Gérez les collections de menaces

Publié: 2024-01-22

ExtraHop Reveal (x) peut s'appliquer renseignement sur les menaces à l'activité de votre réseau en fonction des collections de menaces fournies par Extrahop, CrowdStrike ou d'autres sources gratuites et commerciales.

Avant de commencer

- En savoir plus sur renseignements sur les menaces.
- Tu dois avoir Privilèges d'administration du système et des accès sur chaque console et sonde pour gérer les collections de menaces.
- Si votre déploiement ExtraHop inclut une console, nous vous recommandons de gestion des transferts de tous les capteurs connectés à la console pour activer ou désactiver les collectes de menaces intégrées sur l'ensemble de votre système.

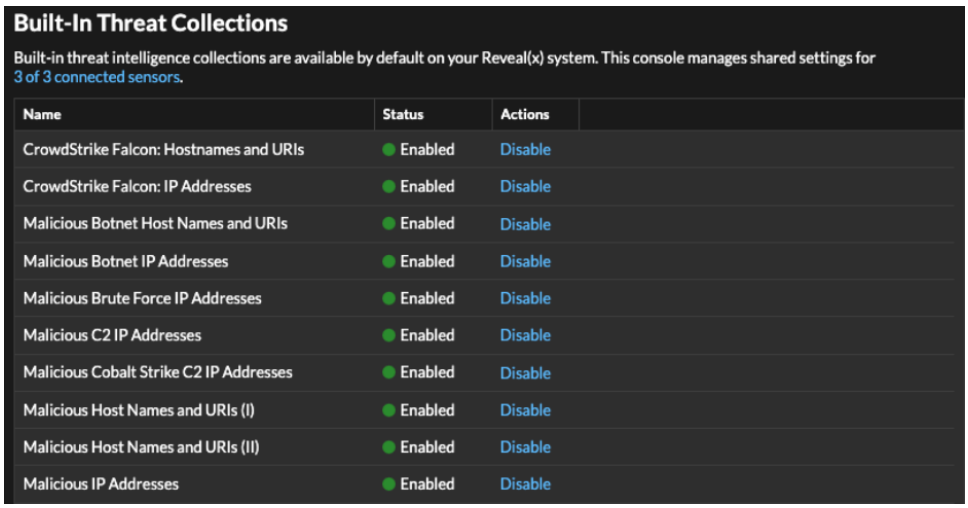
Activer ou désactiver les collections de menaces intégrées

Les collections de menaces intégrées d'ExtraHop et de CrowdStrike identifient les indicateurs de compromission dans l'ensemble du système.

Les collections de menaces activées mettent automatiquement à jour les systèmes connectés aux services cloud ExtraHop. Vous pouvez confirmer la connectivité sur Services cloud ExtraHop page dans les paramètres d'administration.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Renseignements sur les menaces**.
3. Dans le tableau des collections de menaces intégrées, cliquez sur **Activer** ou **Désactiver** dans la colonne Actions.

   Le système vérifie automatiquement les mises à jour des collections de menaces ExtraHop et CrowdStrike toutes les 6 heures.



Importer une collecte des menaces

Téléchargez des collections de menaces provenant de sources gratuites et commerciales pour identifier les indicateurs de compromission dans l'ensemble du système ExtraHop. Étant donné que les données relatives aux renseignements sur les menaces sont mises à jour fréquemment (parfois quotidiennement), il se peut que vous deviez mettre à jour une collecte des menaces avec les données les plus récentes. Lorsque vous mettez à jour une collecte des menaces avec de nouvelles données, la collection est supprimée et remplacée, et n'est pas ajoutée à une collection existante.

Vous devez télécharger les collections de menaces individuellement sur votre console et sur tous les capteurs connectés.

Voici quelques considérations concernant le téléchargement de collections de menaces.

- Les collections de menaces personnalisées doivent être formatées dans STIX (Structured Threat Information Expression) sous forme de fichiers TAR compressés, tels que .TGZ ou TAR.GZ. Reveal (x) prend actuellement en charge les versions 1.0 à 1.2 de STIX.
- Vous pouvez télécharger directement des collections de menaces sur Reveal (x) 360 pour une gestion autonome capteurs. Contactez le support ExtraHop pour télécharger une collecte des menaces vers ExtraHop Managed capteurs.
- Le nombre maximum d'observables qu'une collecte des menaces peut contenir dépend de la mémoire et de la licence de votre sonde. Pour garantir la réussite des téléchargements dans les limites de vos capteurs et de votre licence, nous vous recommandons de diviser les collections en fichiers de moins de 3 000 observables, avec une taille totale de collection inférieure à 1 million d'observables. Contactez votre représentant ExtraHop pour plus d'informations sur les limites de licence et de plate-forme pour le téléchargement de collections de menaces.
- Tu peux télécharger des fichiers STIX via l'API REST.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Renseignements sur les menaces**.
3. Cliquez **Gérer les collections personnalisées**.
4. Cliquez **Télécharger une nouvelle collection**.
5. Dans le champ ID de collection, saisissez un identifiant de collection unique. L'identifiant ne peut contenir que des caractères alphanumériques et les espaces ne sont pas autorisés.
6. Cliquez **Choisissez un fichier** et sélectionnez un `.tgz` fichier contenant un fichier STIX.
7. Tapez un nom d'affichage dans le champ Nom d'affichage.
8. Cliquez **Collection de téléchargements**.
9. Répétez ces étapes pour chaque connexion sonde et sur tous consoles.