin or not. Possible values are true and false.</td>
</tr>
<tr>
<td>elastic_username</td>
<td>QRadar user name</td>
</tr>
<tr>
<td>elastic_password</td>
<td>QRadar password</td>
</tr>
<tr>
<td>source</td>
<td>Source of the request to run the workflow. Supported inputs are: Trusted Security Circles or security incident task.</td>
</tr>
<tr>
<td>max_rows</td>
<td>Maximum rows to return from the query. The limit depends on the third-party integration.</td>
</tr>
<tr>
<td>days_to_search</td>
<td>Days to search from the current day backwards. Default is 7.</td>
</tr>
<tr>
<td>query</td>
<td>Search syntax. $(observable) is the default.</td>
</tr>
</tbody>
</table>
QRadar Event QueryActivity activity

The **QRadar Event Query** workflow activity searches the QRadar event logs for malicious indicators.

The **QRadar Event QueryActivity** activity can be used with any workflow to search the Elasticsearch event logs.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Query succeeded.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to verify the query. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>User name for the QRadar system.</td>
</tr>
<tr>
<td>password</td>
<td>Password for the QRadar system.</td>
</tr>
<tr>
<td>observables</td>
<td>The list of observables from Trusted Security Circles or the security incident task to search for. Returned in JSON format.</td>
</tr>
<tr>
<td>base_url</td>
<td>Base URL of the third-party integration API.</td>
</tr>
<tr>
<td>link_base_url</td>
<td>Link to an IBM QRadar instance, when available.</td>
</tr>
<tr>
<td>source</td>
<td>Source of the request to run the workflow. Supported inputs are: Trusted Security Circles or security incident task.</td>
</tr>
<tr>
<td>max_rows</td>
<td>Maximum rows to return from the query. The limit depends on the third-party integration.</td>
</tr>
<tr>
<td>days_to_search</td>
<td>Days to search from the current day backwards. Default is 7.</td>
</tr>
<tr>
<td>query</td>
<td>Search syntax. $({observable})$ is the default.</td>
</tr>
</tbody>
</table>
Output variables
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>output</td>
<td>Output of the query in JSON format.</td>
</tr>
</tbody>
</table>

Persist Observable Sightings activity
The **Persistent Observable Sightings** workflow activity retrieves observables from the third-party integration.

The **Persistent Observable Sightings** activity can be used with any workflow to record observables found in the third-party integration.

Results
Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Observables retrieved.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to gather observables. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables
Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sightingsResponse</td>
<td></td>
</tr>
<tr>
<td>taskId</td>
<td>Task identifier.</td>
</tr>
</tbody>
</table>

Output variables
The output variables contain data that can be used in subsequent activities.
### Security Operations Integration - Splunk Sightings Search workflow

**Security Operations - Splunk Sightings Search** workflow is the implementation for the Splunk integration launched by the **Security Operations Integration - Sightings Search workflow**.

**Before you begin**

Role required: sn_si_analyst

**About this task**

Workflow process activities include:

- Execution Tracking - Begin activity
- Collect Splunk Configurations activity
- Capability Execution Tracking - Failure activity
- Checks to see if the MID Server is running or not.
- Splunk Event Query activity
- Persist Observable Sightings activity - returns search results in an array.
- Capability Execution Tracking - Complete activity

Activities specific to this workflow are described here. For more information on other activities, see [Common integration workflow activities](#).

---

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Collect Splunk Configurations activity

The Collect Splunk Configurations workflow activity gathers configuration information to use in the workflow.

The Collect Splunk Configuration activity can be used with any workflow to gather the Splunk configuration settings.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Configuration succeeded.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to verify the configuration. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>Source of the request to run the workflow. Supported inputs are: Trusted Security Circles or security incident task.</td>
</tr>
<tr>
<td>days_to_search</td>
<td>Days to search from the current day backwards. Default is 7.</td>
</tr>
<tr>
<td>max_rows</td>
<td>Maximum rows to return from the query. The limit depends on the third-party integration.</td>
</tr>
<tr>
<td>observables</td>
<td>The list of observables from Trusted Security Circle or the security incident task to search for. Returned in JSON format.</td>
</tr>
<tr>
<td>query</td>
<td>Search syntax. $(observable) is the default.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.
Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpoint_base</td>
<td>Base URL of the third-party integration API.</td>
</tr>
<tr>
<td>link_endpoint_base</td>
<td>Links to the Splunk web interface, when available.</td>
</tr>
<tr>
<td>use_default_workflows</td>
<td>Determines use of the workflow that was installed with the plugin. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• true - use the workflow</td>
</tr>
<tr>
<td></td>
<td>• false - do not use the workflow</td>
</tr>
<tr>
<td>elastic_username</td>
<td>Splunk user name.</td>
</tr>
<tr>
<td>elastic_password</td>
<td>Splunk password.</td>
</tr>
<tr>
<td>source</td>
<td>Source of the request to run the workflow. Supported inputs are: Trusted Security Circles or security incident task.</td>
</tr>
<tr>
<td>max_rows</td>
<td>Maximum rows to return from the query. The limit depends on the third-party integration.</td>
</tr>
<tr>
<td>days_to_search</td>
<td>Days to search from the current day backwards. Default is 7.</td>
</tr>
<tr>
<td>query</td>
<td>Search syntax. $(observable) is the default.</td>
</tr>
</tbody>
</table>

Splunk Event Query activity

The **Splunk Event Query** workflow activity searches the Splunk event logs for malicious indicators.

The **Splunk Event Query Activity** activity can be used with any workflow to search the Splunk event logs.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Splunk</td>
</tr>
</tbody>
</table>
Results (continued)

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to verify Splunk query. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>User name for the Splunk system.</td>
</tr>
<tr>
<td>password</td>
<td>Password for the Splunk system.</td>
</tr>
<tr>
<td>observables</td>
<td>The list of observables from Trusted Security Circle or the security incident task to search for. Returned in JSON format.</td>
</tr>
<tr>
<td>base_url</td>
<td>URL of the Splunk integration endpoint.</td>
</tr>
<tr>
<td>link_base_url</td>
<td>Link to the Splunk web interface, when available.</td>
</tr>
<tr>
<td>source</td>
<td>Source of the request to run the workflow. Supported inputs are: Trusted Security Circles or security incident task.</td>
</tr>
<tr>
<td>max_rows</td>
<td>Maximum rows to return from the query. The limit depends on the third-party integration.</td>
</tr>
<tr>
<td>days_to_search</td>
<td>Days to search from the current day backwards. Default is 7.</td>
</tr>
<tr>
<td>query</td>
<td>Search syntax. $(observable) is the default.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Output variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variable</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>output</td>
</tr>
</tbody>
</table>
The **Persistent Observable Sightings** activity can be used with any workflow to record observables found in the third-party integration.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Observables retrieved.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to gather observables. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sightingsResponse</td>
<td></td>
</tr>
<tr>
<td>taskId</td>
<td>Task identifier.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>response</td>
<td></td>
</tr>
</tbody>
</table>

**View Sightings Search Results**

You can review Sightings Search Results for internal and external malicious indicators.

