Integrate RevealX Enterprise with Splunk Enterprise Security SIEM

Published: 2025-04-08

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.

To configure this integration, you establish a connection between the SIEM and the ExtraHop system, and you create detection notification rules that send webhook data to the SIEM. Integrating the ExtraHop system with Splunk Enterprise Security SIEM is supported on both RevealX 360 and RevealX Enterprise.

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 Enterprise
  - You must log in on a console running firmware version 9.8 or later.
  - Your user account must have Full Write privileges.
  - 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.
  - Your ExtraHop system must be connected to ExtraHop Cloud Services.
- Splunk SIEM
  - 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 over TCP 443 (HTTPS).

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click the System Settings icon and then click **Notification Rules**.
3. Click one of the following options:
   - For NDR modules, select **Security Detection**.
   - For NPM modules, select **Performance Detection**.
4. In the Name field, type a unique name for the notification rule.
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. From the **Target** drop-down list, select **Custom Webhook**.
8. In the Payload URL field, type the URL or hostname of the SIEM server that will receive webhook data.

   The URL must include the port number, similar to the following example:
   `https://192.0.2.0:8088/services/collector/event`
9. Click **Show Advanced Connection Options** and configure the following settings:
   a) In the Custom Headers section, click **Add Header** and specify the following custom `key:value` pair:
      - In the **Key** field, type `Authorization`.
      - In the **Value** field, type `SPLUNK <HEC token>` where `<HEC token>` is the value of the token that will authenticate the connection to the SIEM.

      This key and value will be added to the header of the webhook HTTP POST request.
   b) Select an authentication type.
      - No Authentication
      - Basic Authentication

        Enter the username and password for the target application.
      - Bearer Token

        Enter the access token for the target application.
   c) Configure the connection method.
      - Direct Connection
        - Select to route the webhook through a configured global proxy. (RevealX Enterprise only.)
        - Select to skip server certificate verification.
      - Proxy through a connected sensor
        - Select the proxy sensor.
        - Select to skip server certificate verification.
        - Select to route the webhook through a global proxy that is configured for the selected sensor.
10. Under Notification Behavior, select **Send for every detection update** to receive a notification every time the detection is updated, which is recommended for comprehensive visibility into detection activity when exporting detection data to a SIEM.
11. Under Payload Options, select Custom Payload to populate the webhook payload with custom JSON.
    a) In the Edit Payload window, add the following required fields and values to the payload:

```
{
"time": {{time / 1000}},
"event": {{base | safe}},
"index": "main",
"sourcetype": "extrahop-rx360-detection"
}
```

    Replace "`main`" with the name of the index that will store the webhook data.
    b) Edit the remaining fields that you want to include in the payload
12. In the Options section, the **Enable notification rule** checkbox is enabled by default. Deselect the checkbox to disable the notification rule.
13. Click **Save**.

Next steps

- Check that your rule has been created and added to the Notification Rules table.
- Click a rule name from the table to modify or delete that rule.
- Install the ExtraHop RevealX App for Splunk to view a detections dashboard and alerts.

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.

Chart	Description
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.