# Intégrer Reveal(x) Enterprise à Cortex XSOAR

Publié: 2023-09-19

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 des périphériques.

Avant de pouvoir configurer cette intégration, vous devez générer une clé API REST ExtraHop et l'ajouter lorsque vous configurez l'intégration ExtraHop Reveal(x) pour Cortex XSOAR.

## Configuration requise

**ExtraHop Reveal(x) Enterprise**

- Votre compte utilisateur doit disposer de privilèges d'écriture complets ou supérieurs sur Reveal(x) Enterprise.
- Votre système Reveal(x) Enterprise doit être connecté à un capteur ExtraHop avec la version 9.2 ou ultérieure du micrologiciel.
- 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 API REST.

**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

## Générer une clé API REST

Vous devez générer une clé 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 à partir de Cortex XSOAR.

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

## 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) Enterprise auquel cette instance d'intégration se connectera.
5. Désélectionnez **On Cloud** et saisissez la clé API REST que vous avez générée à partir de votre système Reveal(x) Enterprise dans le champ **API Key**.
6. Terminez la configuration de l'instance d'intégration conformément à la documentation de référence de l'intégration ExtraHop pour Cortex XSOAR.