

Intégrer Reveal(x) 360 avec Cortex XSOAR

Publié: 2023-09-19

Cette intégration vous permet d'exporter les détections Reveal(x) 360 vers Cortex XSOAR et d'exécuter des playbooks de réponse, ainsi que d'interroger les paquets Reveal(x) 360 et l'activité des périphériques.

Pour configurer cette intégration, vous devez [créer des informations d'identification Cortex XSOAR](#), puis les ajouter lorsque vous [configurez l'intégration ExtraHop Reveal\(x\) pour Cortex XSOAR](#).

Configuration requise


ExtraHop Reveal(x) 360

- Votre compte utilisateur doit avoir des [privileges](#) sur Reveal(x) 360 pour l'administration du système et des accès.
- Votre système Reveal(x) 360 doit être connecté à un capteur ExtraHop avec la version 9.2 ou ultérieure du micrologiciel.
- Votre système Reveal(x) 360 doit être [connecté aux ExtraHop Cloud Services](#).

Cortex XSOAR

- Vous devez disposer de la version 6.5 ou ultérieure de Cortex XSOAR.
- Vous devez disposer des packs de contenu Cortex XSOAR suivants :
 - Base version 1.31.62 ou ultérieure
 - Common Playbooks version 2.2.4 ou ultérieure
 - Common Scripts version 1.11.22 ou ultérieure
 - Filters and Transformers version 1.0.2 ou ultérieure
 - CVE Search version 1.0.14 ou ultérieure

Créer des identifiants pour l'intégration de Cortex XSOAR

1. Connectez-vous à Reveal(x) 360.
2. Cliquez sur l'icône System Settings (Paramètres du système) , puis sur **Integrations (Intégrations)**.
3. Cliquez sur la tuile **Cortex XSOAR**.
4. Cliquez sur **Create Credential (Créer un justificatif)**. La page affiche l'ID et le secret générés.
5. Copiez et stockez l'ID et le secret, dont vous aurez besoin pour configurer l'intégration ExtraHop Reveal(x) pour Cortex XSOAR.
6. Cliquez sur **Terminé**.

L'identifiant est également ajouté à la page [ExtraHop REST API Credentials](#) où vous pouvez consulter l'état de l'identifiant, copier l'ID ou supprimer l'identifiant.

Installer et configurer l'intégration ExtraHop pour Cortex XSOAR

1. Téléchargez et installez [l'intégration ExtraHop pour Cortex XSOAR](#) à partir de la place de marché XSOAR, conformément à la documentation de [présentation de la place de marché Cortex XSOAR](#).
2. Dans l'intégration installée, cliquez sur **Add Instance (Ajouter une instance)**.
3. Saisissez un **nom** unique pour l'instance d'intégration.

4. Saisissez l'**URL** du système Reveal(x) 360 auquel cette instance d'intégration se connectera.
5. Sélectionnez **On Cloud** et entrez les identifiants **Client ID** et **Client Secret** que [vous avez créés et copiés depuis votre système Reveal\(x\) 360](#).
6. Terminez la configuration de l'instance d'intégration conformément à la documentation de [référence ExtraHop integration for Cortex XSOAR](#).