Threat intelligence

Published: 2023-06-14

Threat intelligence provides known data about suspicious IP addresses, domains, hostnames, and URIs that can help identify risks to your organization.

Threat intelligence data sets, called threat collections, are available by default in your ExtraHop system, from free and commercial sources in the security community, and from partner integrations with ExtraHop Reveal(x) 360.

When the ExtraHop system observes activity that matches an entry in a threat collection (called an indicator of compromise), a detection is generated for the connection to a suspicious endpoint and the suspicious entry is marked with a camera icon or other visual cues.

Threat collections

The ExtraHop system supports threat collections from several sources.

Because cyber threat intelligence is community-driven, there are many external sources for threat collections. Data from these collections 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 focus on a specific type of intrusion, such as one collection for malware and another collection for botnets.

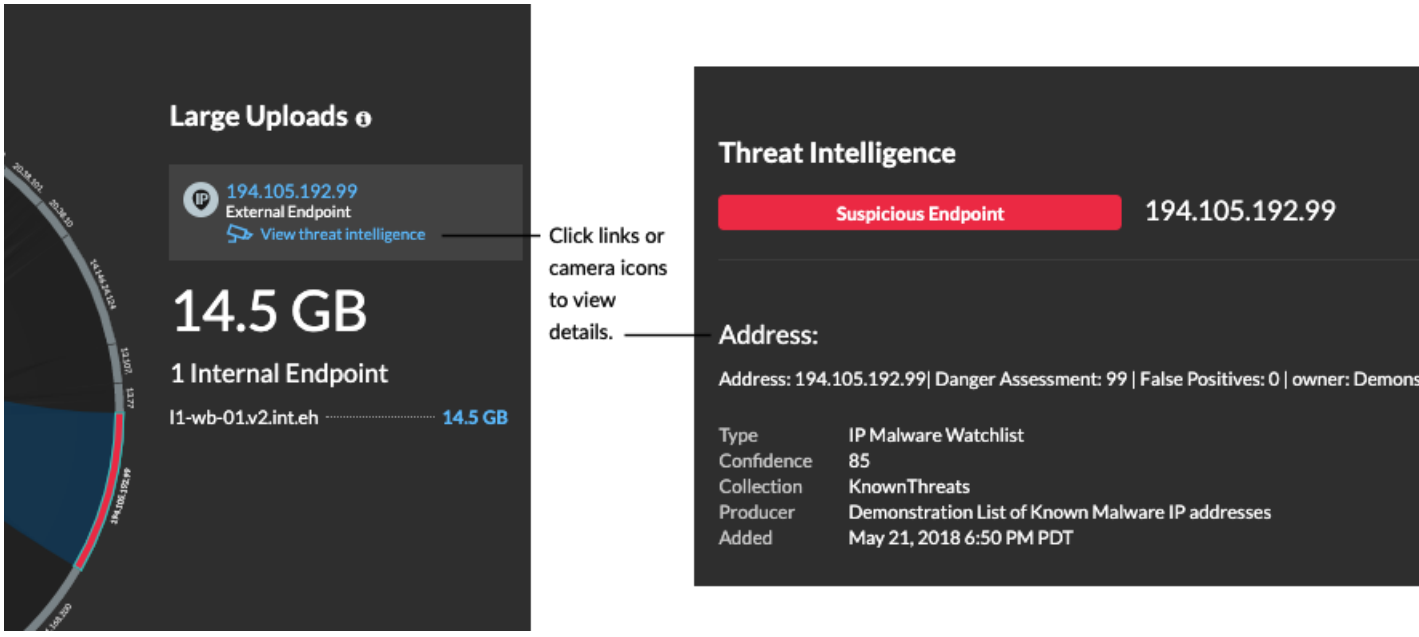
ExtraHop-curated threat collections are enabled by default and updated every 12 hours. Suspicious IP addresses, domains, hostnames, and URIs appear in system charts and records.

Free and commercial collections offered by the security community that are formatted in Structured Threat Information eXpression (STIX) as TAR or TAR.GZ files can be uploaded manually or through the REST API to ExtraHop systems. STIX version 1.0 - 1.2 are currently supported. You must upload each threat collection individually to all connected sensors.

Threat collections from partner integrations must be imported to ExtraHop Reveal(x) 360.

Investigating threats

After the Reveal(x) system observes an indicator of compromise, the suspicious IP address, domain, hostname, or URI is marked with a camera icon or other visual cue so you can investigate directly from the tables and charts you are viewing.

