Intégrez RevealX 360 à QRadar SOAR

Publié: 2025-02-13

Cette intégration permet à IBM Security QRadar SOAR d'exporter les données d'équipement et de détection depuis le système ExtraHop via l'API REST ExtraHop. Vous pouvez consulter les données exportées dans QRadar SOAR pour avoir un aperçu de la façon dont vos appareils communiquent dans votre environnement et pour visualiser les détections de menaces réseau.

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 9.6 ou ultérieure du firmware.
  - Votre système RevealX 360 doit être connecté à ExtraHop Cloud Services.
  - Votre système RevealX 360 doit être configuré pour permettre la génération de clés d'API REST.
  - S'il est configuré, liste d'autorisations doit inclure l'adresse IP qui permettra d'accéder à l' API REST.
- QRadar SOAR
  - Vous devez disposer de QRadar SOAR version 46.0 ou ultérieure

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. Procédez comme suit pour installer et configurer l'application ExtraHop pour QRadar SOAR :
   a) Téléchargez et installez le ExtraHop pour IBM SOAR application depuis le site IBM App Exchange.
   b) Dans le panneau droit du site de téléchargement, cliquez sur **Afficher** à côté de Documentation pour télécharger un PDF du guide d'utilisation de l'application.
   c) Dans la configuration de l'application, entrez les informations d'identification de l'API REST ExtraHop que vous avez créées et copiées pour l'intégration QRadar SOAR :
      - **ID d'authentification**
      - **Clé secrète**
   d) Terminez la configuration de l'application en suivant les instructions de la documentation.