

Intégrez RevealX 360 au SIEM nouvelle génération de CrowdStrike Falçon

Publié: 2024-10-26

Cette intégration permet au SIEM de nouvelle génération de CrowdStrike Falçon d'exporter les données d'équipement et de détection depuis le système ExtraHop via des règles de notification de détection. Vous pouvez consulter les données exportées dans le SIEM pour mieux comprendre la façon dont vos appareils communiquent dans votre environnement et pour consulter les détections de menaces réseau.


Cette intégration nécessite que vous réalisiez deux tâches. Un administrateur ExtraHop doit configurer la connexion entre le SIEM et le système ExtraHop. Une fois la connexion établie, vous pouvez [créer des règles de notification de détection](#) qui enverra les données du webhook au SIEM.

Les règles de notification de détection associées à cette intégration sont disponibles sur la page de configuration de l'intégration ainsi que sur le [Règles de notification](#) [tableau](#) auquel vous pouvez accéder depuis les paramètres système.

Avant de commencer

Vous devez répondre à la configuration système suivante :

- ExtraHop RevealX 360
 - 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 9.8 ou ultérieure du firmware.
 - Votre système RevealX 360 doit être [connecté à ExtraHop Cloud Services](#).
- Crowd Strike
 - Vous devez disposer de CrowdStrike Falçon Next-Gen SIEM version 1.0 ou ultérieure.
 - Vous devez configurer un connecteur SIEM HEC nouvelle génération CrowdStrike Falçon pour l'ingestion de données.
 - Votre SIEM doit être en mesure de recevoir les données du webhook. Tu peux [ajouter des adresses IP sources statiques à vos contrôles de sécurité](#) pour autoriser les requêtes provenant de RevealX 360 .


1. Connectez-vous à RevealX 360.
2. Cliquez sur l'icône Paramètres système  puis cliquez sur **Intégrations**.
3. Cliquez sur **SIEM de nouvelle génération CrowdStrike Falçon** tuile.
4. Dans le **URL DE L'API** champ, saisissez l'URL fournie par la configuration du connecteur HEC qui recevra les données du webhook
5. Dans le **Clé API** dans le champ, saisissez la clé qui authentifiera la connexion à l'URL.
6. Sélectionnez l'une des options de connexion suivantes :

Option	Description
Connexion directe	Sélectionnez cette option pour configurer une connexion directe depuis cette console RevealX 360 à l'URL fournie.
Proxy via une sonde connectée	Sélectionnez cette option si votre SIEM ne peut pas prendre en charge une connexion directe depuis cette console RevealX 360 en raison de pare-feux ou d'autres contrôles de sécurité. <ol style="list-style-type: none"> 1. Dans le menu déroulant, sélectionnez une sonde connectée qui fera office de proxy.

Option	Description
7.	Cliquez Envoyer un événement de test pour établir une connexion entre le système ExtraHop et le serveur SIEM et pour envoyer un message de test au serveur.
	Un message s'affiche pour indiquer si la connexion a réussi ou échoué. Si le test échoue, modifiez la configuration et testez à nouveau la connexion.
8.	Optionnel : Sélectionnez Ignorer la vérification des certificats de serveur pour contourner la vérification du certificat du serveur SIEM.
9.	Cliquez Enregistrer .

Création d'une règle de notification de détection pour une intégration SIEM

Avant de commencer

- Votre compte utilisateur doit avoir accès au module NDR pour créer des règles de notification de détection de sécurité.
 - Votre compte utilisateur doit avoir accès au module NPM pour créer des règles de notification de détection des performances.
 - Vous pouvez également créer des règles de notification de détection dans les paramètres système. Pour plus d'informations, voir [Création d'une règle de notification de détection](#).
1. Connectez-vous à RevealX 360.
 2. Cliquez sur l'icône Paramètres système  puis cliquez sur **Intégrations**.
 3. Cliquez sur la vignette du SIEM qui sera la cible de la règle de notification de détection.
 4. Cliquez **Ajouter une règle de notification**.
Le Créer une règle de notification La fenêtre s'ouvre dans un nouvel onglet et les champs suivants sont définis sur les valeurs par défaut.
 - Le **Nom** le champ est défini sur le nom du SIEM.
 - Le **Type d'événement** le champ est défini sur **Détection de sécurité**.
 - Le **Cible** le champ est défini sur l'intégration SIEM.
 5. Dans le Descriptif champ, ajoutez des informations sur la règle de notification.
 6. Dans le Critères section, cliquez sur **Ajouter des critères** pour spécifier les critères qui généreront une notification.
 - **Recommandé pour le triage**
 - **Score de risque minimum**
 - **Tapez**
 - **Catégorie**
 - **Technique MITRE** (NDR uniquement)
 - **Délinquant**
 - **Victime**
 - **Rôle de l'appareil**
 - **Participant**
 - **Site**

Les options de critères correspondent à [options de filtrage sur la page Détections](#).

7. Dans Options de charge utile, sélectionnez si vous souhaitez envoyer le [charge utile par défaut](#) ou saisissez une charge utile JSON personnalisée.

- **Charge utile par défaut**

Remplissez la charge utile du webhook avec un ensemble de champs de détection de base.

Dans la liste déroulante Ajouter des champs de charge utile, vous pouvez cliquer sur les champs supplémentaires que vous souhaitez inclure dans la charge utile.

- **Charge utile personnalisée**

Tapez votre propre charge utile directement dans la fenêtre Aperçu de la charge utile (JSON).



Conseil Pour personnaliser une charge utile par défaut, copiez-la depuis la fenêtre d'aperçu, puis passez à **Charge utile personnalisée**, puis collez la charge utile dans la fenêtre d'aperçu pour la modifier.

Vous pouvez également copier-coller des exemples de charges utiles à partir du [Référence de notification du Webhook](#).

8. Cliquez **Connexion de test**.

Un message intitulé Notification de test sera envoyé pour confirmer la connexion.

9. Dans le Options section, la **Activer la règle de notification** La case à cocher est activée par défaut. Décochez la case pour désactiver la règle de notification.

10. Cliquez **Enregistrer**.

Prochaines étapes

- Revenez à la page de configuration de l'intégration pour vérifier que votre règle a été créée et ajoutée au tableau.
- Cliquez **Modifier** pour modifier ou supprimer une règle.

Integration Status

Status: ● Integration Enabled
 Proxy Sensor: ● prod-pdx-eda-6100v

[Send Test Event](#) [Change Credentials](#) [Delete Credentials](#)

Notification Rules

This integration is configured as the target for the following notification rules.

Name	Event Type	Status	Author	
All System Alerts	Security Detection	● Enabled	maebybluth	Edit
NOC	Performance Detection	● Disabled	tobias	Edit

[Add Notification Rule](#)