Bedrohungsinformationen

Veröffentlicht: 2023-09-14

Threat Intelligence liefert bekannte Daten über verdächtige IP-Adressen, Domains, Hostnamen und URIs, anhand derer Risiken für Ihr Unternehmen identifiziert werden können.

Bedrohungsinformationsdatensätze, sogenannte Bedrohungssammlungen, sind standardmäßig in Ihrem ExtraHop-System, aus kostenlosen und kommerziellen Quellen in der Sicherheits-Community und von Partnerintegrationen mit ExtraHop Reveal (x) 360.

Wenn das ExtraHop-System Aktivitäten beobachtet, die mit einem Eintrag in einer Bedrohungssammlung übereinstimmen (ein sogenannter Indikator für eine Gefährdung), wird eine Erkennung für die Verbindung zu einem verdächtigen Endpunkt generiert und der verdächtige Eintrag wird mit einem Kamerasymbol gekennzeichnet. oder andere visuelle Hinweise.

Sammlungen von Bedrohungen

Das ExtraHop-System unterstützt Bedrohungssammlungen 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 wahren und das Rauschen zu reduzieren, empfehlen wir Ihnen, Ihre Uploads auf hochwertige Threat-Intelligence-Daten zu beschränken, die sich auf eine bestimmte Art von Eindringversuchen konzentrieren, z. B. eine Sammlung für Malware und eine andere Sammlung für Botnetze.

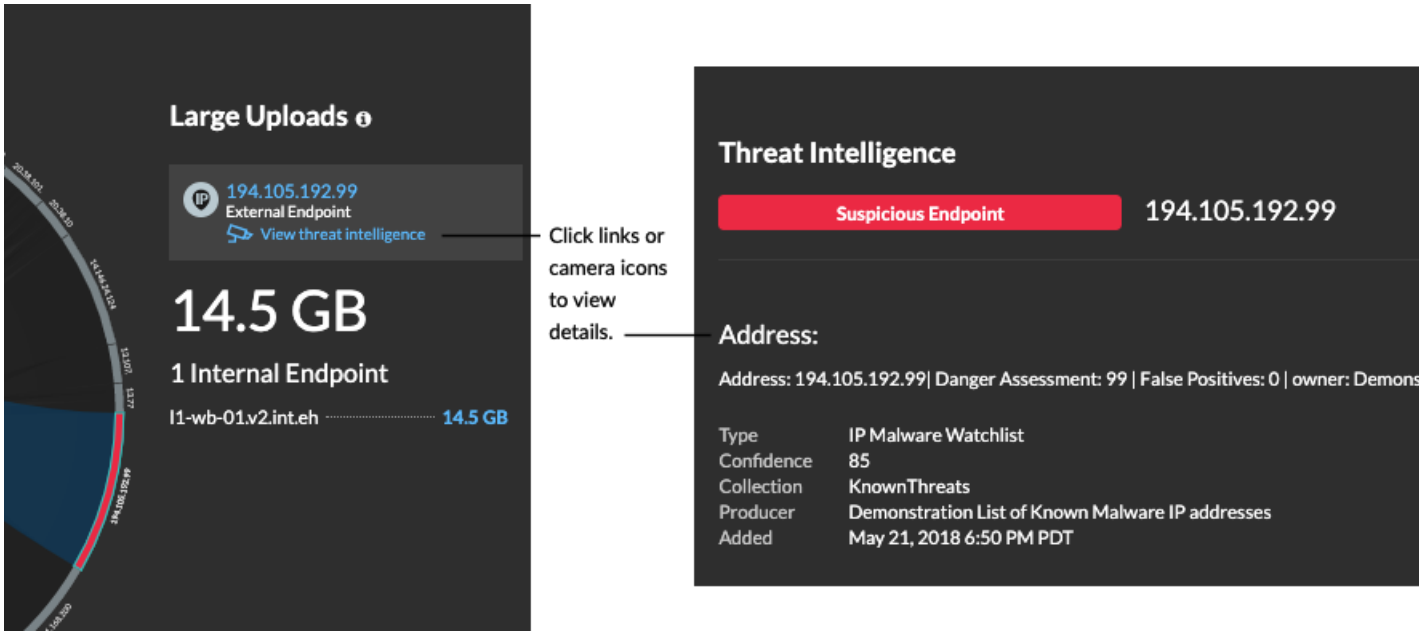
Von ExtraHop kuratierte Bedrohungssammlungen werden alle 12 Stunden aktualisiert. Verdächtige IP-Adressen, Domains, Hostnamen und URIs werden in Systemdiagrammen und Aufzeichnungen angezeigt.

