Integrate RevealX Enterprise with QRadar

Published: 2025-01-10

This integration enables you to view metrics from RevealX Enterprise in IBM Security QRadar to gain behavioral insights about your environment.

Before you can configure this integration, you must generate an ExtraHop REST API key and then add the key when you configure the ExtraHop App for QRadar.

System requirements

ExtraHop RevealX Enterprise

- Your user account must have full write privileges ⧉ or higher on RevealX Enterprise.
- Your RevealX Enterprise system must be connected to an ExtraHop sensor with firmware version 8.8 or later.
- Your RevealX Enterprise system must be connected to ExtraHop Cloud Services ⧉.
- Your RevealX Enterprise system must be configured to allow REST API key generation ⧉.

QRadar

- You must have IBM Security QRadar version 7.4.1 FP2 or later.

Generate a REST API key

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

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 App for QRadar

1. Download and install the ExtraHop App for QRadar ⧉ from the IBM Exchange site.
2. From the right panel of the download page, click **View** next to Documentation to download a PDF of the user guide.
3. From the installed app, click **Add ExtraHop System**.
4. From the Instance Type drop-down menu, select **On Prem Instance**.
5. In the **ExtraHop System** field, type the hostname of the RevealX Enterprise system this app will connect to.
6. Enter the key that you generated from your RevealX Enterprise system in the **API Key** field.
7. Complete the configuration of the ExtraHop App for QRadar according to the downloaded documentation.