Threat intelligence

Published: 2020-02-23

Threat intelligence is a collection of information about malicious IP addresses, threat actor techniques, and other indicators of compromise that can help your organization detect attacks. Threat intelligence information, commonly shared in the Structured Threat Information eXpression (STIX) file format, can be obtained through free and commercial sources and curated with threat intelligence platforms. But to receive benefits from threat intelligence, you must apply this information to your network data. After you obtain the STIX files that you care the most about from your threat intelligence platforms, you can upload them to the Discover and Command appliances in your ExtraHop Reveal(x) system. Reveal(x) then automatically finds indicators of compromise, so that you can view these suspicious objects in the context of your real-time network data.

Definitions

Here are some important terms about threat intelligence:

STIX

Structured Threat Information eXpression (STIX) is the language and serialization format for standardizing, conveying, and sharing data about cyber threat intelligence data. STIX files are commonly supported by the threat intelligence community and platforms. ExtraHop currently supports STIX 1.0 - 1.2.

TAXII

Trusted Automated eXchange of Indicator Information (TAXII) is a free and open transport mechanism that standardizes the automated exchange of cyber threat information. TAXII clients commonly share STIX files with threat intelligence platforms. Reveal(x) is not a TAXII client. You must first obtain STIX files from a threat intelligence platform or TAXII server and then upload the STIX files to your Discover and Command appliances through the Web UI or REST API.

Threat collection

A threat collection is the name for the STIX 1.x file that is uploaded to the Discover and Command appliances. A threat collection contains a single STIX file.

Observables

An observable is a STIX schema component that specifies a suspicious object. Reveal(x) matches the following types of observables to objects in wire data:

- Hostnames
- IP addresses
- URIs

Note: The maximum number of observables that a threat collection can contain depends on your platform and license. Contact your ExtraHop representative for more information.

Indicators

An indicator is a STIX schema component that specifies context for an observable. For example, an indicator can specify a time range or information source. Reveal(x) displays indicator information for suspicious objects that match observables in a threat collection.

Indicators of compromise

Indicators of compromise are artifacts that match observables in threat collections. Indicators of compromise appear in the ExtraHop Web UI as a suspicious host, URI, or IP address, and are marked with a red camera icon.

Suspicious Host

A hostname observed in wire data that was found within a domain in a threat collection.

Suspicious IP

An IP address observed in wire data that exactly matched an IP address in a threat collection.

Suspicious URI

A URI observed in wire data that exactly matched a URI in a threat collection.

How threat intelligence works

First, obtain the STIX files that you care the most about from your threat intelligence platforms. The STIX file schema includes many components to help standardize diverse types of cyber threat intelligence data. Examples of these components include observables, indicators, incidents, campaigns, threat actors, and more. Then, upload the files to Discover and Command appliances through the Web UI or REST API to create a threat collection.

The threat collection is the basis for finding indicators of compromise in your network data. Reveal(x) specifically evaluates observables within a threat collection to identify suspicious hostnames, IP addresses, and URIs. Suspicious objects that match threat collections are marked with a red camera icon. Click the red camera icon to see threat collection details, including indicator components that were included in the original STIX file.

Selecting STIX files

Because cyber threat intelligence is community-driven, there are many sources of threat intelligence data. Data from these sources can vary in quality or relevance to your environment. To maintain accuracy and reduce noise, we recommend that you limit your uploads to high-quality threat intelligence data that you care the most about. Dedicate a threat collection to one type of intrusion or threat, such as one collection for malware and another collection for botnets.

When you find an indicator of compromise, you can then launch investigations.

