

Intégrer Reveal(x) 360 avec CrowdStrike Falcon LogScale

Publié: 2023-09-19

Cette intégration vous permet d'exporter les détections de sécurité de Reveal(x) 360 vers LogScale afin de visualiser les données de détection dans un système centralisé, améliorant ainsi le contexte des détections et réduisant le temps de confirmation des menaces.

Configuration requise

ExtraHop Reveal(x) 360

- Votre compte utilisateur doit avoir des privilèges sur Reveal(x) 360 pour l'administration du système et des accès ou la configuration du cloud.
- Votre système Reveal(x) 360 doit être connecté à un capteur ExtraHop avec la version 9.3 ou ultérieure du micrologiciel.
- Votre système Reveal(x) 360 doit être connecté à ExtraHop Cloud Services.

CrowdStrike Falcon LogScale

- Vous devez disposer de CrowdStrike Falcon LogScale version 1.92.0 ou ultérieure.
- Vous devez configurer l'[API LogScale HTTP Event Collector](#) pour l'acquisition de données.

Configurer l'intégration de CrowdStrike Falcon LogScale

1. Connectez-vous au système Reveal(x) 360.
2. Cliquez sur l'icône System Settings (Paramètres du système) , puis cliquez sur **Integrations (Intégrations)**.
3. Cliquez sur la tuile **CrowdStrike Falcon LogScale**.
4. Dans le champ **LogScale Host**, tapez ou sélectionnez le nom d'hôte de votre point d'extrémité LogScale.
5. Dans le champ **HEC Token**, saisissez le jeton d'ingestion que vous avez configuré pour le collecteur d'événements HTTP LogScale.
6. Cliquez sur **Send Test Event**, puis vérifiez que l'événement a été reçu par votre point d'extrémité LogScale. L'arrivée de l'événement test peut prendre plusieurs minutes.
7. Optionnel : Configurez l'option d'intégration suivantes:
 - a) Cliquez sur **Exporter les détections de sécurité Reveal(x) 360**.
 - b) Cliquez sur **Add Criteria** pour configurer le filtre qui détermine quelles détections de sécurité sont exportées vers votre point de terminaison LogScale.
8. Optionnel : Cliquez sur **Change Credentials** pour mettre à jour le nom d'hôte LogScale ou le jeton HEC.
9. Optionnel : Cliquez sur **Désactiver l'intégration** pour conserver les informations d'identification et les options actuelles, mais désactiver l'intégration LogScale.
10. Cliquez sur **Enregistrer**.