Intégrer Reveal(x) 360 à Splunk

Publié: 2023-09-19

Cette intégration vous permet d'afficher les détections de menaces réseau et les informations comportementales de Reveal(x) 360 dans Splunk.

Pour configurer cette intégration, vous devez créer des identifiants d'intégration Splunk et les ajouter à la configuration du module complémentaire ExtraHop pour Splunk.

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 8.8 ou ultérieure du micrologiciel.
- Votre système Reveal(x) 360 doit être connecté aux ExtraHop Cloud Services.

Splunk

- Vous devez disposer de la version 8.1 de Splunk ou d'une version ultérieure.

Créer les identifiants d'intégration Splunk

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**.
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 **Terminé**.

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

Prochaines étapes
Installez et configurez le module complémentaire ExtraHop pour Splunk.

Installer et configurer le module complémentaire ExtraHop pour Splunk

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

Prochaines étapes
Exportez les détections et les mesures Reveal(x) 360 et affichez-les dans Splunk conformément aux instructions figurant dans le document ExtraHop Add-On for Splunk Details.