Threat intelligence

Published: 2021-09-01

Threat intelligence provides known data about suspicious IP addresses, 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 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.

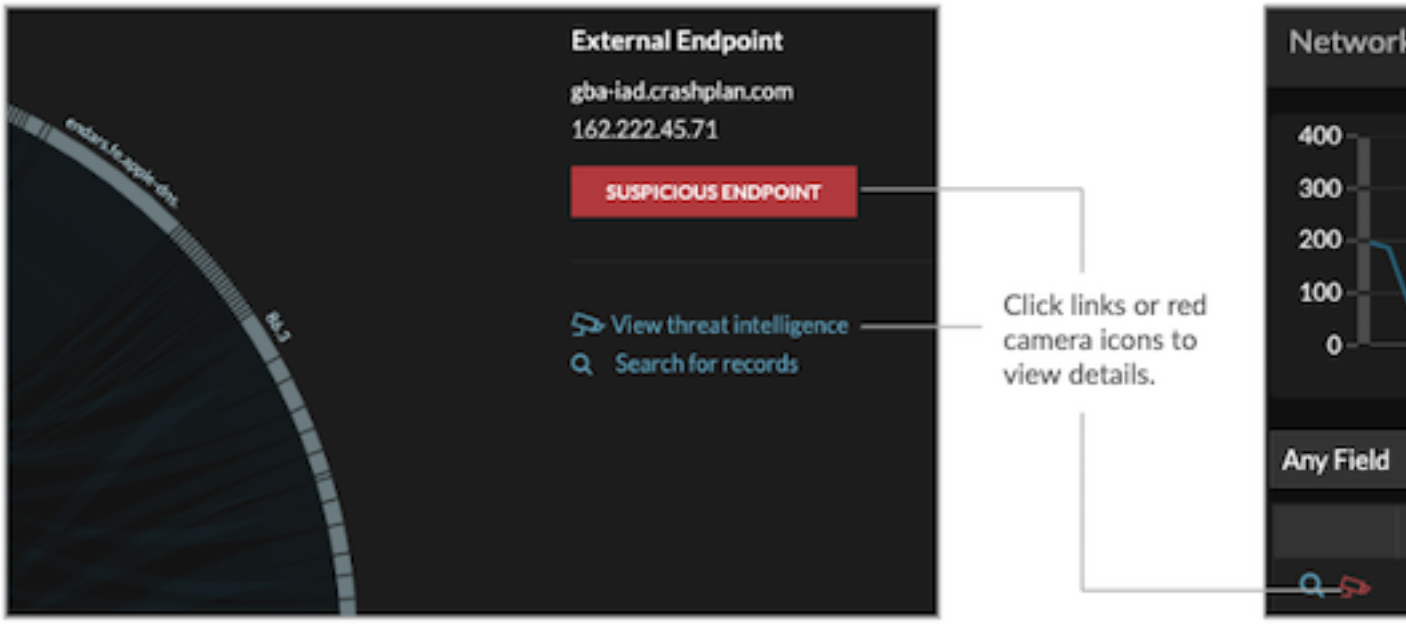
Before you begin

- You must enable these collections in the system to display threat intelligence in system charts and records.
- You can directly upload threat collections to Reveal(x) 360 systems for self-managed sensors. Contact ExtraHop Support to upload a threat collection to ExtraHop-managed sensors.

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. Learn more about uploading 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.

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

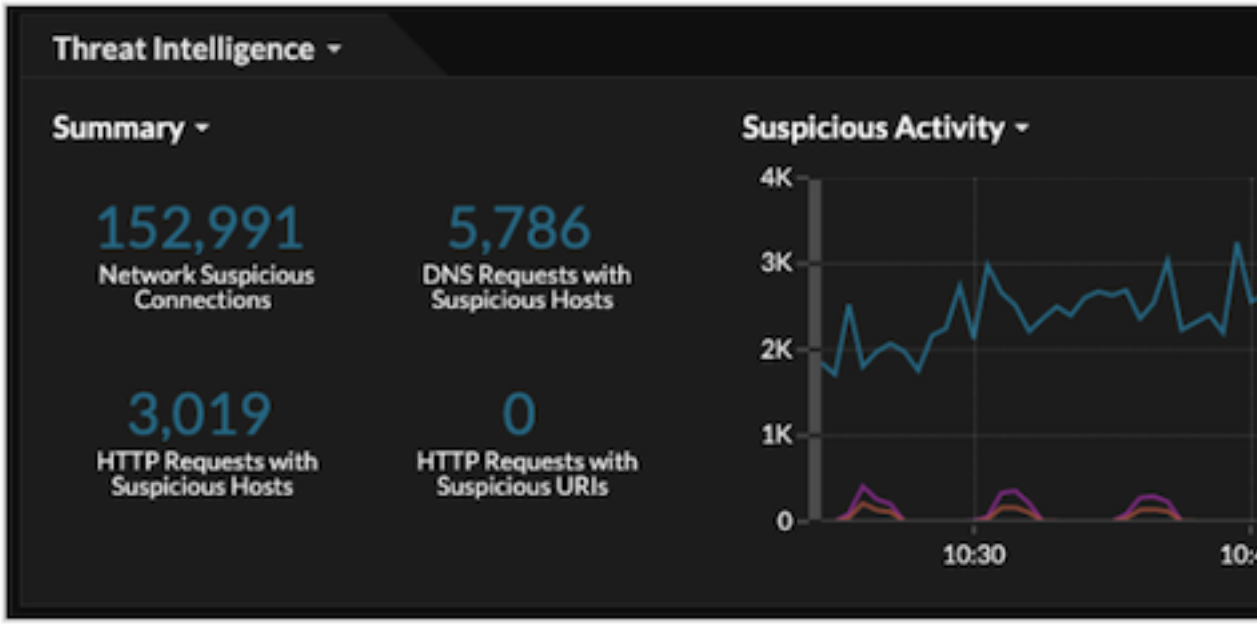
Reveal(x) displays threat intelligence throughout the system, so you can investigate indicators of compromise directly from the tables and charts you are viewing.

