

Gérer les collections de menaces

Publié: 2023-09-19

ExtraHop Reveal(x) peut appliquer des [renseignements sur les menaces](#) à l'activité de votre réseau en fonction des collections de menaces fournies par Extrahop, des intégrations de partenaires ou d'autres sources gratuites et commerciales

. Pour ajouter des renseignements sur les menaces provenant de CrowdStrike, voir [Intégrer Reveal\(x\) 360 à CrowdStrike](#).


Avant de commencer

- En savoir plus sur les [renseignements sur](#) les menaces.
- Vous devez disposer des [privilèges d'administration du système et des accès](#) sur chaque console et capteur pour gérer les collections de menaces.

Activer ou désactiver les collections de menaces créées par ExtraHop

Les collections de menaces ExtraHop sont activées par défaut et identifient les indicateurs de compromission dans l'ensemble du système.

Les collections de menaces ExtraHop mettent automatiquement à jour les systèmes connectés aux services ExtraHop Cloud. Vous pouvez confirmer la connectivité sur la page [ExtraHop Cloud Services](#) 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 sur **Décisionnel** sur les menaces.
3. Dans le tableau ExtraHop Threat Intelligence, cochez ou décochez la case **Enabled (Activé)** dans la colonne Status (État).

Le système vérifie automatiquement les mises à jour des collections de menaces créées par ExtraHop toutes les 12 heures. La colonne Dernière mise à jour indique la date et l'heure de la dernière mise à jour.

ExtraHop Threat Collections			
ExtraHop-curated threat intelligence collections are available by default on your Reveal(x) system.			
Name	Last Updated	Status	
Malicious Host Names and URIs	2021-02-27 14:30:26	<input checked="" type="checkbox"/> Enabled	
Malicious Botnet IP Addresses	2021-10-25 14:54:36	<input checked="" type="checkbox"/> Enabled	
Malicious Botnet Host Names and URIs	2021-10-25 14:54:36	<input checked="" type="checkbox"/> Enabled	
Malicious Brute Force IP Addresses	2021-10-25 14:54:37	<input checked="" type="checkbox"/> Enabled	
Malicious IP Addresses from Machine Learning Service	2021-07-08 14:53:11	<input checked="" type="checkbox"/> Enabled	
Malicious Cobalt Strike C2 IP Addresses	2021-10-25 14:54:37	<input checked="" type="checkbox"/> Enabled	
Malicious IP Addresses	2021-10-25 14:54:36	<input checked="" type="checkbox"/> Enabled	
Malicious Host Names and URIs from Machine Learning Service	2021-07-23 15:25:01	<input checked="" type="checkbox"/> Enabled	
Malicious C2 IP Addresses	2021-10-25 14:54:37	<input checked="" type="checkbox"/> Enabled	


Télécharger une collection de menaces

Téléchargez des collections de menaces provenant de sources gratuites et commerciales afin d'identifier les indicateurs de compromission dans l'ensemble du système ExtraHop. Les données de renseignements sur les menaces étant fréquemment mises à jour (parfois quotidiennement), il se peut que vous deviez mettre à jour une collection de menaces avec les données les plus récentes. Lorsque vous mettez à jour une

collection de menaces avec de nouvelles données, la collection est supprimée et remplacée, et non ajoutée à une collection existante.

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

.

- Les collections de menaces personnalisées doivent être formatées en STIX (Structured Threat Information eXpression) sous forme de fichiers TAR.GZ. Reveal(x) prend actuellement en charge les versions STIX 1.0 - 1.2.
 - Vous pouvez télécharger directement des collections de menaces vers Reveal(x) 360 pour les capteurs autogérés. Contactez l'assistance ExtraHop pour télécharger une collection de menaces vers les capteurs gérés par ExtraHop.
 - Le nombre maximum d'observables qu'une collection de menaces peut contenir dépend de votre plateforme et de votre licence. Contactez votre représentant ExtraHop pour plus d'informations.
 - Vous pouvez 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 sur **Intelligence des menaces**.
 3. Cliquez sur **Gérer les collections personnalisées**.
 4. Cliquez sur **Télécharger une nouvelle collection**.
 5. Dans le champ ID de la collection, saisissez un ID de collection unique. L'ID ne peut contenir que des caractères alphanumériques et les espaces ne sont pas autorisés.
 6. Cliquez sur **Choisir un fichier** et sélectionnez un fichier `.tgz` contenant un fichier STIX.
 7. Saisissez un nom d'affichage dans le champ Nom d'affichage.
 8. Cliquez sur **Télécharger la collection**.
 9. Répétez ces étapes pour chaque capteur connecté et sur toutes les consoles.