Manage threat collections

Published: 2024-04-08

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.

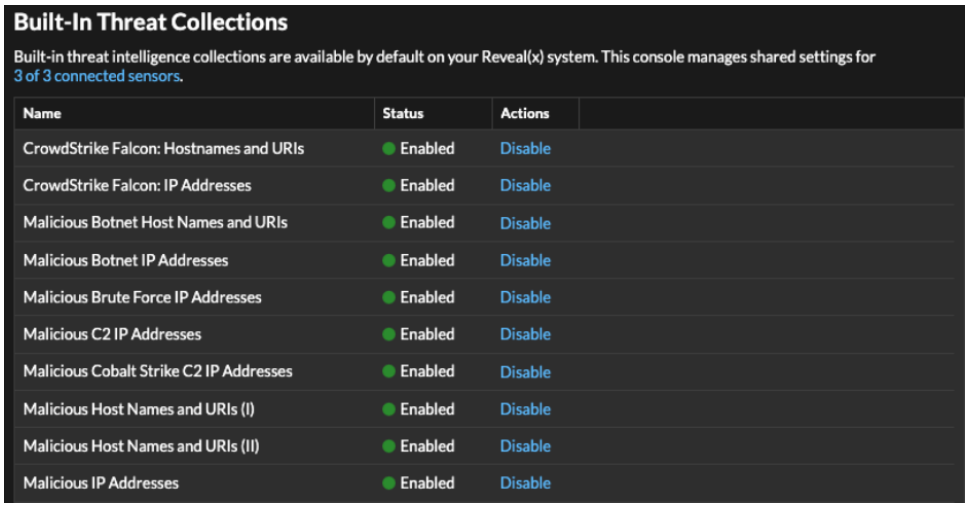
Enable or Disable built-in threat collections

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 on all consoles and each connected sensor.

Add a TAXII feed

Threat collections can be delivered to your environment over the Trusted Automated Exchange of Intelligence Information (TAXII) protocol.

TAXII feeds can vary in quality or relevance to your environment. To maintain accuracy and reduce noise, we recommend that you only add feeds from reliable sources that provide high-quality threat intelligence data.

Before you begin

- TAXII feed indicators are processed by ExtraHop Cloud Services. The ExtraHop system must be connected to ExtraHop Cloud Services to add a TAXII feed.
- Users must be granted NDR module access and have administrator privileges to complete the tasks in this guide.

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 TAXII feed section, click **Add TAXII Feed**.
4. In the Name field, type a unique name for the TAXII feed.
5. In the TAXII Server Discovery URL field, type the discovery URL for your TAXII feed provider.
6. From the TAXII version dropdown, select the TAXII protocol version of the feed.
7. Select an authentication type.
   - No authentication
   - Basic authentication

     Enter the username and password for the target feed.
8. Specify a certificate for the target feed.

- No certificate
- Basic certificate

  Copy and paste the contents of the PEM-encoded certificate chain into the basic certificate field. A valid trust path must exist from the certificate to a trusted root.

9. Click **Test Connection** to confirm URL, authentication, and certificate settings.
10. Click **Next**.
11. From the Collections for Enrichment dropdown, select the threat collections that will result in a suspicious tag when an indicator match occurs.
12. From the Collections for Detection Creation dropdown, select the threat collections that will result in a detection when an indicator match occurs.

    Note: You can assign a collection to both enrichment and detection creation. If a collection is not assigned to the enrichment option, the collection will not be updated during polling and indicators from the collection will not appear in your system.

13. In the Maximum Lookback field, type the number of days in the past you want to accept indicators from the threat collection.

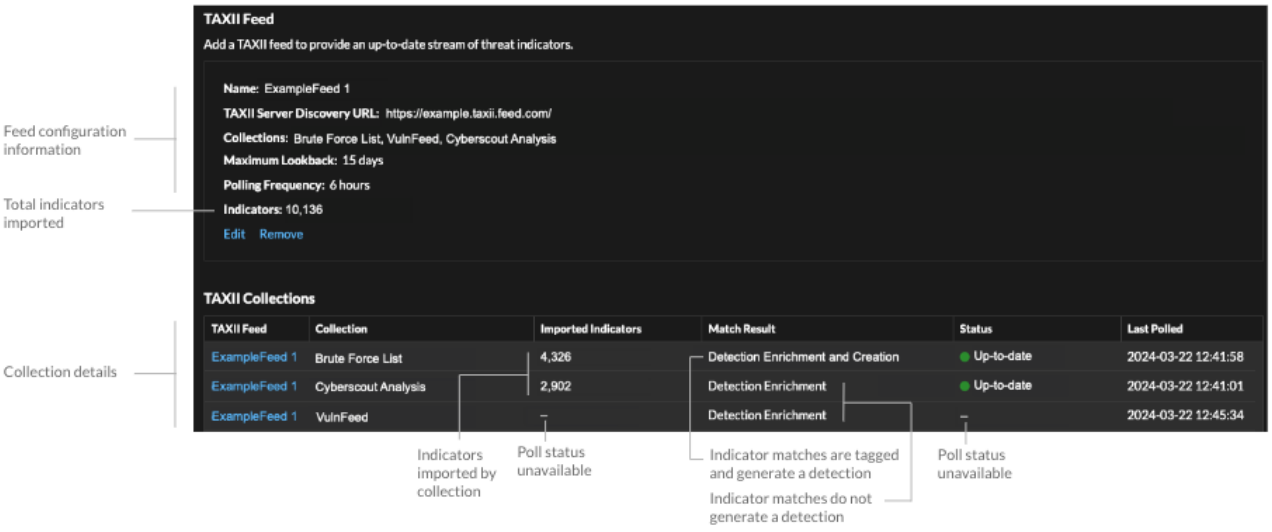
    You can set this value to a number between 1 and 15 days. The feed will only accept indicators that were created during this lookback period.

14. In the Polling Frequency field, type the number of hours between polling the TAXII feed for threat collection updates.

    You can set this value to a number between 1 and 24 hours.

15. Click **Save**.

TAXII feed configuration information displays in the TAXII Feed section of the Threat Intelligence page, including the specified lookback period, polling frequency, and total number of indicators contained in the feed. The TAXII Collections table contains details about the individual collections in the feed.



Here are some considerations about TAXII feeds:

- The time required to poll the TAXII feed and process indicators is based on the number of indicators in the feed. For reference, polling a feed with 500,000 indicators in the specified lookback period could take an hour or more.
- Indicator types that are not recognized by the ExtraHop system, benign endpoint indicators, and indicators marked as revoked will be removed from the feed during polling.

- In the TAXII collections table, the collection status will display a dash (-) until the collection is up-to-date. If this status does not resolve to up-to-date, test your connection to the TAXII server, then check your TAXII feed provider to make sure that the collection still exists in the feed, that your credentials grant access to the collection, and that you have not exceeded polling limits set by the provider.