**Before you begin**

Role required: sn_si.analyst

**About this task**

.
**Procedure**

1. Navigate to a security incident.

2. Select the **Sightings Search Results** tab from **Show IoC** Related List group to view the list of sightings searches.

![Sightings Search Results](image)

**Note:** This data can be shared with Trusted Security Circle.

### Sightings Search Results

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Sightings Search identifier.</td>
</tr>
<tr>
<td>Observable count</td>
<td>Number of observables searched for.</td>
</tr>
<tr>
<td>Internal Sightings</td>
<td>Aggregated count of internal sightings.</td>
</tr>
<tr>
<td>External Sightings</td>
<td>Aggregated count of external sightings. (Received from threat sharing.)</td>
</tr>
<tr>
<td>Matched configuration items</td>
<td>Aggregated count of configuration items that matched an existing record in your cmdb.</td>
</tr>
<tr>
<td>Start date range</td>
<td>Time to start looking for sightings.</td>
</tr>
<tr>
<td>End date range</td>
<td>Time to stop looking for sightings.</td>
</tr>
<tr>
<td>Updated</td>
<td>Date and time of last modification.</td>
</tr>
</tbody>
</table>

To view the details of a single search:

3. Click on a Sightings Search in the **Sightings Search Results** list. The Sightings Search Result form displays.
## Sightings Search Results form

<table>
<thead>
<tr>
<th>Detail</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Internal Sightings Search identifier.</td>
</tr>
<tr>
<td>Observable count</td>
<td>Count of observables searched for by this query.</td>
</tr>
<tr>
<td>Internal sightings</td>
<td>Count of internal sightings for this search.</td>
</tr>
<tr>
<td>External sightings</td>
<td>Count of external sightings for this search. (Received from Trusted Security Circle.)</td>
</tr>
<tr>
<td>Unmatched hosts</td>
<td>List of potential configuration items for this search that were not matched with any records in your cmdb.</td>
</tr>
<tr>
<td>Task</td>
<td>Security incident task identifier.</td>
</tr>
<tr>
<td>Start date range</td>
<td>Time the sightings search started.</td>
</tr>
<tr>
<td>Detail</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>End date range</td>
<td>Time the sightings search stopped.</td>
</tr>
<tr>
<td>Updated</td>
<td>Date and time of last modification.</td>
</tr>
<tr>
<td>Sightings Search Details</td>
<td>Type, number of sightings and modification date.</td>
</tr>
<tr>
<td>Matched Configuration Items</td>
<td>Count of configuration items that matched an existing record in your cmdb. Lists the CI and the Sighting.</td>
</tr>
<tr>
<td>Threat Shares</td>
<td>List of the threats shared with Trusted Security Circle.</td>
</tr>
</tbody>
</table>

**Share Sightings Search results**

You can share local sightings details or results that are associated with a particular search with your Trusted Security Circle.

**Before you begin**

Role required: sn_si.analyst

**About this task**

Sharing can be automated using the following Security Incident Response Properties.

- Automatically share the results of a sightings search to the default ServiceNow trusted circle
- Include observables with no local sightings when automatically sharing sightings search results
- Respond with local sightings whenever a threat share is received from a trusted circle

**Procedure**

1. Navigate to a security incident.
2. Click the Show IoC related list and select the **Sightings Search Results** tab to view the list of sightings searches.
3. Click on a sightings search result.
4. On the **Sightings Search Result** form, click the **Share sighting search result** related link.
   The Sighting Search Result Share dialog box appears.
5. Enter a **Name** for this observable share record.

6. Enter a **Description** of the observables to share.

7. Choose **Circles** to share the observables with.

8. Click **Submit**.
   The observable(s) are shared with the specified Trusted Circle.

**Share observables from a security incident**

Observables can be shared from a security incident in Security Incident Response to members in your trusted circle.

**Before you begin**
Role required: sn_si.analyst
**Procedure**

1. Navigate to a security incident.

2. Select the **Observables** tab from **Show IoC** Related List group.

3. Click on an observable.

4. On the **Observable** form click the **Share observable** related link. The Observable Share dialog box appears.

5. Enter a **Name** for this threat share record.

6. Enter a **Description** of the selected observables.

7. Choose **Circles** to share the observables with.

8. Click **Submit**.

The observable(s) are shared with the specified Trusted Circle.
9. You can view the threat share records by clicking the Threat shares tab.
10. If any of the shared observables contain sightings, the sightings are also shared and can be viewed by clicking the Sightings tab.

**View Sightings Search Details**
Review the aggregate details of all sighting searches.

**Before you begin**
Role required: sn_si.analyst

**About this task**

**Procedure**
1. Navigate to a security incident.
2. Select the Sightings Search Details tab from Show IoC Related List group to view the list of sightings searches.

**Note:** This data can be shared with Trusted Security Circle.

### Sightings Search Details

<table>
<thead>
<tr>
<th>Detail</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observable</td>
<td>List of all observables searched for by query.</td>
</tr>
<tr>
<td>Observable type</td>
<td></td>
</tr>
<tr>
<td>Internal sightings</td>
<td>Count of internal sightings for all searches.</td>
</tr>
<tr>
<td>External sightings</td>
<td>Count of external sightings for all searches. (Received from threat sharing.)</td>
</tr>
<tr>
<td>Sighting search</td>
<td>Sightings Search identifier.</td>
</tr>
<tr>
<td>Updated</td>
<td>Date and time of last modification.</td>
</tr>
</tbody>
</table>

**Security Operations Integration - Threat Lookup capability**

The Threat Lookups capability performs threat intelligence lookups to determine whether one or more observables are associated with known security threats.
The **Threat Lookups** capability has a workflow, **Security Operations Integration - Threat Lookup workflow**. When the capability workflow runs, it executes additional workflows for the activated implementations. You can specify an implementation to use to perform a lookup on the selected observables, or you can perform the lookup using all implementations.

**Note:** If no implementations are available, capability actions are not displayed in product menus.

**Security Operations Integration - Threat Lookup workflow**

The **Security Operations Integration - Threat Lookup** capability workflow accesses available threat lookup implementations and executes the implementation workflows associated with each to perform threat lookups of selected observables.

**Before you begin**

Role required: **sn_ti.write**

**About this task**

This workflow can be triggered in these ways.

- by selecting one or more observables from the Observables list and selecting **Run threat lookup** from the **Actions on selected rows** choice list.
- by opening an observable record and clicking the **Run threat lookup** related link.
- From the Observables related list in a security incident.

Each method then allows you to specify which lookup implementations to be used to scan the selected observables. The associated implementation workflows are executed to perform the lookups.
Activities specific to this workflow are described here. For more information on other activities, see Common integration workflow activities.

Get Supported Security Capabilities activity

The Get Supported Capabilities workflow activity retrieves the name and number of integrations that are active and support the requested capability.

