

Intégrez Reveal (x) Enterprise à Cortex XSOAR

Publié: 2023-10-01

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

Avant de configurer cette intégration, vous devez [générer une clé d'API REST ExtraHop](#) puis ajoutez la clé lorsque vous [configurer l'intégration ExtraHop Reveal \(x\) pour Cortex XSOAR](#).

Exigences du système

ExtraHop Reveal (x) Enterprise

- Votre compte utilisateur doit avoir [privilèges d'écriture complets](#) ou supérieur sur Reveal (x) Enterprise.
- Votre système Reveal (x) Enterprise doit être connecté à un ExtraHop sonde avec la version 9.2 ou ultérieure du firmware.
- Votre système Reveal (x) Enterprise doit être [connecté à ExtraHop Cloud Services](#).
- Votre système Reveal (x) Enterprise doit être [configuré pour permettre la génération de clés d' API REST](#).

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

Génération d'une clé d'API REST

Vous devez générer une clé d'API ExtraHop avant de pouvoir configurer l' intégration ExtraHop pour Cortex XSOAR. La clé API vous permet d'accéder à l'intégration et d' effectuer des opérations depuis Cortex XSOAR.

1. `<extrahop-hostname-or-IP-address>`Connectez-vous au système ExtraHop via `https ://`.
2. Cliquez sur l'icône utilisateur dans le coin supérieur droit de la page, puis sur **Accès à l'API**.
3. Dans le Générer une clé d'API section, tapez une description pour la nouvelle clé, puis cliquez sur **Générer**.
4. Faites défiler la page vers le Clés d'API section et copiez la clé d'API qui correspond à votre description.

Installation et configuration de l'intégration ExtraHop pour Cortex XSOAR

1. Téléchargez et installez le [Intégration ExtraHop pour Cortex XSOAR](#) depuis le XSOAR Marketplace conformément au [Présentation du marché Cortex XSOAR](#) documentation.
2. À partir de l'intégration installée, cliquez sur **Ajouter une instance**.
3. Tapez un nom unique **Nom** pour l'instance d'intégration.

4. Tapez le **URL** du système Reveal (x) Enterprise auquel cette instance d'intégration se connectera.
5. Désélectionner **Sur le cloud** et entrez le **Clé d'API REST** que vous avez généré à partir de votre système Reveal (x) Enterprise dans le **Clé d'API** champ.
6. Configuration complète de l'instance d'intégration conformément au [Intégration ExtraHop pour Cortex XSOAR Reference](#) [documentation](#).