ExtraHop 9.9
ExtraHop System-Benutzerhandbuch

Weitere Informationen finden Sie unter https://docs.extrahop.com.

Veröffentlicht: 2025-01-04

ExtraHop Networks
Seattle, WA 98101
877-333-9872 (US)
+44 (0)203 7016850 (EMEA)
+65-31585513 (APAC)
www.extrahop.com

Inhaltsübersicht

Über diesen Leitfaden

Dieses Handbuch enthält Informationen über das ExtraHop-System für die ExtraHop Discover- und Command-Appliances.

Dieses Handbuch soll Benutzern helfen, die Architektur und Funktionalität des ExtraHop-Systems zu verstehen und zu lernen, wie die im gesamten System verfügbaren Steuerelemente, Felder und Optionen bedient werden.

Zusätzliche Ressourcen sind über die folgenden Links verfügbar:

- Informationen zu den Administratormerkmalen und -funktionen der ExtraHop Discover- und Command-Appliances finden Sie in der ExtraHop Admin-UI-Leitfaden
- Sehen Sie sich die vollständige ExtraHop-Dokumentation an: https://docs.extrahop.com.
- Sehen Sie sich die Online-Schulungsmodule auf der ExtraHop-Website an: https://www.extrahop.com/go/training/.

Kontaktiere uns

Wir freuen uns über Ihr Feedback.

Bitte teilen Sie uns mit, wie wir dieses Dokument verbessern können. Senden Sie Ihre Kommentare oder Vorschläge an documentation@extrahop.com.

- **Website des Support-Portals:** https://customer.extrahop.com/s/
- **Telefon:**
  - 877-333-9872 (UNS)
  - +44 (0) 203 7016850 (EMEA)
  - +65-31585513 (APAC)

Einführung in das ExtraHop-System

In diesem Handbuch wird erklärt, wie das ExtraHop-System Ihre Daten sammelt und analysiert und wie die Kernsystemkomponenten und -funktionen Ihnen helfen, auf Erkennungen, Metriken, Transaktionen und Pakete über den Verkehr in Ihrem Netzwerk zuzugreifen.

Mithilfe von Workflows zur Überwachung der Netzwerkleistung können Sie überwachen, wie Dienste und Geräte miteinander interagieren und wie Transaktionen in Ihrem Netzwerk über die Datenverbindungsschicht (L2) zur Anwendungsebene (L7) Fluss. Mithilfe von Workflows zur Netzwerkerkennung und Reaktion können Sie Daten untersuchen, die aufgrund von Leistungseinbußen bis hin zu verdächtigen Verhaltensweisen erkannt wurden. Außerdem erhalten Sie einen Überblick darüber, welche Geräte an den MITRE ATT&CK-Taktiken, -Techniken und -Verfahren (TTPs) beteiligt waren, die mit fortgeschrittenen, mehrstufigen Angriffskampagnen in Verbindung stehen.

Video: Sehen Sie sich die entsprechende Schulung an: ExtraHop Systemübersicht

Plattform-Architektur

Das ExtraHop-System ist mit modularen Komponenten maßgeschneidert, die in Kombination Ihren individuellen Umweltanforderungen gerecht werden.

Module

ExtraHop-Module bieten eine Kombination aus Lösungen, Komponenten und Cloud-basierten Diensten, die für mehrere Anwendungsfälle einen Mehrwert bieten.

Module sind für Network Detection and Response (NDR) und Network Performance Monitoring (NPM) erhältlich, mit zusätzlichen Modulen für Intrusion Detection Systems (Intrusion Detection System) und Packet Forensics.

Administratoren können die rollenbasierte Zugriffskontrolle (RBAC) aktivieren, indem sie Benutzern Zugriff auf das NDR-Modul, das NPM-Modul oder beides gewähren.

Überwachung der Netzwerkleistung

Mit dem NPM-Modul können privilegierte Benutzer die folgenden Arten von Systemaufgaben ausführen.

- Benutzerdefinierte Dashboards anzeigen, erstellen und ändern. Benutzer können auch ein Dashboard für ihre Standard-Landingpage auswählen.
- Konfigurieren Sie Benachrichtigungen und Benachrichtigungen per E-Mail für diese Warnungen.
- Leistungserkennungen anzeigen.

Netzwerkerkennung und Reaktion

Mit dem NDR-Modul können privilegierte Benutzer die folgenden Arten von Systemaufgaben ausführen.

- Sehen Sie sich die Seite mit der Sicherheitsübersicht an.
- Sehen Sie sich Sicherheitserkennungen an.
- Untersuchungen anzeigen, erstellen und ändern.
- Sehen Sie sich die Bedrohungsinformationen an.

Benutzer, denen Zugriff auf beide Module gewährt wurde, dürfen alle diese Aufgaben ausführen. Sehen Sie die Leitfaden zur Migration um mehr über die Migration von Benutzern zum rollenbasierten Zugriff mit diesen Modulen zu erfahren.

Diese zusätzlichen Module sind auch für bestimmte Anwendungsfälle verfügbar:

Paket-Forensik

Das Packet Forensics Modul kann entweder mit dem NDR- oder NPM-Modul kombiniert werden, um eine vollständige PCAP, Speicherung und Abruf zu ermöglichen.

Systeme zur Erkennung von Eindringlingen

Das IDS-Modul muss mit dem NDR-Modul kombiniert werden und bietet Erkennungen auf der Grundlage von IDS-Signaturen nach Industriestandard. Die meisten ExtraHop-Paketsensoren sind für das IDS-Modul geeignet, sofern der Sensor für das NDR-Modul lizenziert ist.

Hinweis: Durchsatz kann beeinträchtigt werden, wenn mehr als ein Modul auf dem Sensor aktiviert ist.

Funktionen

Das ExtraHop-System bietet einen umfangreichen Funktionsumfang, mit dem Sie Erkennungen, Metriken, Aufzeichnungen und Pakete organisieren und analysieren können, die mit dem Verkehr in Ihrem Netzwerk verbunden sind.

Modul- und Systemzugriff werden bestimmt durch Benutzerrechte die von Ihrem ExtraHop-Administrator verwaltet werden.

Globale Funktionen

Die folgenden Funktionen sind in allen ExtraHop-Systemen verfügbar und erfordern keine speziellen Module.

- Überblick über das Netzwerk
- Perimeter im Überblick
- Karten der Aktivitäten
- Active Directory Directory-Dashboard
- Generatives KI-Dashboard
- Geplante Dashboard-Berichte
- Erkennungsverfolgung
- Vermögenswerte
- Rekorde
- Pakete
- Integrationen (nur RevealX 360)
- API-Zugriff
- Prioritäten der Analyse
- Metrischer Katalog
- Bündel
- Trigger
- KI-Suchassistent (Vermögenswerte und Aufzeichnungen)

Funktionen des NDR-Moduls

Die folgenden Funktionen sind in ExtraHop-Systemen mit dem Network Detection and Response (NDR) - Modul verfügbar.

- Überblick über die Sicherheit
- KI-Suchassistent
- Berichte über Sicherheitsoperationen
- Integrierte Sicherheits-Dashboards
- Sicherheitserkennungen
- MITRE karte
- Ermittlungen

- Optimierungsregeln für Sicherheitserkennungen
- Benachrichtigungsregeln für Sicherheitserkennungen und Bedrohungsinformationen
- Bedrohungsinformationen
- Bedrohungsinformationen
- Datei-Analyse
- Dateiextraktion (Paketforensik erforderlich)

Funktionen des NPM-Moduls

Die folgenden Funktionen sind in ExtraHop-Systemen mit dem Network Performance Management (NPM) -Modul verfügbar.

