Upload a threat intelligence collection to ExtraHop Reveal(x)

Published: 2018-11-07

By uploading threat intelligence information in the form of the Structured Threat Information eXpression (STIX) file format to your Discover and Command appliances, you can find suspicious hosts, IP addresses, and URIs in the ExtraHop Web UI.

Before you begin
Learn about threat intelligence.

Note: This topic applies only to ExtraHop Reveal(x) Premium and Ultra.

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.

1. Log into the Admin 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. In the System Configuration section, 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 `.tar` or `.tgz` file that contains a STIX file.
7. Click **Upload**.

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

Update a threat collection

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.

Tip: The REST API offers a way to automate these updates across all appliances.

1. In the System Configuration section, click **Threat Intelligence**.
2. In the Actions column of the collection you want to update, click **Update**.
3. Optional: If you want to only change the display name of the collection, type a new name in the Display Name field and then click **Update**.
4. Click **Choose file** and select a `.tar` or `.tar.gz` file that contains a STIX file.
5. Click **Update**.

After the upload completes, the threat collection is updated.