

Intégrez RevealX 360 à Splunk

Publié: 2024-07-03

Cette intégration vous permet de consulter les détections de menaces réseau et les informations comportementales de RevealX 360 dans Splunk.

Pour configurer cette intégration, vous devez [créer des informations d'identification pour l'intégration Splunk](#) puis ajoutez-les à la configuration du [Module complémentaire ExtraHop pour Splunk](#).

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 8.8 ou ultérieure du firmware.
- Votre système RevealX 360 doit être [connecté à ExtraHop Cloud Services](#).

Splunk

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

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

1. Connectez-vous à RevealX 360.
2. Cliquez sur l'icône Paramètres système  puis cliquez sur **Intégrations**.
3. Cliquez sur **Splunk** 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 du module complémentaire ExtraHop pour Splunk](#).

Installation et configuration du module complémentaire ExtraHop pour Splunk

1. Téléchargez le [Module complémentaire ExtraHop pour Splunk](#) depuis le site de SplunkBase.
2. Installez et configurez le module complémentaire conformément à la documentation suivante :
 - [À propos de l'installation des modules complémentaires Splunk](#)
 - [Module complémentaire ExtraHop pour Splunk Details](#)

3. Dans les champs de configuration suivants, saisissez **informations d'identification** que vous avez créé et copié pour l'intégration Splunk :

- **Identifiant du client**
- **Secret du client**

Prochaines étapes

Exportez les détections et les métriques de RevealX 360 et visualisez-les dans Splunk en suivant les instructions du [Module complémentaire ExtraHop pour Splunk Details](#).