Threat intelligence and records

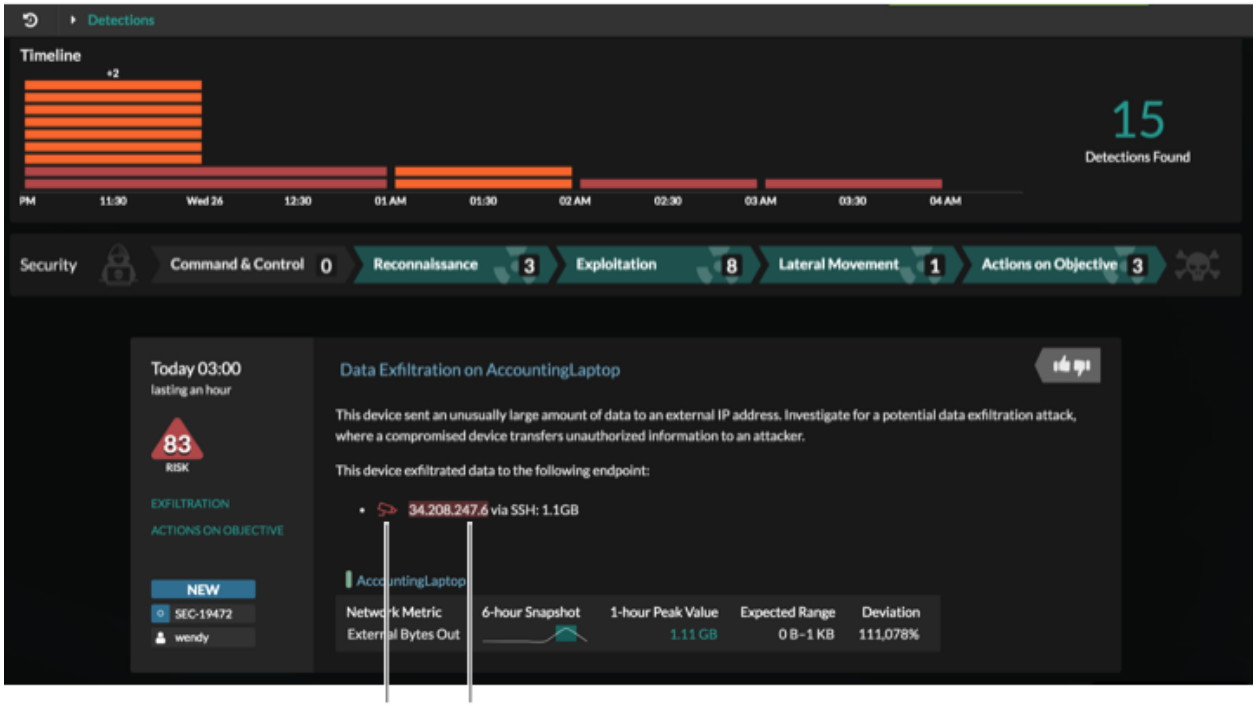
Record query results that contain suspicious IP addresses, hostnames, and URIs appear with a red camera icon next to the record.

It is important to note that there might be discrepancies with the threat intelligence information that appears in the records table based on when the record was created versus when the threat collection was uploaded or updated. For example, if the threat collection is uploaded after the record is created, the camera icon does not appear in query results.

