EXTRAHOP

ExtraHop RevealX and Google SecOps SIEM Integration User Guide

v1.0.0

Table of Contents

Table of Contents **2**
Overview **3**
Google SecOps SIEM Platform 3
ExtraHop RevealX Platform 3
Google SecOps Integration for ExtraHop RevealX 3
Prerequisites **3**
Ingest data from ExtraHop RevealX into Google SecOps SIEM **4**
Configure a WebHook Feed in Google SecOps 4
Step 1: Create an HTTPS webhook feed 4
Step 2: Create an API key for the webhook feed 5
Configure a SIEM Connection and Webhooks 6
View Parsed Logs in SecOps SIEM **7**
Mappings **7**
Dashboards **11**
Import a Dashboard into Google SecOps SIEM 11
ExtraHop RevealX Dashboard 12
Create Correlation Rules for Detections and Alerts **16**
Create a new correlation rule 16
Limitations **16**
Troubleshooting **17**
Events are successfully ingested but not displayed in search results 17
Dashboard is not updated 17

Overview

This document contains instructions for ingesting ExtraHop RevealX detection data into a Google SecOps SIEM through webhooks, viewing detection dashboards, and creating correlation rules.

Google SecOps SIEM Platform

Google SecOps SIEM is a cybersecurity telemetry platform for threat hunting and threat intelligence and is part of the Google Cloud Platform. This platform stores log events it receives in either the original raw log or in a structured Unified Data Model (UDM) log. The Unified Data Model (UDM) defines the schema for parsing and Configuration Based Normalizers (CBN) describe how to log data that is transformed to the UDM schema.

ExtraHop RevealX Platform

ExtraHop RevealX helps organizations by providing a comprehensive network detection and response solution for tracking security threats and IT operations.

You can understand and secure your environment by analyzing all network interactions in real time and by leveraging machine learning to identify threats, deliver critical applications, and secure investments in the hybrid cloud.You can also monitor how applications consume network resources, how systems and devices communicate, and how transactions flow across the data link layer (L2) to the application layer (L7) in your network.

Google SecOps Integration for ExtraHop RevealX

This integration enables Google SecOps SIEM to receive real-time detection data from ExtraHop RevealX through HTTP webhooks, which enrich threat detection and response capabilities with comprehensive network data.

Prerequisites

Google SecOps

- Google SecOps SIEM instance and permissions to create a new feed.
- API Key credentials of the Google Cloud Platform on which Google SecOps SIEM instance is hosted.
- Access to an ExtraHop RevealX instance to ingest data into Google SecOps SIEM.

ExtraHop RevealX 360

- System and Access Administration privileges
- NDR module access
- ExtraHop RevealX sensor with firmware version 9.9 or later
- Connection to ExtraHop Cloud Services

Ingest data from ExtraHop RevealX into Google SecOps SIEM

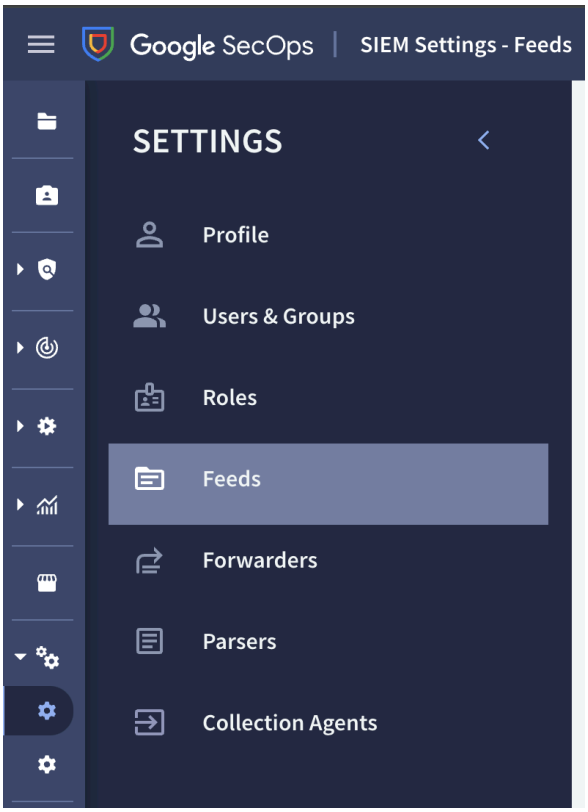
Complete the following steps to ingest data from ExtraHop RevealX into Google SecOps SIEM:

1. Configure an HTTPS webhook feed in Google SecOps SIEM to receive detection data.
2. Configure a connection to Google SecOps SIEM and specify webhook payload criteria from RevealX

Configure a WebHook Feed in Google SecOps

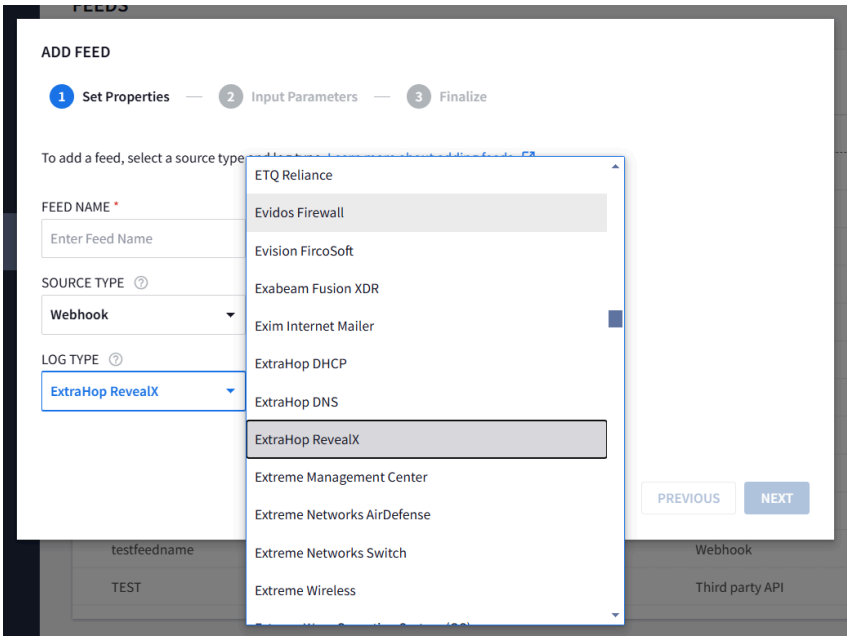
Step 1: Create an HTTPS webhook feed

1. In **Google SecOps**, go to **SIEM Settings > Feeds**.



Google SecOps: SIEM Settings

2. Click **Add New**.



Google SecOps: Add Feed

3. Type a **Feed Name**.
4. Select **Webhook** from the **Source Type** list
5. Select **ExtraHop RevealX** from the Log type list and then click **Next**.
6. Select the default input parameter values and then click **Next**.
7. Click **Submit**.
8. Click **Generate Secret Key** and then copy and store the key, which can only be viewed once.
9. From the **Details** tab, copy and save the field endpoint URL from the **Endpoint Information** field.
10. Click **Done.**

For more information, see Setup Feed of type - HTTPS Webhook.

Step 2: Create an API key for the webhook feed

An API key for the Google Cloud Platform is required to ingest events into Google SecOps SIEM through webhooks.

1. From the Google Cloud console, go to the Credentials page.
2. Click **Create Credentials**, and then select **API Key**.
3. Click **Restrict Key** to limit API key access to Google SecOps SIEM API.
4. Click **Copy** to copy and save the generated API key.

For more information, see Create API Keys in GCP and restrict access.

Configure a SIEM Connection and Webhooks

From your ExtraHop system, configure the Google SecOps SIEM integration to establish a connection between the SIEM and ExtraHop RevealX. After the connection is established, you can create detection notification rules that will send webhook data to Google SecOps SIEM.

