Integrate Reveal(x) Enterprise with Splunk SOAR

Published: 2023-05-12

This integration enables you to export network threat detections, metrics, and packet data from Reveal(x) Enterprise into Splunk SOAR.

Before you can configure this integration, you must generate an ExtraHop REST API key and then add the key when you configure the ExtraHop App for Splunk SOAR.

System requirements

ExtraHop Reveal(x) Enterprise

- Your user account must have full write privileges or higher on Reveal(x) Enterprise.
- Your Reveal(x) Enterprise system must be connected to an ExtraHop sensor with firmware version 9.0 or later.
- Your Reveal(x) Enterprise system must be connected to ExtraHop Cloud Services.
- Your Reveal(x) Enterprise system must be configured to allow REST API key generation.

Splunk SOAR

- You must have Splunk SOAR version 5.3 or later.

Generate a REST API key

You must generate an ExtraHop API key before you can configure the ExtraHop App for Splunk SOAR. The API key enables you to gain access to the integration and perform operations from Splunk SOAR.

1. Log in to the ExtraHop system through https://<extrahop-hostname-or-IP-address>.
2. Click the User icon at the top right corner of the page, and then click **API Access**.
3. In the Generate an API Key section, type a description for the new key, and then click **Generate**.
4. Scroll down to the API Keys section and copy the API key that matches your description.

Install and configure the ExtraHop App for Splunk SOAR

1. Download and install the ExtraHop App for Splunk SOAR from the Splunkbase site according to the Splunk Add-Ons and Apps documentation.
2. From the installed app, click **Configure New Asset**.
3. From the Type of Asset drop-down list, select **Reveal(x) Enterprise**.
4. Type the **IP address or hostname** of the Reveal(x) Enterprise system that this asset will connect to.
5. Enter the key that you generated from your Reveal(x) Enterprise system in the **REST API key** field.
6. Click the **Documentation** link on the asset configuration page and complete the configuration of ExtraHop App for Splunk SOAR according to the documentation.