


Threat intelligence

Published: 2021-08-27

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 Reveal(x) system, from free and commercial sources in the security community, and from [partner integrations with Reveal\(x\) 360](#).

When the Reveal(x) system observes activity that matches an entry in a threat collection (called an indicator of compromise), the suspicious entry is marked with a camera icon  or other visual cue.

Threat collections

The Reveal(x) system supports threat collections from several sources

ExtraHop-curated threat collections are included by default and can help identify suspicious IP addresses, domains, hostnames, and URIs. You must [enable these collections](#) in the system to display threat intelligence in system charts and records.

You can manually [upload free and commercial collections offered by the security community](#) to your Reveal(x) system. Custom threat collections must be formatted in Structured Threat Information eXpression (STIX) as TAR or TAR.GZ files. Reveal(x) currently supports STIX version 1.0 - 1.2.



Tip: [You can upload STIX files through the REST API.](#)

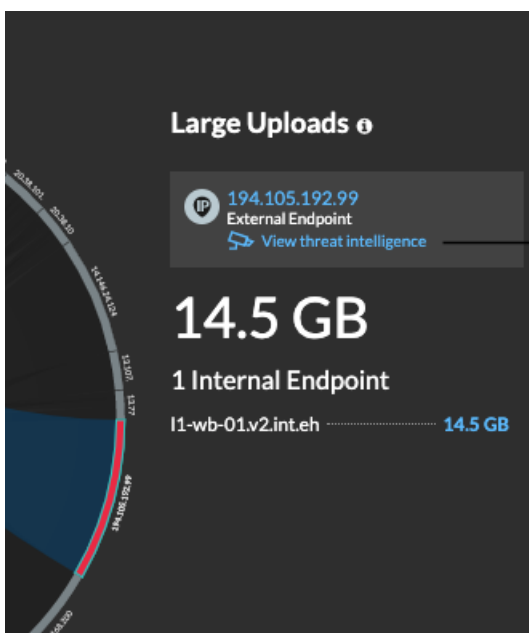


Note: Because cyber threat intelligence is community-driven, there are many external sources for threat collections. Data from these collections can vary in quality or relevance to your environment. To maintain accuracy and reduce noise, we recommend that you limit your uploads to high-quality threat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

Threat collections from partner integrations must be imported to Reveal(x) 360. See [Integrate Reveal\(x\) 360 with CrowdStrike](#).

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.



Click links or camera icons to view details.

Threat Intelligence

Suspicious Endpoint 194.105.192.99

Address:
Address: 194.105.192.99 | Danger Assessment: 99 | False Positives: 0 | owner: Demon

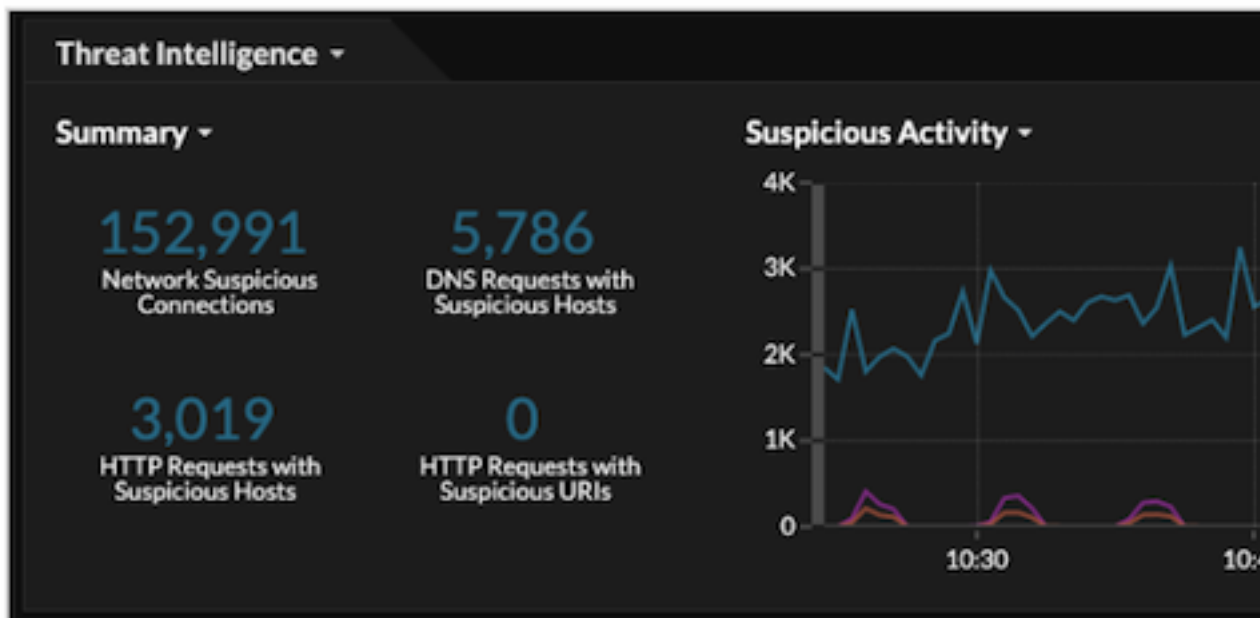
Type	IP Malware Watchlist
Confidence	85
Collection	KnownThreats
Producer	Demonstration List of Known Malware IP addresses
Added	May 21, 2018 6:50 PM PDT

