Integrate RevealX Enterprise with CrowdStrike Falcon Next-Gen SIEM

Published: 2025-05-18

This integration enables the CrowdStrike Falcon Next-Gen 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 accelerate response times.

To configure this integration, you must provide information to establish a connection between the SIEM and the ExtraHop system, and you must create detection notification rules that send webhook data to the SIEM. Integrating the ExtraHop system with CrowdStrike Falcon Next-Gen SIEM is supported on both RevealX 360 and RevealX Enterprise.

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 RevealX 360 system must be connected to ExtraHop Cloud Services.
  - 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.
- CrowdStrike Falcon
  - You must have CrowdStrike Falcon Next-Gen SIEM version 1.0 or later.
  - You must have a CrowdStrike subscription for Falcon Next-Gen SIEM or Falcon Next-Gen SIEM 10GB.
  - You must have Administrator access to the CrowdStrike Falcon console.
  - 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.
  - From the CrowdStrike Falcon console, you must go to the Data Connectors page to add and configure the "HEC/HTTP Event Connector". This is a generic CrowdStrike connector that you can filter for by name.
    - You must select **JSON** as the data type.
    - You must select **extrahop-revealx360 (Extrahop Revealx360)** as the parser.
    - You must generate and copy an API URL and an API key for the HEC/HTTP Event Connector.

    It might take several minutes for the data connector to become active.

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 **Create**.
4. Click one of the following options:
   - For NDR modules, select **Security Detection**.
   - For NPM modules, select **Performance Detection**.
5. In the Name field, type a unique name for the notification rule.
6. In the Description field, add information about the notification rule.
7. 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.

8. From the Target drop-down list, select **Custom Webhook**.
9. In the Payload URL field, type the URL that you generated for the data connector in the CrowdStrike Falcon console.

   This URL will receive webhook data and is similar to the following example: `https://ca4cbf14318146c5911ee7507a2ab854.ingest.us-2.crowdstrike.com/services/collector`
10. Click **Show Advanced Connection Options**.
11. From the Authentication section, click **Bearer Token** and then enter the API key that you generated for the HEC/HTTP Event Connector in the CrowdStrike Falcon console.
12. From the Connection Method section, select one of the following methods:

Option	Description
Direct Connection	Select this option to configure a direct connection from this RevealX console to the provided URL. • (Optional): Select to route the webhook through a configured global proxy. • (Optional): Select to skip server certificate verification.
Proxy through a connected sensor	Select this option if your SIEM cannot support a direct connection from this RevealX 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 to skip server certificate verification. 3. (Optional): Select to send data through the global proxy configured on the selected sensor.

13. 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.
14. Under Payload Options, select **Custom Payload** to populate the webhook payload with custom JSON.
15. In the Edit Payload window, add the following required fields and values to the payload:

```
{
"time": {{time / 1000}},
"sourcetype": "extrahop-rx360-detection",
"event": {{ dict(base, **{'sourcetype': 'extrahop-rx360-detection'}) |
 safe}}
}
```

16. Edit the remaining fields that you want to include in the payload.

17. Click **Send Test Payload**.

    A message titled Test Notification will be sent to the Payload URL to confirm the connection.

    Note: After testing the connection, confirm that you received the notification in the target application. RevealX Enterprise displays an error message if the test notification was not successful.

18. In the Options section, the **Enable notification rule** checkbox is enabled by default. Deselect the checkbox to disable the notification rule.
19. 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.