# Threat intelligence

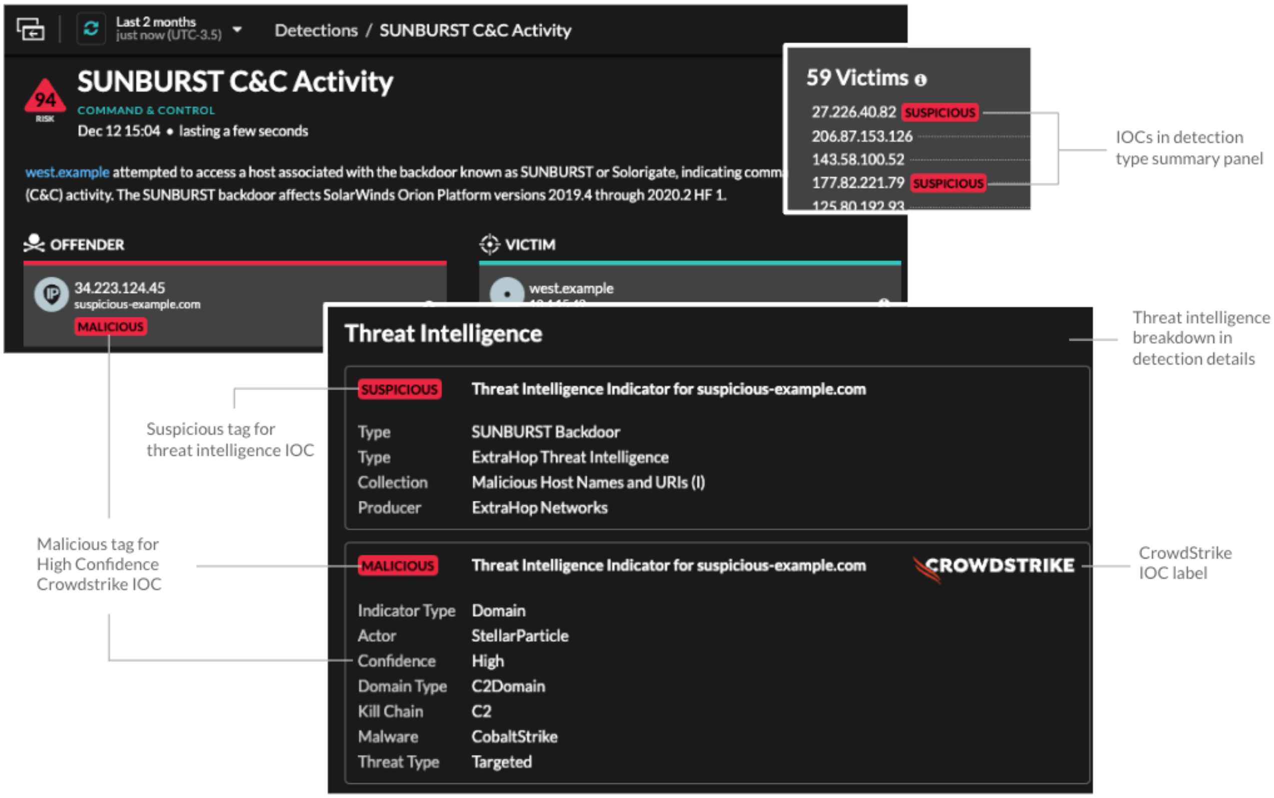
Published: 2024-01-26

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

**Video:** See the related training: Threat Intelligence

Threat intelligence data sets, called threat collections, contain lists of suspicious endpoints known as indicators of compromise (IOCs). When the ExtraHop system observes activity that matches an entry in a threat collection, a detection is generated for the suspicious connection.

Participants that match a threat collection are tagged as Suspicious. (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 .



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 comm
(C&C) activity. The SUNBURST backdoor affects SolarWinds Orion Platform versions 2019.4 through 2020.2 HF 1.

34.223.124.45
suspicious-example.com

west.example

27.226.40.82
206.87.153.126
143.58.100.52
177.82.221.79
125.80.192.93

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

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

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

Curated threat collections from ExtraHop and CrowdStrike Falcon are available by default in your ExtraHop system. You can also upload custom collections from free and commercial sources in the security community.