The Get Supported Capabilities activity can be used with any workflow to determine which capabilities are supported.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Integration that supports the capability found.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to find an active integration that supports the capability. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityName</td>
<td>Name of the capability.</td>
</tr>
<tr>
<td>taskId</td>
<td>System identifier for any task associated with the workflow.</td>
</tr>
<tr>
<td>domainId</td>
<td>System identifier for any domain associated with the workflow.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>supportedCapabilities</td>
<td>List of integrations that support the capability.</td>
</tr>
<tr>
<td>capabilityCount</td>
<td>Number of integrations that support the capability.</td>
</tr>
</tbody>
</table>

**Capability Execution Tracking - No Impls activity**

The **Capability Execution Tracking - No Impls** workflow activity creates an error record when no integration capability implementation is found.

The **Capability Execution Tracking- No Impls** activity can be used with any abstract integration capability workflow to handle the error condition when no configured capability implementation is available.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The execution tracking record state is set to <strong>Error</strong> and a message indicating the error is recorded.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.
### Output variables

There are no output variables.

### Change the order of workflow execution

Integration capability implementations specify the workflow to be executed. In the base system, workflows are executed sequentially, in the order specified in the implementation. You can change the order as needed.

**Before you begin**

Role required: sn_sec_cmn.write

**Procedure**

1. Navigate to **Security Operations > Integrations > Integration Capabilities**.

2. Select the integration capability for which you want to change the execution order.
3. Select the implementation you want to modify.

4. Change the Order to a higher or lower number. Lower numbers have a higher execution priority.

5. Click Submit.

Common integration workflow activities

Many of the workflows associated with third-party integrations include the same activities. For example, activities for beginning and completing processing.

Execution Tracking - Begin activity

The Execution Tracking - Begin workflow activity starts the auditing process for a Security Operations Integration workflow that operates on observables.

The Execution Tracking - Begin activity can be used with any workflow to begin recording the progress of the workflow in an audit.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>An audit record is created.</td>
</tr>
</tbody>
</table>
Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityId</td>
<td>System identifier of the Integration Capability being executed.</td>
</tr>
<tr>
<td>isImpl</td>
<td>Flag that specifies whether auditing is done for an Integration Capability workflow or an Integration Capability implementation workflow. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• false - denotes auditing on an abstract Integration Capability workflow such as Sightings Search. (default.)</td>
</tr>
<tr>
<td></td>
<td>• true - denotes auditing on an Integration Capability implementation workflow. For example, Splunk or Elasticsearch.</td>
</tr>
<tr>
<td>taskId</td>
<td>System identifier for any task associated with the workflow.</td>
</tr>
<tr>
<td>observableList</td>
<td>One or more observable SysIDs to perform the desired action.</td>
</tr>
<tr>
<td></td>
<td>Used as a workflow input.</td>
</tr>
<tr>
<td>workflowContextId</td>
<td>System identifier of the associated workflow context record. Supplied by the system.</td>
</tr>
<tr>
<td>workflowName</td>
<td>Name of the workflow. Supplied by the system.</td>
</tr>
<tr>
<td>parentCapabilityExecutionId</td>
<td>System identifier of the audit record that launched the implementation workflow. Only required for Integration Capability implementation workflows such as Splunk, Elasticsearch, and VirusTotal.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.
Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityExecutionId</td>
<td>System identifier of the audit record.</td>
</tr>
</tbody>
</table>

Capability Execution Tracking - Complete activity

The **Capability Execution Tracking - Complete** workflow activity updates the audit record when the workflow is complete.

The **Capability Execution Tracking - Complete** activity can be used with any workflow to record the completion of the workflow.

Note: The **Return Value** array from the **Parallel Launcher** core activity contains an array of results from all integration workflows run and prompts the successful completion of execution tracking.

Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The audit record state is updated to <strong>Complete</strong>.</td>
</tr>
</tbody>
</table>

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityExecutionId</td>
<td>System identifier for the audit record. This field was the output from any of the Begin auditing activities.</td>
</tr>
<tr>
<td>workflowName</td>
<td>Name of the workflow. Supplied by the system.</td>
</tr>
<tr>
<td>message</td>
<td>Completion message.</td>
</tr>
</tbody>
</table>

Output variables

There are no output variables.
**Capability Execution Tracking - Failure activity**

The **Capability Execution Tracking - Failure** workflow activity records a failure to the audit record.

The **Capability Execution Tracking - Failure** activity can be used with any workflow to record a failure condition.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The audit record state is set to <strong>Error</strong> and a message indicating the error is recorded.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilityExecutionId</td>
<td>System identifier for the audit record. This is the output from any of the Begin auditing activities.</td>
</tr>
<tr>
<td>errorMessage</td>
<td>Message indicating the reason for the failure.</td>
</tr>
<tr>
<td>workflowName</td>
<td>Name of the workflow. Supplied by the system.</td>
</tr>
</tbody>
</table>

**Output variables**

There are no output variables.

**Create Enrichment Data records activity**

The **Create enrichment data records** workflow activity creates or updates enrichment records to use in the workflow.

The **Create Enrichment Data records** activity can be used with any workflow to update enrichment records in the workflow.

**Results**

Possible results for this activity are:
### Results

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Enrichment record updated.</td>
</tr>
<tr>
<td>Failure</td>
<td>Enrichment record not updated. More error information is available in the</td>
</tr>
<tr>
<td></td>
<td>activity output error.</td>
</tr>
</tbody>
</table>

### Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>task_id</td>
<td>Task identifier.</td>
</tr>
<tr>
<td>content</td>
<td>Raw content (running processes data).</td>
</tr>
<tr>
<td>enrichment_mapping_id</td>
<td>Enrichment mapping identifier.</td>
</tr>
<tr>
<td>ci_id</td>
<td>Configuration item identifier.</td>
</tr>
<tr>
<td>reference_value</td>
<td>Unused.</td>
</tr>
</tbody>
</table>

### Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>GlideRecords created using the enrichmentUtils script.</td>
</tr>
</tbody>
</table>

### Security Operations workflow triggers

Security Operations workflow triggers contain a condition on a table. All workflows attached to the workflow trigger record run when the condition is met.

### Create Security Operations workflow triggers

Create a workflow trigger that contains a condition on a table.
Before you begin
Roles required:

- To read: sn_sec_cmn.read
- To create or update: sn_sec_cmn.write
- To delete: sn_sec_cmn.admin

Several contains several workflow triggers in the base system:

**Configuration item changes on an active Security Incident**
Uses integration to enrich CI-related data as configuration items change.

**Rescan vulnerable group**
Rescans a vulnerable group, using the Scan vulnerability workflow, when you Close/Ignore the group.

**Rescan vulnerable item**
Rescans a vulnerable item, using the Scan vulnerability item workflow when you Close/Ignore the item.

Procedure
2. Click New.
3. Fill in the fields on the form, as appropriate.

