

Integrieren Sie Reveal (x) 360 mit Cortex XSOAR

Veröffentlicht: 2023-09-30

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

Um diese Integration zu konfigurieren, müssen Sie [Cortex XSOAR-Anmeldeinformationen erstellen](#) und fügen Sie dann diese Anmeldeinformationen hinzu, wenn Sie [konfigurieren Sie die ExtraHop Reveal \(x\) -Integration für Cortex XSOAR](#).

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 9.2 oder höher.
- Ihr Reveal (x) 360-System muss [verbunden mit ExtraHop Cloud Services](#).

Cortex XSOAR

- Sie müssen Cortex XSOAR Version 6.5 oder höher haben.
- Sie benötigen die folgenden Cortex XSOAR-Inhaltspakete:
 - Basisversion 1.31.62 oder höher
 - Common Playbooks Version 2.2.4 oder höher
 - Common Scripts Version 1.11.22 oder höher
 - Filters and Transformers Version 1.0.2 oder höher
 - CVE Search Version 1.0.14 oder höher

Anmeldeinformationen für die Cortex XSOAR-Integration erstellen

1. Loggen Sie sich bei Reveal (x) 360 ein.
2. Klicken Sie auf das Symbol Systemeinstellungen  und dann klicken **Integrationen**.
3. Klicken Sie auf **Cortex XSOAR** Kachel.
4. klicken **Credential erstellen**.
Auf der Seite werden die generierte ID und das Geheimnis angezeigt.
5. Kopieren und speichern Sie die ID und das Geheimnis, die Sie für die Konfiguration der ExtraHop Reveal (x) -Integration für Cortex XSOAR benötigen.
6. klicken **Erledigt**.

Der Berechtigungsnachweis wird 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. Downloaden und installieren Sie das [ExtraHop-Integration für Cortex XSOAR](#) aus dem XSOAR Marketplace laut [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 den **URL** des Reveal (x) 360-Systems, mit dem diese Integrationsinstanz eine Verbindung herstellen wird.
5. Wählen **In der Cloud** und gib den **Kunden-ID** und **Geheimer Kundenschlüssel** Anmeldedaten, die [Sie haben es von Ihrem Reveal \(x\) 360-System erstellt und kopiert](#).
6. Vollständige Konfiguration der Integrationsinstanz gemäß [ExtraHop-Integration für Cortex XSOAR Referenz](#) [Dokumentation](#).