Kostenlose und kommerzielle Sammlungen, die von der Sicherheitsgemeinschaft angeboten werden die in Structured Threat Information eXpression (STIX) als TAR- oder TAR.GZ -Dateien formatiert sind, können manuell hochgeladen werden oder über die REST-API zu ExtraHop-Systemen. STIX Versionen 1.0 - 1.2 werden derzeit unterstützt. Sie müssen jede Bedrohungssammlung einzeln auf alle angeschlossenen Sensoren hochladen.

Bedrohungssammlungen von Partnerintegrationen müssen in ExtraHop Reveal (x) 360 importiert werden.

Untersuchung von Bedrohungen

Nachdem das Reveal (x) -System einen Hinweis auf eine Gefährdung festgestellt hat, wird die verdächtige IP-Adresse, Domain, Hostname oder URI mit einem Kamerasymbol oder einem anderen visuellen Hinweis gekennzeichnet, sodass Sie die Untersuchung direkt anhand der angezeigten Tabellen und Diagramme durchführen können.



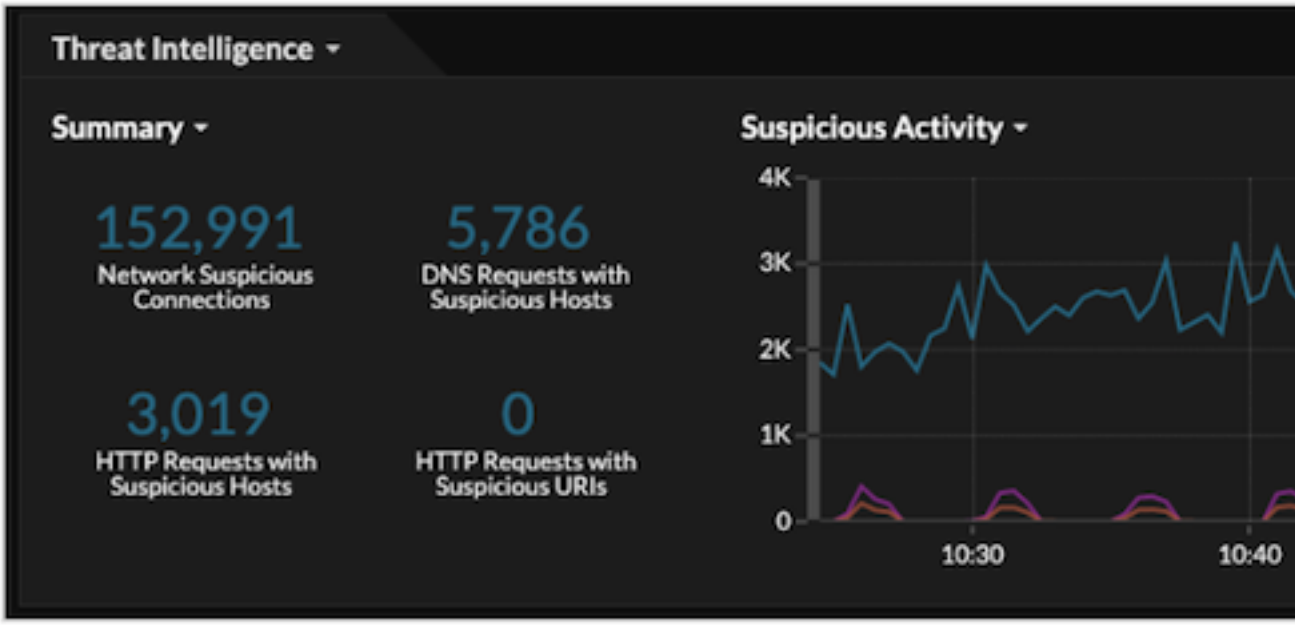
- Wenn die Bedrohungssammlung hinzugefügt oder aktualisiert wird, nachdem das System die verdächtige Aktivität beobachtet hat, werden Bedrohungsinformationen erst dann auf diese IP-Adresse, diesen Hostnamen oder diese URI angewendet, wenn die verdächtige Aktivität erneut auftritt.
- Wenn eine von ExtraHop kuratierte Bedrohungssammlung aktualisiert wird, führt das ExtraHop-System eine automatische Retrospektive Erkennung (ARD) durch, bei der nach neuen Domains gesucht wird, die Anzeichen für eine Gefährdung in den Datensätzen der letzten 7 Tage sind. Wenn eine Übereinstimmung gefunden wird, generiert das System eine retrospektive Erkennung .
- Wenn Sie eine Bedrohungssammlung deaktivieren oder löschen, werden alle Indikatoren aus den zugehörigen Metriken und Datensätzen im System entfernt.