Go to Integrate RevealX 360 with Google SecOps SIEM for instructions.

View Parsed Logs in Google SecOps SIEM

Complete the following steps to view ingested, parsed logs in Google SecOps SIEM:

1. In the Google SecOps SIEM search field, type the following UDM Query:
   `metadata.log_type = "EXTRAHOP" AND metadata.product_name = "RevealX"`
2. Specify the time interval to search.
3. Click **Run Search**.

   The search might take several minutes to complete depending on the data and time interval. Upon completion, UDM events are displayed on the Events tab. You can open UDM events to view mapped fields and the raw log data.

Mappings

UDM Field Name	Raw Log Field Name	Mapping Logic
metadata.vendor_name		This field is set to “ExtraHop”
metadata.product_name		This field is set to “RevealX”
metadata.event_type		This field is set to “SCAN_NETWORK”
metadata.event_timestamp	time	
metadata.description	description	
metadata.product_event_type	type	
metadata.product_log_id	id	
principal.ip	src.device.ipaddrs, src.ipaddr	“src.device.ipaddrs” is an array and “src.ipaddr” is a string. A combination of both values is mapped.
principal.hostname	src.hostname	
principal.mac	src.device.macaddr	
principal.user.email_addresses	src.username	If “src.username” is of type email, then map it to “principal.user.email_addresses” or else map it to “principal.user.userid”.
principal.user.userid		
principal.asset.asset_id	src.device.oid	
principal.asset.attribute.labels[src_device_role]	src.device.role	

<table>
<tr><td>principal.asset.attribute.labels[src_endpoint]</td><td>src.endpoint</td><td></td></tr>
<tr><td>principal.asset.attribute.labels[src_device_name]</td><td>src.device.name</td><td></td></tr>
<tr><td>target.ip</td><td>dst.device.ipaddrs, dst.ipaddr</td><td>“dst.device.ipaddrs” is an array and “dst.ipaddr” is a string. A combination of both values is mapped.</td></tr>
<tr><td>target.hostname</td><td>dst.hostname</td><td></td></tr>
<tr><td>target.mac</td><td>dst.device.macaddr</td><td></td></tr>
<tr><td>target.user.email_addresses
target.user.userid</td><td>dst.username</td><td>If “dst.username” is of type email, then map it to “target.user.email_addresses” or else map it to “target.user.userid”.</td></tr>
<tr><td>target.asset.asset_id</td><td>dst.device.oid</td><td></td></tr>
<tr><td>target.asset.ip</td><td>dst.device.ipaddrs, dst.ipaddr</td><td>“dst.device.ipaddrs” is an array and “dst.ipaddr” is a string. A combination of both values is mapped.</td></tr>
<tr><td>target.asset.hostname</td><td>dst.hostname</td><td></td></tr>
<tr><td>target.asset.mac</td><td>dst.device.macaddr</td><td></td></tr>
<tr><td>target.asset.attribute.labels[dst_endpoint]</td><td>dst.endpoint</td><td></td></tr>
<tr><td>target.asset.attribute.labels[dst_device_role]</td><td>dst.device.role</td><td></td></tr>
<tr><td>target.asset.attribute.labels[dst_device_name]</td><td>dst.device.name</td><td></td></tr>
<tr><td>security_result.category</td><td>categories_ids</td><td>“categories_ids” is mapped as follows:
<table>
<tr><th>Raw Value</th><th>Mapped Value</th></tr>
<tr><td>sec.attack, sec.exploit</td><td>EXPLOIT</td></tr>
<tr><td>sec.botnet, sec.command</td><td>NETWORK_COMMAND_AND_CONTROL</td></tr>
<tr><td>sec.cryptomining, sec.ransomware</td><td>SOFTWARE_MALICIOUS</td></tr>
<tr><td>sec.dos</td><td>NETWORK_DENIAL_OF_SERVICE</td></tr>
</table></td></tr>
</table>

