Integrieren Sie Reveal (x) 360 mit Splunk SOAR

Veröffentlicht: 2024-04-10

Diese Integration ermöglicht es Ihnen, Erkennungen von Netzwerkbedrohungen, Metriken und Paketdaten von Reveal (x) 360 nach Splunk SOAR zu exportieren.

Um diese Integration zu konfigurieren, müssen Sie Splunk SOAR-Anmeldeinformationen erstellen und fügen Sie dann diese Anmeldedaten hinzu, wenn Sie die ExtraHop App für Splunk SOAR konfigurieren.

Anforderungen an das System

ExtraHop Reveal (x) 360

- Ihr Benutzerkonto muss Privilegien auf Reveal (x) 360 für System- und Zugriffsadministration.
- Ihr Reveal (x) 360-System muss mit einem ExtraHop verbunden sein Sensor mit Firmware-Version 9.0 oder höher.
- Ihr Reveal (x) 360-System muss verbunden mit ExtraHop Cloud Services.

Splunk

- Sie benötigen Splunk SOAR Version 5.3 oder höher.

Anmeldedaten für die Splunk SOAR-Integration erstellen

1. Loggen Sie sich bei Reveal (x) 360 ein.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Integrationen**.
3. Klicken Sie auf **Splunk SOAR** Kachel.
4. klicken **Anmeldeinformationen erstellen**.
   Auf der Seite werden die generierte ID und das Geheimnis angezeigt.
5. Optional: Wenn Sie bereits Anmeldeinformationen für den REST-API-Zugriff erstellt haben, können Sie diese auf die Integration anwenden. klicken **Wählen Sie vorhandene Anmeldeinformationen**, wählen Sie einen Berechtigungsnachweis aus der Dropdownliste aus und klicken Sie dann auf **Wählen**.
6. Kopieren und speichern Sie die ID und das Geheimnis, die Sie benötigen, um das ExtraHop Add-On für Splunk zu konfigurieren.
7. klicken **Erledigt**.

Die Anmeldeinformationen werden auch dem hinzugefügt ExtraHop REST-API-Anmeldeinformationen Seite , auf der Sie den Status der Anmeldeinformationen anzeigen, die ID kopieren oder die Anmeldeinformationen löschen können.

Nächste Schritte
Installieren und konfigurieren Sie die ExtraHop App für Splunk SOAR.

Installieren und konfigurieren Sie die ExtraHop App für Splunk SOAR

1. Downloaden und installieren Sie das ExtraHop App für Splunk SOAR von der Splunkbase-Site gemäß der Splunk-Add-Ons und -Apps Dokumentation.
2. Klicken Sie in der installierten App auf **Neues Asset konfigurieren**.
3. Aus dem Art des Vermögenswerts Drop-down-Liste, wählen **Enthüllen (x) 360**.

4. Geben Sie in den folgenden Konfigurationsfeldern den Anmeldedaten Sie haben für die Splunk SOAR-Integration erstellt und kopiert:
   - **Kunden-ID**
   - **Geheimer Kundenschlüssel**
5. Klicken Sie auf **Dokumentation** klicken Sie auf der Asset-Konfigurationsseite und schließen Sie die Konfiguration der ExtraHop App für Splunk SOAR gemäß der Dokumentation ab.

Nächste Schritte
Exportieren Sie Reveal (x) 360-Erkennungen, -Metriken und -Pakete nach Splunk SOAR und leiten Sie Aktionen wie das Abrufen von Geräteinformationen oder das Taggen eines Gerät ein, indem Sie der Konfigurationsdokumentation folgen.