

Threat intelligence


Published: 2020-02-24


Threat intelligence provides known data about suspicious IP addresses, hostnames, and URIs that can help identify risks to your organization. These data sets, called threat collections, are available by default in your Reveal(x) system and from free and commercial sources in the security community.

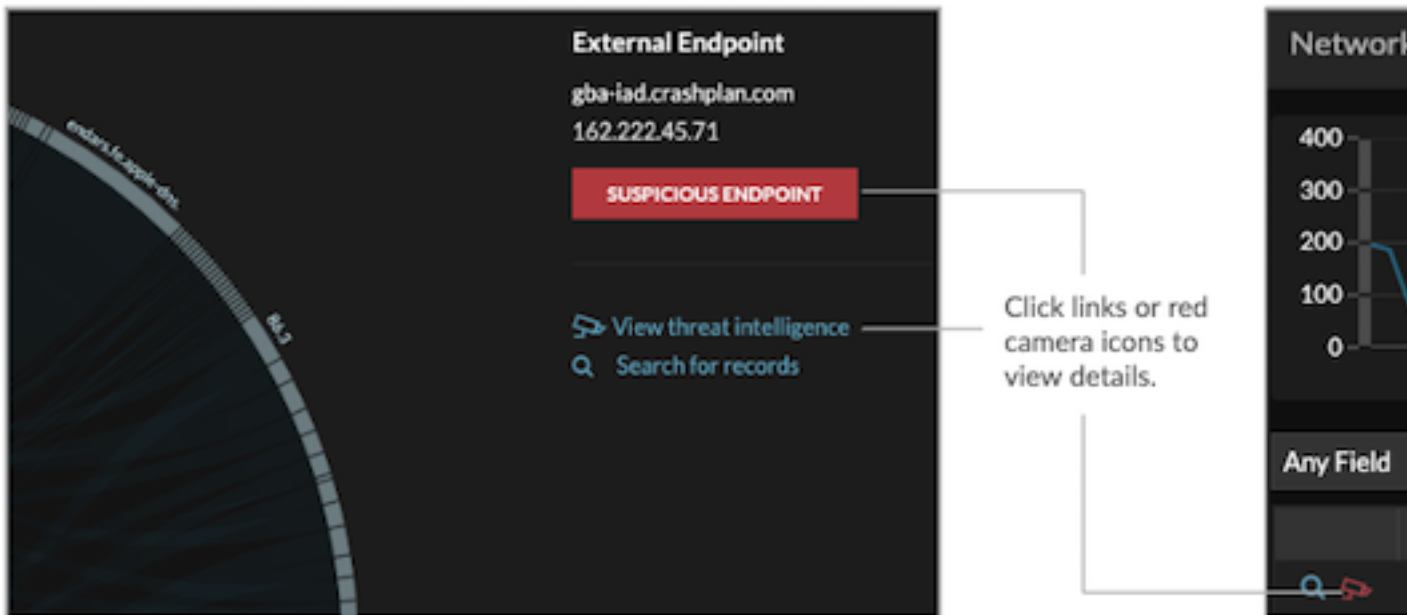
Threat collections

The Reveal(x) system includes threat collections that help identify suspicious IP addresses, hostnames, and URIs. You must enable these collections in the system to display threat intelligence in system charts and records.

The security community also offers free and commercial threat collections, which can be uploaded to your Reveal(x) system as a custom threat collection. 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.

