

Integrate Reveal(x) 360 with Splunk SOAR

Published: 2022-09-27

This integration enables you to export network threat detections, metrics, and packet data from Reveal(x) 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 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 9.0 or later.
- Your Reveal(x) 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 Reveal(x) 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. Copy and store the ID and secret, which you will need to configure the ExtraHop Add-On for Splunk.
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.


Next steps

[Install and configure the ExtraHop App for Splunk SOAR](#).

Install and configure the ExtraHop App for Splunk SOAR

1. Download the [ExtraHop App for Splunk SOAR](#) from the SplunkBase site.
2. Install and configure the add-on according to the following documentation:
 - [About Installing Splunk Add-Ons and Apps](#)
 - [ExtraHop App for Splunk SOAR Details](#)
3. In the following configuration fields, enter the [credentials](#) you created and copied for the Splunk SOAR integration:
 - **Client ID**
 - **Client Secret**

Next steps

Export Reveal(x) 360 detections, metrics, and packets to Splunk SOAR and initiate actions such as getting device information or tagging a device according to the instructions in the [ExtraHop App for Splunk SOAR](#) .