Integrate Reveal(x) 360 with Cortex XSOAR

Published: 2023-07-10

This integration enables you to export Reveal(x) 360 detections to Cortex XSOAR and run response playbooks, as well as query Reveal(x) 360 packets and device activity.

To configure this integration, you must create Cortex XSOAR credentials and then add those credentials when you configure the ExtraHop Reveal(x) integration for Cortex XSOAR.

System requirements

ExtraHop Reveal(x) 360

- Your user account must have privileges ↗ on Reveal(x) 360 for System and Access Administration.
- Your Reveal(x) 360 system must be connected to an ExtraHop sensor with firmware version 9.2 or later.
- Your Reveal(x) 360 system must be connected to ExtraHop Cloud Services ↗.

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

Create Cortex XSOAR integration credentials

1. Log in to Reveal(x) 360.
2. Click the System Settings icon ⚙ and then click **Integrations**.
3. Click the **Cortex XSOAR** tile.
4. Click **Create Credential**.
   The page displays the generated ID and secret.
5. Copy and store the ID and secret, which you will need to configure the ExtraHop Reveal(x) integration for Cortex XSOAR.
6. Click **Done**.

The credential is also added to the ExtraHop REST API Credentials ↗ page where you can view the credential status, copy the ID, or delete the credential.

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) 360 system this integration instance will connect to.

5. Select **On Cloud** and enter the **Client ID** and **Client Secret** credentials that you created and copied from your Reveal(x) 360 system.
6. Complete configuration of the integration instance according to the ExtraHop integration for Cortex XSOAR Reference ☑ documentation.