Integrate RevealX Enterprise with Google Security Operations SIEM

Published: 2025-06-11

This integration enables Google Security Operation (SecOps) 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 will provide information to establish a connection between your Google SecOps SIEM and the ExtraHop system, and you will create detection notification rules that will send webhook data to the SIEM. Integrating the ExtraHop system with Google SecOps SIEM is supported on both RevealX 360 and RevealX Enterprise.

After the connection is established and notification rules are configured, you can view Extrahop detection data from your Google SecOps SIEM in a dashboard and in alerts generated by rules that correlate to detection risk scores.

Before you begin

You must meet the following system requirements:

- ExtraHop RevealX Enterprise
  - You must log in on a console running firmware version 9.8.6 or later.
  - Your user account must have Full Write privileges.
  - Your RevealX 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.
- Google Security Operations SIEM
  - You must have a Google SecOps SIEM instance.
  - You must create an HTTPS webhook feed in Google SecOps SIEM that will receive ExtraHop RevealX detection data.
  - Copy and the save the following information that is generated when you create the ExtraHop RevealX webhook feed:
    - Secret key
    - Endpoint URL
    - API key

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, enter the endpoint URL that you generated from the ExtraHop RevealX webhook feed.

   This URL will receive webhook data and is similar to the following example:

   ```
   https://{region}-chronicle.googleapis.com/v1alpha/projects/{project}/
   locations/{location}/instances/{instance}/feeds/{feed}:importPushLogs
   ```

10. Click **Show Advanced Connection Options**.
11. In the Custom Headers section, click **Add Header** and specify the following custom key:value pair:
    a) In the **Key** field, type `X-goog-api-key`.
    b) In the **Value** field, type the API key that you generated from the ExtraHop RevealX webhook feed.
12. Click **Add Header** and specify the following custom key:value pair:
    a) In the **Key** field, type `X-Webhook-Access-Key`.
    b) In the **Value** field, type the secret key that you generated from the ExtraHop RevealX webhook feed.
13. From the Authentication section, select one of the following authentication types:

Option	Description
No Authentication	Select this option if you do not want to require credentials to access the target application.
Basic Authentication	Select this option to specify the user and password required to access the target application.
Bearer Token	Select this option to specify the bearer token required to access the target application.

14. 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.

Option	Description
	3. (Optional): Select to send data through the global proxy configured on the selected sensor.

15. 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.
16. Under Payload Options, select **Custom Payload** to populate the webhook payload with custom JSON.
17. Optional: From the **Add Payload Fields** drop-down menu, click additional fields that you want to include in the payload.
18. 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.
19. In the Options section, the **Enable notification rule** checkbox is enabled by default. Deselect the checkbox to disable the notification rule.
20. 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.

View ExtraHop detection data in Google Security Operations SIEM

ExtraHop provides access to a GitHub repository that contains files that you can import into Google SecOps SIEM to install a dashboard of ExtraHop detections and alert rules based on detection risk scores. After detection data is received by your Google SecOps SIEM, you can view the detections dashboard and the rules that will generate alerts from your SIEM.

Before you begin
You must import the dashboard and rule files from the ExtraHop GitHub repository to Google SecOps SIEM:

- Download the ExtraHop RevealX.json file and import the file as a dashboard.
- Copy the code from the rules file and paste the code into a new rule.

1. Log into your Google Security Operations SIEM.
2. Complete the following steps to view the detections dashboard:
   a) From the navigation panel, click **Dashboards & Reports** > **Native Dashboards**.
   b) From the dashboard list, click **ExtraHop RevealX Dashboard**.

   The dashboard displays the following charts:

Chart	Description
Recommended Detection Events	Displays the total number of recommended detections generated during the selected time period.
Total Detection Events	Displays the number of detections generated during the selected time period.

Chart	Description
Maximum Risk Score	Displays the highest risk score associated with detections generated during the selected time period.
Top Recommended Detection Events	Displays the top 10 recommended detections generated during the selected time period and the number of times each detection occurred.
Top 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 IP Map	Displays the geolocations of source IP addresses associated with detections generated during the selected time period.
Destination IP Map	Displays the geolocations of destination IP addresses associated with detections generated during the selected time period.
Recent Detection Events	Displays the most recent detections generated during the selected time period and detection details such as risk score, category, and URL

3. Complete the following steps to view alert rules:
   a) Click **Detection** from the menu icon.
   b) Click the **Rules & Detections** tab.
      The Rules Dashboard displays the following rules:
      - Low Severity generates an offense for detections recommended for triage with a risk score between 1 and 30.
      - Medium Severity generates an offense for detections recommended for triage with a risk score between 31 and 79.
      - High Severity generates an offense for detections recommended for triage with a risk score between 80 and 99.
   c) Hover over a rule and click the menu icon to the right to change rule settings.