Integrate Reveal(x) Enterprise with Cortex XSOAR

Published: 2023-09-30

This integration enables you to export Reveal(x) Enterprise detections to Cortex XSOAR and run response playbooks, as well as query Reveal(x) Enterprise packets and device activity.

Before you can configure this integration, you must generate an ExtraHop REST API key and then add the key when you configure the ExtraHop Reveal(x) integration for Cortex XSOAR.

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 9.2 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 .

Cortex XSOAR

- You must have Cortex XSOAR version 6.5 or later.
- You must have the following Cortex XSOAR content packs:

  - Base version 1.31.62 or later
  - Common Playbooks version 2.2.4 or later
  - Common Scripts version 1.11.22 or later
  - Filters and Transformers version 1.0.2 or later
  - CVE Search version 1.0.14 or later

Generate a REST API key

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

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 integration for Cortex XSOAR

1. Download and install the ExtraHop integration for Cortex XSOAR from the XSOAR Marketplace according to the Cortex XSOAR Marketplace Overview documentation.
2. From the installed integration, click **Add Instance**.
3. Type a unique **Name** for the integration instance.
4. Type the **URL** of the Reveal(x) Enterprise system this integration instance will connect to.

5. Deselect **On Cloud** and enter the REST API key that you generated from your Reveal(x) Enterprise system in the **API Key** field.

6. Complete configuration of the integration instance according to the ExtraHop integration for Cortex XSOAR Reference ☑ documentation.