**Workflow Triggers**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the workflow trigger.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the workflow trigger.</td>
</tr>
<tr>
<td>Table</td>
<td>The table containing the workflow trigger.</td>
</tr>
<tr>
<td></td>
<td>If you selected the <strong>Use filter group</strong> check box and selected a filter group, this field defaults to the table associated with the selected filter group.</td>
</tr>
<tr>
<td>Condition</td>
<td>Use the <strong>condition builder</strong> to define the criteria for the workflow trigger.</td>
</tr>
<tr>
<td></td>
<td>If you selected the <strong>Use filter group</strong> check box and selected a filter group, the <strong>Condition</strong> fields are not displayed.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Active | Select this check box to activate the workflow trigger.
Use filter group | Select this check box to use a predefined filter group or create a new filter group to define the workflow trigger criteria.
Filter group | Select the filter group to use for defining workflow triggers. This field appears only if the **Use filter groups** check box is selected.

4. When you have completed your entries, right-click in the form header and select **Save**.

The **Workflows** tab appears. It contains workflows that are run when all filter conditions or filter group conditions are met.

5. To add workflows, perform these steps.
a. In the Workflows tab, click **Edit**.

b. Use the condition builder, if needed, to locate the workflows you want to select, or use the slushbucket to select workflows and move them to the Workflows List.

c. Click **Save**.
   The selected workflows are added.

6. Click **Update**.

**Security Operations Orchestration**

Users can interact with and retrieve data from Windows or UNIX-based systems and environments using activity packs and workflows in Security Operations Orchestration.

Security Operations Orchestration saves time by eliminating manual processes and obtaining contextual information to remediate incidents. The Security Operations products have standard activity packs and workflows that are included and activated in each of the plugins.

To create and access additional orchestration activities that are not available with the standard offering Security Operations products, purchase a full orchestration license.

- Security Incident Response Orchestration workflows:
  - Security Incident Response - Get Network Statistics workflow
  - Security Operations System Command Integration - Get Running Processes workflow
  - Create Lookup Request for IoC Changes workflow
  - Security Operations Integration - Email Search and Delete workflow

- Threat Intelligence Orchestration workflows:
  - Threat Intelligence - Run IoC Lookup workflow
  - Update security incident with lookup results workflow

- Vulnerability Response Orchestration workflows:
  - Scan vulnerability workflow
  - Scan vulnerability item workflow

**Security Operations orchestration workflows**

Several workflows are included with Security Operations.
Scan vulnerability workflow

The **Vulnerability Response > Scan Vulnerability** workflow rescans a vulnerability group.

**About this task**

This workflow is triggered by **Rescan vulnerable group** during a **Close/Ignore** action.

Workflow process activities include:

- Variables for Create Scan Record for Vulnerabilities activity
- Log Message
Procedure
1. Navigate to Vulnerability > Vulnerabilities > Vulnerability Groups.
2. Open a vulnerability group.
3. Click Close/Ignore.
5. Choose Fixed for the Substate.
6. Choose Wait for confirmation from the next scan for Close now?
   For the vulnerability group and vulnerable items, the State changes to Pending Confirmation, the Substate changes to Fixed, and a rescan runs.

Variables for Create Scan Record for Vulnerabilities activity
Vulnerability scans for single or multiple vulnerable items can be run using the Create Scan Record for Vulnerabilities workflow activity included in the base system. When the input is passed to the activity, it creates a scan record.

Input variables
Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskids</td>
<td>A string of comma-separated sysIds that define the expected inputs. This field is mandatory.</td>
</tr>
</tbody>
</table>

Output variables
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scanResult</td>
<td>Returns True if the input is not empty. A scan record is created for the taskIds.</td>
</tr>
</tbody>
</table>

Scan vulnerability item workflow
The Vulnerable Response > Scan Vulnerability Item workflow rescans a vulnerable item.
About this task
This workflow is triggered by **Rescan vulnerability**, during a **Close/Ignore** action.

Workflow process activities include:

**Variables for Create Scan Record for Vulnerabilities activity**

Log Message

---

**Procedure**

1. Navigate to **Vulnerability > Vulnerabilities > Vulnerable Items**.
2. Open a vulnerability item.
3. Click **Close/Ignore**.
4. Choose **Closed** for the **Desired State**.
5. Choose **Fixed** for the **Substate**.
   The **State** of the group changes to **Pending Confirmation**, the **Substate** changes to **Fixed**, and a rescan runs.

**Update security incident with lookup results workflow**

The **Update security incident with lookup results** workflow updates existing security incidents with lookup results.

**Before you begin**
Role required: sn_si.basic

**About this task**
This workflow is triggered by a business rule on the lookup table which monitors when the **Result** field changes to Failed.

Workflow process activities include:
- **Roll up lookup info to security incident activity**
- **Update Task Worknotes activity**

**Security Operations orchestration activities**
Many activities are included with Security Operations for use in workflows.

**Create Enrichment Data records activity**
The **Create enrichment data records** workflow activity creates or updates enrichment records to use in the workflow.
The Create Enrichment Data records activity can be used with any workflow to update enrichment records in the workflow.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Enrichment record updated.</td>
</tr>
<tr>
<td>Failure</td>
<td>Enrichment record not updated. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>task_id</td>
<td>Task identifier.</td>
</tr>
<tr>
<td>content</td>
<td>Raw content (running processes data).</td>
</tr>
<tr>
<td>enrichment_mapping_id</td>
<td>Enrichment mapping identifier.</td>
</tr>
<tr>
<td>ci_id</td>
<td>Configuration item identifier.</td>
</tr>
<tr>
<td>reference_value</td>
<td>Unused.</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>GlideRecords created using the enrichmentUtils script.</td>
</tr>
</tbody>
</table>

**Get Configuration Item FQDN activity**

The Security Common Orchestration > Get Configuration Item FQDN workflow activity retrieves the fully qualified domain name (FQDN) of a configuration item. This activity can accelerate the investigation and remediation process.
The **Get Configuration Item FQDN** activity can be used with any workflow to retrieve the fully qualified domain name (FQDN) of a configuration item.

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Input variables</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Variable</strong></td>
</tr>
<tr>
<td>cmdb_ci.id</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Output variables</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Variable</strong></td>
</tr>
<tr>
<td>fqdn</td>
</tr>
</tbody>
</table>

**Additional Notes**

The fqdn field on the configuration item must be populated.

**Get Email Details from Exchange Server activity**

The Get Email Details from Exchange Server activity performs a search for emails in the designated Exchange server(s) using the search queries defined, and returns details from the subject, recipient, and sender parameters.

**Input variables**

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Input variables</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Variable</strong></td>
</tr>
<tr>
<td>targetId</td>
</tr>
<tr>
<td>search_query</td>
</tr>
</tbody>
</table>
Output variables
The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>response</td>
<td>Email details retrieved for each email found for the given search query.</td>
</tr>
</tbody>
</table>

Exit Conditions
Possible exit conditions for this activity are:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No emails found</td>
<td>When the email count is zero, no emails were found for the given search query.</td>
</tr>
<tr>
<td>Threat emails found</td>
<td>When the email count is greater than zero, and email details were returned for the given search query.</td>
</tr>
<tr>
<td>Error executing at exchange</td>
<td>When an error occurred while executing the powershell script in the Exchange Server.</td>
</tr>
</tbody>
</table>

Get IP from CI activity
This workflow activity determines the IPV4 address associated with a configuration item (CI).

