Intégrez Reveal (x) 360 à Splunk SOAR

Publié: 2024-04-10

Cette intégration vous permet d'exporter les détections de menaces réseau, les métriques et les données de paquets depuis Reveal (x) 360 vers Splunk SOAR.

Pour configurer cette intégration, vous devez créer des informations dÈRE SPLUNK SOAR puis ajoutez ces informations dcredenti-identification lorsque vous configurer l'application ExtraHop pour Splunk SOAR.

Exigences du système

ExtraHop Reveal (x) 360

- Votre compte utilisateur doit avoir privilèges sur Reveal (x) 360 pour l' administration des systèmes et des accès.
- Votre système Reveal (x) 360 doit être connecté à un ExtraHop sonde avec la version 9.0 ou ultérieure du firmware.
- Votre système Reveal (x) 360 doit être connecté à ExtraHop Cloud Services.

Splunk

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

Création d'informations d'identification pour l'intégration Splunk SOAR

1. Connectez-vous à Reveal (x) 360.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Intégrations**.
3. Cliquez sur **Splunk SOAR** tuile.
4. Cliquez **Créer un justificatif**.
   La page affiche l'identifiant et le secret générés.
5. Optionnel : Si vous avez déjà créé un identifiant pour accéder à l'API REST, vous pouvez l'appliquer à l'intégration. Cliquez **Sélectionnez un justificatif d'identité existant**, sélectionnez un identifiant dans la liste déroulante, puis cliquez sur **Sélectionnez**.
6. Copiez et stockez l'identifiant et le code secret dont vous aurez besoin pour configurer le module complémentaire ExtraHop pour Splunk.
7. Cliquez **Terminé**.

Le justificatif est également ajouté au Informations d'identification de l'API REST ExtraHop page où vous pouvez consulter l'état des informations d'identification, copier l'identifiant ou supprimer les informations d'identification.

Prochaines étapes
Installez et configurez l'application ExtraHop pour Splunk SOAR.

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 **Révéler (x) 360**.

4. Dans les champs de configuration suivants, entrez informations d'identification vous avez créé et copié pour l'intégration Splunk SOAR :
   - **Identifiant du client**
   - **Secret du client**
5. 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.

Prochaines étapes

Exportez les détections, les métriques et les paquets Reveal (x) 360 vers Splunk SOAR et lancez des actions telles que l'obtention d'informations sur l'équipement ou le balisage d'un équipement en suivant la documentation de configuration.