Integrate RevealX 360 with CrowdStrike Falcon Next-Gen SIEM

Published: 2025-02-14

This integration enables CrowdStrike Falcon Next-Gen SIEM to export device and detection data from the ExtraHop system through detection notification rules. You can view exported data in the SIEM to gain insight into how your devices are communicating in your environment and to view network threat detections.

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.

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 ⧉.

- CrowdStrike

    - You must have CrowdStrike Falcon Next-Gen SIEM version 1.0 or later.
    - You must configure a CrowdStrike Falcon Next-Gen SIEM HEC connector ⧉ for data ingest and set the following field values:

        - Data Type: JSON
        - Parsers: json-for-action

    - You must generate and copy an API URL and an API key from the HEC connector.
    - 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 **CrowdStrike Falcon Next-Gen SIEM** tile.
4. Enter the following information that you generated and copied from the CrowdStrike HEC connector:
    a) In the **API URL** field, type the URL that will receive webhook data.
    b) In the **API Key** field, type the key that will authenticate the connection to the URL.
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. 2. (Optional): Select **Connect through the global proxy server configured for the selected**

Option	Description
	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.

Integration Status

Status: ● Integration Enabled
Proxy Sensor: ● prod-pdx-eda-6100v

[Send Test Event]   Change Credentials   Delete Credentials

Notification Rules
This integration is configured as the target for the following notification rules.

Name	Event Type	Status	Author	
All System Alerts	Security Detection	● Enabled	maebybluth	Edit
NOC	Performance Detection	● Disabled	tobias	Edit

Add Notification Rule