- 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:

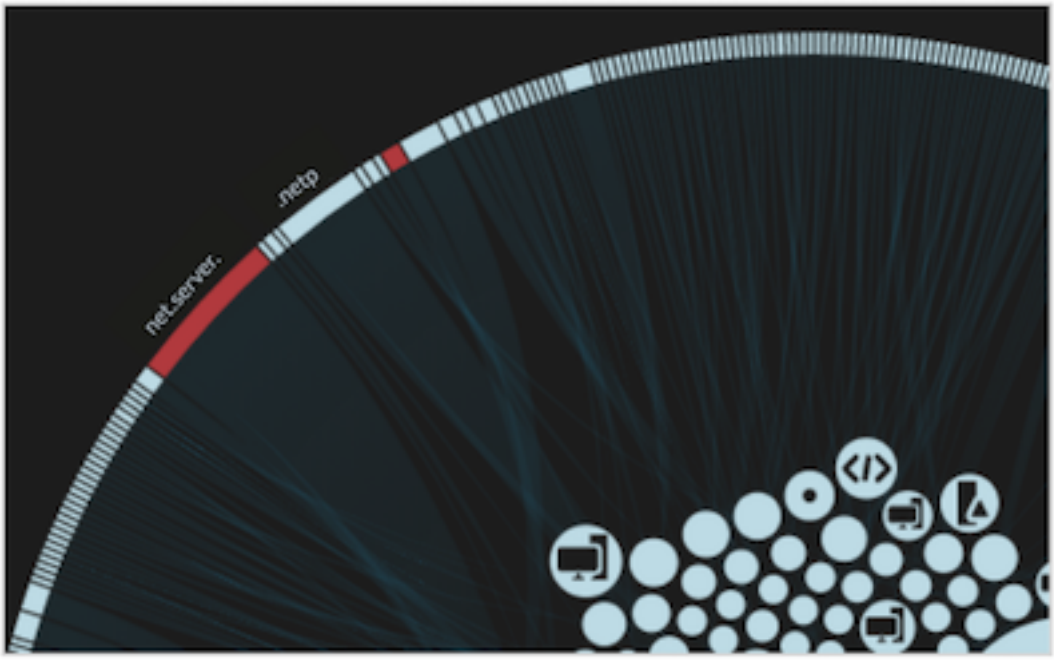
Security Dashboard

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.