- Benutzerdefinierte Dashboards
- Integrierte Leistungs-Dashboards
- Leistungserkennungen
- Optimierungsregeln für Leistungserkennungen
- Benachrichtigungsregeln für Leistungserkennungen
- Warnmeldungen

Funktionen von Packet Forensics

Die folgenden Funktionen sind in ExtraHop-Systemen mit dem Modul Packet Forensics verfügbar.

- Paketerfassung
- Packetstore-Unterstützung
- Dateiextraktion (NDR erforderlich)

IDS-Funktionen

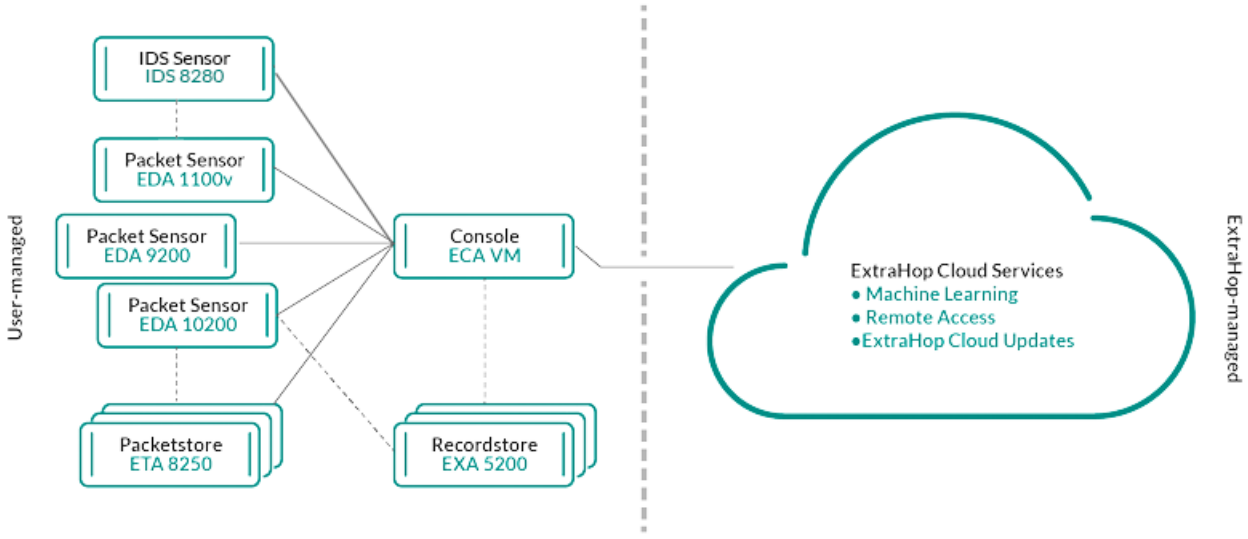
Die folgenden Funktionen sind in ExtraHop-Systemen mit dem Modul Intrusion Detection System (IDS) verfügbar.

- IDS-Erkennungen

Lösungen

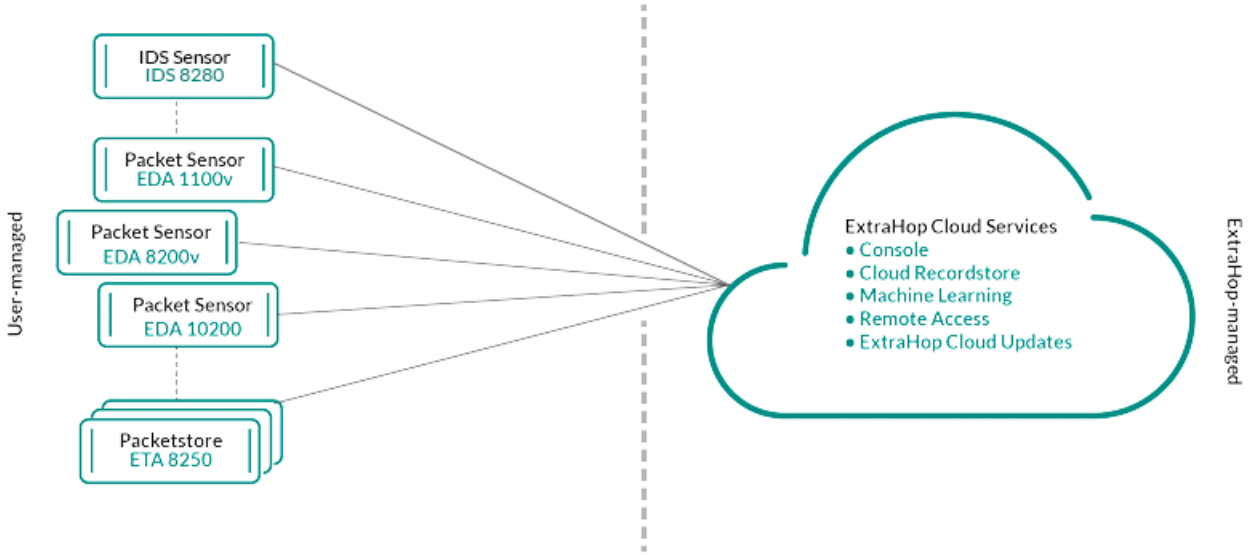
RevealX Enterprise

RevealX Enterprise ist eine selbstverwaltete Lösung, die Folgendes umfasst Sensoren, Konsolen, Paketspeicher, Plattenspeicher und Zugriff auf ExtraHop Cloud Services.



RevealX 360

RevealX 360 ist eine Software-as-a-Service (SaaS) -Lösung, die umfasst Sensoren und Paketspeicher und beinhaltet einen Cloud-basierten Recordstore mit Standard Investigation, einem Konsoleund Zugriff auf ExtraHop Cloud Services.



Komponenten

Jede Lösung bietet eine Reihe von Komponenten, die auf Ihre Umgebungsanforderungen zugeschnitten sind: Sensoren, Paketspeicher, Plattenspeicher und ein Konsole für zentralisiertes Management und einheitliche Datenansichten.

Paket-Sensoren

Paketsensoren erfassen, speichern und analysieren Metrik Daten über Ihr Netzwerk. Je nach Sensorgröße sind mehrere Ebenen der Datenanalyse, -erfassung und -speicherung verfügbar. Diese Sensoren sind sowohl in NPM- als auch in NDR-Modulen als physische, virtuelle und cloudbasierte Optionen in Größen erhältlich, die auf Ihre Analyseanforderungen zugeschnitten sind.

IDS-Sensoren

Die Sensoren des Intrusion Detection Systems (Intrusion Detection System) sind in Paketsensoren integriert, um Erkennungen auf der Grundlage der branchenüblichen IDS-Signatur zu generieren.

IDS-Sensoren werden als Zusatzmodul zum NDR-Modul eingesetzt. IDS-Sensoren sind eine physische Appliance mit einem zugehörigen Paketsensor und sind für RevealX 360- oder RevealX Enterprise-Umgebungen verfügbar.

Durchflusssensoren

Flusssensoren sind nur für RevealX 360 verfügbar und erfassen ausschließlich VPC-Flow-Logs, sodass Sie den von AWS-SaaS-Diensten verwalteten Datenverkehr sehen können.

Plattenläden

Recordstores lassen sich in Sensoren integrieren und Konsolen zu Transaktions- und Flow-Aufzeichnungen speichern das kann im gesamten ExtraHop-System abgefragt werden. Recordstores können als eigenständige physische oder virtuelle Optionen bereitgestellt und als Drittanbieter-Verbindungen zu Splunk oder BiqQuery von RevealX Enterprise unterstützt werden. RevealX 360 mit Standard Investigation bietet einen vollständig gehosteten, cloudbasierten Recordstore. Recordstores sind in Paketen mit NPM- und NDR-Modulen erhältlich.

