Gérez les collections de menaces

Publié: 2025-02-04

ExtraHop RevealX 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 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.

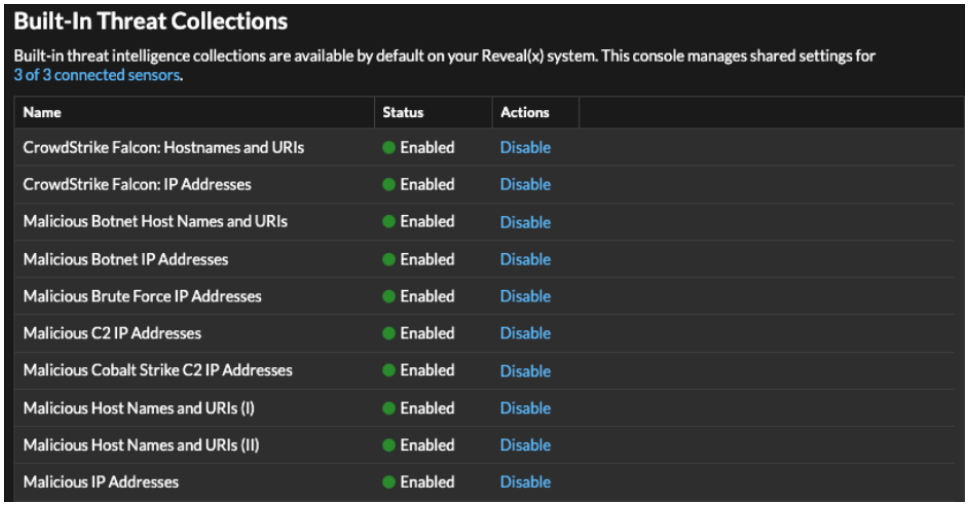
Activer ou désactiver les collections de menaces intégrées

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.



Télécharger 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.

Important: Les téléchargements de fichiers STIX sont désormais obsolètes et la date de suppression est prévue pour mars 2025.

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. RevealX prend actuellement en charge le téléchargement des versions 1.0 à 1.2 des fichiers STIX.
- Vous pouvez télécharger directement des collections de menaces sur RevealX 360 pour une gestion autonome capteurs. Contactez le support ExtraHop pour télécharger une collection de menaces sur 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 tous consoles et chacun connecté sonde.

Ajouter un flux TAXII

Les collections de menaces peuvent être transmises à votre environnement via le protocole TAXII (Trusted Automated Exchange of Intelligence Information).

Les flux TAXII peuvent varier en termes de qualité ou de pertinence par rapport à votre environnement. Pour maintenir la précision et réduire le bruit, nous vous recommandons de n'ajouter que des flux provenant de sources fiables fournissant des renseignements sur les menaces de haute qualité.

Avant de commencer

- Les indicateurs de flux TAXII sont traités par ExtraHop Cloud Services. Le système ExtraHop doit être connecté à ExtraHop Cloud Services pour ajouter un flux TAXII.

- Les flux TAXII ne peuvent être gérés depuis une console que par les utilisateurs disposant de l'accès et de l'administration du module NDR privilèges.
- Les indicateurs d'alimentation TAXII ne sont fournis qu'aux capteurs connectés exécutant les versions 9.6.0 et ultérieures du firmware.
- RevealX prend actuellement en charge les flux TAXII pour les versions 2.0 à 2.1 de TAXII qui contiennent des versions de fichiers STIX 2.0 à 2.1

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 la section flux TAXII, cliquez sur **Ajouter un flux TAXII**.
4. Dans le champ Nom, saisissez un nom unique pour le flux TAXII.
5. Dans le champ URL de découverte du serveur TAXII, saisissez l'URL de découverte de votre fournisseur de flux TAXII.
6. Dans le menu déroulant Version TAXII, sélectionnez la version du protocole TAXII du flux.
7. Sélectionnez un type d'authentification.
   - Pas d'authentification
   - Authentification de base

     Entrez le nom d'utilisateur et le mot de passe du flux cible.
8. Spécifiez un certificat pour le flux cible.
   - Pas de certificat
   - certificat CA

