Integrieren Sie RevealX 360 mit Splunk

Veröffentlicht: 2025-02-12

Diese Integration ermöglicht es Ihnen, Erkennungen von Netzwerkbedrohungen und Verhaltensinformationen von RevealX 360 in Splunk einzusehen.

Hinweis Veraltete Integration

Die Splunk-Integration ist veraltet. Bitte migrieren Sie Ihre Integration auf Splunk SIEM für Unternehmenssicherheit Integration.

Anforderungen an das System

ExtraHop RevealX 360

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

- Ihr Benutzerkonto muss Privilegien auf RevealX 360 für System- und Zugriffsadministration.
- Ihr RevealX 360-System muss mit einem ExtraHop verbunden sein Sensor mit Firmware-Version 8.8 oder höher.
- Ihr RevealX 360-System muss verbunden mit ExtraHop Cloud Services.

Splunk

- Sie müssen Splunk Version 8.1 oder höher haben.

Anmeldedaten für die Splunk-Integration erstellen

1. Loggen Sie sich in RevealX 360 ein.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann auf **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 im Dropdownmenü einen Berechtigungsnachweis 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
- ExtraHop-Add-On für Splunk-Details

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

Nächste Schritte
Exportieren Sie RevealX 360-Erkennungen und -Metriken und zeigen Sie sie in Splunk gemäß den Anweisungen in der ExtraHop-Add-On für Splunk-Details.