Intégrez Reveal (x) 360 à CrowdStrike

Publié: 2024-01-22

Intégrez ExtraHop Reveal (x) 360 à CrowdStrike pour améliorer la visibilité et le contrôle de vos appareils.

Exigences du système

ExtraHop Reveal (x) 360

- Votre compte utilisateur doit disposer de 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 ExtraHop sonde avec la version 8.8 ou ultérieure du firmware. La version 8.9 ou ultérieure est requise pour activer l' option d'intégration pour le confinement des équipements.
- Votre système Reveal (x) 360 doit être connecté à ExtraHop Cloud Services.

Crowd Strike

- Vous devez disposer du jeton de sécurité fourni par ExtraHop dans votre e-mail de bienvenue ou dans votre identifiant client, votre secret client et votre point de terminaison de l'API CrowdStrike.

  Note: Si vous effectuez une mise à niveau de votre système ExtraHop, vous devrez saisir de nouvelles informations d'identification pour configurer de nouvelles options d'intégration.
- La portée du client de l'API CrowdStrike doit inclure les autorisations READ pour Indicators (Falçon) afin d'activer les options d'intégration pour l'affichage de liens vers les appareils CrowdStrike ou les renseignements sur les menaces de CrowdStrike Falçon.
- La portée du client de l'API CrowdStrike doit inclure les autorisations READ et WRITE pour les hôtes afin d'activer l'option d'intégration pour le confinement des équipements.

Configurer l'intégration de CrowdStrike

1. Connectez-vous au système Reveal (x) 360.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Intégrations**.
3. Cliquez sur la vignette CrowdStrike.
4. Choisissez l'une des options suivantes :
   - Cliquez **Entrez le jeton de sécurité** si vous avez reçu un jeton d'ExtraHop lors de votre inscription à un essai gratuit.
     1. Collez le jeton de sécurité de votre e-mail de bienvenue dans le **Jeton de sécurité CrowdStrike** champ.
     2. Cliquez **Connecter**.
   - Cliquez **Entrez l'ID client et le code secret**.
     1. Entrez votre identifiant client CrowdStrike dans le champ ID client de l'API.
     2. Entrez le secret de votre client CrowdStrike dans le champ Secret du client de l'API.
     3. Sélectionnez le point de terminaison de votre région d'API CrowdStrike dans la liste déroulante.
     4. Cliquez **Connexion de test** pour s'assurer que le système ExtraHop peut communiquer avec CrowdStrike Falçon .
     5. Cliquez **Connecter**.

5. Optionnel : Configurez l'une des options d'intégration suivantes :

   Note: L'intégration ne peut pas importer plus de 50 000 indicateurs au total depuis CrowdStrike.

   - Sélectionnez **Afficher des liens vers CrowdStrike Falçon à des fins de renseignement sur les menaces** . Cliquez sur les liens pour afficher renseignements sur les menaces dans CrowdStrike Falçon.
   - Sélectionnez **Afficher les liens vers CrowdStrike pour les appareils sur lesquels le logiciel Falçon est installé**. Les appareils doivent être locaux et disposer d'une adresse MAC. Les liens apparaissent sur le Page de présentation de l'appareil pour les appareils CrowdStrike.
   - Sélectionnez **Permettre aux utilisateurs de contenir les appareils CrowdStrike détectés dans Reveal (x) 360**. (Nécessite un accès en lecture et en écriture aux hôtes). Une option apparaît pour initier le confinement des appareils CrowdStrike qui participent à une détection de sécurité. Les utilisateurs doivent disposer d'un accès via la politique globale de contrôle d'accès aux détections et disposer de privilèges d'écriture complets ou supérieurs pour lancer le confinement.

6. Cliquez **Enregistrer**.