Paketshops

Packetstores integrieren sich in Sensoren und Konsolen zur Verfügung stellen kontinuierliche PCAP und ausreichend Speicherplatz für eingehendere Untersuchungen und forensische Anforderungen. Packetstores können als eigenständige physische oder virtuelle Optionen bereitgestellt werden und sind als Zusatzmodul für Paketforensik sowohl für NPM- als auch für NDR-Module verfügbar.

Konsolen

Konsolen bieten eine browserbasierte Oberfläche, die eine Kommandozentrale für alle verbundenen Komponenten bietet. Konsolen können als eigenständige virtuelle oder cloudbasierte Optionen für RevealX Enterprise bereitgestellt werden und sind in RevealX 360 enthalten.

Die folgende Tabelle bietet einen Überblick über die für jede Lösung verfügbaren Optionen.

	RevealX Enterprise		**RevealX 360**	
	Körperlich	Virtuell/Cloud	Körperlich	Virtuell/Cloud
Paketsensor				
	SEIT 1200	EDA 1100 V AWS	SEIT 1200	EDA 1100 V AWS
	SEIT 6200	EDA 1100v Azurblau	SEIT 6200	EDA 1100v Azurblau
	AB 820	EDA 1100 V GCP	AB 820	EDA 1100 V GCP
	SEIT 8320	EDA 6320v GCP	SEIT 8320	EDA 6320v GCP
	SEIT 9200	EDA 8370v GCP	SEIT 9200	EDA 8370v GCP
	SEIT 9300	EDA 1100 V Linux KVM	SEIT 9300	EDA 1100 V Linux KVM
	VON 10200	EDA 1100 v VMware	VON 10200	EDA 1100 v VMware
	VON 10300	EDA 6100 v VMware	VON 10300	EDA 610 V AWS

	RevealX Enterprise		RevealX 360	
		EDA 610 V AWS		EDA 6100v Azurblau
		EDA 6100v Azurblau		EDA 6100 v VMware
		EDA 820 V AWS		EDA 820 V AWS
		RevealX Ultra AWS mit 1 Gbit/s und 10 Gbit/s		RevealX Ultra AWS mit 1 Gbit/s und 10 Gbit/s
		RevealX Ultra 1 Gbit/s und 10 Gbit/s GCP		RevealX Ultra 1 Gbit/s und 10 Gbit/s GCP
IDS-Sensor				
	Intrusion Detection System 8280 Intrusion Detection System 980	Intrusion Detection System 1280 v VMware Intrusion Detection System 6280v VMWare	Intrusion Detection System 8280 Intrusion Detection System 980	Intrusion Detection System 1280 v VMware Intrusion Detection System 6280v VMWare
Durchflusssensor	N/A	N/A	N/A	
				EFC 1291v AWS (PVC)
				EFC 1292v (NetFlow)
Paketspeicher				
	BETA 6150	ETA 1150v AWS	BETA 6150	ETA 1150v AWS
	BETA 8250	ETA 1150v Azurblau	BETA 8250	ETA 1150v Azurblau
		ETA 1150 V GCP		ETA 1150 V GCP
		ETA 1150v VMware		ETA 1150v VMware
		ETA 6150v VMware		ETA 6150v VMware

	RevealX Enterprise		RevealX 360	
				In Ultra-Abonnements enthalten
Plattenladen	EXA 5200	EXA 5100 v AWS EXA 5100v Azurblau EXA 5100v Hyper-V EXA 5100v Linux KVM EXA 5100 v VMware	N/A	In Premium- und Ultra-Abonnements enthalten
Konsole	N/A	ECA-GESETZE ECA Azure ECA GCP ECA Hyper-V ECA Linux KVM ECA VMWare	N/A	In allen Abos enthalten

ExtraHop Cloud-Dienste

ExtraHop Cloud-Dienste aktualisiert die Sensoren automatisch mit neuen Erkennungen und kritischen Bedrohungsinformationen sowie mit Funktionserweiterungen und ermöglicht Ihren Account-Teams den Zugriff auf Fernsupport und professionelle Services.

Intelligente Sensoranalytik

Das ExtraHop-System bietet eine browserbasierte Oberfläche mit Tools, mit denen Sie Daten untersuchen und visualisieren, Ergebnisse sowohl in Top-down- als auch Bottom-up-Workflows untersuchen und anpassen können, wie Sie Ihre Netzwerkdaten sammeln, anzeigen und teilen. Fortgeschrittene Benutzer können sowohl administrative als auch Benutzeraufgaben über das automatisieren und skripten ExtraHop REST-API und passen Sie die Datenerfassung an über ExtraHop-Trigger-API, bei dem es sich um ein JavaScript-IDE-Tool handelt.

Das Herzstück des ExtraHop-Systems ist ein intelligentes Sensor das Metrikdaten über Ihr Netzwerk erfasst, speichert und analysiert — und je nach Bedarf verschiedene Ebenen der Datenanalyse, -erfassung und -speicherung bietet. Fühler sind mit Speicher ausgestattet, der ein Metrik-Lookback von 30 Tagen unterstützt. Beachten Sie, dass der tatsächliche Lookback je nach Verkehrsmustern, Transaktionsraten, der Anzahl der Endpunkte und der Anzahl der aktiven Protokolle variiert.

Konsolen dienen als Kommandozentrale mit Verbindungen zu mehreren Sensoren, Recordstores und Packetstores, die über Rechenzentren und Zweigstellen verteilt sind. Alle RevealX 360-Bereitstellungen enthalten eine Konsole; RevealX Enterprise kann virtuelle oder Cloud-Varianten bereitstellen.

Konsolen bieten einheitliche Datenansichten für alle Ihre Standorte und ermöglichen es Ihnen, bestimmte erweiterte Konfigurationen zu synchronisieren (z. B. löst aus und Warnungen) und Einstellungen (Tuning-Parameter, Analyse-Prioritäten, und Plattenläden).

In den folgenden Abschnitten werden die wichtigsten Funktionskomponenten des ExtraHop-Systems und deren Zusammenspiel beschrieben.

Sensortypen

Die Art von Sensor Die Art der Daten, die Sie bereitstellen, bestimmt die Art der Daten, die gesammelt, gespeichert und analysiert werden.

Daten verdrahten
Paketsensoren und Intrusion Detection System (IDS) -Sensoren beobachten unstrukturierte Pakete passiv über einen Port-Mirror oder greifen auf die Daten zu und speichern sie im lokalen Datenspeicher. Die Paketdaten werden einer Stream-Verarbeitung in Echtzeit unterzogen, bei der die Pakete in die folgenden Phasen in strukturierte wire data umgewandelt werden:

1. TCP-Zustandsmaschinen werden neu erstellt, um eine vollständige Reassemblierung durchzuführen.
2. Pakete werden gesammelt und in Flows gruppiert.
3. Die strukturierten Daten werden auf folgende Weise analysiert und verarbeitet:
    - Transaktionen werden identifiziert.
    - Geräte werden automatisch erkannt und anhand ihrer Aktivität klassifiziert.
    - Metriken werden generiert und mit Protokollen und Quellen verknüpft, und die Metrikdaten werden dann in Metrikzyklen aggregiert.
4. Wenn neue Metriken generiert und gespeichert werden und der Datenspeicher voll wird, werden die ältesten vorhandenen Metriken gemäß dem First-in-First-Out-Prinzip (FIFO) überschrieben.

Flow-Daten
Ein Fluss ist eine Reihe von Paketen, die Teil einer einzelnen Verbindung zwischen zwei Endpunkten sind. Fluss Sensoren sind für RevealX 360 verfügbar und bieten eine kontinuierliche Netzwerktransparenz auf der Grundlage von VPC-Flow-Protokollen, um AWS-Umgebungen abzusichern. VPC-Flow-Logs ermöglichen es Ihnen , Informationen über den IP-Verkehr zu und von Netzwerkschnittstellen in Ihrer VPC zu erfassen. Sie werden als Flow-Log-Datensätze aufgezeichnet, bei denen es sich um Protokollereignisse handelt, die aus Feldern bestehen, die den Datenverkehrsfluss beschreiben. Diese Protokolldaten ermöglichen es Ihnen, mithilfe fortschrittlicher maschineller Learning-Erkennungen nach Bedrohungen zu suchen.

