Integrieren Sie Reveal (x) 360 mit Splunk

Veröffentlicht: 2024-04-10

Diese Integration ermöglicht es Ihnen, die Erkennung von Netzwerkbedrohungen und Verhaltensinformationen von Reveal (x) 360 in Splunk einzusehen.

Um diese Integration zu konfigurieren, müssen Sie Anmeldedaten für die Splunk-Integration erstellen und füge sie dann der Konfiguration des hinzu ExtraHop Add-On für Splunk .

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 8.8 oder höher.
- Ihr Reveal (x) 360-System muss verbunden mit ExtraHop Cloud Services.

Splunk

- Sie benötigen Splunk Version 8.1 oder höher.

Anmeldedaten für die Splunk-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 das **Splunk** Fliese.
4. Klicken Sie **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 Sie **Wählen Sie vorhandene Anmeldeinformationen aus**, wählen Sie einen Berechtigungsnachweis aus der Dropdownliste aus und klicken Sie dann auf **Wählen Sie**.
6. Kopieren und speichern Sie die ID und das Geheimnis, die Sie benötigen, um das ExtraHop Add-On für Splunk zu konfigurieren.
7. Klicken Sie **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 das ExtraHop Add-On für Splunk.

Installieren und konfigurieren Sie das ExtraHop Add-On für Splunk

1. Laden Sie das herunter ExtraHop Add-On für Splunk von der SplunkBase-Website.
2. Installieren und konfigurieren Sie das Add-on gemäß der folgenden Dokumentation:
   - Über die Installation von Splunk-Add-Ons
   - Einzelheiten zum ExtraHop-Add-On für Splunk

3. Geben Sie in den folgenden Konfigurationsfeldern den Anmeldedaten Sie haben für die Splunk-Integration erstellt und kopiert:
   - **Kunden-ID**
   - **Geheimer Kundenschlüssel**

Nächste Schritte
Exportieren Sie Reveal (x) 360-Erkennungen und -Metriken und zeigen Sie sie in Splunk gemäß den Anweisungen in der Einzelheiten zum ExtraHop-Add-On für Splunk.