The Get IP from CI activity can be used with any workflow to retrieve the IPv4 address of a CI.

Input variables
Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ci_sys_id</td>
<td>Configuration item system identifier</td>
</tr>
</tbody>
</table>
**Output variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_addr</td>
<td>IPv4 address. If the IP address cannot be determined, this value is empty.</td>
</tr>
</tbody>
</table>

**Exit Conditions**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>An IPv4 address was returned.</td>
</tr>
<tr>
<td>Failure</td>
<td>An IPv4 address could not be determined.</td>
</tr>
</tbody>
</table>

**Get Network Statistics via netstat activity**

The *Security Common Orchestration - Get Network Statistics via netstat* workflow activity retrieves the network statistics for an affected resource on a Windows-based system. This activity can accelerate the investigation and remediation process.

The *Get Network Statistics via netstat* activity can be used with any workflow to retrieve network statistics from a Windows-based system. The machine is queried with the *netstat* command including the `-a` and `-o` parameters. To enhance the output data, *get-process* command is also invoked.

**Results**

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Network statistics were retrieved in JSON format.</td>
</tr>
<tr>
<td>Failure</td>
<td>An error occurred while attempting to retrieve network statistics. More error information is available in the activity output error.</td>
</tr>
</tbody>
</table>
Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>The fully qualified domain name (FQDN) or IP address of the target system.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>response</td>
<td>A JSON string representing the current running processes on the target machine.</td>
</tr>
<tr>
<td></td>
<td>JSON data includes:</td>
</tr>
<tr>
<td></td>
<td>pid</td>
</tr>
<tr>
<td></td>
<td>Process identifier</td>
</tr>
<tr>
<td></td>
<td>local_port</td>
</tr>
<tr>
<td></td>
<td>Local port for the network transaction</td>
</tr>
<tr>
<td></td>
<td>state</td>
</tr>
<tr>
<td></td>
<td>Status of the TCP connection.</td>
</tr>
<tr>
<td></td>
<td>Note: This field is null for UDP connections.</td>
</tr>
<tr>
<td></td>
<td>local_address</td>
</tr>
<tr>
<td></td>
<td>Local fully qualified domain name (FQDN) or IP address</td>
</tr>
<tr>
<td></td>
<td>remote_address</td>
</tr>
<tr>
<td></td>
<td>Remote fully qualified domain name (FQDN) or IP address</td>
</tr>
<tr>
<td></td>
<td>protocol</td>
</tr>
<tr>
<td></td>
<td>TCP or UDP</td>
</tr>
<tr>
<td></td>
<td>remote_port</td>
</tr>
<tr>
<td></td>
<td>Remote port of the network transaction</td>
</tr>
<tr>
<td></td>
<td>path</td>
</tr>
<tr>
<td></td>
<td>The file path of the process executable</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Output variables (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hash</td>
<td>The hash value of the process executable. The hash is in SHA-256 for PowerShell V4 or higher. Otherwise, the hash is in MD5.</td>
</tr>
</tbody>
</table>

Restrictions

The MID Server must support **PowerShell**.

SHA-256 hash requires PowerShell V4.

Get running processes via WMI activity

The **Get Running Processes** workflow activity retrieves the running processes of a configuration item on a Windows-based system. This activity can accelerate the investigation and remediation process.

The **Get Running Processes via WMI** activity can be used with any workflow to retrieve running processes on a Windows-based system.

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>The fully qualified domain name (FQDN) or IP address of the target system.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>response</td>
<td>A JSON string representing the current running processes on the target system.</td>
</tr>
</tbody>
</table>

JSON data includes:
Output variables (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pid</td>
<td>The process identifier</td>
</tr>
<tr>
<td>name</td>
<td>The name of the process</td>
</tr>
<tr>
<td>Owner</td>
<td>The name of the process owner</td>
</tr>
<tr>
<td>owner_sid</td>
<td>The system identifier of the process owner</td>
</tr>
<tr>
<td>owner_domain</td>
<td>The domain of the process owner</td>
</tr>
<tr>
<td>path</td>
<td>The file path of the process executable</td>
</tr>
<tr>
<td>hash</td>
<td>The hash value of the process executable. The hash is in SHA-256 for PowerShell V4 or higher. Otherwise, the hash is in MD5.</td>
</tr>
</tbody>
</table>

Restrictions
The MID Server must support **PowerShell**.
SHA-256 hash requires PowerShell V4.

Search/Delete Threat Email in Exchange activity
The Search/Delete Threat Email in Exchange activity performs a search for emails in the designated Exchange server(s) using the search queries defined, and returns the details.

Input variables
Input variables determine the initial behavior of the activity.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>Mandatory target host identifier field where the Exchange Server is located and the powershell script will be executed.</td>
</tr>
<tr>
<td>search_query</td>
<td>Mandatory search query used to find emails in the Exchange Server across all mailboxes.</td>
</tr>
<tr>
<td>operation</td>
<td>Operation to be executed on the Exchange server. Possible values are: • search • delete</td>
</tr>
<tr>
<td>delete_from_recovery</td>
<td>Choose to delete emails from the recovery folder on the Exchange server. Possible values are: • true • false</td>
</tr>
</tbody>
</table>

**Output variables**

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>emailCount</td>
<td>The total number of emails found during the search/delete operations for the given search query.</td>
</tr>
</tbody>
</table>

**Exit Conditions**

Possible exit conditions for this activity are:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No emails found</td>
<td>When the email count is zero, no emails were found for the given search query.</td>
</tr>
<tr>
<td>Threat emails found</td>
<td>When the email count is greater than zero, and email details were returned for the given search query.</td>
</tr>
</tbody>
</table>
Exit Conditions (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error executing at exchange</td>
<td>When an error occurred while executing the powershell script in the Exchange Server.</td>
</tr>
</tbody>
</table>

Update Task Worknotes activity

The **Security Common Orchestration - Update Task Worknotes** workflow activity updates the **Activity** section (work notes) of a task record. This is useful for logging information.

The **Update Task Worknotes** activity can be used with any workflow to update the work notes of any task record.

Input variables

Input variables determine the initial behavior of the activity.