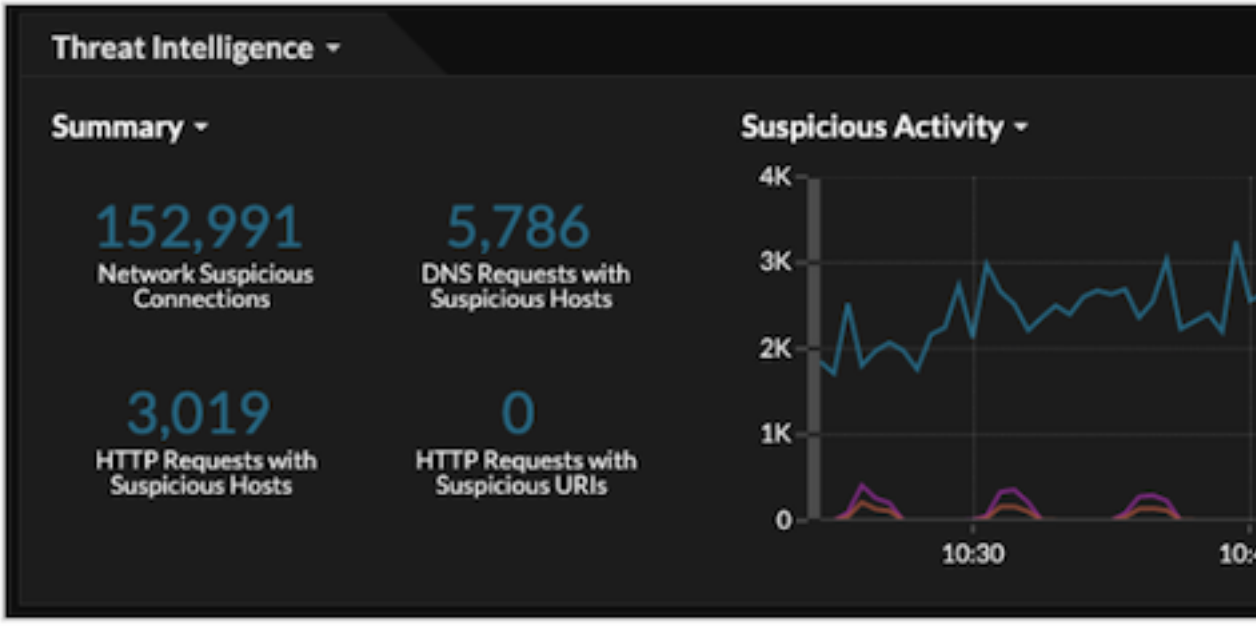


- If the threat collection is added or updated after the system has observed the suspicious activity, threat intelligence is not applied to that IP address, hostname, or URI until the suspicious activity occurs again.
- If an ExtraHop-curated threat collection is updated, the ExtraHop system performs Automated Retrospective Detection (ARD), which searches for new domains that are indicators of compromise in records for the past 7 days. If a match is found, the system generates a retrospective detection.
- If you disable or delete a threat collection, all indicators are removed from the related metrics and records in the system.

Here are some places in the Reveal(x) system that show the indicators of compromise found in your threat collections:

