Integrieren Sie Reveal (x) 360 mit QRadar SOAR

Veröffentlicht: 2024-04-10

Diese Integration ermöglicht es IBM Security QRadar SOAR, Gerät- und Erkennungsdaten aus dem ExtraHop-System über die ExtraHop REST-API zu exportieren. Sie können exportierte Daten in QRadar SOAR einsehen, um einen Einblick in die Kommunikation Ihrer Geräte in Ihrer Umgebung zu erhalten und um Erkennungen von Netzwerkbedrohungen einzusehen.

Bevor Sie beginnen

Sie müssen die folgenden Systemanforderungen erfüllen:

- ExtraHop Enthüllen (x) 360
  - Ihr Benutzerkonto muss Privilegien auf Reveal (x) 360 für System- und Zugriffsverwaltung.
  - Ihr Reveal (x) 360-System muss mit einem ExtraHop verbunden sein Sensor mit Firmware-Version 9.6 oder höher.
  - Ihr Reveal (x) 360-System muss verbunden mit ExtraHop Cloud Services.
- QRadar SOAR
  - Sie müssen QRadar SOAR Version 46.0 oder höher haben

1. Gehen Sie wie folgt vor, um ExtraHop REST-API-Anmeldeinformationen für die Integration zu erstellen:
   a) Loggen Sie sich bei Reveal (x) 360 ein.
   b) Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Integrationen**.
   c) Klicken Sie auf die Kachel der Integration, die Sie konfigurieren möchten.
   d) klicken **Anmeldeinformationen erstellen**.
   Auf der Seite werden die generierte ID und das Geheimnis angezeigt.
   e) Optional: Wenn Sie bereits Anmeldeinformationen für den REST-API-Zugriff erstellt haben, können Sie diese auf die Integration anwenden. klicken **Wählen Sie vorhandene Anmeldeinformationen aus**, wählen Sie einen Berechtigungsnachweis aus der Dropdownliste aus und klicken Sie dann auf **Wählen**.
   f) Kopieren und speichern Sie die ID und das Geheimnis, die Sie zur Konfiguration der ExtraHop-App benötigen.
   g) klicken **Erledigt**.
   Die Anmeldeinformationen werden dem hinzugefügt ExtraHop REST-API-Anmeldeinformationen Seite, auf der Sie den Status der Anmeldeinformationen anzeigen, die ID kopieren oder die Anmeldeinformationen löschen können.
2. Gehen Sie wie folgt vor, um die ExtraHop-App für QRadar SOAR zu installieren und zu konfigurieren:
   a) Downloaden und installieren Sie das ExtraHop für IBM SOAR App von der IBM App Exchange-Website.
   b) Klicken Sie im rechten Bereich der Download-Site auf **Ansicht** neben Dokumentation, um ein PDF des App-Benutzerhandbuchs herunterzuladen.
   c) Geben Sie in der App-Konfiguration die ExtraHop REST-API-Anmeldeinformationen ein, die Sie für die QRadar SOAR-Integration erstellt und kopiert haben:
      - **Authentifizierungs-ID**
      - **Geheimer Schlüssel**
   d) Beenden Sie die Konfiguration der App gemäß den Anweisungen in der Dokumentation.