

Bedrohungsinformationen

Veröffentlicht: 2024-01-31

Bedrohungsinformationen liefern bekannte Daten über verdächtige IP-Adressen, Domänen, Hostnamen und URIs, die Ihnen helfen können, Risiken für Ihr Unternehmen zu identifizieren.

▶ **Wenden Sie sich die entsprechende Schulung an:** [Bedrohungsinformationen](#)

Bedrohungsinformationsdatensätze, sogenannte Bedrohungssammlungen, enthalten Listen verdächtiger Endpunkte, die als Indicators of Compromise (IOCs) bezeichnet werden. Wenn das ExtraHop-System Aktivitäten beobachtet, die einem Eintrag in einer Bedrohungssammlung entsprechen, wird eine Erkennung für die verdächtige Verbindung generiert.

Teilnehmer, die einer Bedrohungssammlung entsprechen, werden als Verdächtig markiert. (Bei CrowdStrike-IOCs, bei denen das Konfidenzniveau hoch ist, wird der Teilnehmer als böseartig markiert.) Aufzeichnungen, die den verdächtigen Eintrag enthalten, sind mit einem Kamerasymbol gekennzeichnet 📹.

The screenshot displays a detection event titled "SUNBURST C&C Activity" with a risk level of 94. The event description states: "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." The interface shows an offender IP of 34.223.124.45 (suspicious-example.com) and a victim IP of west.example (192.168.1.10).

Annotations in the image include:

- IOCs in detection type summary panel:** A panel titled "59 Victims" lists several IP addresses, with two marked as "SUSPICIOUS": 27.226.40.82, 206.87.153.126, 143.58.100.52, 177.82.221.79, and 125.80.192.93.
- Threat intelligence breakdown in detection details:** A "Threat Intelligence" panel shows two indicators for "suspicious-example.com":
 - SUSPICIOUS:** Threat Intelligence Indicator for suspicious-example.com. Type: SUNBURST Backdoor. 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. This entry includes a "CROWDSTRIKE" IOC label.
- Suspicious tag for threat intelligence IOC:** Points to the "SUSPICIOUS" tag in the first threat intelligence entry.
- Malicious tag for High Confidence CrowdStrike IOC:** Points to the "MALICIOUS" tag in the second threat intelligence entry.

Kuratierte Bedrohungssammlungen von ExtraHop und CrowdStrike Falcon sind standardmäßig in Ihrem ExtraHop-System verfügbar. Sie können auch benutzerdefinierte Sammlungen aus kostenlosen und kommerziellen Quellen in der Sicherheits-Community hochladen.

Sammlungen von Bedrohungen

Das ExtraHop-System unterstützt das Sammeln von Bedrohungen aus verschiedenen Quellen.

Da Cyber-Bedrohungsinformationen von der Community gesteuert werden, gibt es viele externe Quellen für die Erfassung von Bedrohungen. Daten aus diesen Sammlungen können in ihrer Qualität oder Relevanz für Ihre Umgebung variieren. Um die Genauigkeit zu gewährleisten und Störungen zu reduzieren, empfehlen wir, dass Sie Ihre Uploads auf qualitativ hochwertige Bedrohungsdaten beschränken, die sich

auf eine bestimmte Art von Eindringlingen konzentrieren, z. B. eine Sammlung für Malware und eine andere Sammlung für Botnets.

Von ExtraHop oder CrowdStrike Falcon kuratierte Bedrohungssammlungen werden alle 6 Stunden aktualisiert. Verdächtige IP-Adressen, Domains, Hostnamen und URIs erscheinen in Systemdiagrammen und Datensätzen.

[Kostenlose und kommerzielle Sammlungen, die von der Sicherheits-Community angeboten werden](#) die in Structured Threat Information eXpression (STIX) als komprimierte TAR-Dateien wie .TGZ oder TAR.GZ formatiert sind, können manuell hochgeladen werden oder [über die REST-API](#) zu ExtraHop-Systemen. STIX Version 1.0 - 1.2 werden derzeit unterstützt. Sie müssen jede Bedrohungssammlung einzeln auf Ihre Konsole und alle angeschlossenen Sensoren hochladen.

Untersuchung von Bedrohungen

Nachdem das Reveal (x) -System einen Indikator für eine Gefährdung festgestellt hat, wird die verdächtige IP-Adresse, Domain, Hostname oder URI in den Erkennungszusammenfassungen und auf einzelnen Erkennungskarten als Verdächtig oder Böartig markiert. In Tabellen und Diagrammen sind Kompromissindikatoren mit einem Kamerasymbol gekennzeichnet, sodass Sie direkt in den Tabellen und Diagrammen, die Sie gerade ansehen, Nachforschungen anstellen können.