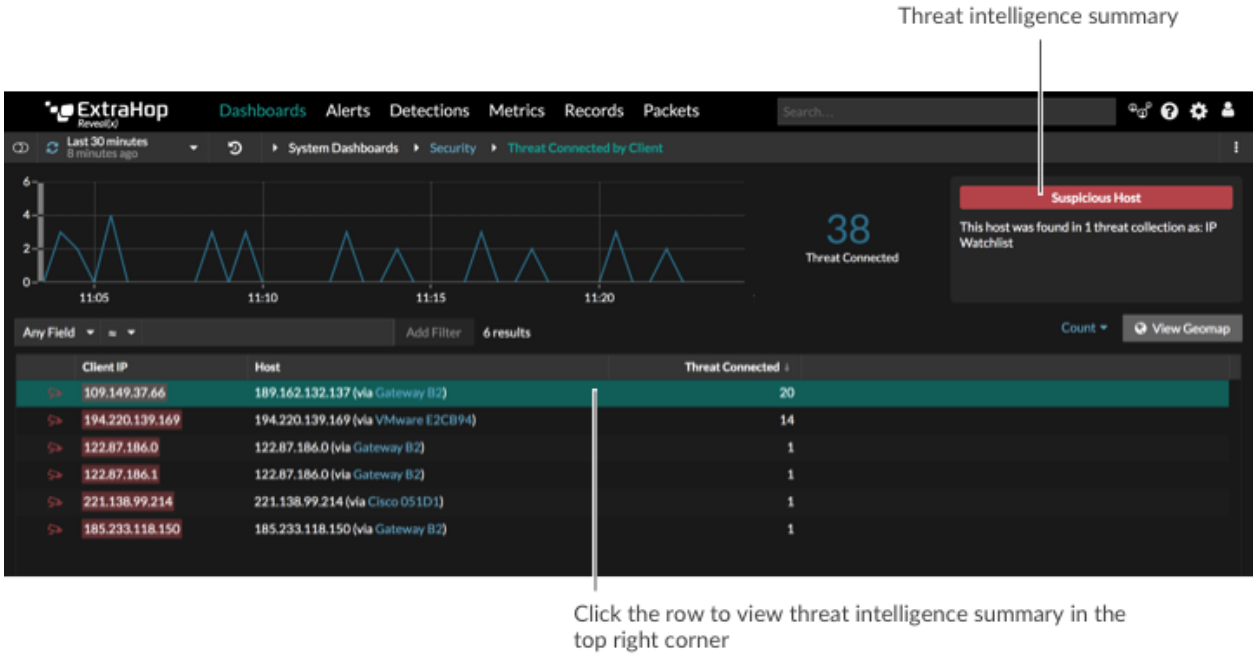
Note: Additional trigger configuration is not required to check if a record contains suspicious objects.

Finding indicators of compromise

When Reveal(x) identifies an indicator of compromise based on a threat collection, a red camera icon appears next to the suspicious host, IP address, or URI. The hostname or IP address that matches a STIX observable is also highlighted in red, as shown in the following figure.



The red camera icon appears for wire data metrics on a as a signal metric on the Security Overview page, detail page, and detection page. For example, when you drill down on a threat intelligence metric from the Security dashboard or a chart that contains metric data with suspicious IP addresses, a detail page appears, as shown in the following figure.

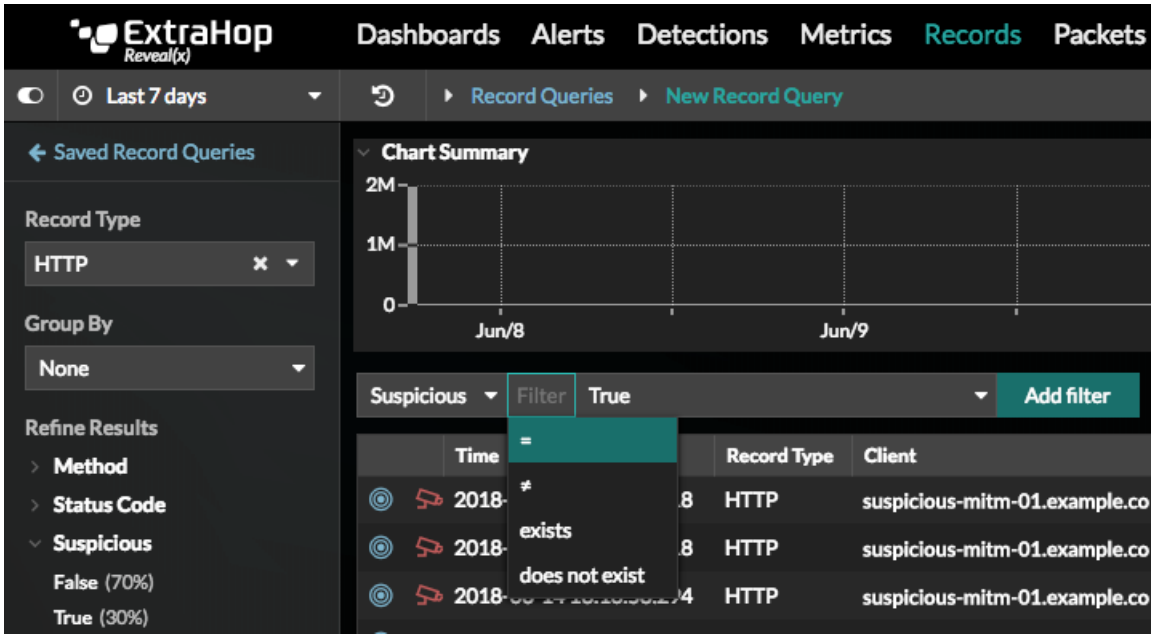


Note: Suspicious objects are only identified in metric data observed after the threat collection is created or updated.