## Threat collections

The ExtraHop system supports threat collections from several sources.

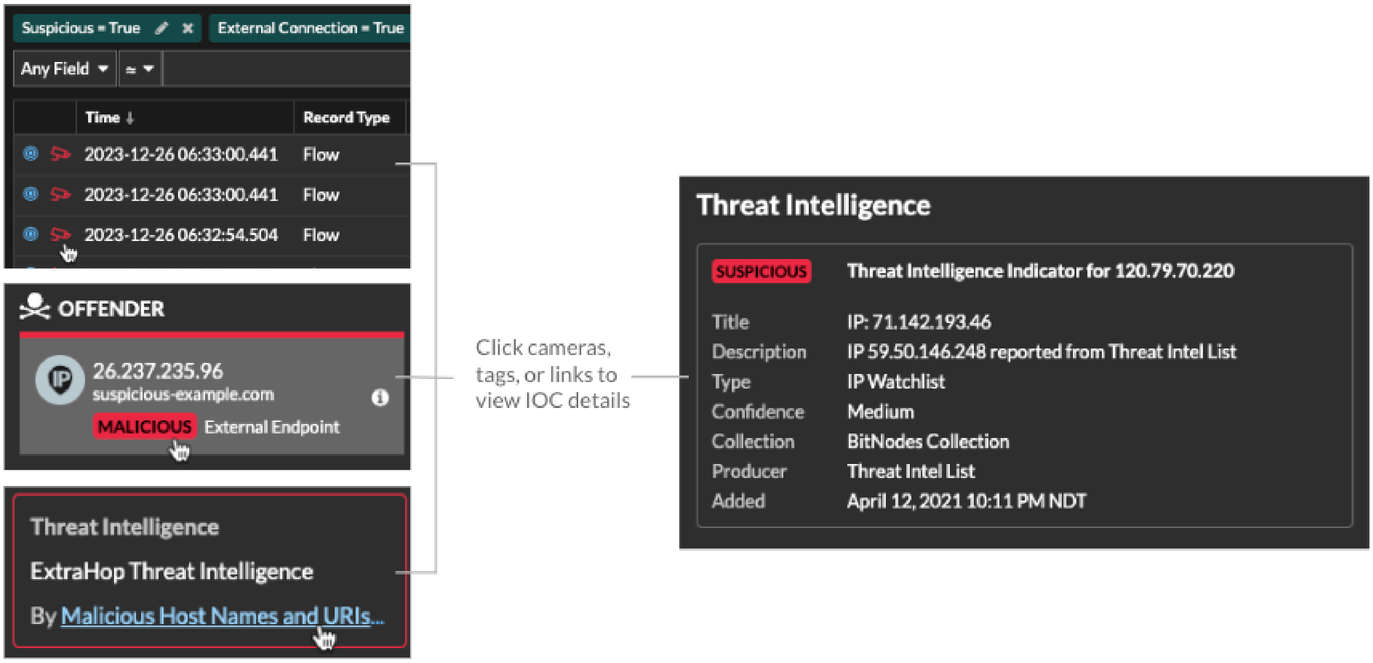
Because cyber threat intelligence is community-driven, there are many external sources for threat collections. Data from these collections can vary in quality or relevance to your environment. To maintain accuracy and reduce noise, we recommend that you limit your uploads to high-quality threat intelligence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

Threat collections curated by ExtraHop or Crowdstrike Falcon are updated every 6 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 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.

## 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.



| Time ↓ | Record Type |
|---|---|
| 2023-12-26 06:33:00.441 | Flow |
| 2023-12-26 06:33:00.441 | Flow |
| 2023-12-26 06:32:54.504 | Flow |

OFFENDER

26.237.235.96
suspicious-example.com
MALICIOUS External Endpoint

Threat Intelligence
ExtraHop Threat Intelligence
By Malicious Host Names and URIs...