<table>
<thead>
<tr>
<th>Input variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variable</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>task_id [string]</td>
</tr>
<tr>
<td>content [string]</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Output variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variable</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>result [string]</td>
</tr>
</tbody>
</table>

Roll up lookup info to security incident activity

The **Roll up lookup info to security incident** activity can be used with any workflow to gather information from a threat lookup and output a summary of the contents as well as the ID of the originating security incident in task work notes.
Results

Possible results for this activity are:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Lookup report summary rolled up to security incident.</td>
</tr>
<tr>
<td>Failure</td>
<td>Originating task and lookup summary report are empty.</td>
</tr>
</tbody>
</table>

Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scanID[string]</td>
<td>Lookup identifier.</td>
</tr>
</tbody>
</table>

Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>siId[string]</td>
<td>Security incident identifier.</td>
</tr>
<tr>
<td>response[string]</td>
<td>Summary of lookup results including: IoC value, Result, Failure reason, lookup reference, and so on.</td>
</tr>
</tbody>
</table>

Write content to record as attachment activity

This activity writes the content passed in from an input and creates a designated attachment to a given record.

The Write content to record as attachment activity can be used with any workflow to write content and attach it to a record.

Input variables

Input variables determine the initial behavior of the activity.
### Input variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tablename</td>
<td>The table name for the record. This input field is mandatory.</td>
</tr>
<tr>
<td>sysid</td>
<td>The system identifier (sys_id) of a task record. This input field is mandatory.</td>
</tr>
<tr>
<td>payload</td>
<td>The plain text content to be written as an attachment. This input field is mandatory.</td>
</tr>
<tr>
<td>filename</td>
<td>The attachment file name.</td>
</tr>
</tbody>
</table>

### Output variables

The output variables contain data that can be used in subsequent activities.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>Indicates whether the update was successful.</td>
</tr>
</tbody>
</table>
Index

A
activate and configure the Check Point Anti-bot - Email Parser integration
422
Activate and configure the CrowdStrike Falcon Host integration
466
activate plugin
2527
Add a security incident to a security case
183
Add affected users to existing cases
2502
Add artifacts to a case
2486
Add CIs to existing cases
2498
Add closure information to a security incident
281
Add IoCs and observables to an existing case in Threat Intelligence
2490
Add related records to a security incident
227
Add security incidents to existing cases in Security Incident Response
2495
administering trusted security circles
2527
Administrator lockdown
60
Annotate case artifacts
2510
appliance transform map
1892, 2293
Application Vulnerability Integration
CPE import
2061
Application Vulnerability Management
Assignment Rules
2079, 2081
calculator rules
2083
CI lookup rules
2075
installed with components
2100
integrations
2114
Remediation Target Rules
2090
view remediation target status
2095
Vulnerabilities
Form fields
2063
Application Vulnerability Management creates a severity map
2088
Application Vulnerability Managements create an application vulnerability calculator
2084
ci identifier rules
2076
Application Vulnerability Response
2050, 2060, 2072, 2099
Application vulnerable item
2096
assign users to user groups
2072
CI Lookup Rules
2078
configure CWE scheduled job
2060
create remediation target rules
2093
filtering rules
2089
install and configure
2056
monitor progress
2103
My Application
Vulnerabilities dashboard
2111
PA dashboard
2106
Performance Analytics
2105
user groups and roles
2069
vulnerability libraries
2062
Artifact exclusion and inclusion
2508
asset group transform map
1891, 2292
Associate a knowledge article with a playbook task
297
associated indicator types
2334
attachments as retrieveData return values
2005
Attack modes and methods
2327, 2328
attack modes/methods
2329, 2330, 2330
auto-assignment
based a selected workflow
196
based on agent ratings
197
based on location
197
based on skills
197
based on time zone
197
using group coverage areas
197
using multiple selection criteria
197
automatic
manual
security analyst assignment
196
security analyst assignment
196
security analysts assigning using a workflow
196
manually assigning
196
workflow-based
security analyst assignment
196
B
BSM map
242
C
Calculate the severity of a security incident
243
Case creation from security artifacts
2488
Case Management
2479
Cases from affected users
2500
Cases from configuration items
2496
Cases in Security Incident Response
2494
Cases in Threat Intelligence
2488
change
created from security incident
181
Change the order of workflow execution
2750
Check MID Server Status
2654
Check Point Anti-bot - Email Parser integration
422
Close security incidents
279
closure codes
279
Collect CrowdStrike Falcon Host Configurations activity
468
configuration
security incident response
56
Configuration Compliance
2128, 2129, 2131, 2158, 2210, 2212, 2214
Assignment Rules
2133
close test result group
2249
correlation
2220
create a calculator
2203
create a change request
2248
create a criticality map
1696, 2209
Create assignment rules
2182
create calculator group
2196
create test group from test results list
2188
create test result group from Test Result Groups
2184
criticality mapping
2157, 2208
discovery
2210
import issues
2219
install and activate
2168
integrations
2252
reporting
2229
technologies
2213
Test Result Group
2135
Test Results fields
2227
view test results
2225
configuration response
2168
configure for MID Server access
1229
Configure the job queue
2526
Configure the sightings threshold
2532
configure third-party integrations
2593
create groups
74
Create a case from affected users
2500
Create a case from CIs
2496
Create a case from Threat Intelligence
2488
Create a case in Case Management
2483
Create a security incident from shared observables
2540
Create a Trusted Security Circles profile
2531
Create an observable from a case
2491
Create an operating system group
2578
Create cases from security incidents in Security Incident Response
2494
Create domain-separated property overrides
2576
Create email matching rules for user-reported phishing
90
create email parsers
2556
create IoC lookup request by populating the fields
1390
Create multiple security annotations for observables
2585
Create post incident review assignment rules
267, 277
create runbook
88
Create Scan Record for Vulnerabilities activity
2050, 2760
create scan request for IoC changes workflow
1389
Create security annotations for CIs
2584
Create security annotations for users
2586
create vulnerable items
1641
CrowdStrike Falcon Intelligence
overview
2457
Security Operations integrations
2457
CrowdStrike Falcon Intelligence integration
466
custom report processor scripts
2007
customer service case
182

D
Data imported into security alerts
150
Define new on-demand orchestrations
221
Delete phishing emails
244
Disable notification-related business rules prior to initial record import
1865, 2266
Disable the default vulnerability calculator
1864, 1904, 2265
domain separation
activating plugins
2523
Domain separation for Trusted Security Circles
2521
download ServiceNow security operations application
1090
dynamic search list transform map
1889, 2290

E
Email notifications
1605
e-mail parsing
2553
e-mail properties
2552, 2553
Email Search and Delete workflow
2624
Email templates
1606
Enrich Observable WhoIs workflow
2472
enrich security incident data from threat logs on the firewall
212
Exclude case artifacts
2508
execute procDump activity
1401
Execution Tracking Begin Mail Search) activity
incident created from security incident

indicator sources

Indicators of compromise

install security operations add-on for splunk

install third-party integrations

integration

integration factory script

integration troubleshooting

invoke process dump on an enriched process on Windows

IoC data

IoCs

Join a Trusted Security Circle

knowledge

create knowledge

Lookups

Manage security incident details

Manage vulnerable items individually

manual security analyst assignment

manual search commands

manually run vulnerability integrations

Microsoft Exchange - Perform Email Search and Deletion workflow

Multi-record, custom field Splunk alert examples

multiple call integrations

multiple record Splunk alert

national vulnerability database

on-demand update

NVD and CWE data import data

NVD data feeds

NVD integration

Integrations import run status

optional modifications

overview

pre-requisites

NVD Vulnerability Integration CPE import

installation and activate
manual import
1848

O
Observable Enrichment
Lookup activity
2473
observable sources
2340
Observables
2336, 2336, 2339
on-demand orchestration
218
on-demand update
national vulnerability
database
1615
overview
2129