The screenshot displays the ExtraHop interface for threat intelligence. At the top, filters are set to 'Suspicious = True' and 'External Connection = True'. Below this is a table of suspicious flows:

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

Below the table is an 'OFFENDER' card for IP 26.237.235.96 (suspicious-example.com), marked as 'MALICIOUS External Endpoint'. A 'Threat Intelligence' card is also visible, titled 'ExtraHop Threat Intelligence' and 'By Malicious Host Names and URIs...'. A detailed view of a threat intelligence indicator for IP 120.79.70.220 is shown on the right:

Threat Intelligence Indicator for 120.79.70.220	
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

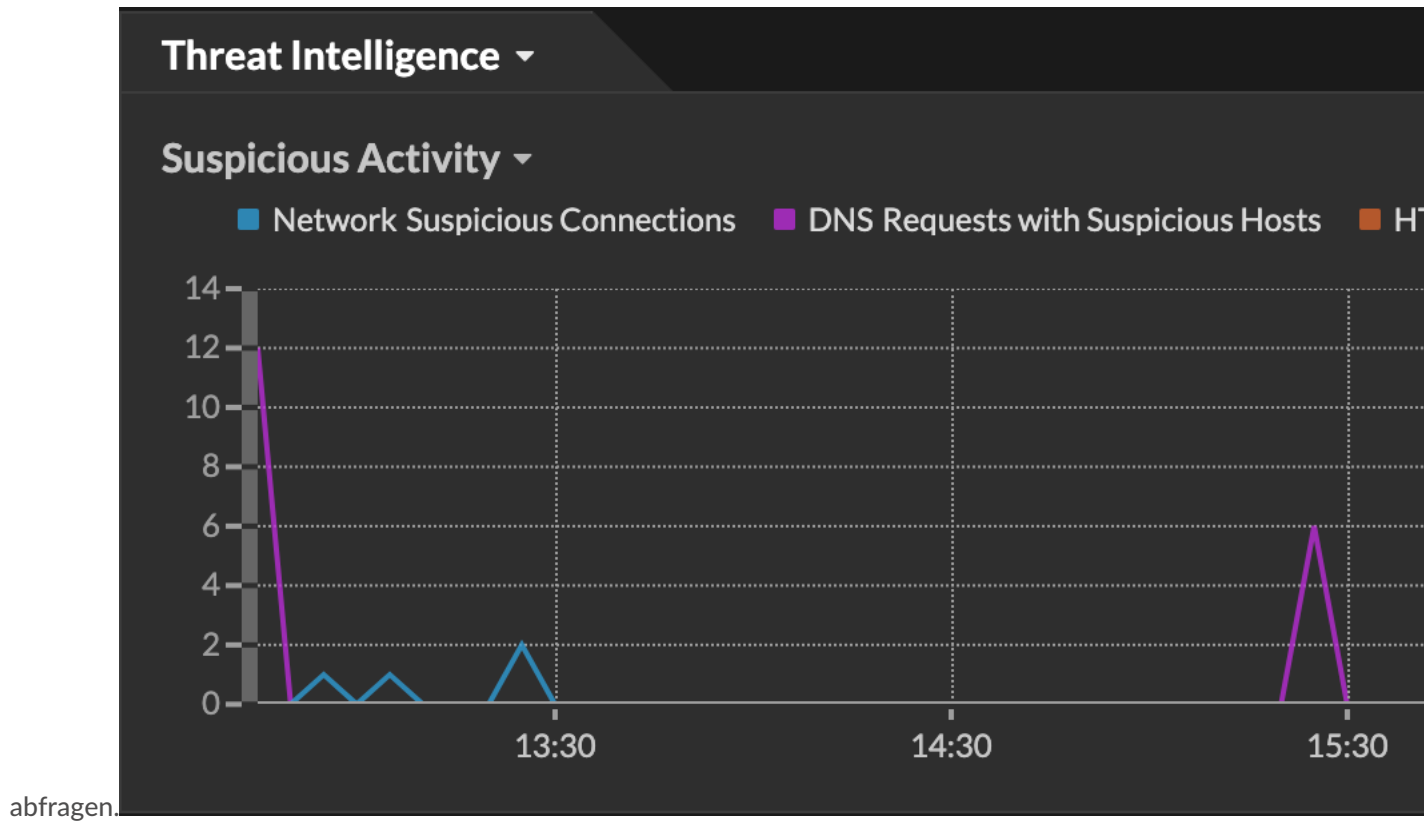
A callout box with the text 'Click cameras, tags, or links to view IOC details' points to camera icons in the flow table and the offender card.

