

Threat intelligence

Published: 2024-04-08

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

▶ **View** the related training: [Threat Intelligence](#) ↗

Threat intelligence data sets, called threat collections, contain lists of suspicious endpoints known as indicators of compromise (IOCs).

Participants that match a threat collection are tagged as Suspicious in detections, detection summaries, system charts, and records. (For CrowdStrike IOCs where the confidence level is High, the participant is tagged as Malicious.) Records that contain the suspicious entry are marked with a camera icon 📷. In many cases, an indicator match also generates a detection for the suspicious connection.

SUNBURST C&C Activity
 94 RISK
 COMMAND & CONTROL
 Dec 12 15:04 • lasting a few seconds

west.example attempted to access a host associated with the backdoor known as SUNBURST or Solarigate, indicating comm. (C&C) activity. The SUNBURST backdoor affects SolarWinds Orion Platform versions 2019.4 through 2020.2 HF 1.

59 Victims

- 27.226.40.82 **SUSPICIOUS**
- 206.87.153.126
- 143.58.100.52
- 177.82.221.79 **SUSPICIOUS**
- 125.80.192.93

OFFENDER
 34.223.124.45
 suspicious-example.com
MALICIOUS

VICTIM
 west.example

Threat Intelligence

SUSPICIOUS Threat Intelligence Indicator for suspicious-example.com

- Type: SUNBURST Backdoor
- Type: ExtraHop Threat Intelligence
- Collection: Malicious Host Names and URIs (I)
- Producer: ExtraHop Networks

MALICIOUS Threat Intelligence Indicator for suspicious-example.com **CROWDSTRIKE**

- Indicator Type: Domain
- Actor: StellarParticle
- Confidence: High
- Domain Type: C2Domain
- Kill Chain: C2
- Malware: CobaltStrike
- Threat Type: Targeted

Annotations:

- IOCs in detection type summary panel
- Threat intelligence breakdown in detection details
- Suspicious tag for threat intelligence IOC
- Malicious tag for High Confidence CrowdStrike IOC
- CrowdStrike IOC label

Threat collections

The ExtraHop system supports threat collections from several sources.

Built-in threat collections

Curated threat collections from ExtraHop and CrowdStrike Falcon are available by default in your ExtraHop system. Built-in collections are updated every 6 hours. You can [enable or disable built-in threat collections](#) ↗ from the Threat Intelligence page.

STIX file uploads

Free and commercial collections offered by the security community that are formatted in Structured Threat Information eXpression (STIX) as compressed TAR files, such as .TGZ or TAR.GZ, 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 your console and all connected sensors.

TAXII feed

Threat collections can be delivered to your environment from a reliable source over the Trusted Automated Exchange of Intelligence Information (TAXII) protocol. A TAXII feed can provide a consistent stream of updated threat indicators. You can [add a TAXII feed](#) from the Threat Intelligence page.

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 STIX file uploads to high-quality threat intelligence data that focuses on a specific type of intrusion, such as one collection for malware and another collection for botnets. Similarly, we recommend that you limit TAXII feeds to reliable and high-quality sources.

Investigating threats

After the Reveal(x) system observes an indicator of compromise, the suspicious IP address, domain, hostname, or URI is marked as Suspicious or Malicious in detection summaries and on individual detection cards. In tables and charts, indicators of compromise are marked with a camera icon so you can investigate directly from the tables and charts you are viewing.

The screenshot illustrates the integration of threat intelligence into the ExtraHop interface. It shows three main components:

- Table of Suspicious Records:** A table with columns 'Time' and 'Record Type'. It lists three records with timestamps and 'Flow' types. Each record has a camera icon in the left margin, indicating that clicking it will lead to more details.
- Offender Card:** A card for an offender with IP 26.237.235.96 and domain suspicious-example.com. It is labeled 'MALICIOUS External Endpoint' and also features a camera icon.
- Threat Intelligence Card:** A detailed card for a 'Threat Intelligence Indicator for 120.79.70.220'. It lists various attributes: Title (IP: 71.142.193.46), Description (IP 59.50.146.248 reported from Threat Intel List), Type (IP Watchlist), Confidence (Medium), Collection (BitNodes Collection), Producer (Threat Intel List), and Added (April 12, 2021 10:11 PM NDT).

