

Intégrez RevealX 360 à CrowdStrike FalconLogScale

Publié: 2024-07-03

Cette intégration vous permet d'exporter les détections de sécurité de RevealX 360 vers LogScale pour afficher les données de détection dans un système centralisé, améliorant ainsi le contexte des détections et réduisant le temps nécessaire pour confirmer les menaces.

Exigences du système

Hop Reveal X 360 supplémentaire

- Votre compte utilisateur doit disposer de privilèges sur RevealX 360 pour l'administration du système et des accès ou la configuration du cloud.
- Votre système RevealX 360 doit être connecté à un ExtraHop sonde avec la version 9.3 ou ultérieure du firmware.
- Votre système RevealX 360 doit être [connecté à ExtraHop Cloud Services](#).

Balance à journaux CrowdStrike Falcon

- Vous devez disposer de CrowdStrike Falcon LogScale version 1.92.0 ou ultérieure.
- Vous devez configurer [API de collecte d'événements HTTP LogScale](#) pour l'ingestion de données.

Configurer l'intégration de CrowdStrike Falcon LogScale

1. Connectez-vous au système RevealX 360.
2. Cliquez sur l'icône Paramètres système  puis cliquez sur **Intégrations**.
3. Cliquez sur **Balance à journaux CrowdStrike Falcon** tuile.
4. À partir du **Hôte LogScale** dans la liste déroulante, sélectionnez le nom d'hôte de votre point de terminaison LogScale.
5. Optionnel : Si vous avez sélectionné un centre de données CrowdStrike comme hôte, saisissez votre sous-domaine client dans le **Préfixe du client** champ. Le préfixe est ajouté au nom d'hôte et affiché dans Hôte d'ingestion LogScale champ, similaire à l'exemple suivant :

Connect to CrowdStrike Falcon LogScale

LogScale Host
CrowdStrike Datacenter US-1

Customer Prefix
extrahop

LogScale Ingest Host
extrahop.ingest.logscale.us-1.crowdstrike.com

Ingest Token
.....

Send Test Event Cancel Save

6. Dans le **Jeton d'ingestion** dans le champ, saisissez le jeton d'ingestion que vous avez configuré pour le collecteur d'événements HTTP LogScale.
7. Cliquez **Envoyer un événement de test**, puis vérifiez que l'événement a été reçu par votre point de terminaison LogScale. L'arrivée de l'événement test peut prendre plusieurs minutes.
8. Optionnel : Configurez les options d'intégration suivantes :
 - a) Cliquez **Exporter les détections de sécurité de RevealX 360**.
 - b) Cliquez **Ajouter des critères** pour configurer le filtre qui détermine quelles détections de sécurité sont exportées vers votre point de terminaison LogScale.
9. Optionnel : Cliquez **Modifier les informations d'identification** pour mettre à jour le nom d'hôte LogScale ou le jeton HEC.
10. Optionnel : Cliquez **Désactiver l'intégration** pour conserver les informations d'identification nécessaires et les options actuelles, mais désactiver l'intégration LogScale.
11. Cliquez **Enregistrer**.