Flow-Logs werden aufgenommen, dedupliziert und dann in Flows gruppiert. Die Flows werden dann mit Daten (wie MAC-Adressen) angereichert, die von AWS EC2-APIs abgefragt werden.

Die Flüsse werden dann auf folgende Weise analysiert und verarbeitet:

- Geräte werden automatisch anhand ihrer an bestimmten Ports beobachteten Aktivität erkannt und klassifiziert.
- Grundlegende L2-L4-Metriken werden generiert und in Metrikzyklen aggregiert.
- ExFlow-Datensatztypen werden generiert und veröffentlicht.

Metriken, Datensätze und Pakete

ExtraHop-Sensoren erfassen und speichern mehrere Tiefen der Netzwerkinteraktion als Metriken. Metriken sind aggregierte Beobachtungen über Endpunktinteraktionen im Laufe der Zeit. Packetstores sammeln und speichern die zwischen zwei Endpunkten übertragenen Rohdaten als Pakete. Plattenläden Sammeln und Speichern von Datensätzen, bei denen es sich um strukturierte Informationen über Transaktions-, Nachrichten- und Netzwerkflüsse handelt.

Sie können all diese Interaktionen von einzelnen Sensoren aus anzeigen und abfragen oder von einem Konsole das ist mit einem komplexen Einsatz von Sensoren, Paketspeichern und Plattenläden verbunden.

Wenn ein Client beispielsweise eine HTTP-Anfrage an einen Server sendet, enthält jeder Datentyp Folgendes:

- Das Paket enthält die Rohdaten, die bei der Interaktion gesendet und empfangen wurden.
- Der zugehörige Datensatz enthält die mit einem Zeitstempel versehenen Metadaten über die Interaktion: den Zeitpunkt der Anfrage, die IP-Adresse des Client und Server, die angeforderte URI, etwaige Fehlermeldungen.
- Die zugehörige Metrik (HTTP-Anfragen) enthält eine Zusammenfassung dieser Interaktion mit anderen beobachteten Interaktionen während des angegebenen Zeitraums, z. B. wie viele Anfragen aufgetreten sind, wie viele dieser Anfragen erfolgreich waren, wie viele Clients Anfragen gesendet haben und wie viele Server die Anfragen erhalten haben.

Sowohl Metriken als auch Datensätze können angepasst werden, um spezifische Metadaten auf JavaScript-Basis zu extrahieren und zu speichern löst aus. Während das ExtraHop-System über 4.600 integrierte Metriken, vielleicht möchten Sie eine erstellen benutzerdefinierte Metrik, die 404-Fehler sammelt und aggregiert nur von kritischen Webservern. Und vielleicht möchten Sie Ihren Plattenspeicher nur maximieren, indem Sie Erfassung von Transaktionen, die über einen verdächtigen Port stattgefunden haben.

Erkennung von Geräten

Nachdem ein Gerät erkannt wurde, beginnt das ExtraHop-System mit der Erfassung von Metriken, die auf der für dieses Gerät konfigurierten Analyseebene basieren. Du kannst Finde ein Gerät nach ihrer MAC-Adresse, IP-Adresse oder ihrem Namen (z. B. ein aus dem DNS-Verkehr beobachteter Hostname, NetBIOS-Name, Cisco Discovery Protocol (CDP) -Name, DHCP-Name oder ein benutzerdefinierter Name, den Sie dem Gerät zugewiesen haben).

Das ExtraHop-System kann Geräte anhand ihrer MAC-Adresse (L2 Discovery) oder anhand ihrer IP-Adressen (L3 Discovery) erkennen und verfolgen. L2 Discovery bietet den Vorteil, dass Messwerte für ein Gerät auch dann verfolgt werden können, wenn die IP-Adresse durch eine DHCP-Anfrage geändert oder neu zugewiesen wird. Standardmäßig ist das ExtraHop-System für L2 Discovery konfiguriert.

IPv4- und IPv6-Adressen von Geräten werden anhand von ARP-Nachrichten (Address Resolution Protocol), NDP-Antworten (Neighbor Discovery Protocol), lokalen Broadcasts oder lokalem Subnetz-Multicast-Verkehr ermittelt. Die MAC-Adresse und die IP-Adresse für Geräte werden in den Suchergebnissen im gesamten System zusammen mit den Geräteinformationen angezeigt.

L2-Entdeckung

In L2 Discovery erstellt das ExtraHop-System einen Geräteeintrag für jede lokale MAC-Adresse, die über das Kabel erkannt wurde. IP-Adressen werden der MAC-Adresse zugeordnet, aber Metriken werden zusammen mit der MAC-Adresse des Gerät gespeichert, auch wenn sich die IP-Adresse ändert.

IP-Adressen, die außerhalb von lokal überwachten Broadcast-Domänen beobachtet werden, werden auf einem der eingehenden Router in Ihrem Netzwerk aggregiert. Wenn ein Gerät eine DHCP-Anfrage über einen Router sendet, der als DHCP-Relay-Agent fungiert, erkennt das ExtraHop-System die IP-Adresse und ordnet sie der MAC-Adresse des Gerät zu. Wenn sich die IP-Adresse für das Gerät mit einer nachfolgenden Anfrage über den DHCP-Relay-Agenten ändert, aktualisiert das ExtraHop-System seine Zuordnung und verfolgt die Gerätemetriken weiterhin anhand der MAC-Adresse.