- 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 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 Dashboard

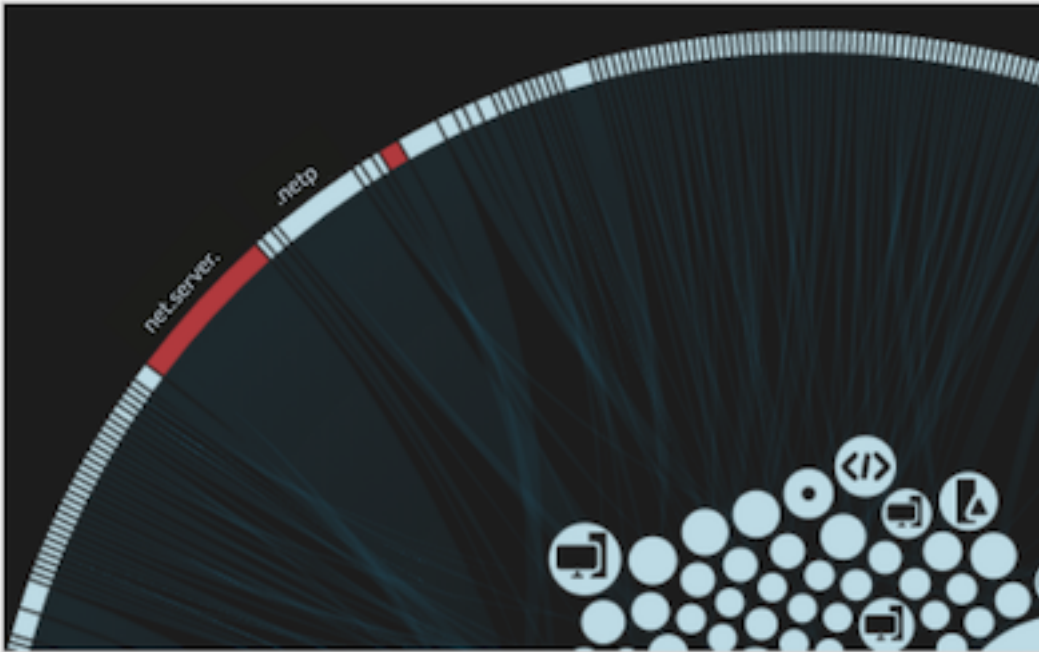
The [Threat Intelligence region](#) contains metrics for suspicious activity that matches the data in your threat collections. By clicking any metric, such as HTTP Requests with Suspicious Hosts, you can drill down on the metric for details or query records for related



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.

The screenshot displays a detection alert with the following components:



- Alert Header:** A red triangle icon containing the number '60' and the word 'RISK' below it. To the right, the text reads 'Outbound Suspicious Connection' in white, with 'CAUTION' in red below it.
- Description:** A white text block stating: 'This client connected to a device with a suspicious IP address. This IP address is considered found in your Reveal(x) system. Investigate to determine if this client is the victim of a malw'.
- Offender Section:** A red horizontal line above the word 'OFFENDER' in white. Below it is a dark grey box containing a green circular icon with a white triangle, the domain 'work-031.sea.example.com', the IP address '192.168.6.120', and a small cluster of blue dots.
- Visualizations:** Below the offender box, there are two tabs: 'TCP Metric' and '5m Snapshot'. Under 'TCP Metric', the text 'Suspicious Connections' is shown above a line graph with a single red peak. The '5m Snapshot' tab is active, and '30s' is visible on the right.
- Investigation Steps:** A dark grey box with the title 'INVESTIGATION STEPS' in white, followed by a red arrow icon and the text 'View the suspicious IP address' in red.

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.

Records

Suspicious = True  

Any Field ▾ ≈ ▾

	Time ↓
 	2019-09-18 10:50:02.346
 	2019-09-18 10:50:02.346
 	2019-09-18 10:50:02.099
 	2019-09-18 10:50:02.099