P
parent child relationships
231
Perform additional tasks on a
security incident
229
Perform lookups on
observables
2341
Perform on-demand
orchestration from the
Security Incident form
219
Perform on-demand
orchestration from the
Security Incident list
220
Perform threat enrichment on
observables
2343
plugins
activate
2527
policies
2131
post incident review
254
compose questions
262
perform
258
problem
created from security
incident
181
process definition
67, 69
creating
63
security incident response
63
Publish to Watchlist activity
469

Q
Qualys
create host detection
import domain separation
1860, 2261
Qualys REST messages
1893, 2294
Qualys transformation
1889, 2290
Qualys Vulnerability
Integration
1865, 1889, 1889, 1890, 1891,
1892, 2266, 2290, 2290, 2291,
2292, 2293
advanced configurations
and modifications
1866, 2267
attachments not appearing
1882, 2283
check XML attachment
property size
1883, 2284
custom outbound REST
message
2009
data retrieval limitations
1884, 2285
install
1858, 2259
integration run status
1713
modify Qualys to
ServiceNOw priority and
state mappings
1866, 2267
modify transform maps
1883, 2284
optional configurations and
modifications
1859, 2261
outbound REST message
1870, 2271
overview
1884, 2285
Qualys scanner
1870, 2271
Qualys Vulnerability
Integration troubleshooting
1882, 2283
restrict write to record
1867, 2268
setup scanner appliances
1868, 2269
Questionnaires
create categories
260

R
Rapid7 Vulnerability
Integration
create host detection
import domain separation
1915
install and activate
1904
integration run status
1886, 1920, 2287
overview
1897
pre-requisites
1903
record deduplication
1919
rate scanners
scan rate limits applied to
1881, 2282
record creation form a
security incident
181
Register new Security
Operations applications
223
Register the Trusted Security
Circles central instance for
each domain
2525
Register the Trusted Security
Circles client to the central
instance
2528
related attack modes/
methods
2334
Related details for case
artifacts
2503
related IoC
2338
related observables
2333, 2339
Repair security incident SLAs
87
response tasks
create
185
REST APIs for third-party
integration with Security
Operations
2614
Restricted Caller Access
61
Return excluded artifacts to a
case
2509
risk score weights
85
Run a sightings search
2492
run default lookup sources
2479
run lookup workflow 2475
run procdump 1399
runbook 88, 241

S
scan rate limits
applied to scanners 1881, 2282
scan vulnerability workflow 2045, 2758
scan vulnerability item workflow 2048, 2760
scan vulnerability workflow 2043
scan vulnerable items workflow 2046
scanning vulnerable items 1879, 2280
scans 214
scans of vulnerabilities or vulnerable items 1872, 2273
scheduled jobs
Application Vulnerability Response 2050, 2060, 2072, 2099
configure NVD update 1612, 2060
Vulnerability Response 1450, 1452, 1482, 1612
script include 69
Search for security artifacts 2512
search security incidents 2587
Search/Delete Threat Email in Exchange activity 845, 2769
security analyst assignment manual 196
security analysts assigning 196
assigning using a workflow 196
automatically assigning 196
manually assigning 196
Security artifact analysis 2503
security event 1092
security groups 2579
security incident 1093
creating from forms 140
Escalate 253
lookup attachments 215
Security Incident - Confidential Data Exposure - Template 1403
Security Incident - Denial of Service - Template 1405
Security Incident - Lost Equipment - Template 1408
Security Incident - Malicious Software - Template 1410
Security Incident - Phishing - Template 1413
Security Incident - Policy Violation - Template 1416
Security Incident - Reconnaissance - Template
1418
Security Incident - Rogue Server or Service - Template
1420
Security Incident - Spam - Template
1422
Security Incident - Unauthorized Access - Template
1424
Security Incident - Web/BBS Defacement - Template
1426
security incident analysis
41
security incident calculator groups
75
security incident calculators
75, 78
security incident catalog
submit lookup requests
215
submit scan requests
217
Security Incident Catalog
145
Security Incident Confidential Data Exposure flow template
1430
security incident creation
139
Security Incident Denial of Service flow template
1431
Security Incident Lost Equipment flow template
1434
Security Incident Malicious Software flow template
1435
security incident orchestration
1387
Security Incident Phishing flow template
1437
Security Incident Policy Violation flow template
1439
Security Incident Reconnaissance flow template
1441
security incident response
182, 231, 240
correct invalid state
73
process definition
64
process selection
66
Security Incident Response
217
access explorer
357
add security incident map
363
modify security incident map
363
monitoring
357
overview
358
security incident map
362
Security Incident Response flows and flow templates
1429
security incident response lost equipment workflow templates
1408
security incident response observables
202
Security Operations Integration - CI Enrichment workflow 2629
Security Operations Integration - Enrich CI capability 2628
Security Operations Integration - Enrich Observable capability 2633
Security Operations Integration - Enrich Observable workflow 2634
Security Operations Integration - Threat Lookup workflow 2747
Security Operations Integration - Threat Lookups capability 2746
security operations integration capabilities
block request 2621
  run block request 2621
get network statistics 2636
get running processes 2646
isolate host 2681
  run isolate host 2681
isolate host or endpoint 2681
publish to watchlist 2697
  run publish to watchlist 213
sightings search 2702
configuration 310, 2702
run sighting search 2533, 2705
Security Operations Integration Reference 2588
security operations integration workflow activities
capability - determine CIs 2637, 2648, 2683
capability execution tracking - no impls 2627, 2632, 2635, 2641, 2650, 2685, 2701, 2713, 2722, 2749
check session status 2658
close session 2663
collect arcsight configuration 2716
collect carbon black configuration 2653, 2688, 2693
collect elasticsearch configurations 2721
collect McAfee configurations 2726
collect QRadar configurations 2731
collect splunk configurations 2735
combine results 2680
create command process 2659, 2660
create session 2657
determine observables 2698
determine shell script by os
1396, 2676
elasticsearch event query
2723
enrichment data map
2571
execute shell script
2679
execution tracking - begin
cis
2638
extract shell script from mid script
2678
filter allowed observables
2623, 2699, 2711
get IP from CI
2652, 2666, 2687, 2693
get observable sightings queries
2714
get running processes via powershell
2677
get sensor ID
2655, 2689, 2694
get supported security capabilities
2626, 2631, 2634, 2640, 2649, 2684, 2700, 2712, 2748
HPE Security ArcSight event query
2718
map processes data
2662
McAfee ESM event query
2728
persist observable sightings
2719, 2724, 2729, 2734, 2738
QRadar event query
2732
set network isolatation enabled
2690, 2695
sightings search - determine observables
2710
splunk event query
2737
tanium build get processes request
2667
tanium get result data from response
1239, 1246, 2673
update sensor
2691, 2696
security operations integration workflows
arcsight logger sightings search
2715
block request
2622
carbon black - get running processes
2651
carbon black - isolate host or endpoint
2686
carbon black - remove host isolation
2692
elasticsearch sightings search
2720
get network statistics
2636
get running processes
2647
isolate host
2682
mcAfee esm sightings search
2725
palo alto networks firewall launcher
922
QRadar sightings search
sighting search
splunk sightings search
system command - get running processes
tanium get running processes
Security Operations integrations
Carbon Black
CrowdStrike Falcon Intelligence
CrowdStrike Falcon Intelligence
activate and configure
Elasticsearch - Incident Enrichment
activate and configure
Have I been pwned?
activate and configure
setup
HPE ArcSight Logger - Incident Enrichment
activate and configure
IBM QRadar
activate and configure
McAfee ESM - Incident Enrichment
activate and configure
OPSWAT Metadefender
activate and configure
setup
Palo Alto Networks AutoFocus
activate and configure
workflow activities
AutoFocus search session
fetch search results
workflows
check and block value
get AutoFocus session info enrichment workflow
Firewall activate and configure
setup
MID Server setup
workflow activities
block request status
block value
blocked status
get API Key
get Firewall config
927, 931
get job data action
933
refresh EDL
928
workflows
get threat log data from the firewall to enrich security incident observables
929
WildFire
setup
936
workflow activities
get PCAP
939
get PDF
940
workflows
get WildFire data enrichment
937
Recorded Future
2465
activate and configure
2466
Splunk - Incident Enrichment
1224
activate and configure
1224
Splunk Add-on
1090
Tanium
1226
activate and configure
1227
setup
1227
VirusTotal
2467
activate and configure
2468
setup
2468
WhoisXML API
2470
activate and configure
2471
setup
2471
Security Operations Integrations - Email Search and Delete capability
2624
security operations integrations workflows publish to watchlist
2697
security operations orchestration
2758
Security Operations unmatched email view and process
2564
Security Support Common
244
installed components
2587
security tags
2579
set up or change the instance
1091
setting up Threat Intelligence
2305
setup
2474
Share an observable from a security incident to a Trusted Security Circle
2744
Share an observable from Threat Intelligence
2538
Share Sightings Search results
2536, 2742
Shodan Exploit Integration manual import
1929 overview
1924 set import time
1929
Shodan Vulnerability Integration
install

