

Intégrez RevealX Enterprise à QRadar

Publié: 2024-08-08

Cette intégration vous permet de consulter les métriques de RevealX Enterprise dans IBM Security QRadar afin d'obtenir des informations comportementales sur votre environnement.

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

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](#).

QRadar

- Vous devez disposer de la version 7.4.1 FP2 ou ultérieure d'IBM Security QRadar.

Génération d'une clé d'API REST

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

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.

Installez et configurez l'application ExtraHop pour QRadar

1. Téléchargez et installez le [Application ExtraHop pour QRadar](#) depuis le site IBM Exchange.
2. Dans le panneau droit de la page de téléchargement, cliquez sur **Afficher** à côté de Documentation pour télécharger le guide de l'utilisateur au format PDF.
3. Dans l'application installée, cliquez sur **Ajouter un système ExtraHop**.
4. À partir du Type d'instance liste déroulante, sélectionnez **Instance sur site**.
5. Dans le **Système ExtraHop** dans le champ, saisissez le nom d'hôte du système RevealX Enterprise auquel cette application se connectera.
6. Entrez la clé que vous avez générée à partir de votre système RevealX Enterprise dans le **Clé API** champ.
7. Terminez la configuration de l'application ExtraHop pour QRadar conformément à la documentation téléchargée.