An einigen Stellen im Reveal (x) -System werden die in Ihren Bedrohungssammlungen gefundenen Bedrohungsindikatoren angezeigt:

Dashboard zur Erhöhung der Sicherheit

Die Region „Bedrohungsinformationen“ enthält Metriken für verdächtige Aktivitäten, die mit den Daten in Ihren Bedrohungssammlungen übereinstimmen. Wenn Sie auf eine beliebige Metrik klicken, z. B. auf HTTP-Anfragen mit verdächtigen Hosts, können

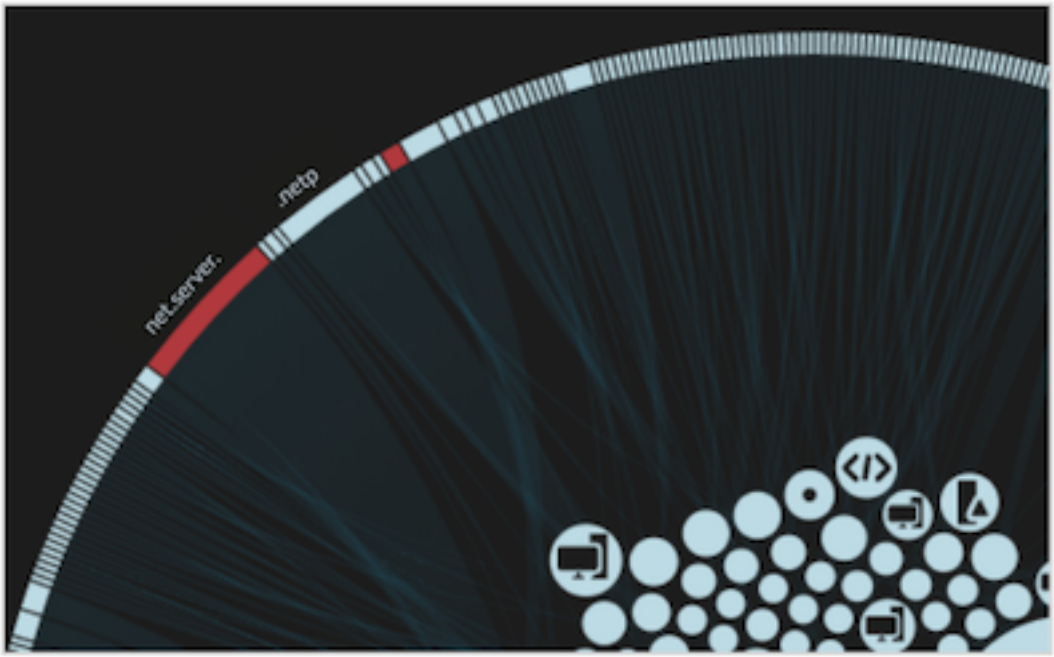
Sie Details zu der Metrik aufrufen oder Datensätze für zugehörige Transaktionen



abfragen.