Click cameras, tags, or links to view IOC details

Threat Intelligence

SUSPICIOUS Threat Intelligence Indicator for 120.79.70.220

| | |
|---|---|
| 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 |
| Added | April 12, 2021 10:11 PM NDT |

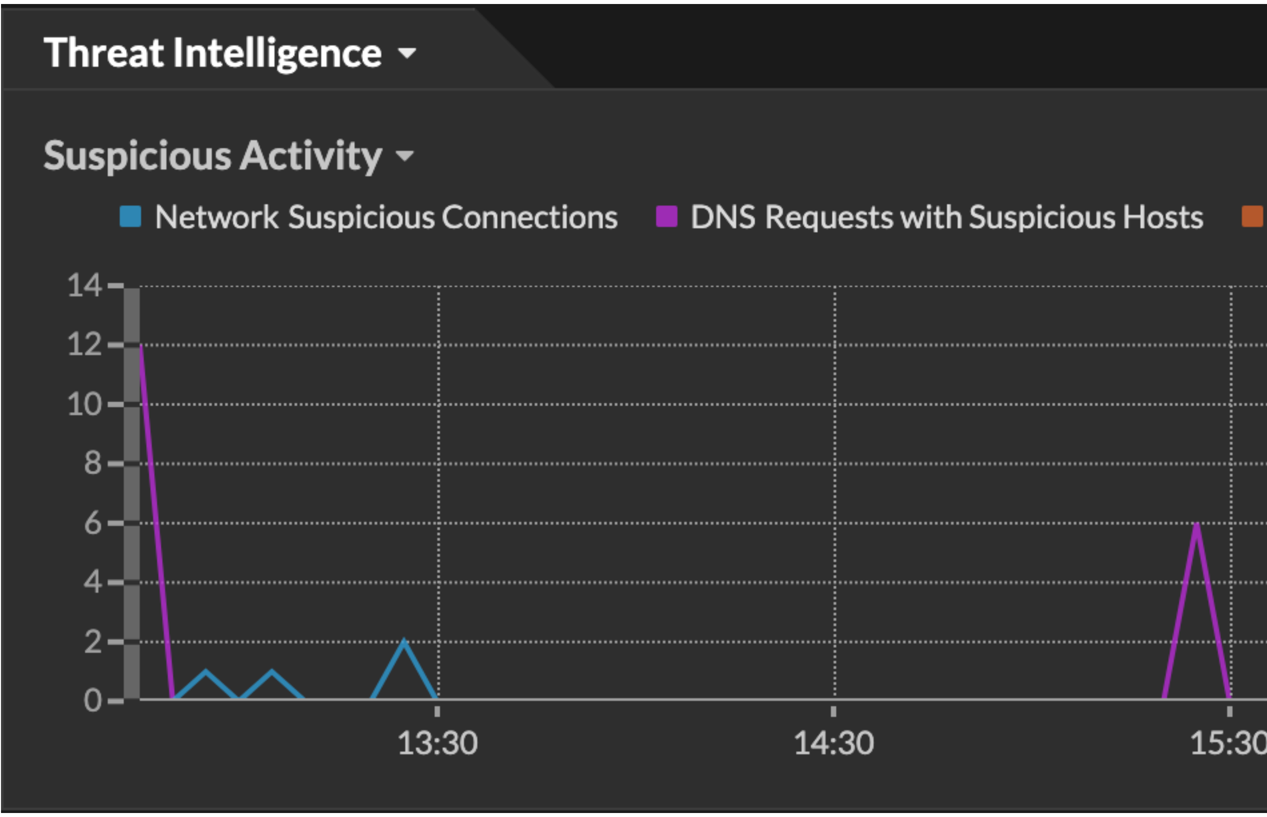
- If the threat collection is added or updated after the system has observed the suspicious activity, threat intelligence is not applied to that IP address, hostname, or URI until the suspicious activity occurs again.
- (Reveal(x) 360 only) If a built-in ExtraHop or CrowdStrike threat collection is updated, 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

