

Intégrez RevealX 360 à Splunk Enterprise Security SIEM

Publié: 2025-03-28

Cette intégration permet au SIEM Splunk Enterprise Security d'exporter les données de détection depuis le système ExtraHop via des règles de notification de détection. Vous pouvez consulter les données exportées dans le SIEM afin de mieux comprendre les menaces de sécurité dans votre environnement et d'accélérer les temps de réponse.

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.

Une fois la connexion établie et les règles de notification configurées, vous pouvez [installer l'application ExtraHop RevealX pour Splunk](#) sur votre Splunk SIEM. L'application fournit un tableau de bord des données de détection et des règles de corrélation qui génèrent des alertes de détection dans Splunk.

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](#).
 - Splunk
 - Vous devez disposer de Splunk Enterprise version 9.1 ou ultérieure
 - Vous devez configurer un Splunk Enterprise [connecteur HEC](#) 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 **Splunk Enterprise Security (SIEM)** tuile.
 4. Procédez comme suit pour configurer la connexion entre le SIEM Splunk Enterprise Security et le système ExtraHop :
 - a) Dans le **Hôte d'ingestion** dans le champ, saisissez l'URL ou le nom d'hôte du serveur SIEM qui recevra les données du webhook.
 - b) Dans le **Port d'ingestion** dans le champ, saisissez le numéro de port qui recevra les données du webhook.
 - c) Dans le **Indice** champ, saisissez le nom de l'index qui stockera les données du webhook.
 - d) Dans le **Jeton HEC** dans le champ, saisissez le jeton qui authentifiera la connexion à l'hôte d'ingestion.
 5. 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.

Option	Description
Proxy via une sonde connectée	<p>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.</p> <ol style="list-style-type: none"> 1. Dans le menu déroulant, sélectionnez une sonde connectée qui fera office de proxy. 2. (Facultatif) : Sélectionnez Connectez-vous via le serveur proxy global configuré pour la sonde sélectionnée pour envoyer des données via un proxy mondial. (Disponible uniquement si la sonde sélectionnée exécute RevealX Enterprise.
6. 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.
7. Optionnel : Sélectionnez Ignorer la vérification des certificats de serveur pour contourner la vérification du certificat du serveur SIEM.	
8. 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](#).

- En dessous 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 le menu déroulant Ajouter des champs de charge utile, vous pouvez cliquer sur les champs supplémentaires que vous souhaitez inclure dans la charge utile.
 - Charge utile personnalisée**
Renseignez la charge utile du webhook avec un JSON personnalisé.
Vous pouvez modifier la charge utile personnalisée suggérée dans le **Modifier la charge utile** fenêtre.
- Cliquez **Connexion de test**.
Un message intitulé Notification de test sera envoyé pour confirmer la connexion.
- 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.
- 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.

The screenshot shows the 'Integration Status' section with 'Status: Integration Enabled' and 'Proxy Sensor: prod-pdx-eda-6100v'. Below this are buttons for 'Send Test Event', 'Change Credentials', and 'Delete Credentials'. The 'Notification Rules' section indicates that the 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

At the bottom of the Notification Rules section, there is a link: [Add Notification Rule](#).

Installez l'application ExtraHop RevealX pour Splunk

L'application ExtraHop RevealX pour Splunk reçoit les données de détection ExtraHop RevealX du collecteur d'événements Splunk afin de créer un tableau de bord de détection et de générer des alertes d'événements de détection dans Splunk en fonction de règles de corrélation.

- Téléchargez le [Application ExtraHop RevealX pour Splunk](#) de Splunkbase.

2. Connectez-vous à votre Splunk SIEM.
3. À partir du **Apps** liste déroulante, cliquez sur **Gérer les applications**.
4. Dans le coin supérieur droit, cliquez sur **Installez l'application à partir d'un fichier**.
5. Cliquez **Choisissez un fichier**, puis sélectionnez l'application téléchargée.
6. Cliquez **Téléverser** et suivez les instructions.
7. À partir du **Apps** liste déroulante, cliquez sur **Application ExtraHop RevealX pour Splunk** pour ouvrir l'application dans votre Splunk SIEM.

Le tableau de bord ExtraHop Detections Overview s'affiche par défaut et contient les graphiques suivants :

Diagramme	Descriptif
Détections recommandées	Affiche le nombre total de détections recommandées générées au cours de la période sélectionnée.
Nombre total de détections	Affiche le nombre de détections générées au cours de la période sélectionnée.
Score de risque maximal	Affiche l'indice de risque le plus élevé associé aux détections générées au cours de la période sélectionnée.
Détections les plus recommandées	Affiche les 10 détections les plus recommandées générées au cours de la période sélectionnée et le nombre de fois que chaque détection s'est produite.
Principales catégories de détection	Affiche les 10 principales catégories de détection associées aux détections générées au cours de la période sélectionnée, ainsi que le pourcentage et le nombre de détections pour chaque catégorie.
Les meilleures techniques MITRE	Affiche les 10 principales techniques MITRE associées aux détections générées au cours de la période sélectionnée et le nombre de détections pour chaque technique.
Principales sources	Affiche les 10 principaux hôtes sources associés aux détections générées au cours de la période sélectionnée et le nombre de détections pour chaque source.
Destinations les plus prisées	Affiche les 10 principaux hôtes de destination associés aux détections générées au cours de la période sélectionnée et le nombre de détections pour chaque destination.
Sources et destinations	Affiche le flux de sources et de destinations associés aux détections générées au cours de la période sélectionnée.
Détections récentes	Affiche les détections les plus récentes générées au cours de la période sélectionnée et les détails de détection tels que le score de risque, la catégorie et l'URL

8. Procédez comme suit pour consulter les règles de corrélation fournies dans l'application :
 - a) À partir du **Réglages** liste déroulante, cliquez sur **Recherches, rapports et alertes**.

- b) À partir du **Propriétaires** liste déroulante, cliquez sur **Tous**
- Le tableau affiche les règles de corrélation suivantes qui sont activées par défaut :
- Des alertes de faible gravité sont générées pour les détections dont le score de risque est compris entre 1 et 30.
 - Des alertes de gravité moyenne sont générées pour les détections dont le score de risque est compris entre 31 et 79.
 - Des alertes de gravité élevée sont générées pour les détections dont le score de risque est compris entre 80 et 99.
9. À partir du **Activité** liste déroulante, cliquez sur **Alertes déclenchées** pour consulter les alertes générées à partir des règles de corrélation.