

Intégrez RevealX 360 à Splunk SOAR

Publié: 2024-11-04

Cette intégration vous permet d'exporter des détections de menaces réseau, des métriques et des données de paquets depuis RevealX 360 vers Splunk SOAR.

Pour configurer cette intégration, vous devez [créer des informations d'identification Splunk SOAR](#) puis ajoutez ces informations d'identification lorsque vous [configurez l'application ExtraHop pour Splunk SOAR](#).

Exigences du système

Hop Reveal X 360 supplémentaire

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

[Installation et configuration de l'application ExtraHop pour Splunk SOAR](#).

Installation et configuration de l'application ExtraHop pour Splunk SOAR

1. Téléchargez et installez le [Application ExtraHop pour Splunk SOAR](#) depuis le site de Splunkbase selon le [Modules complémentaires 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 **RevealX 360**.

4. Dans les champs de configuration suivants, entrez le **informations d'identification** que vous avez créé et copié pour l'intégration Splunk SOAR :
 - **Identifiant du client**
 - **Secret du client**
5. Cliquez sur **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 de RevealX 360 vers Splunk SOAR et lancez des actions telles que l'obtention d'informations sur l'équipement ou le balisage d'un appareil en suivant la documentation de configuration.