

Integrieren Sie RevealX Enterprise mit Cortex XSOAR

Veröffentlicht: 2024-08-07

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

Bevor Sie diese Integration konfigurieren können, müssen Sie [Generieren Sie einen ExtraHop REST-API-Schlüssel](#) und füge dann den Schlüssel hinzu, wenn du [konfigurieren Sie die ExtraHop RevealX-Integration für Cortex XSOAR](#).

Anforderungen an das System

ExtraHop RevealX Enterprise

- Ihr Benutzerkonto muss [volle Schreibrechte](#) oder höher auf RevealX Enterprise.
- Ihr RevealX Enterprise-System muss mit einem ExtraHop verbunden sein Sensor mit Firmware-Version 9.2 oder höher.
- Ihr RevealX Enterprise-System muss [verbunden mit ExtraHop Cloud Services](#).
- Ihr RevealX Enterprise-System muss [konfiguriert, um die Generierung von REST-API-Schlüsseln zu ermöglichen](#).

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


Generieren Sie einen REST-API-Schlüssel

Sie müssen einen ExtraHop-API-Schlüssel generieren, bevor Sie die ExtraHop-Integration für Cortex XSOAR konfigurieren können. Mit dem API-Schlüssel können Sie auf die Integration zugreifen und Operationen von Cortex XSOAR aus ausführen.

1. <extrahop-hostname-or-IP-address>Melden Sie sich über https://beim ExtraHop-System an.
2. Klicken Sie in der oberen rechten Ecke der Seite auf das Benutzersymbol und dann auf **API-Zugriff**.
3. In der Generieren Sie einen API-Schlüssel Abschnitt, geben Sie eine Beschreibung für den neuen Schlüssel ein, und klicken Sie dann auf **Generieren**.
4. Scrollen Sie nach unten zum API-Schlüssel Abschnitt und kopieren Sie den API-Schlüssel , der Ihrer Beschreibung entspricht.

Installieren und konfigurieren Sie die ExtraHop-Integration für Cortex XSOAR

1. Laden Sie das herunter und installieren Sie es [ExtraHop-Integration für Cortex XSOAR](#) aus dem XSOAR Marketplace gemäß [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 **URL** des RevealX Enterprise-Systems, zu dem diese Integrationsinstanz eine Verbindung herstellen wird.
5. Abwählen **Auf der Cloud** und gib das **REST-API-Schlüssel** die Sie aus Ihrem RevealX Enterprise-System generiert haben in der **API-Schlüssel** Feld.
6. Vollständige Konfiguration der Integrationsinstanz gemäß [ExtraHop-Integration für Cortex XSOAR Reference](#)  Dokumentation.