		<table><tr><td>sec.exfil, Exfiltration</td><td>DATA_EXFILTRATION</td></tr><tr><td>sec.recon</td><td>NETWORK_RECON</td></tr><tr><td>perf.auth</td><td>AUTH_VIOLATION</td></tr><tr><td>sec.caution</td><td>NETWORK_SUSPICIOUS</td></tr></table>In other cases, map with UNKNOWN_CATEGORY
security_result.category_details	categories_ids	
security_result.detection_fields [categories_array]	categories_array	
security_result.summary	title	
security_result.first_discovered_time	time	
security_result.last_updated_time	mod_time	
security_result.risk_score	risk_score	
security_result.url_back_to_product	url	
security_result.attack_details.tactics.id	mitre_tactics_string	
security_result.attack_details.tactics.name	mitre_tactics_string	
security_result.attack_details.techniques.name	mitre_techniques.name	
security_result.attack_details.techniques.id	mitre_techniques.id	
security_result.priority	recommended	if “recommended” is "true", then map with "HIGH_PRIORITY", or else map with "LOW_PRIORITY"
security_result.priority_details	recommended_factors	
security_result.detection_fields [categories_string]	categories_string	
security_result.detection_fields	src.role	

[src_role]		
security_result.detection_fields [src_type]	src.type	
security_result.detection_fields [dst_role]	dst.role	
security_result.detection_fields [dst_type]	dst.type	
security_result.detection_fields [additional_participants_role]	additional_participants.role	
security_result.detection_fields [additional_participants_type]	additional_participants.type	
about.asset.asset_id	additional_participants.device.oid	
about.hostname	additional_participants.hostname	
about.ip	additional_participants.device.ipaddrs, additional_participants.ipaddr	“additional_participants.device.ipaddrs” is an array and “additional_participants.ipaddr” is a string. A combination of both values is mapped.
about.mac	additional_participants.device.macaddr	
about.user.email_addresses	additional_participants.username	If “additional_participants.username” is of type email, then map it to “about.user.email_addresses” or else map it to “about.user.userid”.
about.user.userid		
about.asset.attribute.labels[additional_participants_device_role]	additional_participants.device.role	if “additional_participants.device.role” is "webserver", then map it to "SERVER", or else map it as "ROLE_UNSPECIFIED".
about.asset.attribute.labels[additional_participants_endpoint]	additional_participants.endpoint	
about.asset.attribute.labels[additional_participants_device_name]	additional_participants.device.name	
additional.fields[is_user_created]	is_user_created	
additional.fields[mitre_techniques_string]	mitre_techniques_string	

additional.fields[%{property_key}]	properties	Map all the dynamic properties with the labels.
additional.fields[assignee]	assignee	
additional.fields[ticket_id]	ticket_id	
additional.fields[resolution]	resolution	
additional.fields[status]	status	

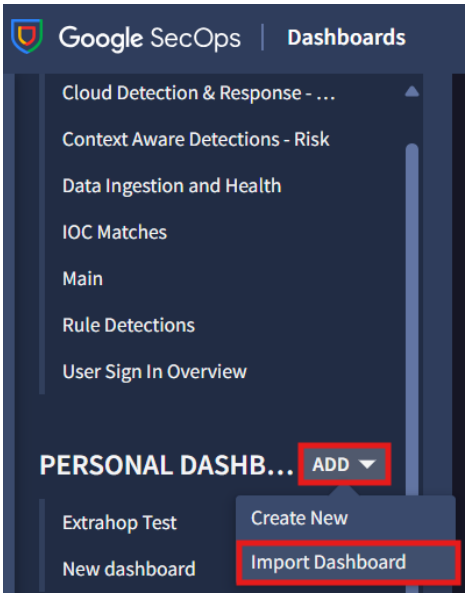
Dashboards

You can visualize and analyze ingested data by creating dashboards in Google SecOps SIEM.