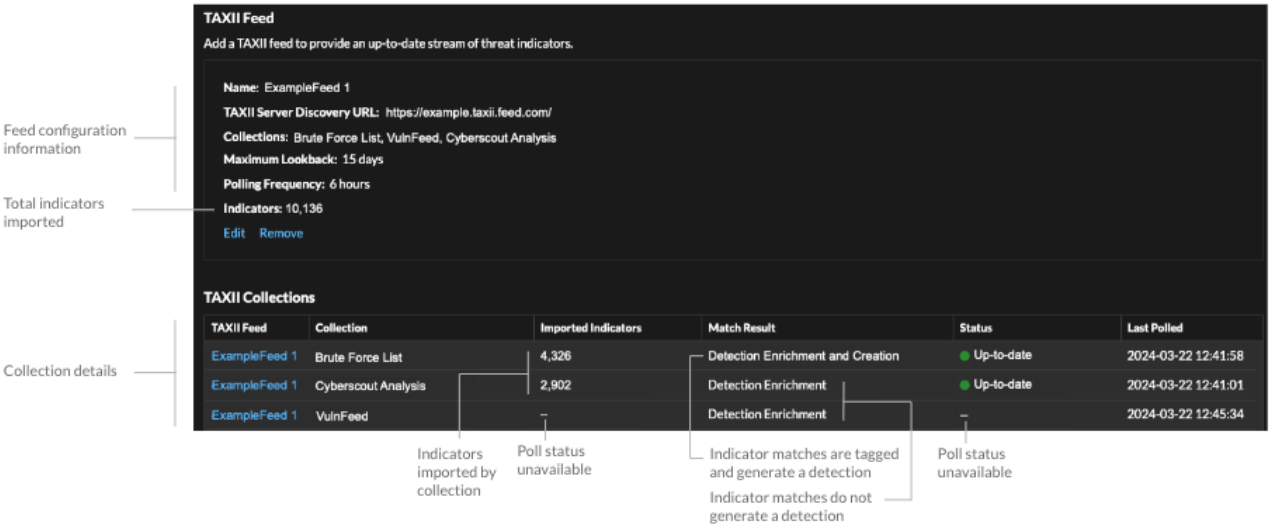
     Le certificat présenté par le serveur TAXII sera vérifié par rapport à ce certificat. Copiez et collez le certificat d' autorité de certification (CA) racine.
9. Cliquez **Connexion de test** pour confirmer les paramètres d'URL, d'authentification et de certificat.
10. Cliquez **Suivant**.
11. Dans le menu déroulant Collections à enrichir, sélectionnez les collections de menaces qui généreront une étiquette suspecte en cas de correspondance d'indicateurs.
12. Dans le menu déroulant Collections pour la création de détections, sélectionnez les collections de menaces qui entraîneront une détection en cas de correspondance d' indicateurs.

    Note: Vous pouvez affecter une collection à la fois à l'enrichissement et à la création de détections. Si aucune collection n'est affectée à l' option d'enrichissement, la collection ne sera pas mise à jour lors du sondage et les indicateurs de la collection n'apparaîtront pas dans votre système.
13. Dans le champ Maximum Lookback, saisissez le nombre de jours passés pendant lesquels vous souhaitez accepter les indicateurs de la collecte des menaces.

    Vous pouvez définir cette valeur sur une valeur comprise entre 1 et 15 jours. Le flux n' acceptera que les indicateurs créés au cours de cette période rétrospective.
14. Dans le champ Fréquence d'interrogation, saisissez le nombre d'heures entre l'interrogation du fil TAXII pour les mises à jour de la collecte des menaces.

    Vous pouvez définir cette valeur sur une valeur comprise entre 1 et 24 heures.
15. Cliquez **Enregistrer**.

Les informations de configuration du flux TAXII s'affichent dans la section Fil TAXII de la page Threat Intelligence, y compris la période de référence spécifiée, la fréquence d'interrogation et le nombre total d'indicateurs contenus dans le flux. Le tableau des collections TAXII contient des informations sur les différentes collections du flux.



Voici quelques considérations concernant les flux TAXII :

- Le temps nécessaire pour interroger les indicateurs d'alimentation et de traitement TAXII est basé sur le nombre d'indicateurs contenus dans le flux. À titre de référence, l'interrogation d'un flux contenant 500 000 indicateurs au cours de la période de référence spécifiée peut prendre une heure ou plus.
- Les types d'indicateurs qui ne sont pas reconnus par le système ExtraHop, les indicateurs de point de terminaison bénins et les indicateurs marqués comme révoqués seront supprimés du flux lors du sondage.
- Dans le tableau des collections TAXII, l'état de la collecte sera affiché par un tiret (-) jusqu'à ce que la collection soit à jour. Si ce statut ne passe pas à jour, testez votre connexion au serveur TAXII, puis vérifiez auprès de votre fournisseur de flux TAXII que la collection existe toujours dans le flux, que vos informations dcidentification autorisent l'accès à la collection et que vous n' avez pas dépassé les limites de sondage définies par le fournisseur. Un état de mise à jour partielle s'affiche si une collection n'est pas complètement mise à jour pendant le sondage. Des mises à jour partielles peuvent se produire si le sondage a été interrompu de façon inattendue ou si la limite de débit d'un fournisseur a été atteinte.