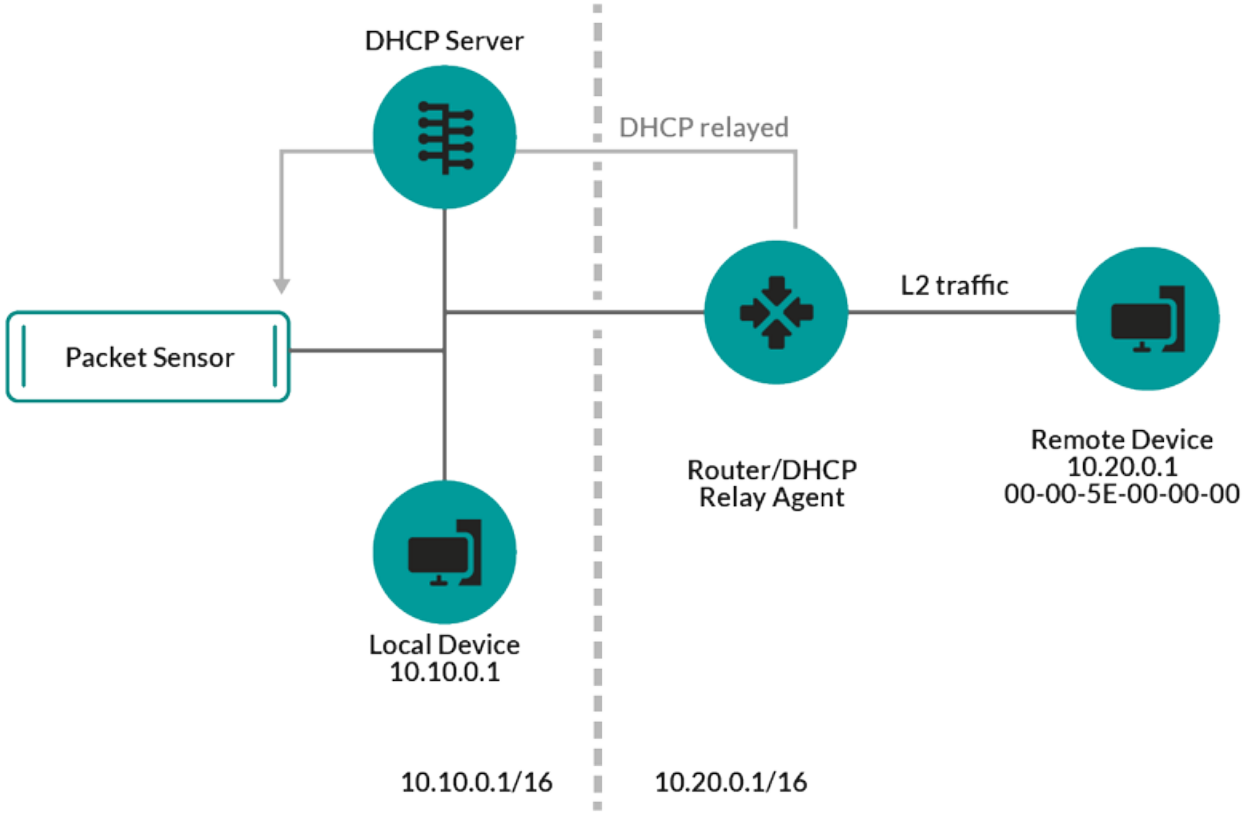


Abbildung 1: Sowohl die MAC-Adresse als auch die IP-Adresse werden für das entferntes Gerät erkannt.

Wenn kein DHCP-Relay-Agent konfiguriert ist, können Remote-Geräte anhand ihrer IP-Adressen erkannt werden über L3-Erkennung per Fernzugriff.

L3-Entdeckung

In L3 Discovery erstellt und verknüpft das ExtraHop-System zwei Einträge für jedes lokal erkannte Gerät: einen übergeordneten L2-Eintrag mit einer MAC-Adresse und einen untergeordneten L3-Eintrag mit IP-Adressen und der MAC-Adresse.

Hier sind einige wichtige Überlegungen zur L3-Entdeckung:

- Wenn auf einem Router Proxy-ARP aktiviert ist, erstellt das ExtraHop-System für jede IP-Adresse, für die der Router ARP-Anfragen beantwortet, ein L3-Gerät.
- Wenn Sie in Ihrem Netzwerk ein Proxy-ARP konfiguriert haben, erkennt das ExtraHop-System möglicherweise automatisch Remote-Geräte.
- L2-Metriken, die keinem bestimmten untergeordneten L3-Gerät zugeordnet werden können (z. B. L2-Broadcast-Verkehr), werden dem L2-Elterngerät zugeordnet.

L3-Erkennung per Fernzugriff

Wenn das ExtraHop-System eine IP-Adresse erkennt, der kein ARP- oder NDP-Verkehr zugeordnet ist, wird dieses Gerät als entferntes Gerät betrachtet. Remote-Geräte werden nicht automatisch erkannt, aber Sie können einen Remote-IP-Adressbereich hinzufügen und Geräte erkennen, die sich außerhalb des lokalen Netzwerk befinden. Für jede IP-Adresse, die innerhalb des Remote-IP-Adressbereichs beobachtet wird, wird ein Geräteeintrag erstellt. (Remote-Geräte haben keine übergeordneten L2-Einträge.)

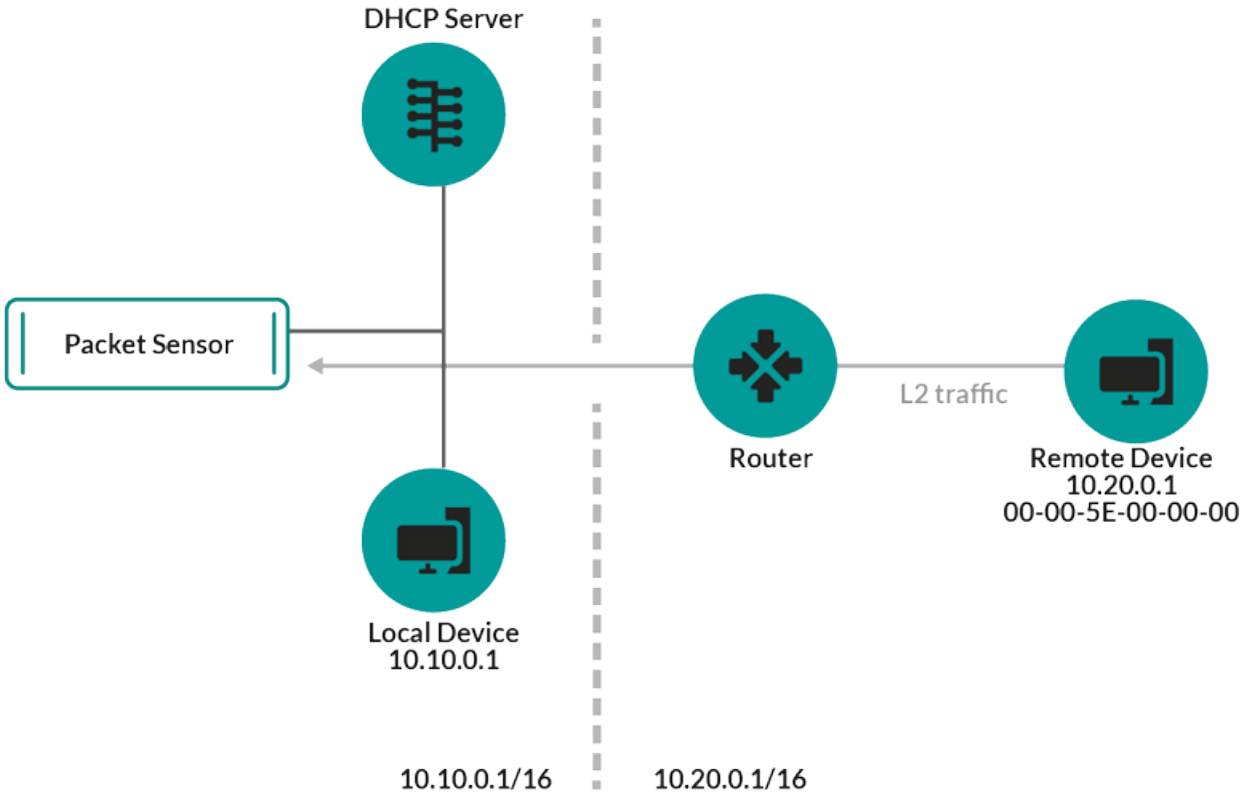


Abbildung 2: Für das entferntes Gerät wird nur die IP-Adresse erkannt.

Im Folgenden finden Sie einige Empfehlungen zur Konfiguration von Remote L3 Discovery:

- Ihre Client-Geräte befinden sich in einem Netzwerksegment, das nicht direkt angezapft wird.
- Ihr Unternehmen verfügt über eine Außenstelle ohne ein ExtraHop-System vor Ort, aber die Benutzer an diesem Standort greifen auf zentrale Rechenzentrumsressourcen zu, die direkt von einem ExtraHop-System überwacht werden. Die IP-Adressen am Remote-Standort können als Geräte erkannt werden.
- Ein Cloud-Dienst oder ein anderer externer Dienst hostet Ihre Remote-Anwendungen und hat einen bekannten IP-Adressbereich. Die Remote-Server innerhalb dieses IP-Adressbereichs können individuell verfolgt werden.

VPN-Entdeckung
VPN-Entdeckung ermöglicht es dem ExtraHop-System, die privaten RFC-1918-IP-Adressen, die VPN-Clients zugewiesen wurden, mit ihren öffentlichen, externen IP-Adressen zu korrelieren. Dieser erweiterte Einblick in den Nord-Süd-Verkehr reduziert Hindernisse bei der Untersuchung von Sicherheitsvorfällen und Leistungsproblemen , an denen externe VPN-Clients beteiligt sind. (Für diese Funktion ist ein VPN-Gateway erforderlich, das vom Benutzer manuell zugewiesen wird.)

