Integrate RevealX 360 with Cortex XSOAR

Published: 2025-01-29

This integration enables you to export RevealX 360 detections to Cortex XSOAR and run response playbooks, as well as query RevealX 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 RevealX integration for Cortex XSOAR.

System requirements

ExtraHop RevealX 360

- Your user account must have privileges on RevealX 360 for System and Access Administration.
- Your RevealX 360 system must be connected to an ExtraHop sensor with firmware version 9.2 or later.
- Your RevealX 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 RevealX 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. Optional: If you have already created a credential for REST API access, you can apply it to the integration. Click **Select Existing Credential**, select a credential from the drop-down menu and then click **Select**.
6. Copy and store the ID and secret, which you will need to configure the ExtraHop RevealX integration for Cortex XSOAR.
7. Click **Done**.
8. Return to the Administration page and click **API Access**.
9. From the REST API Credentials section, copy and save the API endpoint, which you will need to configure the ExtraHop RevealX integration for Cortex XSOAR.

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 RevealX REST API endpoint that you copied from your RevealX 360 system.
5. Select **On Cloud** and enter the **Client ID** and **Client Secret** credentials that you created and copied from your RevealX 360 system.

   The API Key field is not required when configuring this integration on RevealX 360 systems.
6. Complete configuration of the integration instance according to the ExtraHop integration for Cortex XSOAR Reference documentation.