Integrate RevealX 360 with QRadar SOAR

Published: 2024-05-15

This integration enables IBM Security QRadar SOAR to export device and detection data from the ExtraHop system through the ExtraHop REST API. You can view exported data in QRadar SOAR to gain insight into how your devices are communicating in your environment and to view network threat detections.

Before you begin

You must meet the following 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 9.6 or later.
    - Your RevealX 360 system must be connected to ExtraHop Cloud Services ⧉.

- QRadar SOAR

    - You must have QRadar SOAR version 46.0 or later

1. Complete the following steps to create ExtraHop REST API credentials for the integration:
    a) Log in to RevealX 360.
    b) Click the System Settings icon ⚙ and then click **Integrations**.
    c) Click the tile of the integration you want to configure.
    d) Click **Create Credential**.
       The page displays the generated ID and secret.
    e) 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 list and then click **Select**.
    f) Copy and store the ID and secret, which you will need to configure the ExtraHop app.
    g) Click **Done**.
       The credential is added to the ExtraHop REST API Credentials ⧉ page where you can view the credential status, copy the ID, or delete the credential.
2. Complete the following steps to install and configure the ExtraHop app for QRadar SOAR:
    a) Download and install the ExtraHop for IBM SOAR ⧉ app from the IBM App Exchange site.
    b) In the right panel of the download site, click **View** next to Documentation to download a PDF of the app user guide.
    c) In the app configuration, enter the ExtraHop REST API credentials that you created and copied for the QRadar SOAR integration:

        - **Authentication ID**
        - **Secret Key**
    d) Finish configuring the app according to the instructions in the documentation.