Integrate RevealX 360 with Splunk Enterprise Security SIEM

Published: 2025-02-19

This integration enables the Splunk Enterprise Security SIEM to export detection data from the ExtraHop system through detection notification rules. You can view exported data in the SIEM to gain insight into security threats in your environment and to accelerate response times.

This integration requires you to complete two tasks. An ExtraHop administrator must configure the connection between the SIEM and the ExtraHop system. After the connection is established, you can create detection notification rules that will send webhook data to the SIEM.

After the connection is established and notification rules are configured, you can install the ExtraHop RevealX App for Splunk on your Splunk SIEM. The app provides a dashboard of detection data and correlation rules that generate detection alerts in Splunk.

Before you begin

You must meet the following system requirements:

- ExtraHop RevealX 360
  - Your user account must have privileges on RevealX 360 for System and Access Administration.
  - Your RevealX 360 system must be connected to an ExtraHop sensor with firmware version 9.8 or later.
  - Your RevealX 360 system must be connected to ExtraHop Cloud Services.
- Splunk
  - You must have Splunk Enterprise version 9.1 or later
  - You must configure a Splunk Enterprise HEC connector for data ingest.
  - Your SIEM must be able to receive webhook data. You can add static source IP addresses to your security controls to allow requests from RevealX 360.

1. Log in to RevealX 360.
2. Click the System Settings icon and then click **Integrations**.
3. Click the **Splunk Enterprise Security (SIEM)** tile.
4. Complete the following steps to configure the connection between the Splunk Enterprise Security SIEM and the ExtraHop system:
   a) In the **Ingest Host** field, type the URL or hostname of the SIEM server that will receive webhook data.
   b) In the **Ingest Port** field, type the port number that will receive webhook data.
   c) In the **Index** field, type the name of the index that will store the webhook data.
   d) In the **HEC Token** field, type the token that will authenticate the connection to the ingest host.
5. Select one of the following connection options:

Option	Description
Direct Connection	Select this option to configure a direct connection from this RevealX 360 console to the provided URL.
Proxy through a connected sensor	Select this option if your SIEM cannot support a direct connection from this RevealX 360 console due to firewalls or other security controls. 1. From the drop-down menu, select a connected sensor to act as the proxy.

Option	Description
	2. (Optional): Select **Connect through the global proxy server configured for the selected sensor** to send data through a global proxy. (Only available if the selected sensor is running RevealX Enterprise.

6. Click **Send Test Event** to establish a connection between the ExtraHop system and the SIEM server and to send a test message to the server.

   A message is displayed that indicates whether the connection succeeded or failed. If the test fails, edit the configuration and test the connection again.
7. Optional: Select **Skip server certificate verification** to bypass verification of the SIEM server certificate.
8. Click **Save**.

Create a detection notification rule for a SIEM integration

Before you begin

- Your user account must have NDR module access to create security detection notification rules.
- Your user account must have NPM module access to create performance detection notification rules.
- You can also create detection notification rules from System Settings. For more information, see Create a detection notification rule.

1. Log in to RevealX 360.
2. Click the System Settings icon and then click **Integrations**.
3. Click the tile for the SIEM that will be the target of the detection notification rule.
4. Click **Add Notification Rule**.
   The Create Notification Rule window opens in a new tab and the following fields are set to default values.
   - The **Name** field is set to the name of the SIEM.
   - The **Event Type** field is set to **Security Detection**.
   - The **Target** field is set to the SIEM integration.
5. In the Description field, add information about the notification rule.
6. In the Criteria section, click **Add Criteria** to specify criteria that will generate a notification.
   - **Recommended for Triage**
   - **Minimum Risk Score**
   - **Type**
   - **Category**
   - **MITRE Technique** (NDR only)
   - **Offender**
   - **Victim**
   - **Device Role**
   - **Participant**
   - **Site**

   The criteria options match the filtering options on the Detections page.
7. Under Payload Options, select if you want to send the default payload or type in a custom JSON payload.
   - **Default payload**

     Populate the webhook payload with a core set of detection fields.

From the Add Payload Fields drop-down menu, you can click additional fields that you want to include in the payload.