- Wenn die Bedrohungssammlung hinzugefügt oder aktualisiert wird, nachdem das System die verdächtige Aktivität beobachtet hat, werden Bedrohungsinformationen erst dann auf diese IP-Adresse, diesen Hostnamen oder URI angewendet, wenn die verdächtige Aktivität erneut auftritt.
- (Nur Reveal (x) 360) Wenn eine integrierte ExtraHop- oder CrowdStrike-Bedrohungssammlung aktualisiert wird, führt das ExtraHop-System eine automatische Retrospektive Detection (ARD) durch, die nach neuen Domains, Hostnamen, URLs und IP-Adressen sucht, die auf eine Gefährdung in den Datensätzen der letzten 7 Tage hinweisen. Wenn eine Übereinstimmung gefunden wird, generiert das System eine rückwirkende Erkennung.
- Wenn Sie eine Bedrohungssammlung deaktivieren oder löschen, werden alle Indikatoren aus den zugehörigen Metriken und Datensätzen im System entfernt. Erkennungen, die für die Triage auf der Grundlage von Bedrohungsinformationen empfohlen werden, verbleiben im System, nachdem die zugehörige Sammlung deaktiviert wurde.

Hier sind einige Stellen im Reveal (x) -System, an denen die in Ihren Bedrohungssammlungen gefundenen Bedrohungsindikatoren angezeigt werden:

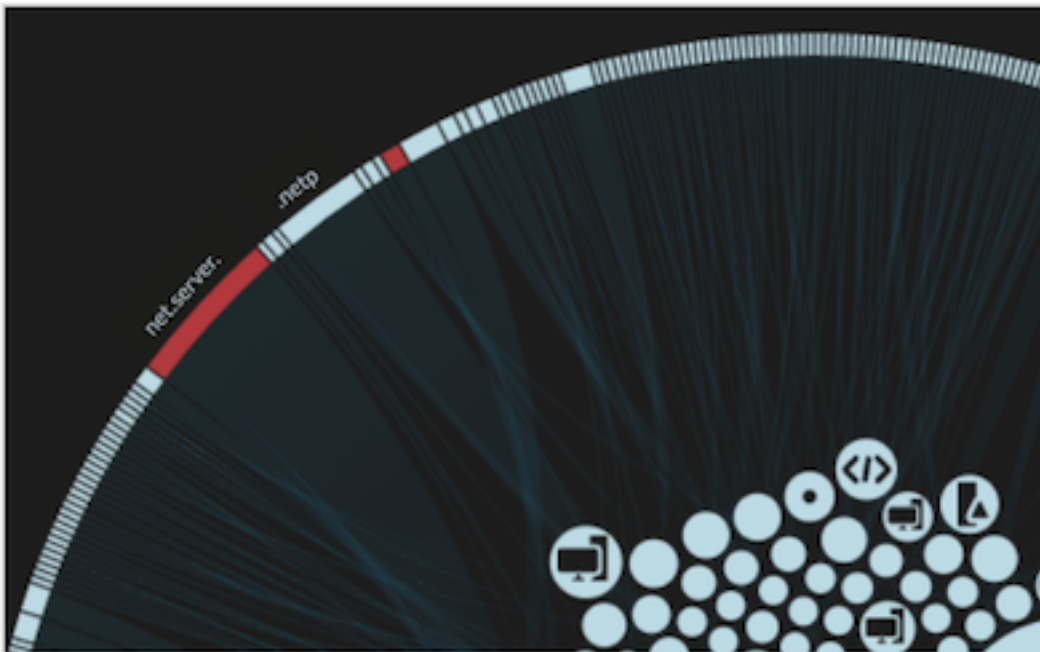
Dashboard zur Erhöhung der Sicherheit

Das [Region „Bedrohungsinformationen“](#) enthält Kennzahlen für verdächtige Aktivitäten, die mit den Daten in Ihren Bedrohungsammlungen übereinstimmen. Wenn Sie auf eine beliebige Metrik klicken, z. B. auf HTTP-Anfragen mit verdächtigen Hosts, können Sie Details zu der Metrik aufrufen oder Datensätze für verwandte Transaktionen



Perimeter im Überblick

In der Halo-Visualisierung sind alle Endpunkte, die mit Einträgen zur Bedrohungserfassung übereinstimmen, rot hervorgehoben.



Erkennungen

Eine Erkennung erfolgt, wenn im Netzwerkverkehr ein Indikator für eine Gefährdung aus einer Bedrohungssammlung erkannt wird.

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

IP

west.example

10.4.15.49

Site: West 2

Angaben zur IP-Adresse

Auf den IP-Adressdetailseiten werden vollständige Bedrohungsinformationen zu IP-Adressindikatoren für kompromittierte IP-Adressen angezeigt.