 **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.

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



Investigating threats

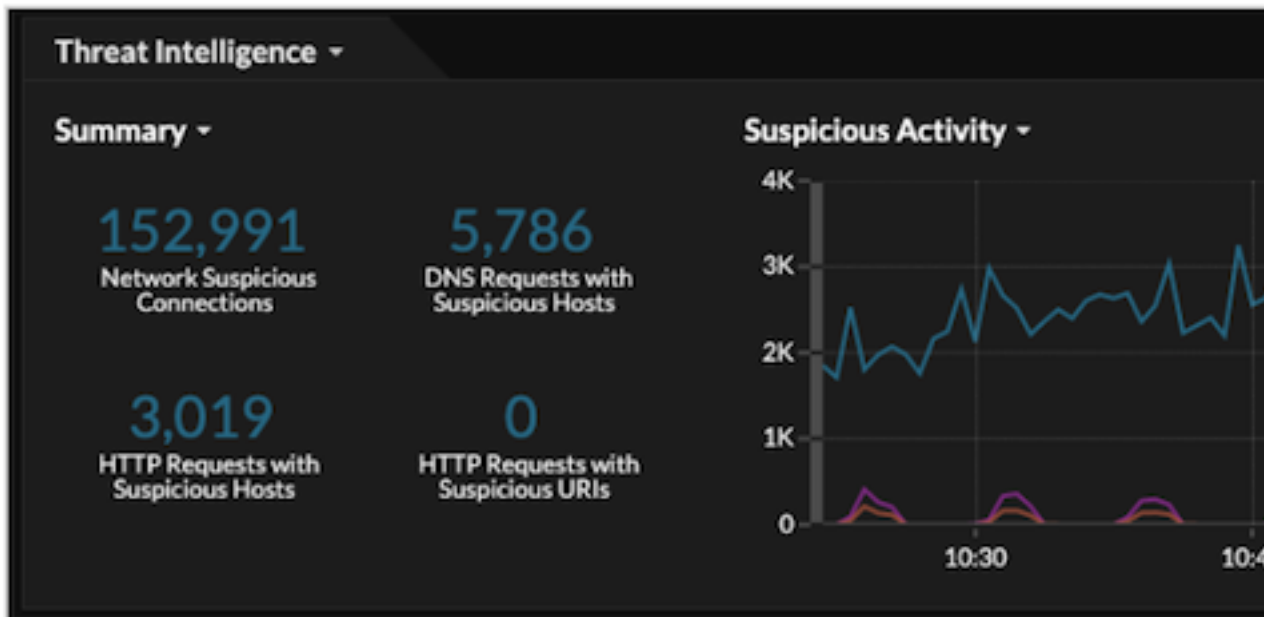
Reveal(x) displays threat intelligence throughout the system, so you can investigate indicators of compromise directly from the tables and charts you are viewing.

- 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 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

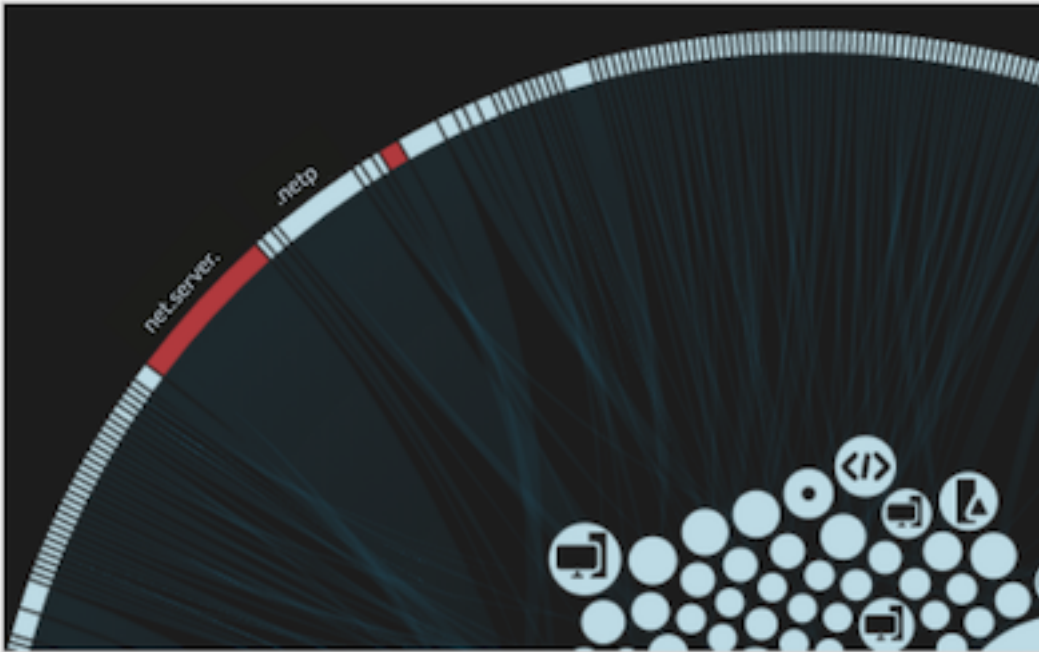
The Threat Intelligence region contains metrics for suspicious activity that matches the data in your threat collections. By clicking any metric, such as HTTP Requests with Suspicious Hosts, you can drill down on the metric for details or query records for related



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.