Import a Dashboard into Google SecOps SIEM

Complete the following steps to import a dashboard:

1. Download the dashboard **.yaml** file for ExtraHop RevealX from the following GitHub repository.
2. Click the SIEM **Dashboards** section from the navigation panel.
3. Click **Add** and then select **Import Dashboard**.



Google SecOps: Import Dashboard

See Import Dashboards into Google SecOps for more information.

ExtraHop RevealX Dashboard

The ExtraHop RevealX dashboard consists of the following panels:

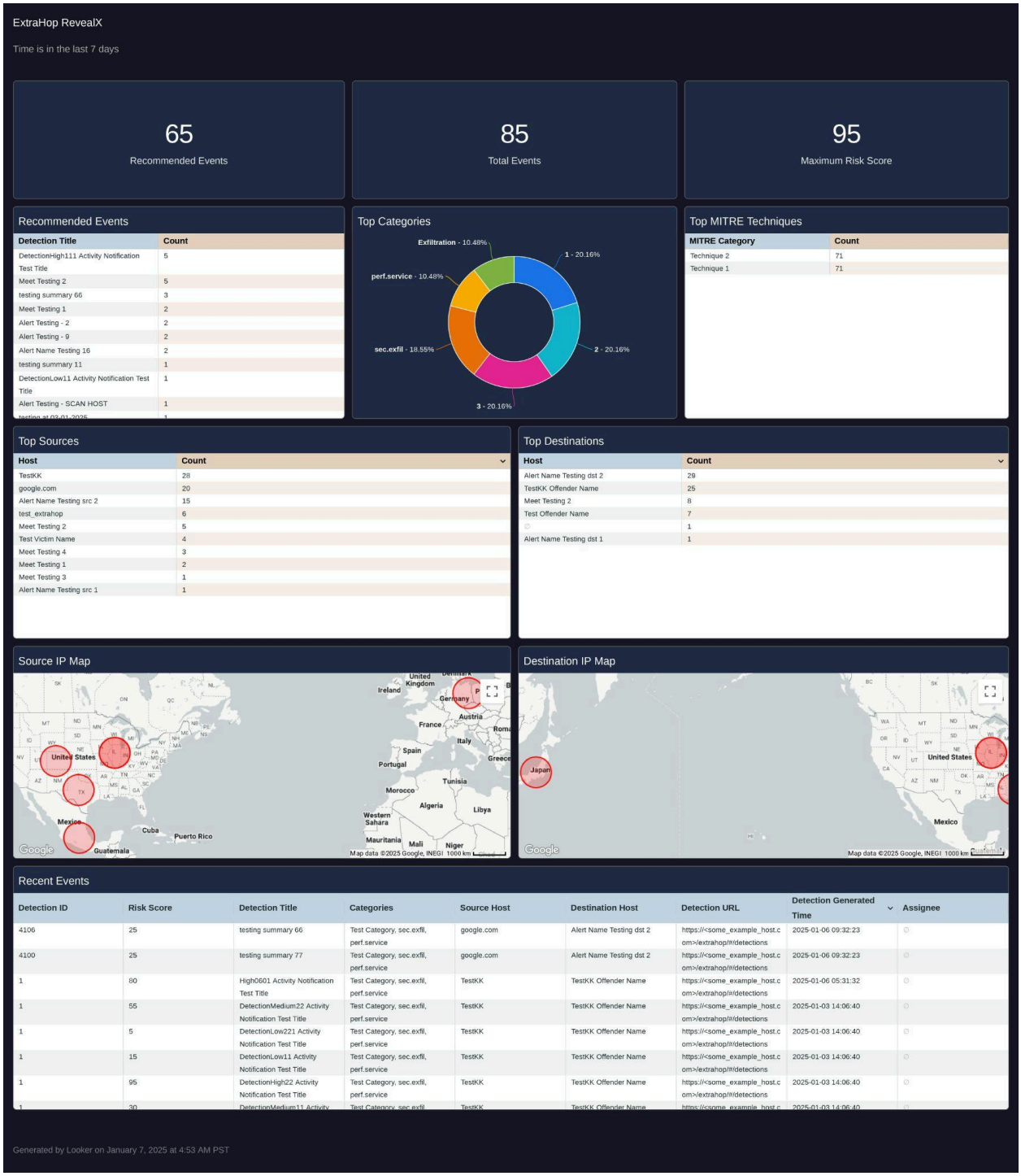
Panel	Description	Type	Default Sorting
Recommended Detection Events	Displays the number of recommended detections generated during the selected time period.	Single Value	-
Total Detection Events	Displays the number of detections generated during the selected time period.	Single Value	-
Maximum Risk Score	Displays the highest risk score associated with detections generated during the selected time period.	Single Value	-
Top Recommended Detection Events	Displays the top 10 recommended detections generated during the selected time period and the number of times each detection occurred.	Table	The count is in descending order
Top Categories	Displays the top detection categories associated with detections generated during the selected time period and the percentage and number of detections for each category.	Donut Chart	-

