Integrieren Sie RevealX 360 mit Cortex XSOAR

Veröffentlicht: 2025-02-04

Diese Integration ermöglicht es Ihnen, RevealX 360-Erkennungen nach Cortex XSOAR zu exportieren und Antwort-Playbooks auszuführen sowie RevealX 360-Pakete und Geräteaktivitäten abzufragen.

Um diese Integration zu konfigurieren, müssen Sie Cortex XSOAR-Anmeldeinformationen erstellen und fügen Sie dann diese Anmeldedaten hinzu, wenn Sie konfigurieren Sie die ExtraHop RevealX-Integration für Cortex XSOAR.

Anforderungen an das System

ExtraShop RevealX 360

- 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 9.2 oder höher.
- Ihr RevealX 360-System muss verbunden mit ExtraHop Cloud Services.

Kortex XSOAR

- Sie benötigen Cortex XSOAR Version 6.5 oder höher.
- Sie müssen über die folgenden Cortex XSOAR-Inhaltspakete verfügen:
  - Basisversion 1.31.62 oder höher
  - Common Playbooks Version 2.2.4 oder höher
  - Common Scripts Version 1.11.22 oder höher
  - Filter und Transformers Version 1.0.2 oder höher
  - CVE Search Version 1.0.14 oder höher

Anmeldedaten für die Cortex XSOAR-Integration erstellen

1. Loggen Sie sich in RevealX 360 ein.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Integrationen**.
3. Klicken Sie auf das **Kortex XSOAR** 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**, wählen Sie im Dropdownmenü einen Berechtigungsnachweis aus und klicken Sie dann auf **Wählen**.
6. Kopieren und speichern Sie die ID und das Geheimnis, die Sie benötigen, um die ExtraHop RevealX-Integration für Cortex XSOAR zu konfigurieren.
7. Klicken Sie **Erledigt**.
8. Kehren Sie zur Administrationsseite zurück und klicken Sie auf **API-Zugriff**.
9. Kopieren und speichern Sie im Abschnitt REST-API-Anmeldeinformationen den API-Endpunkt, den Sie benötigen, um die ExtraHop RevealX-Integration für Cortex XSOAR zu konfigurieren.

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.

Installieren und konfigurieren Sie die ExtraHop-Integration für Cortex XSOAR

1. Laden Sie das herunter und installieren Sie es ExtraHop-Integration für Cortex XSOAR vom XSOAR Marketplace gemäß dem Überblick über den Cortex XSOAR Marketplace Dokumentation.
2. Klicken Sie in der installierten Integration auf **Instanz hinzufügen**.
3. Geben Sie ein Unikat ein **Name** für die Integrationsinstanz.
4. Geben Sie das ein **URL** des RevealX REST-API-Endpunkts, der Sie haben von Ihrem RevealX 360-System kopiert.
5. Wählen Sie **Auf der Cloud** und gib das ein **Kunden-ID** und **Geheimer Kunde** Anmeldedaten, die Sie haben es von Ihrem RevealX 360-System erstellt und kopiert.

   Das Feld API-Schlüssel ist bei der Konfiguration dieser Integration auf RevealX 360-Systemen nicht erforderlich.
6. Vollständige Konfiguration der Integrationsinstanz gemäß ExtraHop-Integration für Cortex XSOAR Reference Dokumentation.