Software-Frame-Deduplizierung

Das ExtraHop-System entfernt standardmäßig doppelte L2- und L3-Frames und -Pakete, wenn Metriken aus Ihrer Netzwerkaktivität erfasst und aggregiert werden.

Das Systemzustand Die Seite enthält Diagramme, in denen doppelte L2- und L3-Pakete angezeigt werden, die vom ExtraHop-System entfernt wurden. Die Deduplizierung funktioniert standardmäßig über 10-Gbit/s-Ports.

L2-Deduplizierung

Bei der L2-Deduplizierung werden identische Ethernet-Frames entfernt, bei denen Ethernet-Header und Payload übereinstimmen müssen. Das ExtraHop-System sucht nach Duplikaten und entfernt global nur das unmittelbar vorhergehende Paket, wenn das Duplikat innerhalb von 1 Millisekunde nach dem Originalpaket eintrifft. Eine L2-Duplizierung liegt normalerweise nur vor, wenn genau dasselbe Paket im Datenfeed zu sehen ist, was in der Regel auf ein Problem mit der Portspiegelung zurückzuführen ist.

L3-Deduplizierung

Die L3-Deduplizierung entfernt TCP- oder UDP-Pakete mit identischen IP-Adress-ID-Feldern im gleichen Fluss, wobei nur das IP-Paket übereinstimmen muss. Der Inhalt aller Header, die dem überprüften IP-Header vorausgehen, kann unterschiedlich sein. Die L3-Deduplizierung wird derzeit nur für IPv4 unterstützt, nicht für IPv6. Das ExtraHop-System sucht nach Duplikaten und entfernt nur das unmittelbar vorhergehende Paket im Fluss, wenn das Duplikat innerhalb von 1 Millisekunde nach dem ursprünglichen Paket ankommt und wenn das Paket in dieselbe Richtung reist. Damit ein Paket dedupliziert werden kann, dürfen zwischen den beiden doppelten Paketen keine anderen Pakete empfangen werden. Darüber hinaus müssen Pakete dieselbe Länge und dasselbe IP-Adress-ID-Feld haben, und TCP-Pakete müssen auch dieselbe TCP-Prüfsumme haben.

Standardmäßig sind Datenflüsse über VLANs aktiviert, und da die L3-Deduplizierung pro Datenfluss erfolgt, entfernt die L3-Deduplizierung dasselbe Paket, das verschiedene VLANs durchläuft. Die L3-Deduplizierung ist oft das Ergebnis der Spiegelung desselben Datenverkehrs über mehrere Schnittstellen desselben Routers, und dieser Verkehr kann als irrelevante TCP-Neuübertragungen im ExtraHop-System auftauchen.

Erkennung von Bedrohungen

Das ExtraHop-System bietet sowohl maschinelles Lernen als auch regelbasiertes Erkennungen die aktive oder potenzielle Bedrohungen, Netzwerkschwächen, die anfällig für Exploits sind, und suboptimale Konfigurationen, die die Netzwerkleistung beeinträchtigen können, identifizieren.

Zusätzlich Diagramme, Visualisierungen, und Karten zur Geräteaktivität ermöglichen Sie die proaktive Bedrohungssuche.

Optimierung der Erkennung

Reduzieren Sie Geräusche und lassen Sie nur kritische Erkennungen erkennen indem Sie Details über Ihr Netzwerk hinzufügen, anhand derer bekannte Parameter wie vertrauenswürdige Domänen und Schwachstellenscanner identifiziert werden können.

Darüber hinaus können Sie Optimierungsregeln erstellen, die bestimmte Erkennungen oder Teilnehmer verbergen und unerwünschte Geräusche weiter reduzieren.

Netzwerk-Lokalität

Standardmäßig wird jedes Gerät mit einer RFC1918-IP-Adresse (in einem 10/8-, 172.16/12- oder 192.168/16 CIDR-Block enthalten) auf dem System als internes Gerät klassifiziert.

Da einige Netzwerkumgebungen jedoch IP-Adressen enthalten, die nicht RFC1918 entsprechen, als Teil ihres internen Netzwerk, können Sie die interne oder externe Klassifizierung für IP-Adressen ändern von der Seite Network Locations.

Bedrohungsinformationen

Das ExtraHop-System umfasst kuratierte Bedrohungsinformationen Feeds von ExtraHop und Crowdstrike Falcon, die über die Cloud aktualisiert werden, sobald neue Bedrohungen entdeckt werden. Du kannst auch Bedrohungssammlungen hinzufügen von einem Drittanbieter.

Bedrohungsinformationen

Bedrohungsinformationen stellen Informationen über unmittelbare Bedrohungen bereit , die auf Netzwerke abzielen. Aktuelle Erkennungen, gezielte Datensatz- und Paketabfragen sowie betroffene Geräte werden

als Ausgangspunkt für Ihre Untersuchung angezeigt. Der Zugriff erfolgt über Überblick über die Sicherheit Seite.

Integrationen
RevealX 360 bietet mehrere Drittanbieter-Integrationen, die das Erkennung- und Reaktionsmanagement verbessern und einen besseren Überblick über den Netzwerkverkehr bieten können.

Kortex XSOAR

Exportieren Sie ExtraHop-Erkennungen, führen Sie Antwort-Playbooks aus und fragen Sie Gerätedetails in Cortex XSOAR ab.

Crowdstrike

Sehen Sie sich Details zu CrowdStrike-Geräten an und fügen Sie diese Geräte aus dem ExtraHop-System hinzu.

Microsoft 365

Importieren Sie Microsoft 365-Erkennungen und -Ereignisse, überwachen Sie Microsoft 365-Metriken in integrierten Dashboards und lassen Sie sich Details zu Risikoereignissen in Datensätzen anzeigen.

Microsoft-Protokollentschlüsselung

Entschlüsseln Sie den Datenverkehr über Microsoft-Protokolle wie LDAP, RPC, SMB und WSMan, um die Erkennung von Sicherheitsangriffen in Ihrer Microsoft Windows-Umgebung zu verbessern.

Q-Radar

Exportieren und betrachten Sie ExtraHop-Erkennungen in Ihrem QRadar SIEM.

Splunk SIEM für Unternehmenssicherheit

Exportieren und zeigen Sie ExtraHop-Erkennungen in Ihrem Splunk SIEM an.

Splunk SOAR

Exportieren und zeigen Sie ExtraHop-Erkennungen, -Metriken und -Pakete in Ihrer Splunk SOAR-Lösung an.

Navigieren im ExtraHop-System

Das ExtraHop-System bietet Zugriff auf Netzwerkaktivitätsdaten und Erkennungsdetails über eine dynamische und hochgradig anpassbare Benutzeroberfläche.

Dieses Handbuch bietet einen Überblick über die globale Navigation und die Steuerelemente, Felder und Optionen, die im gesamten System verfügbar sind. siehe Einführung in das ExtraHop-System um zu erfahren, wie das ExtraHop-System Ihre Daten sammelt und analysiert.

Video: Sehen Sie sich die entsprechende Schulung an: Vollständiger Lernpfad zu den UI-Grundlagen

Unterstützte Browser

Die folgenden Browser sind mit allen ExtraHop-Systemen kompatibel. Wenden Sie die von Ihrem Browser bereitgestellten Barrierefreiheits- und Kompatibilitätsfunktionen an, um über technische Hilfsmittel auf Inhalte zuzugreifen.

