

Intégrez RevealX 360 à Cortex XSOAR

Publié: 2024-07-03

Cette intégration vous permet d'exporter les détections RevealX 360 vers Cortex XSOAR et d'exécuter des playbooks de réponse, ainsi que d'interroger les paquets RevealX 360 et l'activité de l'équipement.

Pour configurer cette intégration, vous devez [créer des informations d'identification Cortex XSOAR](#) puis ajoutez ces informations d'identification lorsque vous [configurez l'intégration ExtraHop RevealX pour Cortex XSOAR](#).

Exigences du système

Hop Reveal X 360 supplémentaire

- Votre compte utilisateur doit avoir [privilèges](#) sur RevealX 360 pour l'administration des systèmes et des accès .
- Votre système RevealX 360 doit être connecté à un ExtraHop sonde avec la version 9.2 ou ultérieure du firmware.
- Votre système RevealX 360 doit être [connecté à ExtraHop Cloud Services](#).

Cortex XSOAR

- Vous devez disposer de Cortex XSOAR version 6.5 ou ultérieure.
- Vous devez disposer des packs de contenu Cortex XSOAR suivants :
 - Version de base 1.31.62 ou ultérieure
 - Common Playbooks version 2.2.4 ou ultérieure
 - Common Scripts version 1.11.22 ou ultérieure
 - Filtres et transformateurs version 1.0.2 ou ultérieure
 - CVE Search version 1.0.14 ou ultérieure

Création d'informations d'identification pour l'intégration Cortex XSOAR

1. Connectez-vous à RevealX 360.
2. Cliquez sur l'icône Paramètres système  puis cliquez sur **Intégrations**.
3. Cliquez sur **Cortex XSOAR** tuile.
4. Cliquez **Créer un justificatif**.
La page affiche l'identifiant et le secret générés.
5. Optionnel : Si vous avez déjà créé un identifiant pour accéder à l'API REST, vous pouvez l'appliquer à l'intégration. Cliquez **Sélectionnez un justificatif d'identité existant**, sélectionnez un identifiant dans la liste déroulante, puis cliquez sur **Sélectionnez**.
6. Copiez et stockez l'ID et le code secret dont vous aurez besoin pour configurer l'intégration ExtraHop RevealX pour Cortex XSOAR.
7. Cliquez **Terminé**.

Le justificatif est également ajouté au [Informations d'identification de l'API REST ExtraHop](#) page où vous pouvez consulter l'état des informations d'identification, copier l'identifiant ou supprimer les informations d'identification.

Installation et configuration de l'intégration ExtraHop pour Cortex XSOAR

1. Téléchargez et installez le [Intégration d'ExtraHop pour Cortex XSOAR](#) depuis le XSOAR Marketplace selon le [Présentation de Cortex XSOAR Marketplace](#) documentation.
2. Dans l'intégration installée, cliquez sur **Ajouter une instance**.
3. Tapez un numéro unique **Nom** pour l'instance d'intégration.
4. Tapez le **URL** du système RevealX 360 auquel cette instance d'intégration va se connecter.
5. Sélectionnez **Sur le cloud** et entrez le **Identifiant du client** et **Secret du client** des informations d'identification qui **que vous avez créé et copié depuis votre système RevealX 360**.
6. Configuration complète de l'instance d'intégration conformément à [Intégration d'ExtraHop pour Cortex XSOAR Reference](#) documentation.