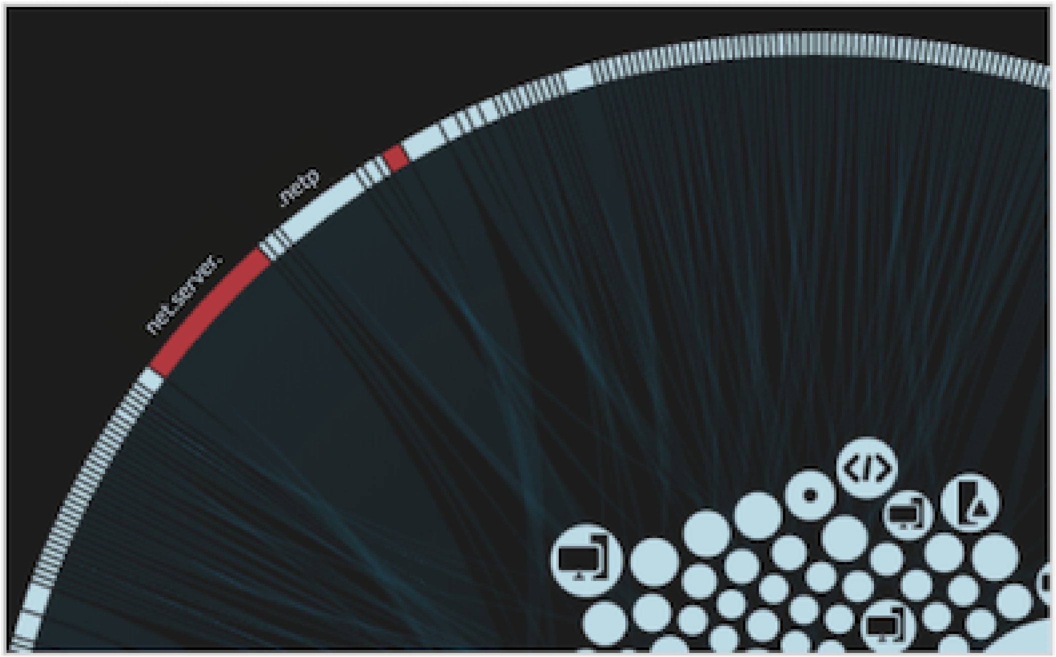
The Threat Intelligence region contains metrics for suspicious activity that matches the data in your threat collections. By clicking any metric, such as HTTP Requests with

Suspicious Hosts, you can drill down on the metric for details or query records for related transactions.


Threat Intelligence
Suspicious Activity
Network Suspicious Connections
DNS Requests with Suspicious Hosts
14
12
10
8
6
4
2
0
13:30
14:30
15:30