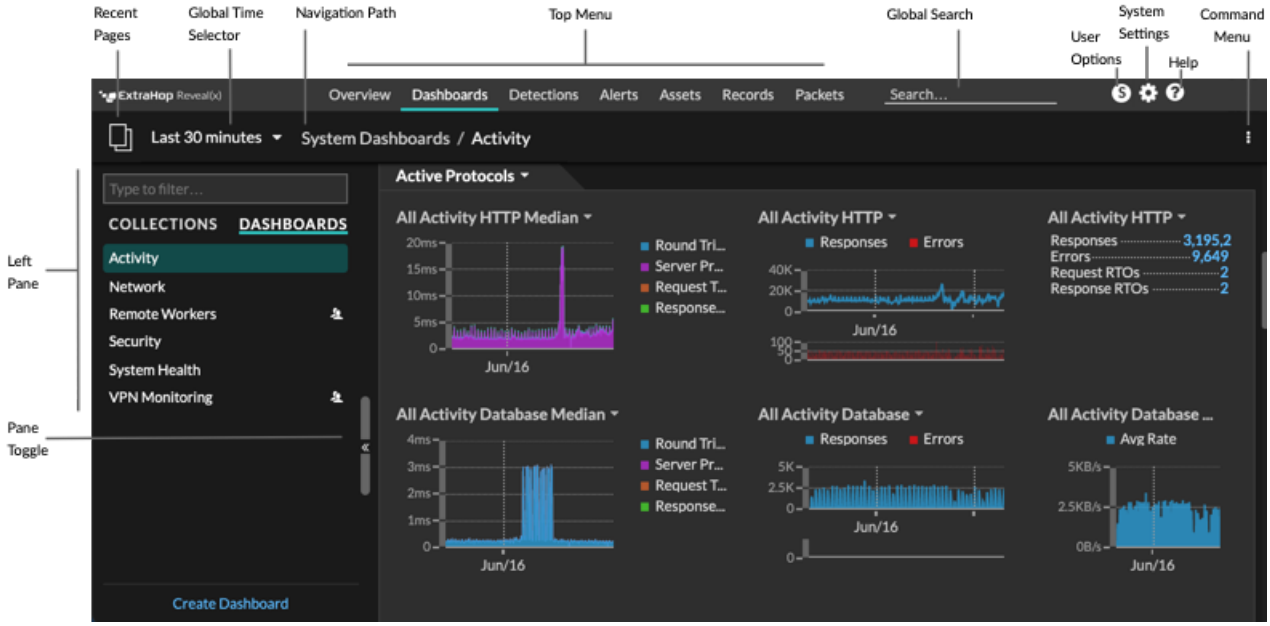
- Firefox
- Google Chrome
- Microsoft Edge
- Safari

Wichtig: Internet Explorer 11 wird nicht mehr unterstützt. Wir empfehlen Ihnen, die neueste Version aller unterstützten Browser zu installieren.

Layout und Menüs

Globale Navigationselemente befinden sich oben auf der Seite und enthalten Links zu den Hauptabschnitten des Systems. In jedem Abschnitt enthält der linke Bereich Links zu bestimmten Seiten oder Daten.

Die folgende Abbildung zeigt sowohl globale Navigationselemente als auch Navigationselemente im linken Bereich.



Hier sind Definitionen der einzelnen globalen Navigationselemente:

Übersichtsseiten

Auf Übersichtsseiten können Sie schnell den Umfang verdächtiger Aktivitäten in Ihrem Netzwerk bewerten, sich über Protokollaktivitäten und Geräteverbindungen informieren und den ein- und ausgehender Datenverkehr in Ihrem Netzwerk untersuchen.

- Sehen Sie sich das an Überblick über die Sicherheit für Informationen über Sicherheitserkennungen in Ihrem Netzwerk.
- Sehen Sie sich das an Überblick über das Netzwerk für Informationen über aktive Geräte in Ihrem Netzwerk.
- Sehen Sie sich das an Perimeter im Überblick für Informationen über den Verkehr, der in und aus Ihrem Netzwerk fließt.

Armaturenbretter

klicken **Armaturenbretter** um Dashboards zur Überwachung aller Aspekte Ihres Netzwerk oder Ihrer Anwendungen anzuzeigen, zu erstellen oder zu teilen. System-Dashboards geben Ihnen einen sofortigen Überblick über die Aktivitäten und potenziellen Sicherheitsbedrohungen in Ihrem Netzwerk.

Warnmeldungen

klicken **Warnmeldungen** um Informationen zu jeder Alarm anzuzeigen, die während des Zeitintervalls generiert wurde.

Erkennungen

Wenn dein Paket oder Fluss Sensor ist mit dem ExtraHop Machine Learning Service verbunden, die Top-Level-Navigation zeigt die **Erkennungen** Speisekarte. Klicken Sie **Erkennungen** um anhand Ihrer wire data identifizierte Erkennungen anzuzeigen. Sie können auf gespeicherte Erkennungen zugreifen, auch wenn Ihre Sensor ist vom Machine Learning Service getrennt.

Hinweis: Erkennungen durch maschinelles Lernen erfordern eine Verbindung zu ExtraHop Cloud Services.

Vermögenswerte

Klicken Sie **Vermögenswerte** um alle Anwendung, Netzwerk oder Gerät zu finden, die vom ExtraHop-System erkannt wurden. Sie können Protokollmetriken für Ihre Ressourcen, aktiven Benutzer oder Netzwerkaktivitäten nach Protokoll anzeigen.

Rekorde

Wenn Ihr ExtraHop-System mit einem konfiguriert ist Recordstore, die Navigation auf oberster Ebene zeigt das Datensatzmenü. Klicken Sie **Rekorde** um alle gespeicherten Datensätze für das aktuelle Zeitintervall abzufragen. Datensätze sind strukturierte Informationen über Transaktionen, Nachrichten und Netzwerkflüsse.

Pakete

Wenn Ihr ExtraHop-System mit einem konfiguriert ist Packetstore, die Navigation auf oberster Ebene zeigt das Menü Pakete. Klicken Sie **Pakete** um alle gespeicherten Pakete für das aktuelle Zeitintervall abzufragen.

Globales Suchfeld

Geben Sie den Namen eines beliebigen Geräts, eines Hostnamens oder einer IP-Adresse, einer Anwendung oder eines Netzwerk ein, um eine Übereinstimmung auf Ihrem Gerät zu finden Sensor oder Konsole. Wenn Sie einen verbundenen Recordstore haben, können Sie nach gespeicherten Datensätzen suchen. Wenn Sie einen verbundenen Packetstore haben, können Sie nach Paketen suchen.

Hilfesymbol

Sehen Sie sich die Hilfeinformationen für die Seite an, die Sie gerade betrachten. Um auf die aktuellsten und umfassendsten ExtraHop-Dokumentationen zuzugreifen, besuchen Sie die ExtraHop Documentation Webseite.

Symbol „Systemeinstellungen“

Greifen Sie auf Systemkonfigurationsoptionen wie Trigger, Alarme, geplante Berichte und benutzerdefinierte Geräte zu und klicken Sie, um das ExtraHop-System und die Version anzuzeigen. Klicken Sie **Hinweise zum System** um eine Liste der Funktionen in der aktuellsten Version und aller Systemhinweise wie ablaufende Lizenzen oder verfügbare Firmware-Upgrades.

Symbol für Benutzeroptionen

Loggen Sie sich ein und melden Sie sich von Ihrem ab Sensor oder Konsole, ändere dein Passwort, wähle das Display-Thema, eine Sprache einstellen und greifen Sie auf API-Optionen zu.

Fenster umschalten

Reduzieren oder erweitern Sie den linken Bereich.

Globaler Zeitselektor

Ändern Sie das Zeitintervall um Anwendung- und Netzwerkaktivitäten anzuzeigen, die vom ExtraHop-System für einen bestimmten Zeitraum beobachtet wurden. Das globale Zeitintervall wird auf alle Metriken im System angewendet und ändert sich nicht, wenn Sie zu verschiedenen Seiten navigieren.