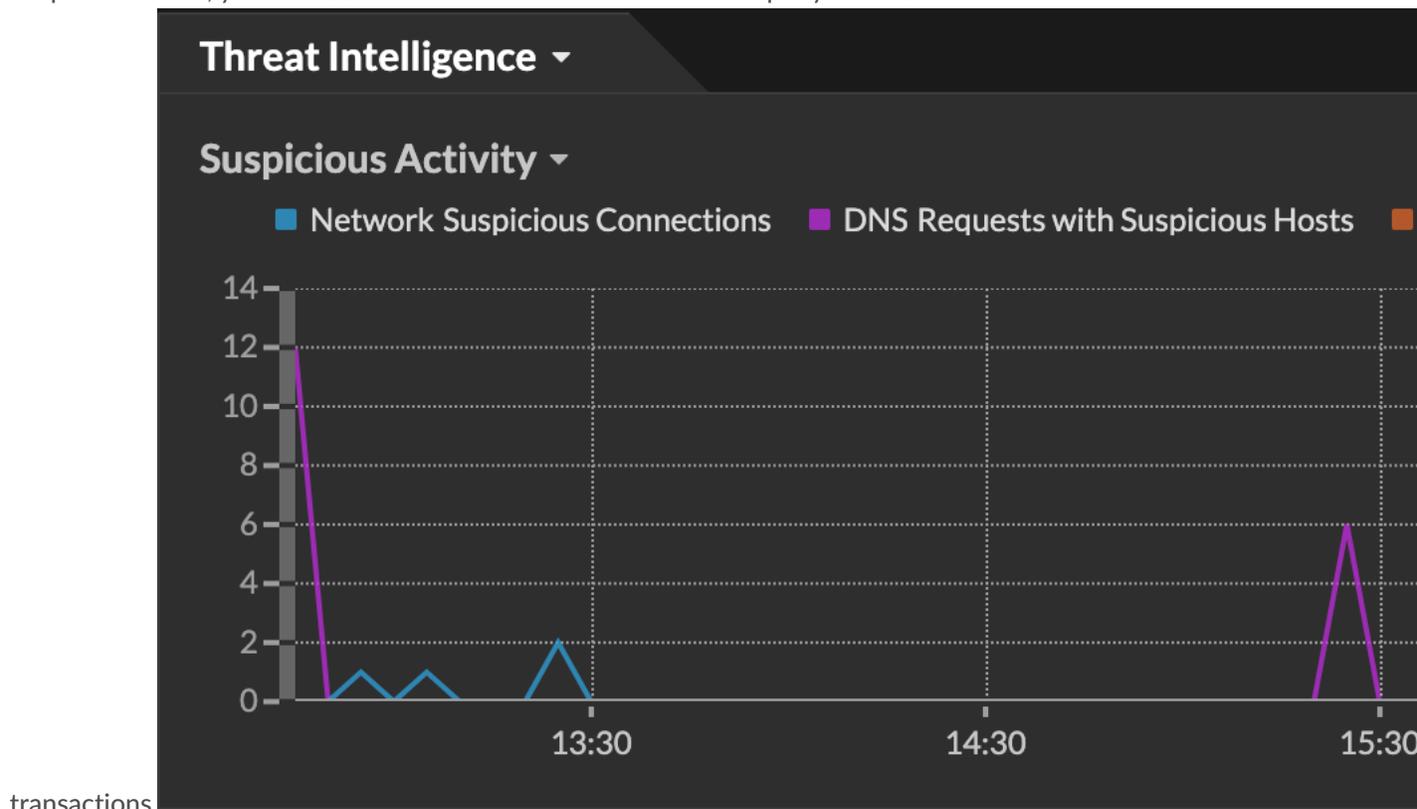
A central text box with arrows pointing to the camera icons in the table and offender card reads: "Click cameras, tags, or links to view IOC details".

- 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.
- (Reveal(x) 360 only) If a built-in ExtraHop or CrowdStrike threat collection is updated, the ExtraHop system performs Automated Retrospective Detection (ARD), which searches for new domains, hostnames, URLs, and IP addresses 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. Detections that are recommended for triage based on threat intelligence will remain in the system after the associated collection is disabled.