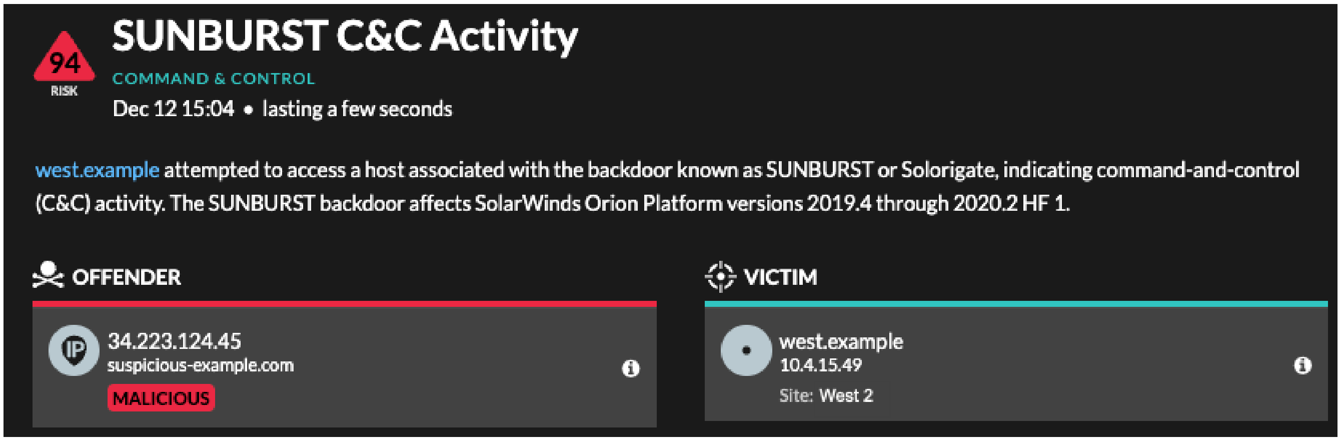
**Perimeter Overview**

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

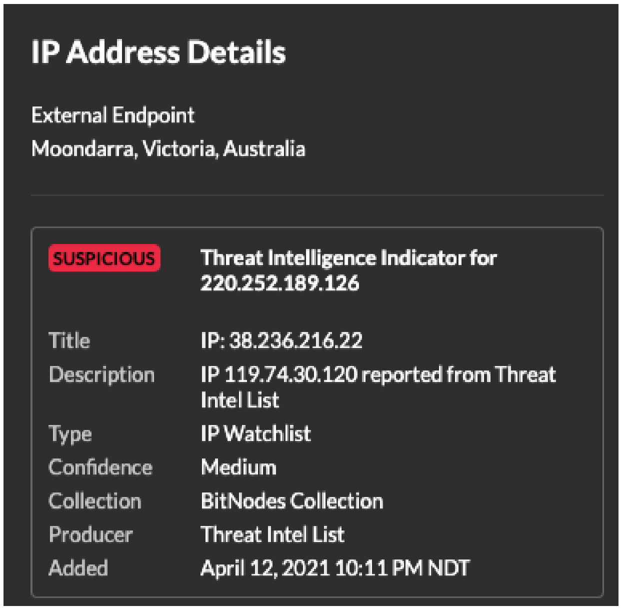
34.223.124.45
suspicious-example.com
MALICIOUS

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

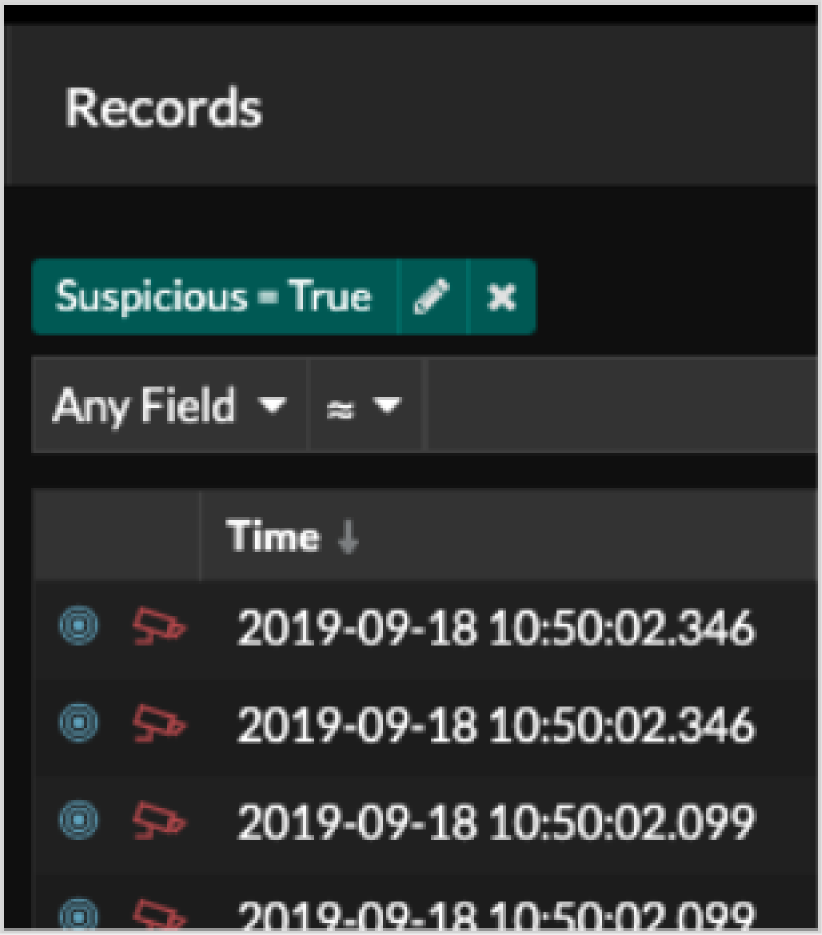
SUSPICIOUS Threat Intelligence Indicator for 220.252.189.126

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



Records

| 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.