Intégrez Reveal (x) 360 à CrowdStrike

Publié: 2023-10-24

Intégrez ExtraHop Reveal (x) 360 à CrowdStrike pour obtenir une visibilité accrue et des renseignements sur les menaces concernant 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 pour 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.

CrowdStrike

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

  Note: Si vous mettez à niveau votre système ExtraHop, vous devrez saisir de nouvelles informations deacdentification pour configurer les nouvelles options d'intégration.
- Le champ d'application du client API CrowdStrike doit inclure les autorisations READ pour les indicateurs (FalconX) afin d'activer les options d'intégration permettant d'afficher des liens vers des appareils CrowdStrike ou d'importer des renseignements sur les menaces depuis CrowdStrike Falçon.
- Le champ d'application du client 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 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 code 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 secret**.
     1. Entrez votre identifiant client CrowdStrike dans le champ ID client API.
     2. Entrez le secret de votre client CrowdStrike dans le champ Secret du client API.
     3. Sélectionnez le point de terminaison de votre région API CrowdStrike dans la liste déroulante.
     4. Cliquez **Tester la connexion** 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 **Importez des informations sur les menaces pour les adresses IP depuis CrowdStrike Falçon**. Un signal visuel apparaît dans le système Reveal (x) 360 pour toute activité correspondant à une entrée du CrowdStrike collecte des menaces.
- Sélectionnez **Importez des informations sur les menaces pour les domaines et les noms d'hôtes depuis CrowdStrike Falçon**. Un signal visuel apparaît dans le système Reveal (x) 360 pour toute activité correspondant à une entrée de la collecte des menaces de CrowdStrike.
- 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 Page de présentation de l'appareil pour les appareils CrowdStrike.
- Sélectionnez **Permettre aux utilisateurs d'empêcher les appareils CrowdStrike d'être détectés dans Reveal (x) 360**. (Nécessite un accès en lecture et en écriture aux hôtes). Une option semble initier le confinement des appareils CrowdStrike qui participent à une détection de sécurité. Les utilisateurs doivent être autorisés à accéder par le biais de la politique globale de contrôle d'accès aux détections et disposer de privilèges d'écriture complète ou supérieurs pour initier le confinement.

6. Cliquez **Sauver**.