Integrate RevealX 360 with Splunk SOAR

Published: 2025-01-10

This integration enables you to export network threat detections, metrics, and packet data from RevealX 360 into Splunk SOAR.

To configure this integration, you must create Splunk SOAR credentials and then add those credentials when you configure the ExtraHop App for Splunk SOAR.

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 9.0 or later.
- Your RevealX 360 system must be connected to ExtraHop Cloud Services.

Splunk

- You must have Splunk SOAR version 5.3 or later.

Create Splunk SOAR integration credentials

1. Log in to RevealX 360.
2. Click the System Settings icon and then click **Integrations**.
3. Click the **Splunk SOAR** 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 Add-On for Splunk.
7. 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.

Next steps
Install and configure the ExtraHop App for Splunk SOAR.

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 menu, select **RevealX 360**.
4. In the following configuration fields, enter the credentials you created and copied for the Splunk SOAR integration:
   - **Client ID**
   - **Client Secret**

5. Click the **Documentation** link on the asset configuration page and complete the configuration of the ExtraHop App for Splunk SOAR according to the documentation.

Next steps

Export RevealX 360 detections, metrics, and packets to Splunk SOAR and initiate actions such as getting device information or tagging a device by following the configuration documentation.