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.	Table	The count is in descending order
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.	Table	The count is in descending order
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.	Table	The count is in descending order
Source IP Map	Displays the geolocations of source IP addresses associated with detections generated during the selected time period.	Google Map	-
Destination IP Map	Displays the geolocations of destination IP addresses associated with detections generated during the selected time period.	Google Map	-
Recent Detection Events	Displays the most recent detections generated during the selected time period and	Table	The time (UTC) is in descending order

	detection details such as risk score, category, and URL.		

Available Filters

Name	Type	Description	Default
Time	Selector	A customized set of time periods that are available to filter detection data on the dashboard.	Past 7 days



Google SecOps: ExtraHop RevealX Dashboard

Create Correlation Rules for Detections and Alerts

Correlation rules scan events ingested into the Google SecOps SIEM to generate detections and alerts for specified anomalies. ExtraHop RevealX provides three rules that you can modify or copy to get started. You can find the ExtraHop RevealX correlation rules in the following GitHub repository.

Create a new correlation rule

1. From Google SecOps SIEM, navigate to **Detections > Rules & Detections**.
2. From the **Rules Editor** tab, click **New**.
3. In the rule editor, clear all the contents, and then copy and paste the code from the GitHub repository.
4. Click **Save New Rule**.
5. To generate alerts from the correlation rule, click the three dots next to the rule name, and enable the **Alerting** option.

See Manage rules using Rules Editor for more information.

Here are some considerations when creating correlation rules for ExtraHop RevealX detections:

- The Recommended field for the raw log must be set to True.
- Events with a risk score >= 80 are categorized as High Severity.
- Events with a risk score >= 30 and < 80 are categorized as Medium Severity.
- Events with a risk score < 30 are categorized as Low Severity.

Limitations

- It might take up to 30 minutes for the latest ingested data to be displayed in the dashboard.
- There can be a delay in creating detections when a live rule is run against ingested events.
- If an ExtraHop RevealX detection that is currently ingested by Google SecOps SIEM is updated and then ingested again, the detection is considered a new event and is displayed as new activity in the dashboard. This condition can result in inconsistent counts between ExtraHop RevealX and the dashboard.
- Google SecOps SIEM derives the coordinates for IP addresses displayed on the Source and Destination IP Maps dashboard panel from various sources and might not display information for all IP addresses. See Enrich events with geolocation data for more information.

Troubleshooting

Events are successfully ingested but not displayed in search results

- The time range for the search is outside of the timestamp associated with the ingested event.
- The timestamp in the raw log must be formatted in the epoch milliseconds.
- The ingested event might be a duplicate event with the same payload.

Dashboard is not updated

If the dashboard does not display updated data 30 minutes after ingesting data, clear the cache and refresh the dashboard.