Intégrer Reveal(x) 360 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) 360 vers Splunk SOAR.

Pour configurer cette intégration, vous devez créer des informations d'identification Splunk SO AR, puis les ajouter lorsque vous configurez l'application ExtraHop pour Splunk SOAR.

Configuration requise

ExtraHop Reveal(x) 360

- Votre compte utilisateur doit avoir des privilèges 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 9.0 ou ultérieure du micrologiciel.
- Votre système Reveal(x) 360 doit être connecté à ExtraHop Cloud Services.

Splunk

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

Créer les identifiants d'intégration Splunk SOAR

1. Connectez-vous à Reveal(x) 360.
2. Cliquez sur l'icône System Settings (Paramètres système), puis cliquez sur **Integrations (Intégrations)**.
3. Cliquez sur le carreau **Splunk SO** AR.
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 le module complémentaire ExtraHop pour Splunk.
6. Cliquez sur **Done (Terminé)**.

L'identifiant est également ajouté à la page ExtraHop REST API Credentials où vous pouvez afficher l'état de l'identifiant, copier l'ID ou supprimer l'identifiant.

Prochaines étapes
Installation et configuration de l'application ExtraHop pour Splunk SOAR.

Installation et configuration de l'application ExtraHop pour Splunk SOAR

1. Téléchargez l'application ExtraHop pour Splunk SOAR depuis le site SplunkBase.
2. Installez et configurez le module complémentaire conformément à la documentation suivante :
   - A propos de l'installation des modules complémentaires et des applications Splunk
   - Détails de l'application ExtraHop pour Splunk SOAR
3. Dans les champs de configuration suivants, saisissez les informations d'identification que vous avez créées et copiées pour l'intégration Splunk SOAR :
   - **ID du client**
   - **Secret du client**

Prochaines étapes
Exporter les détections, métriques et paquets Reveal(x) 360 vers Splunk SOAR et lancer des actions telles que l'obtention d'informations sur les périphériques ou le marquage d'un périphérique conformément aux instructions de l'application ExtraHop pour Splunk SOAR.