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

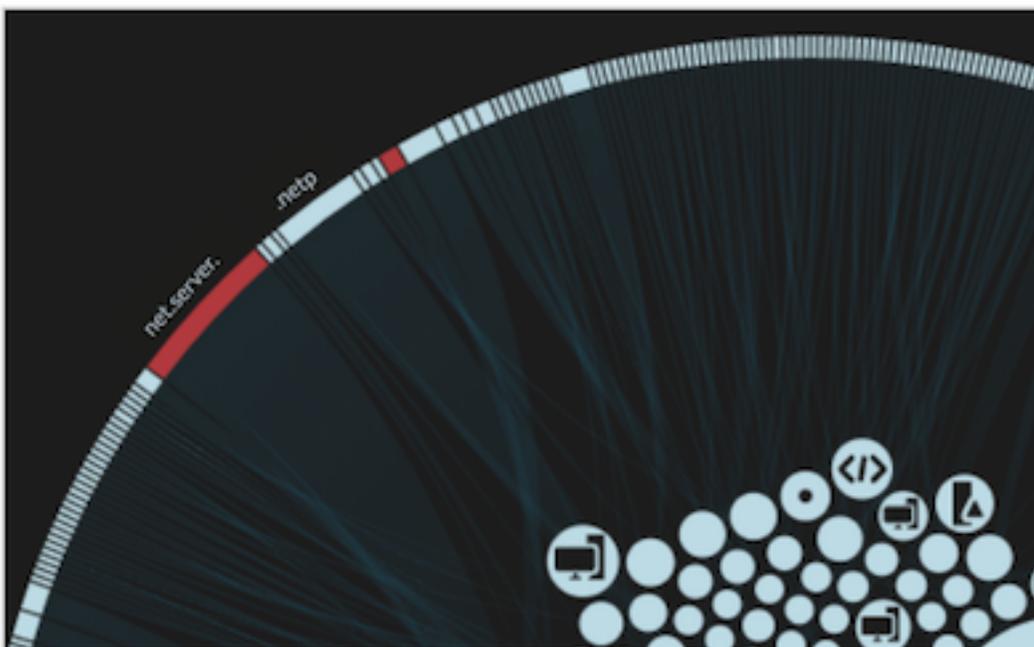
Security Hardening Dashboard

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



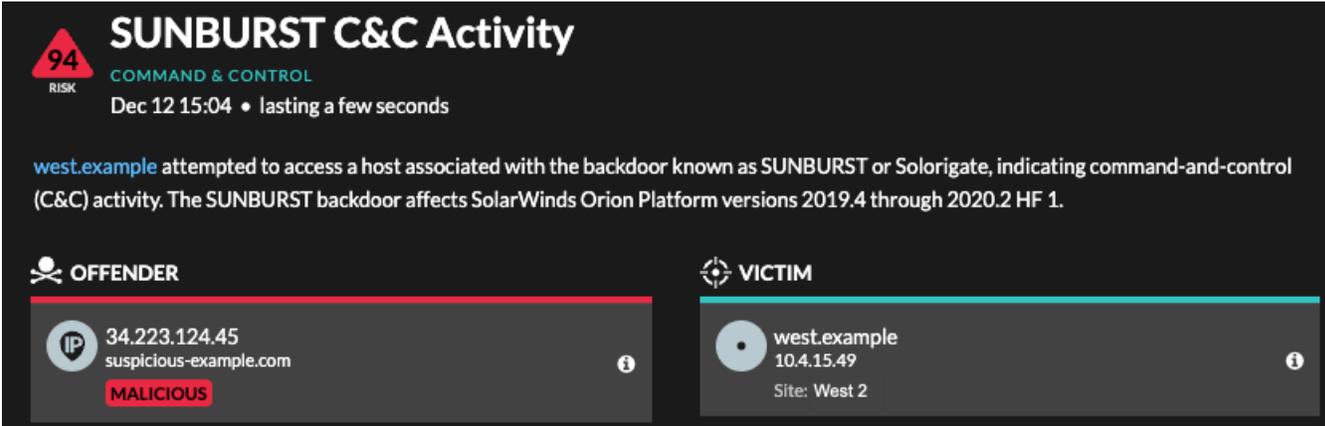
Perimeter Overview

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.



94
RISK

SUNBURST C&C Activity

COMMAND & CONTROL
Dec 12 15:04 • lasting a few seconds

[west.example](#) attempted to access a host associated with the backdoor known as SUNBURST or Solorigate, indicating command-and-control (C&C) activity. The SUNBURST backdoor affects SolarWinds Orion Platform versions 2019.4 through 2020.2 HF 1.

OFFENDER

IP 34.223.124.45
suspicious-example.com
MALICIOUS

VICTIM

west.example
10.4.15.49
Site: West 2

IP Address Details

IP address detail pages display complete threat intelligence for IP address indicators of compromise.



IP Address Details

External Endpoint
Moondarra, Victoria, Australia

SUSPICIOUS	Threat Intelligence Indicator for 220.252.189.126
Title	IP: 38.236.216.22
Description	IP 119.74.30.120 reported from Threat Intel List
Type	IP Watchlist
Confidence	Medium
Collection	BitNodes Collection
Producer	Threat Intel List
Added	April 12, 2021 10:11 PM NDT

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 trifold drop-down, an operator, and a value.
- Click the red camera icon  to view threat intelligence.

The screenshot shows a 'Records' section in a dark-themed interface. At the top, there is a filter bar with 'Suspicious = True' and edit/delete icons. Below that, a search bar shows 'Any Field' and an equals sign operator. The main area is a table with a 'Time' column and a downward arrow. The table contains four rows of records, each with a blue circular icon and a red arrow icon to the left of the 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

Retrospective detections

(Reveal(x) 360 only) When an ExtraHop or CrowdStrike threat collection is updated, the ExtraHop system performs Automated Retrospective Detection (ARD), which searches for new domains, hostnames, URLs, and IP addresses 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.