Intégrez Reveal (x) Enterprise à Splunk SOAR

Publié: 2024-02-16

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

Avant de configurer cette intégration, vous devez générer une clé d' API REST ExtraHop puis ajoutez la clé lorsque vous configurer l' application ExtraHop pour Splunk SOAR.

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 9.0 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.

Splunk SOAR

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

Génération d'une clé d'API REST

Vous devez générer une clé d'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 depuis Splunk SOAR.

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.

Installez et configurez l'application ExtraHop pour Splunk SOAR

1. Téléchargez et installez le Application ExtraHop pour Splunk SOAR depuis le site Splunkbase conformément au Extensions et applications Splunk documentation.
2. Dans l'application installée, cliquez sur **Configurer un nouvel actif**.
3. À partir du Type d'actif liste déroulante, sélectionnez **Reveal (x) Enterprise**.
4. Tapez le **adresse IP ou nom d'hôte** du système Reveal (x) Enterprise auquel cet actif sera connecté.
5. Entrez la clé que vous avez générée à partir de votre système Reveal (x) Enterprise dans le **Clé d'API REST** champ.
6. Cliquez sur le **Documentation** cliquez sur la page de configuration des actifs et terminez la configuration de l'application ExtraHop pour Splunk SOAR conformément à la documentation.