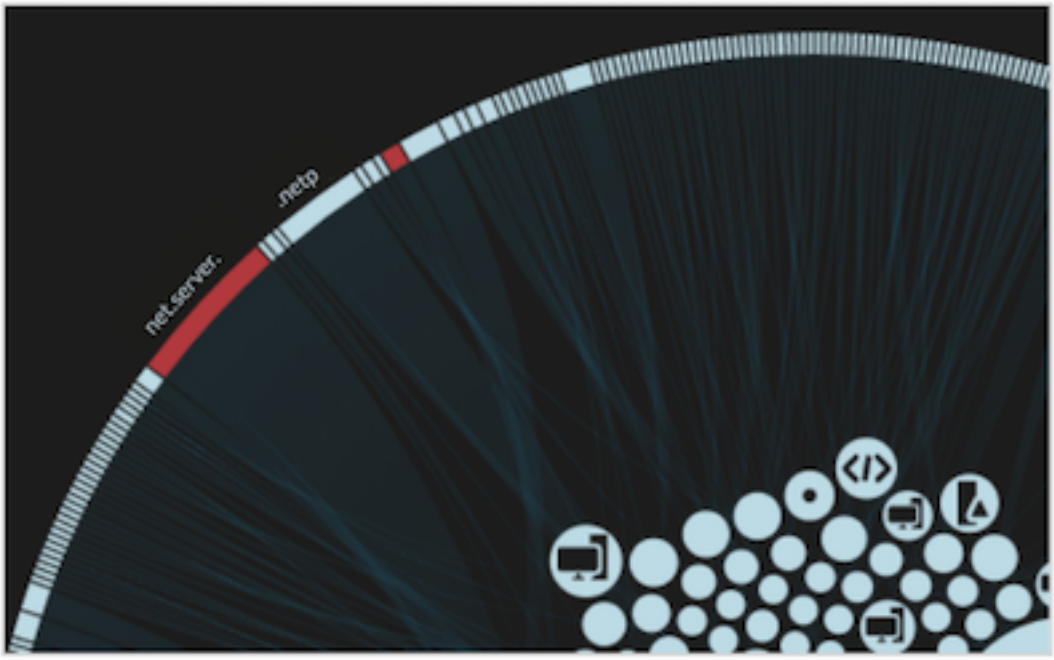
Security Hardening Dashboard

The Threat Intelligence region contains metrics for suspicious activity that matches the data in your threat collections. By clicking any metric, such as HTTP Requests with Suspicious Hosts, you can drill down on the metric for details or query records for related transactions.



