Manage threat collections

Published: 2024-04-01

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

To add threat intelligence from CrowdStrike, see Integrate Reveal(x) 360 with CrowdStrike ⧉.

Before you begin

- Learn about threat intelligence ⧉.
- You must have System and Access Administration privileges ⧉ on each console and sensor to manage threat collections.

Enable or Disable ExtraHop-curated threat collections

ExtraHop threat collections are enabled by default and identify indicators of compromise throughout the system.

ExtraHop 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 ExtraHop Threat Intelligence table, select or clear the **Enabled** checkbox in the Status column.

   The system automatically checks for updates to ExtraHop-curated threat collections every 12 hours. The Last Updated column reflects the date and time of the latest update.

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	☑	Enabled
Malicious Botnet IP Addresses	2021-10-25 14:54:36	☑	Enabled
Malicious Botnet Host Names and URIs	2021-10-25 14:54:36	☑	Enabled
Malicious Brute Force IP Addresses	2021-10-25 14:54:37	☑	Enabled
Malicious IP Addresses from Machine Learning Service	2021-07-08 14:53:11	☑	Enabled
Malicious Cobalt Strike C2 IP Addresses	2021-10-25 14:54:37	☑	Enabled
Malicious IP Addresses	2021-10-25 14:54:36	☑	Enabled
Malicious Host Names and URIs from Machine Learning Service	2021-07-23 15:25:01	☑	Enabled
Malicious C2 IP Addresses	2021-10-25 14:54:37	☑	Enabled

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 TAR.GZ files. 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 platform and license. Contact your ExtraHop representative for more information.
- 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.