1924
Show affected items for a security incident
234
Show enrichment data for a security incident
237
Show IoC information for a security incident
203
Show related items for a security incident
235
Show response task information for a security incident
238
single call integrations
2003
SLA definition
create
86, 1706
solution
112
Solution Management for Vulnerability Response
install
1563
splunk alerts
1094
Splunk error reporting
1096
splunk event actions
1094
start date
1865, 2266
states
1482, 2072, 2158
static search list transform map
1890, 2291
T
Tanium - Get File Details workflow
1230
Tanium - Get running processes workflow
1240
Tanium: Build Check if Done Request activity
1236, 1243, 2669
Tanium: Build Get Result Data Request activity
1238, 1244, 2671
Tanium: Build Get Sensor ID Request activity
1231
Tanium: Build Get-Processes Request activity
1242
Tanium: Determine if done from Response activity
1237, 1244, 2671
Tanium: Execute Request activity
1232, 1233, 1234, 1236, 1238, 1245, 2668, 2670, 2672
Tanium: Get Question ID from Response activity
1235, 1246, 2669
Tanium: Get Sensor ID From Response activity
1234
Tenable Vulnerability Integration
create import domain separation
1994
third-party alert monitoring tools
149
Third-party integrations
third-party vulnerability integration
threat intelligence
Threat Intelligence
set up
Threat Intelligence administration
Threat Intelligence integration with OPSWAT Metadefender
threat intelligence orchestration
Threat Intelligence properties
threat intelligence response workflow activities
roll up lookup info to security incident activity
update security incident with lookup results
Threat Intelligence Sharing installed components tables
threat intelligence workflows and activities
threat lookup submit from catalog
submit from security incident
Threat Lookup - CrowdStrike Falcon Intelligence workflow
Threat Lookup - Have I been pwned? workflow
Threat Lookup - OPSWAT Metadefender workflow
Threat Lookup - Recorded Future workflow
Threat Lookup - VirusTotal workflow
Threat sources
tips for writing integrations
treemap categories
treemaps
category indicators
configure
Trusted Security Circle trusted security circle messages
Trusted Security Circle properties
trusted security circles set up
Trusted Security Circles activate installed components roles messages
Trusted Security Circles and Threat Intelligence sharing guidelines

untrusted third-party SSL certificate
expired third-party SSL certificate
update observable with lookup result
update task work notes

Veracode Application Vulnerability Integration prerequisites
Veracode Vulnerability Integration create import domain separation
install and activate
installation and activate
Integrations import run status
manual import
optional modifications
overview
set import time
view a policy
view authoritative sources

View related details for a configuration item artifact
View related details for a security incident artifact
View related details for an affected user artifact
View related details for an IoC artifact
View related details for an observable artifact
view runbook

View Security Incident Response Orchestration workflow templates
View Security Incident Response Orchestration workflows
view tests
vulnerability calculator groups
vulnerability charts
vulnerability integration
Push data using a REST API endpoint
Vulnerability integration configured to use REST API
vulnerability integration script
vulnerability integrations
Vulnerability Response
1450, 1452, 1482, 1612
Assignment Rules
1464
close vulnerability group
1820
defer a vulnerability group
1819
defer a vulnerable item
1650
Discovered Items
  Form fields
  1478
filtering rules
  1695
homepage
  1773
install and activate
  1539, 1591
limit scan rates
  1880, 2281
mobile application
  2010
monitor remediation progress
  1771
Qualys Vulnerability Integration
  1851, 2252
Setup
  Additional tasks
  1598
Solutions
  exclude CVEs
  1703
Unmatched CIs
  manually reclassify
  1689
Vulnerabilities
  Form fields
  1620
Vulnerability Group
  1466
Vulnerability Groups
  Form fields
  1666
Vulnerability Solution Management
  1506
    Create a solution
    1697
    Solution fields
    1699
    View a solution
    1724
Vulnerability Response email templates
  1606
Vulnerability Response group
  1671
vulnerability response orchestration
  2043
Vulnerability Response orchestration workflow activities
  2049
Vulnerability Response orchestration workflows
  2043
vulnerability scan
  Security Incident Response
  217
  submit from catalog
  217
vulnerability scan requests queue
  1875, 2276
vulnerability scans
  1869, 2270
vulnerable items
  1641
Wildfire workflow activities
  941
workflow triggers
  Security Operations
  2755
workflow-based
security analyst
assignment
196
Write content to record as
attachment activity
917, 934, 942, 2772
write integrations
2588