If a threat collection is deleted from a Discover or Command appliance, the red camera is no longer visible for wire data metrics that previously matched the objects in the deleted threat collection.

Filtering records for indicators of compromise

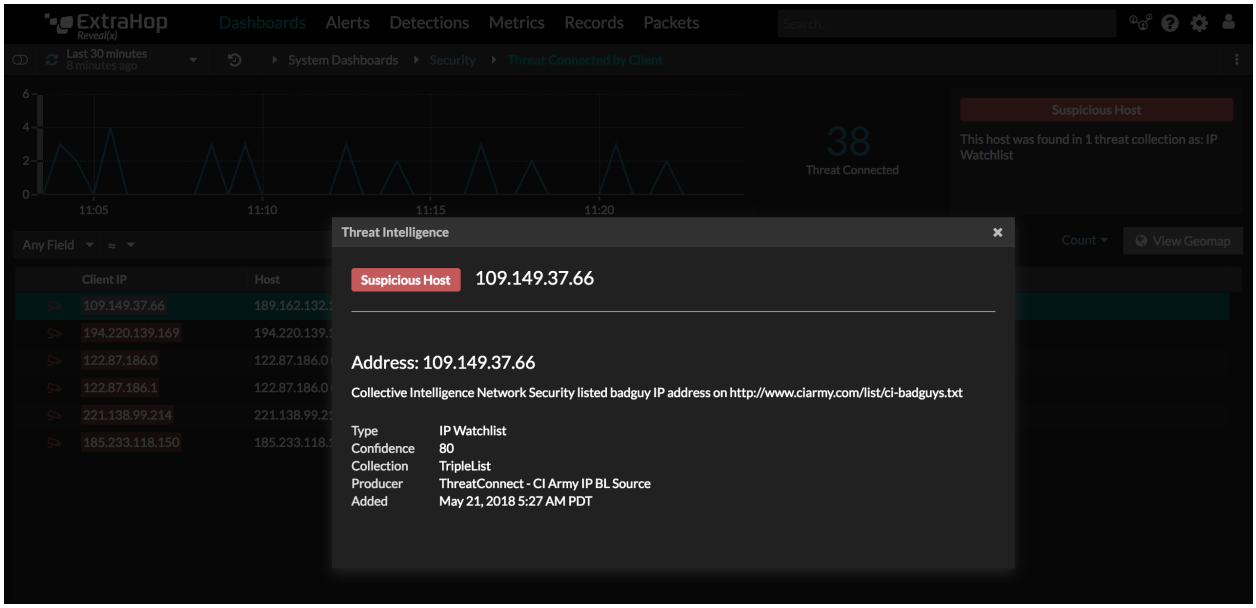
If you have an Explore appliance, the red camera icon also appears in records that contain a suspicious host, IP address, or URI. You can also refine record queries results to quickly find the records with suspicious objects. In the left pane, click **True** or **False** under the Suspicious facet. You can also create a filter by selecting **Suspicious** in the trifield, an operator, and then a value, as shown in the following figure.



If a threat collection is deleted from a Discover or Command appliance, the red camera persists in records for objects that were previously found in the deleted threat collection. Detailed information about the suspicious object and threat intelligence source is no longer available.

Investigating indicators of compromise

Click the red camera icon to access detailed information about the threat intelligence source. After clicking the icon, a window appears that lists all of the relevant STIX information from your threat collection about the suspicious object, as shown in the following figure.



Related topics

Check out the following resources for more information about Reveal(x) security concepts.

- Learn about Security Overview
- View threat intelligence metrics on the Security dashboard
- Upload a threat intelligence collection
- Upload STIX files through the REST API