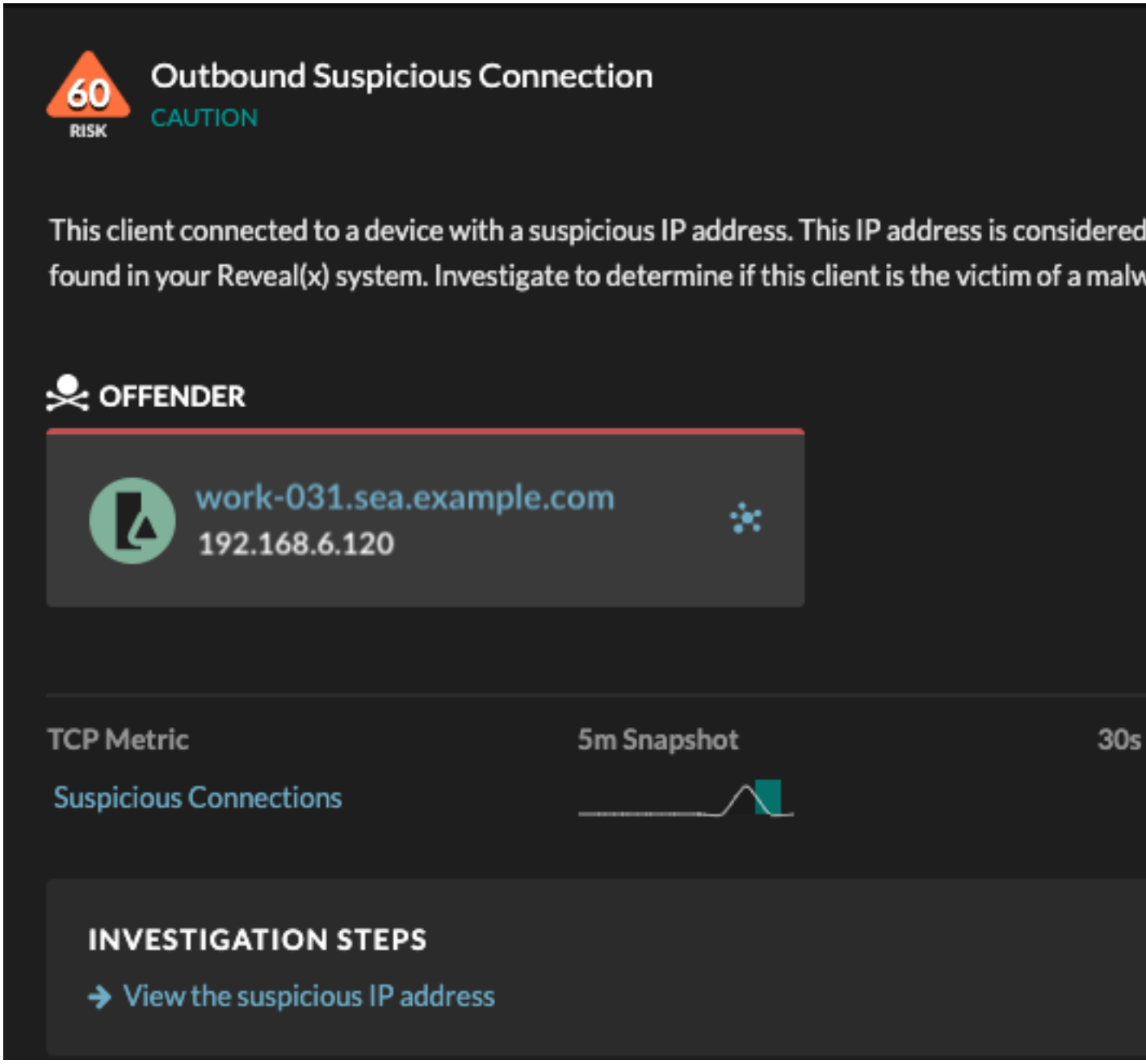
Perimeter Overview

In the halo visualization, any endpoints that match threat collection entries are highlighted in red.



Detections

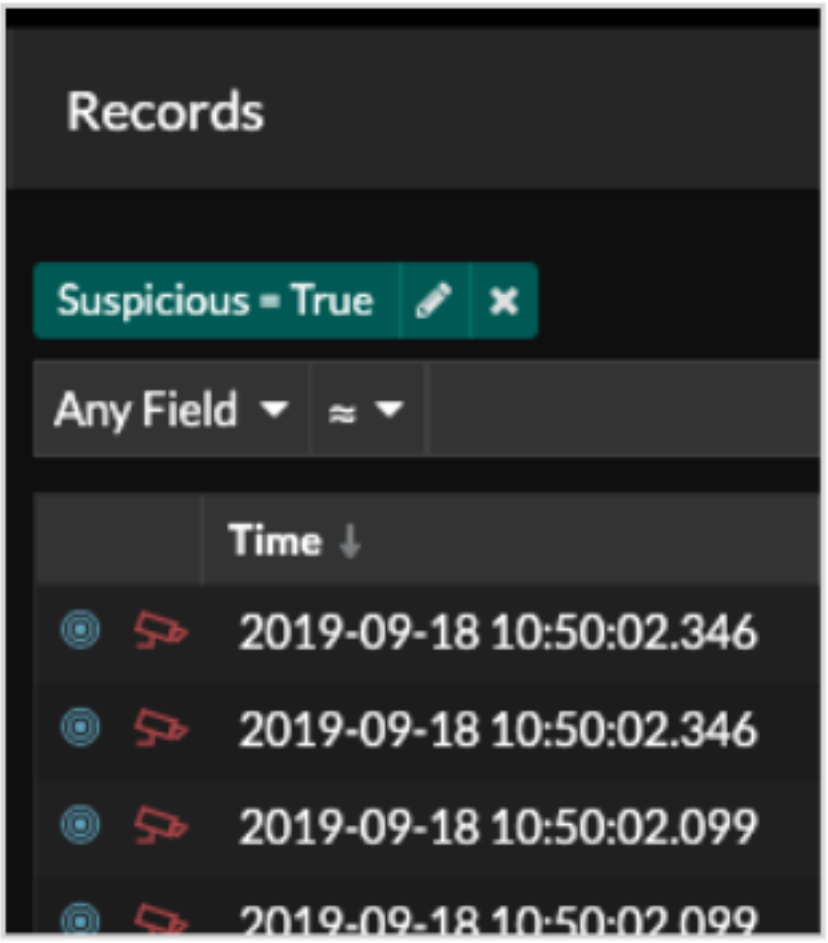
A detection appears when an indicator of compromise from a threat collection is identified in network traffic.



Records

The Records page enables you to directly query for transactions that match threat collection entries.

- Under the Suspicious facet, click **True** to filter for all records with transactions that match suspicious IP addresses, hostnames, and URIs.
- Create a filter by selecting Suspicious, Suspicious IP, Suspicious Domain, or Suspicious URI from the trifield drop-down, an operator, and a value.
- Click the red camera icon to view threat intelligence details.



Retrospective detections

(Reveal(x) 360 only) When an ExtraHop-curated threat collection is updated, the ExtraHop system performs Automated Retrospective Detection (ARD), which searches for new domains that are indicators of compromise in records for the past 7 days. If a past connection to a suspicious domain is identified, the system generates a retrospective detection.

The timestamp on a retrospective detection indicates the time that the activity originally occurred and might not appear in the current detection list. You can find retrospective detections by clicking on the Retrospective Threat Intelligence threat briefing. You can also create a detection notification rule to email you when these types of detections occur.