

Intégrez RevealX 360 à Cisco XDR

Publié: 2025-02-13

Intégrez ExtraHop RevealX 360 à Cisco XDR, un outil de détection et de réponse basé sur le cloud, pour améliorer la visibilité des points de terminaison et accélérer la réponse à la détection. En créant des informations d'identification pour l' API REST ExtraHop, vous pouvez exporter les données d'équipement et de détection RevealX vers Cisco XDR via les opérations de l'API REST ExtraHop.

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**.
 - Cisco XDR
 - Vous devez avoir un rôle d'administrateur sur Cisco XDR.
 - Vous devez disposer du niveau de licence Cisco XDR Advantage ou Cisco XDR Premium.
1. Procédez comme suit pour créer les informations d'identification de l'API REST ExtraHop pour l'intégration :
 - a) Connectez-vous à RevealX 360.
 - b) Cliquez sur l'icône Paramètres système  puis cliquez sur **Intégrations**.
 - c) Cliquez sur la vignette de l'intégration que vous souhaitez configurer.
 - d) Cliquez **Créer un justificatif**.
La page affiche l'identifiant et le secret générés.
 - e) Optionnel : Si vous avez déjà créé un identifiant pour accéder à l'API REST, vous pouvez l'appliquer à l'intégration. Cliquez **Sélectionnez un justificatif d'identité existant**, sélectionnez un identifiant dans le menu déroulant, puis cliquez sur **Sélectionnez**.
 - f) Copiez et stockez l'identifiant et le code secret dont vous aurez besoin pour configurer l'application ExtraHop.
 - g) Cliquez **Terminé**.
L'identifiant est ajouté au **Informations d'identification de l'API REST ExtraHop** page où vous pouvez consulter l'état des informations d'identification, copier l'identifiant ou supprimer les informations d'identification.
 2. Effectuez les étapes suivantes pour **ajouter l'intégration ExtraHop à Cisco XDR**:
 - a) Depuis votre Cisco XDR, cliquez sur **Administration**, puis sélectionnez **Intégrations**.
 - b) Cliquez sur **Tierce** onglet, puis cliquez sur **Commencez** ou **Activer** depuis la carte ExtraHop RevealX 360.
 - c) Cliquez sur l'icône d'agrandissement pour ouvrir le guide d'intégration.
 - d) Renseignez les champs conformément au guide d'intégration détaillé, qui inclut la saisie des informations d'identification de l'API ExtraHop REST que vous avez créées et copiées pour l'intégration.
 - e) Cliquez **Ajouter**.
 3. Exportez l'équipement RevealX et les données de détection vers votre Cisco XDR via **API REST ExtraHop**.