Manage threat collections

Published: 2020-11-06

ExtraHop Reveal(x) includes curated threat collections that identify suspicious hostnames, IP addresses, and URIs in charts and tables throughout the system. You must enable these threat collections before threat intelligence is applied to your network activity. In addition, you can upload threat collections from free or commercial sources as a custom threat collection.

Before you begin

- Learn about threat intelligence.
- You must enable these collections in the system to display threat intelligence in system charts and records.

Here are some important considerations about adding threat collections:

- ExtraHop currently supports STIX versions 1.0 - 1.2.
- 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 directly upload threat collections to Reveal(x) 360 systems for self-managed sensors. Contact ExtraHop Support to upload a threat collection to ExtraHop-managed sensors.

1. Log into the Web UI on your Discover or Command appliance.

   Threat intelligence files are applied only to the local appliance and are not synced between appliances. If you manage your Reveal(x) system through a Command appliance, upload the threat collection to the Command appliance and to each connected Discover appliance.
2. Click the System Settings icon and then click **Threat Intelligence**.
3. Click **Upload New Collection**.
4. Type a unique collection ID in the Collection ID field. The ID can only contain alphanumeric characters. Spaces are not allowed.
5. Type a display name in the Display Name field.
6. Click **Choose file** and select a `.tgz` file that contains a STIX file.
7. Click **Save**.

After the upload completes, the new threat collection appears in the table. You can now view threat intelligence metrics on the Security dashboard.

Enable ExtraHop-curated threat collections

Enable the ExtraHop threat collection to display suspicious hostnames, IP addresses, and URIs in system charts and records.

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 the **Enabled** checkbox in the Status column

Upload a threat collection

Upload threat collections from free and commercial sources to identify suspicious hosts, IP addresses, and URIs in system charts and records. 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 can directly upload threat collections to Reveal(x) 360 systems for self-managed sensors. Contact ExtraHop Support to upload a threat collection to ExtraHop-managed sensors.

  Tip: Upload STIX files through the REST API.

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.

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**.