

# Intégrez RevealX Enterprise à Splunk

Publié: 2024-08-08

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

Avant de pouvoir configurer cette intégration, vous devez [générer une clé d'API REST ExtraHop](#) puis ajoutez la clé lorsque vous [configurer le module complémentaire ExtraHop pour Splunk](#).

## Exigences du système

### ExtraHop RevealX Enterprise

- Votre compte utilisateur doit avoir [privilèges d'écriture complets](#) ou supérieur sur RevealX Enterprise.
- Votre système RevealX Enterprise doit être connecté à un ExtraHop sonde avec la version 8.8 ou ultérieure du firmware.
- Votre système RevealX Enterprise doit être [connecté à ExtraHop Cloud Services](#).
- Votre système RevealX Enterprise doit être [configuré pour permettre la génération de clés d' API REST](#).

### Splunk

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

## Génération d'une clé d'API REST

Vous devez générer une clé d'API ExtraHop avant de pouvoir configurer le module complémentaire ExtraHop pour Splunk. La clé API vous permet d'accéder à l'intégration et d'effectuer des opérations depuis Splunk.

1. <extrahop-hostname-or-IP-address>Connectez-vous au système ExtraHop via https ://.
2. Cliquez sur l'icône utilisateur dans le coin supérieur droit de la page, puis sur **Accès à l'API**.
3. Dans le Générer une clé d'API section, tapez une description pour la nouvelle clé, puis cliquez sur **Générer**.
4. Faites défiler la page vers le Clés d'API section et copiez la clé d'API qui correspond à votre description.

## Installation et configuration du module complémentaire ExtraHop pour Splunk

1. Téléchargez et installez le [Module complémentaire ExtraHop pour Splunk](#) depuis le site de SplunkBase, conformément à [Modules complémentaires et applications Splunk](#) documentation.
2. Dans l'application installée, cliquez sur **Configuration**, puis cliquez sur **Ajouter** à partir du Compte onglet.
3. Tapez un numéro unique **Nom du compte**.
4. À partir du Type d'instance liste déroulante, sélectionnez **Instance sur site**.
5. Tapez le **Nom d'hôte** du système RevealX Enterprise auquel ce compte va se connecter.
6. Entrez la clé que vous avez générée à partir de votre système RevealX Enterprise dans le **Clé API** champ.
7. Terminez la configuration du compte conformément à [Module complémentaire ExtraHop pour la documentation Splunk](#) disponible auprès du Détails onglet sur la page de téléchargement.