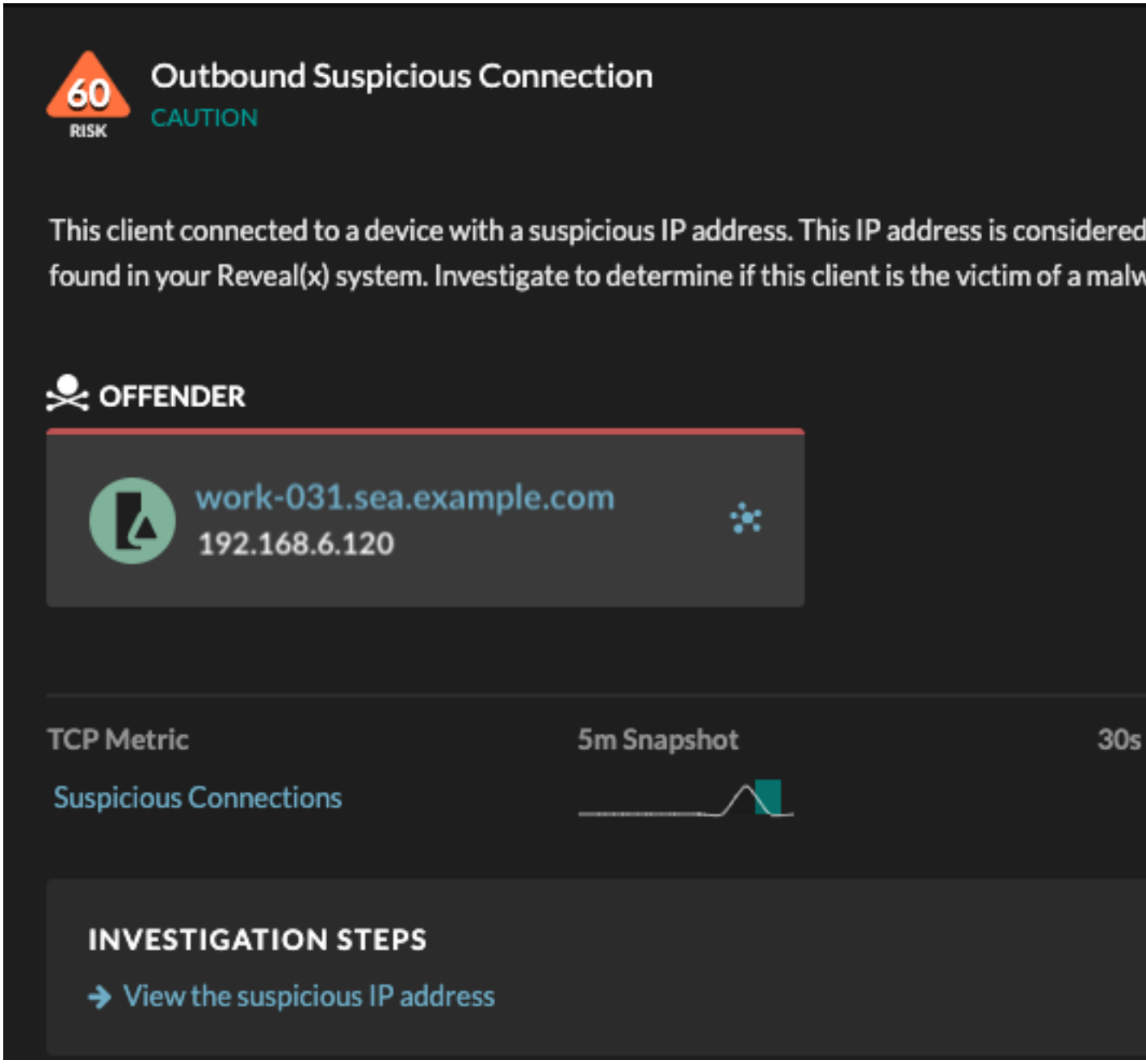
Perimeter Overview

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



Detections

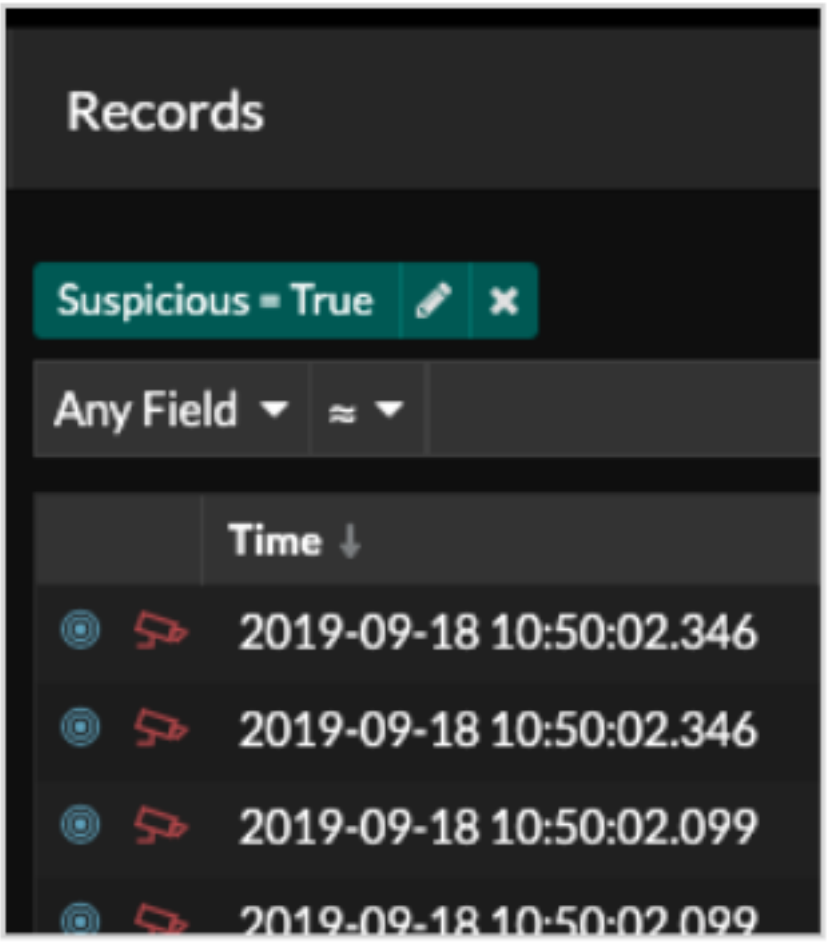
A detection appears when an indicator of compromise from a threat collection is identified in network traffic.



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