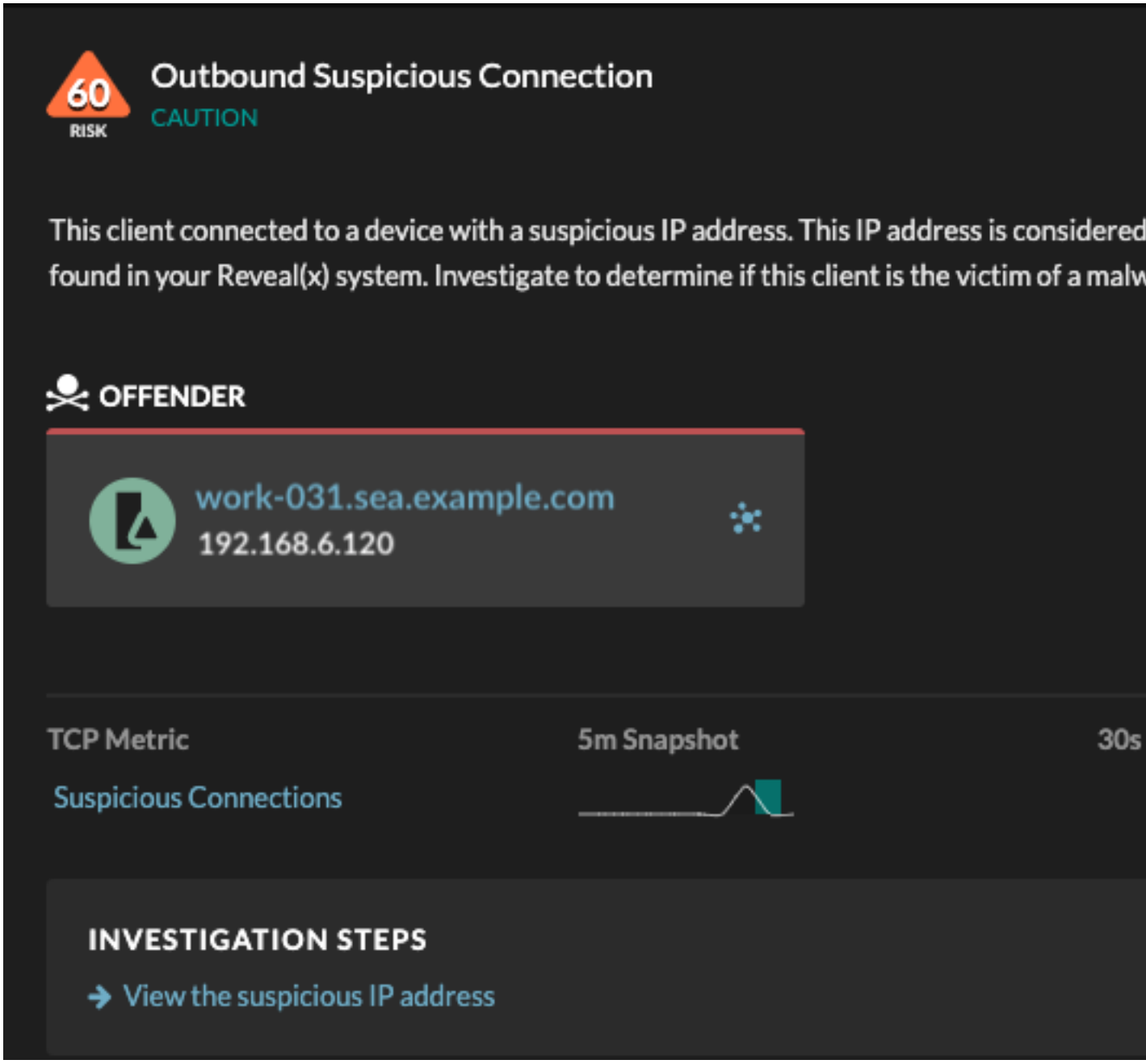
Perimeter im Überblick

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



Erkennungen

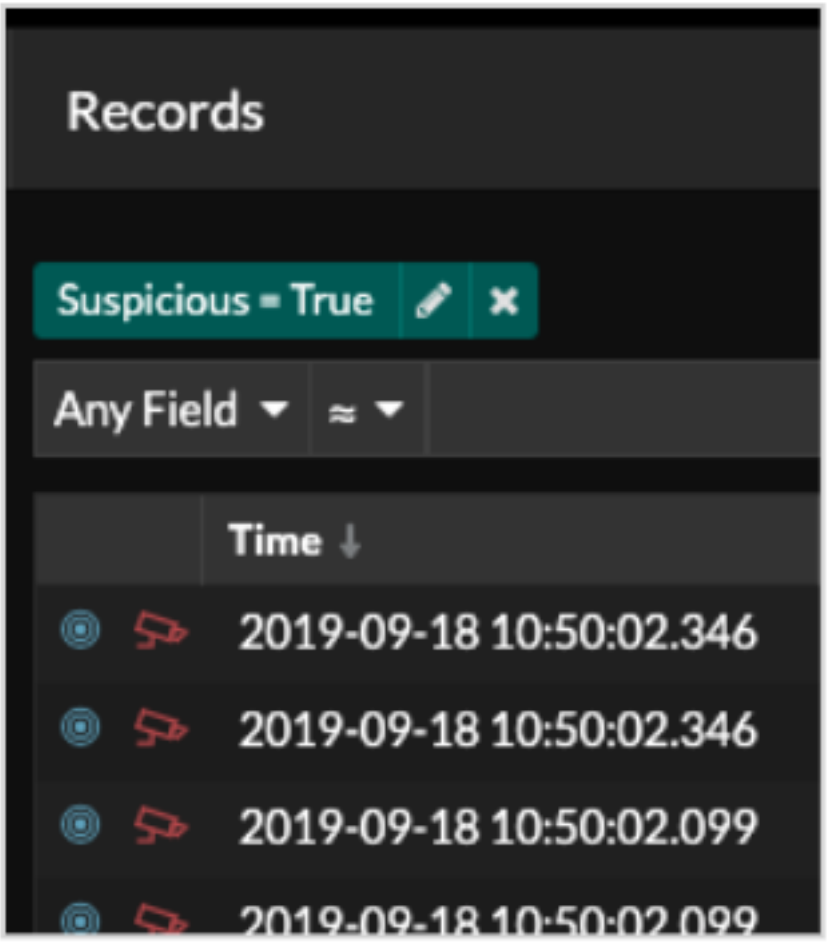
Eine Erkennung erfolgt, wenn im Netzwerkverkehr ein Hinweis auf eine Gefährdung durch eine Bedrohungssammlung erkannt wird.



Rekorde

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

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



Retrospektive Erkennungen

(Nur Reveal (x) 360) Wenn eine von ExtraHop kuratierte Bedrohungssammlung aktualisiert wird, führt das ExtraHop-System Automated Retrospective Detection (ARD) durch. Dabei wird nach neuen Domains gesucht, die Anzeichen für eine Gefährdung in den Datensätzen der letzten 7 Tage sind. Wenn eine frühere Verbindung zu einer verdächtigen Domain identifiziert wird, generiert das System eine rückwirkende Erkennung .

Der Zeitstempel einer retrospektiven Erkennung gibt den Zeitpunkt an, zu dem die Aktivität ursprünglich stattgefunden hat, und erscheint möglicherweise nicht in der aktuellen Erkennungsliste. Sie finden retrospektive Erkennungen, indem Sie auf Retrospective Threat Intelligence klicken. Bedrohungsübersicht. Du kannst auch eine Regel für Erkennungsbenachrichtigungen erstellen um Sie per E-Mail zu benachrichtigen, wenn solche Erkennungen auftreten.