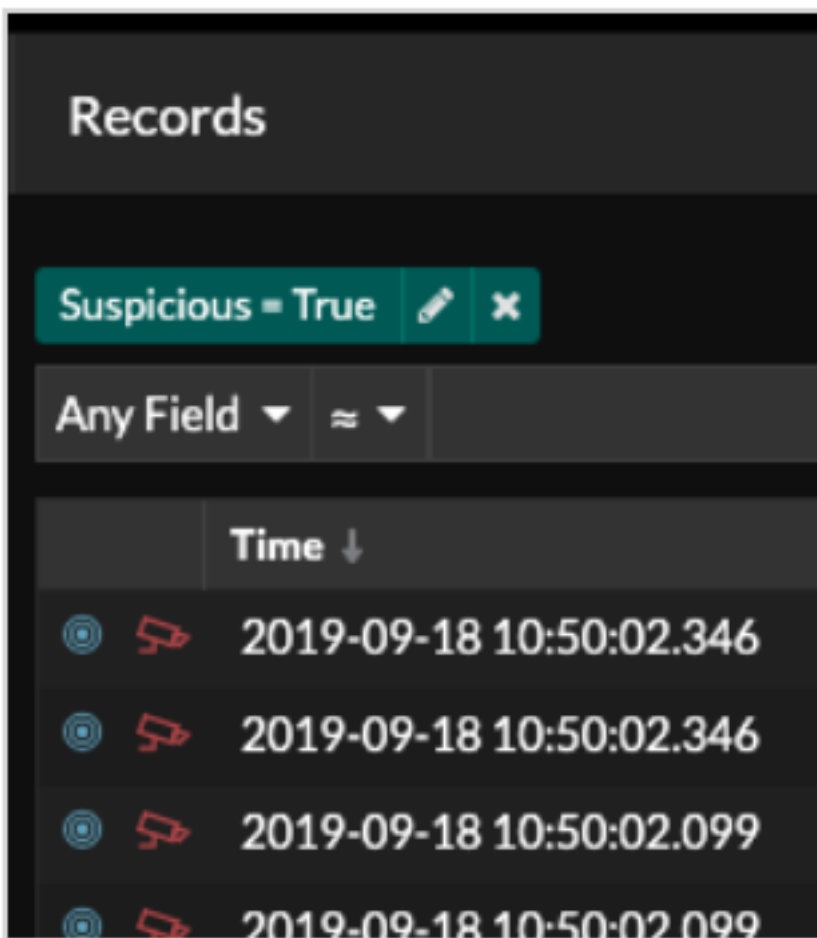
The screenshot displays a detection alert with the following components:

- Risk Level:** A red triangle icon containing the number '60' and the word 'RISK' below it.
- Title:** 'Outbound Suspicious Connection' in large white text, with 'CAUTION' in smaller teal text 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 dark grey box with a red border containing:
 - A skull and crossbones icon followed by the word 'OFFENDER'.
 - A teal circle icon with a white triangle.
 - The domain 'work-031.sea.example.com' and the IP address '192.168.6.120' in white text.
 - A teal cluster of dots icon on the right.
- Visualizations:**
 - 'TCP Metric' and 'Suspicious Connections' labels on the left.
 - '5m Snapshot' and '30s' labels on the right.
 - A line graph showing a peak in suspicious connections, with a teal bar at the end of the line.
- Investigation Steps:** A dark grey box with the title 'INVESTIGATION STEPS' and a teal arrow pointing to the text 'View the suspicious IP address'.









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.



The screenshot displays a 'Records' section with a filter 'Suspicious = True' and a search criteria of 'Any Field ≈'. Below the search bar, a table lists records sorted by 'Time ↓'. Each record entry includes a blue circular icon with a white dot, a red icon of a hand holding a pencil, and a timestamp.

	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

Related topics

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

- Learn about the [Network Overview](#) and [Security Overview](#) pages
- View threat intelligence metrics on the [Security dashboard](#)
- [Manage threat collections](#)
- [Upload STIX files through the REST API](#)