- **Custom payload**

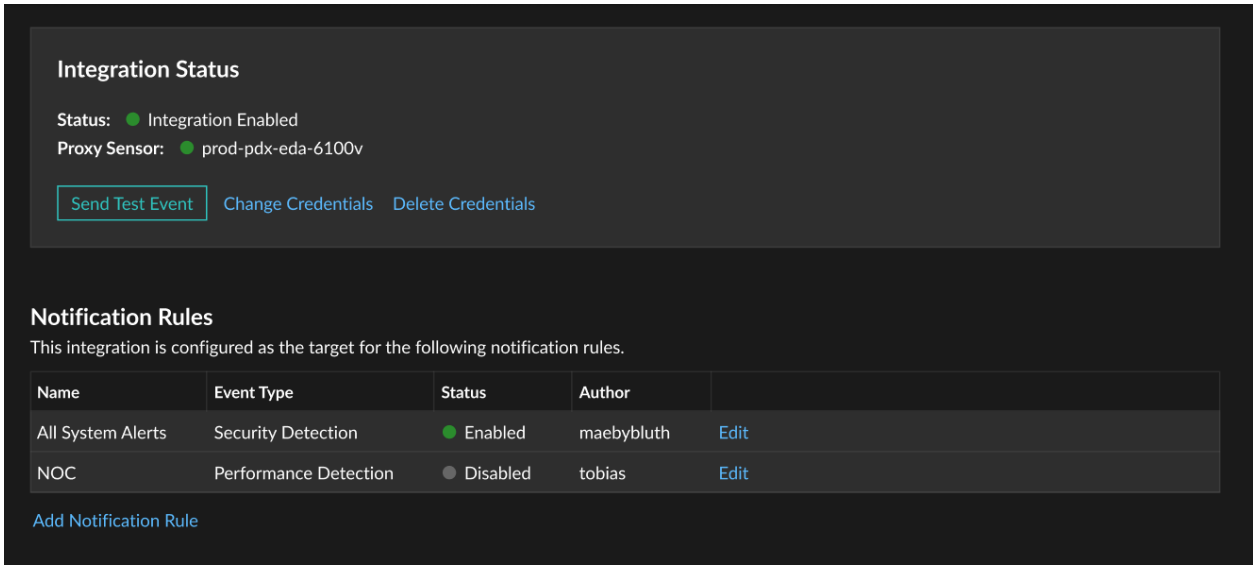
  Populate the webhook payload with custom JSON.

  You can edit the suggested custom payload in the **Edit Payload** window.

8. Click **Test Connection**.
   A message titled Test Notification will be sent to confirm the connection.
9. In the Options section, the **Enable notification rule** checkbox is enabled by default. Deselect the checkbox to disable the notification rule.
10. Click **Save**.

Next steps

- Navigate back to the integration configuration page to check that your rule has been created and added to the table.
- Click **Edit** to modify or delete a rule.



Install the ExtraHop RevealX App for Splunk

The ExtraHop RevealX App for Splunk receives ExtraHop RevealX detection data from the Splunk event collector to build a detection dashboard and to generate detection event alerts in Splunk based on correlation rules.

1. Download the ExtraHop RevealX App for Splunk from Splunkbase.
2. Log in to your Splunk SIEM.
3. From the **Apps** drop-down list, click **Manage Apps** .
4. From the upper right corner, click **Install the app from file**.
5. Click **Choose File**, and then select the downloaded app.
6. Click **Upload** and follow the prompts.
7. From the **Apps** drop-down list, click **ExtraHop RevealX App for Splunk** to open the app in your Splunk SIEM.
   The ExtraHop Detections Overview dashboard is displayed by default and contains the following charts:

Chart	Description
Recommended Detections	Displays the total number of recommended detections generated during the selected time period.
Total Detections	Displays the number of detections generated during the selected time period.
Maximum Risk Score	Displays the highest risk score associated with detections generated during the selected time period.
Top Recommended Detections	Displays the top 10 recommended detections generated during the selected time period and the number of times each detection occurred.
Top Detection Categories	Displays the top 10 detection categories associated with detections generated during the selected time period and the percentage and number of detections for each category.
Top MITRE Techniques	Displays the top 10 MITRE techniques associated with detections generated during the selected time period and the number of detections for each technique.
Top Sources	Displays the top 10 source hosts associated with detections generated during the selected time period and the number of detections for each source.
Top Destinations	Displays the top 10 destination hosts associated with detections generated during the selected time period and the number of detections for each destination.
Sources and Destinations	Displays the flow of sources and destinations associated with detections generated during the selected time period.
Recent Detections	Displays the most recent detections generated during the selected time period and detection details such as risk score, category, and URL

8. Complete the following steps to view the correlation rules provided in the app:
   a) From the **Settings** drop-down list, click **Searches, reports, and alerts**.
   b) From the **Owners** drop-down list, click **All**

      The table displays the following correlations rules that are enabled by default:

      - Low severity alerts are generated for detections with a risk score from 1 to 30.
      - Medium severity alerts are generated for detections with a risk score from 31 to 79.
      - High severity alerts are generated for detections with a risk score from 80 to 99.
9. From the **Activity** drop-down list, click **Triggered Alerts** to view alerts generated from the correlation rules.