Intégrer Reveal(x) Enterprise avec Splunk SOAR

Publié: 2023-09-19

Cette intégration vous permet d'exporter des détections de menaces réseau, des métriques et des données de paquets de Reveal(x) Enterprise vers Splunk SOAR.

Avant de pouvoir configurer cette intégration, vous devez générer une clé API REST ExtraHop et l'ajouter lors de la configuration de l'application ExtraHop pour Splunk SOAR.

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 9.0 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.

Splunk SOAR

- Vous devez disposer de Splunk SOAR version 5.3 ou ultérieure.

Générer une clé API REST

Vous devez générer une clé API ExtraHop avant de pouvoir configurer l'application ExtraHop pour Splunk SOAR. La clé API vous permet d'accéder à l'intégration et d'effectuer des opérations à partir de Splunk SOAR.

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.

Installation et configuration de l'application ExtraHop pour Splunk SOAR

1. Téléchargez et installez l'application ExtraHop pour Splunk SOAR depuis le site Splunkbase conformément à la documentation Splunk Add-Ons and Apps.
2. Dans l'application installée, cliquez sur **Configure New Asset (Configurer un nouveau poste**).
3. Dans la liste déroulante Type de bien, sélectionnez **Reveal(x) Enterprise**.
4. Saisissez l'**adresse IP ou le nom d'hôte** du système Reveal(x) Enterprise auquel ce poste se connectera.
5. Saisissez la clé que vous avez générée à partir de votre système Reveal(x) Enterprise dans le champ **REST API key**.
6. Cliquez sur le lien **Documentation** sur la page de configuration de la ressource et terminez la configuration d'ExtraHop App for Splunk SOAR conformément à la documentation.