IP Address Details


External Endpoint
Moondarra, Victoria, Australia

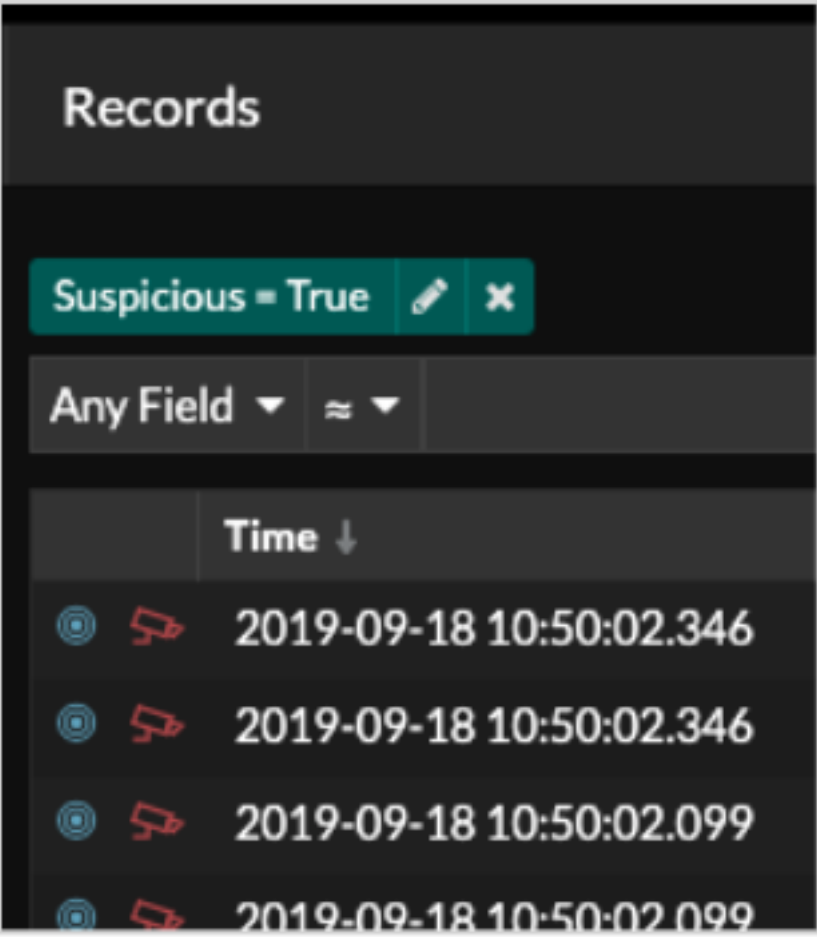
SUSPICIOUS Threat Intelligence Indicator for 220.252.189.126









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

Aufzeichnungen

Auf der Seite „Datensätze“ können Sie direkt nach Transaktionen abfragen, die den Einträgen zur Bedrohungssammlung entsprechen.

- Klicken Sie unter der Facette Verdächtig auf **Wahr** um nach allen Datensätzen mit Transaktionen zu filtern, die mit verdächtigen IP-Adressen, Hostnamen und URIs übereinstimmen.
- Erstellen Sie einen Filter, indem Sie Verdächtige, Verdächtige IP, Verdächtige Domain oder Verdächtige URI aus dem Dreifeld-Dropdownmenü, einen Operator und einen Wert auswählen.
- Klicken Sie auf das rote Kamerasymbol  um Bedrohungsinformationen einzusehen.



		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

Rückwirkende Erkennungen

(Nur Reveal (x) 360) Wenn eine ExtraHop- oder CrowdStrike-Bedrohungssammlung aktualisiert wird, führt das ExtraHop-System eine automatische Retrospektive Detection (ARD) durch, die nach neuen Domains, Hostnamen, URLs und IP-Adressen sucht, die auf eine Gefährdung in den Datensätzen der letzten 7 Tage hinweisen. Wenn eine frühere Verbindung zu einer verdächtigen Domain erkannt wird, generiert das System eine nachträgliche Erkennung.

Der Zeitstempel einer rückwirkenden Erkennung gibt den Zeitpunkt an, zu dem die Aktivität ursprünglich stattgefunden hat und möglicherweise nicht in der aktuellen Erkennungsliste erscheint. Rückwirkende Erkennungen finden Sie, indem Sie auf Retrospective Threat Intelligence klicken [Bedrohungsübersicht](#). Du kannst auch [eine Regel für Erkennungsbenachrichtigungen erstellen](#) um Ihnen eine E-Mail zu senden, wenn diese Arten von Erkennungen auftreten.