Manage threat collections

Published: 2024-04-02

ExtraHop Reveal(x) can apply threat intelligence to your network activity based on threat collections provided by Extrahop, CrowdStrike, or other free and commercial sources.

Before you begin

- Learn about threat intelligence.
- You must have System and Access Administration privileges on each console and sensor to manage threat collections.
- If your ExtraHop deployment includes a console, we recommend that you transfer management of all connected sensors to the console to enable or disable built-in threat collections across your entire system.

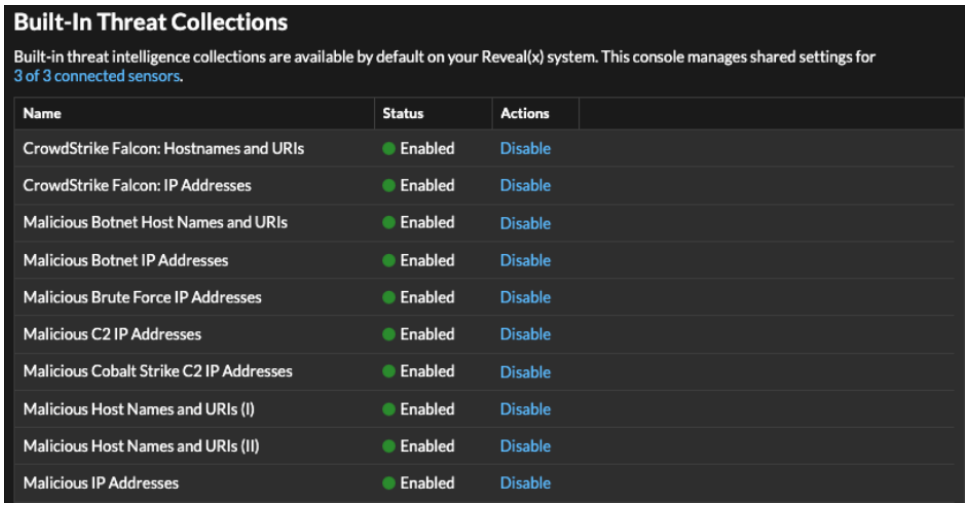
Enable or Disable built-in threat collections

Built-in threat collections from ExtraHop and CrowdStrike identify indicators of compromise throughout the system.

Enabled threat collections automatically update systems that are connected to ExtraHop Cloud Services. You can confirm connectivity on the ExtraHop Cloud Services page in the Administration settings.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click the System Settings icon and then click **Threat Intelligence**.
3. In the Built-In Threat Collections table, click **Enable** or **Disable** in the Actions column.

   The system automatically checks for updates to ExtraHop and CrowdStrike threat collections every 6 hours.



Upload a threat collection

Upload threat collections from free and commercial sources to identify indicators of compromise throughout the ExtraHop system. Because threat intelligence data is updated frequently (sometimes daily), you might need to update a threat collection with the latest data. When you update a threat collection with new data, the collection is deleted and replaced, and not appended to an existing collection.

You must upload threat collections individually to your console, and to all connected sensors.

Here are some considerations about uploading threat collections.

- Custom threat collections must be formatted in Structured Threat Information eXpression (STIX) as compressed TAR files, such as .TGZ or TAR.GZ. Reveal(x) currently supports STIX version 1.0 - 1.2.
- You can directly upload threat collections to Reveal(x) 360 for self-managed sensors. Contact ExtraHop Support to upload a threat collection to ExtraHop-managed sensors.
- The maximum number of observables that a threat collection can contain depends on your sensor memory and license. To ensure successful uploads within the limits of your sensors and license, we recommend breaking collections into files of less than 3,000 observables, with a total collection size of less than 1 million observables. Contact your ExtraHop representative for more information about license and platform limits for uploading threat collections.
- You can upload STIX files through the REST API.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click the System Settings icon and then click **Threat Intelligence**.
3. Click **Manage custom collections**.
4. Click **Upload New Collection**.
5. In the Collection ID field, type a unique collection ID. The ID can only contain alphanumeric characters and spaces are not allowed.
6. Click **Choose file** and select a `.tgz` file that contains a STIX file.
7. Type a display name in the Display Name field.
8. Click **Upload Collection**.
9. Repeat these steps for each connected sensor and on all consoles.