Letzte Seiten

Sehen Sie sich in einem Drop-down-Menü eine Liste der zuletzt besuchten Seiten an und treffen Sie eine Auswahl, um zu einer vorherigen Seite zurückzukehren. Wiederholte Seiten werden dedupliziert und komprimiert, um Platz zu sparen.

Navigationspfad

Sehen Sie sich an, wo Sie sich im System befinden, und klicken Sie auf einen Seitennamen im Pfad , um zu dieser Seite zurückzukehren.

Dropdownmenü im Befehlsmenü

Klicken Sie hier, um auf bestimmte Aktionen für die Seite zuzugreifen, die Sie gerade betrachten. Zum Beispiel, wenn Sie klicken **Armaturenbretter** oben auf der Seite das Befehlsmenü ⋮ bietet Aktionen zum Ändern der Dashboard-Eigenschaften oder zum Erstellen eines neuen Dashboard.

Beginnen Sie mit der Datenanalyse

Beginnen Sie Ihre Reise zur Datenanalyse mit dem ExtraHop-System, indem Sie die unten aufgeführten grundlegenden Workflows befolgen. Sobald Sie sich mit dem ExtraHop-System vertraut gemacht haben, können Sie komplexere Aufgaben wie das Installieren von Bundles und das Erstellen von Triggern erledigen.

Im Folgenden finden Sie einige grundlegende Möglichkeiten, mit dem ExtraHop-System zu navigieren und mit diesem zu arbeiten, um Netzwerkaktivitäten zu analysieren.

Überwachen Sie Kennzahlen und untersuchen Sie interessante Daten

Gute Ausgangspunkte sind die Dashboard zur Netzwerkaktivität und Dashboard zur Netzwerkleistung, die Ihnen Zusammenfassungen wichtiger Kennzahlen zur Anwendungsleistung in Ihrem Netzwerk zeigen. Wenn Sie einen Anstieg des Datenverkehrs, Fehler oder Serververarbeitungszeit feststellen, können Sie mit den Dashboard-Daten interagieren, um bohren Sie nach unten und ermitteln Sie, welche Clients, Server, Methoden oder andere Faktoren zu der ungewöhnlichen Aktivität beigetragen haben.

Anschließend können Sie die Leistungsüberwachung oder Problembehandlung fortsetzen, indem Sie ein benutzerdefiniertes Dashboard erstellen um eine Reihe interessanter Metriken und Geräte zu verfolgen.

Schauen Sie sich Folgendes an Komplettlösungen um mehr über die Überwachung von Daten in Dashboards zu erfahren:

- Überwachen Sie die Leistung Ihrer Website in einem Dashboard
- Überwachen Sie DNS-Fehler in einem Dashboard
- Überwachen Sie den Zustand der Datenbank in einem Dashboard

Suchen Sie nach einem bestimmten Gerät und untersuchen Sie zugehörige Metriken und Transaktionen

Wenn Sie einen langsamen Server untersuchen möchten, können Sie suche nach dem Server im ExtraHop-System anhand des Gerätenamens oder der IP-Adresse und untersuchen Sie dann die Aktivität des Servers auf einer Protokollseite. Gab es einen Anstieg an Antwortfehlern oder Anfragen? War die Serververarbeitungszeit zu hoch oder hat sich die Netzwerklatenz auf die Datenübertragungsrate ausgewirkt? Klicken Sie auf der Geräteseite auf verschiedene Protokolle, um weitere vom ExtraHop-System gesammelte Metrik Daten zu untersuchen. Aufschlüsselung nach Peer-IP-Adressen um zu sehen, mit welchen Clients oder Anwendungen der Server gesprochen hat.

Wenn Ihr ExtraHop-System mit einem verbunden ist Recordstore, Sie können ganze Transaktionen untersuchen, an denen der Server beteiligt war Erstellen einer Datensatzabfrage.

Schauen Sie sich Folgendes an Komplettlösungen um mehr über das Erkunden von Metriken und Datensätzen zu erfahren:

- Erkunden Sie Metriken im ExtraHop-System, um DNS-Fehler zu untersuchen
- Datensätze abfragen, um fehlende Webressourcen zu finden

Verschaffen Sie sich einen Überblick über Änderungen an Ihrem Netzwerk, indem Sie nach Protokollaktivitäten suchen

Sie können Ihr Netzwerk von oben nach unten betrachten, indem Sie sich die integrierten Protokollgruppen ansehen. Eine Protokollgruppe ist eine Sammlung von Geräten, die vom ExtraHop-System auf der Grundlage des über die Leitung beobachteten Protokollverkehrs automatisch gruppiert werden. Sie können beispielsweise neue oder stillgelegte Server finden, die aktiv über ein Protokoll kommunizieren, indem Sie eine Aktivitätskarte erstellen.

Wenn Sie eine Sammlung von Geräten finden, die Sie weiter überwachen möchten, können Sie ein Geräte-Tag hinzufügen oder benutzerdefinierter Gerätename damit diese Geräte im ExtraHop-System leichter auffindbar sind. Du kannst auch eine benutzerdefinierte Gerätegruppe erstellen oder ein benutzerdefiniertes Dashboard um die Aktivität von Gerätegruppe zu überwachen.

Erweiterte Workflows zur Anpassung Ihres ExtraHop-Systems

Nachdem Sie sich mit den grundlegenden Arbeitsabläufen vertraut gemacht haben, können Sie Ihr ExtraHop-System anpassen, indem Sie Warnmeldungen einrichten, benutzerdefinierte Metriken erstellen oder Bundles installieren.

Benachrichtigungen einrichten

Warnmeldungen Verfolgen Sie bestimmte Messwerte, um Sie über Verkehrsabweichungen zu informieren, die auf ein Problem mit einem Netzwerkgerät hinweisen könnten. Einen Schwellenwertalarm konfigurieren um Sie zu benachrichtigen, wenn eine überwachte Metrik einen definierten Wert überschreitet. Konfigurieren Sie eine Trendwarnung um Sie zu benachrichtigen, wenn eine überwachte Metrik von den normalen, vom System beobachteten Trends abweicht.

Erstellen Sie einen Auslöser, um benutzerdefinierte Metriken und Anwendungen zu erstellen

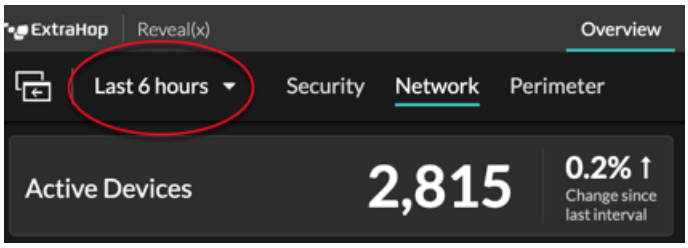
Trigger sind benutzerdefinierte Skripts , die bei einem vordefinierten Ereignis eine Aktion ausführen. Trigger müssen geplant werden, um sicherzustellen, dass ein Auslöser die Systemleistung nicht negativ beeinflusst.

Schauen Sie sich Folgendes an Komplettlösungen um mehr über das Erkunden von Metriken und Datensätzen zu erfahren:

- Erstellen Sie einen Auslöser, um benutzerdefinierte Metriken für HTTP 404-Fehler zu sammeln
- Erstellen Sie einen Auslöser, um Antworten auf NTP-Monlist-Anfragen zu überwachen

Zeitintervalle

Der Zeitselektor wird in der oberen linken Ecke der Navigationsleiste angezeigt und steuert das globale Zeitintervall für Metriken und Erkennungen, die im ExtraHop-System angezeigt werden.



Hier sind einige Überlegungen zu Zeitintervallen:

- Mit der Zeitselektor können Sie ein relatives globales Zeitintervall auswählen, z. B. den letzten Tag, oder einen benutzerdefinierten Zeitraum festlegen.
- Mit dem Zeitselektor können Sie ändere deine angezeigte Zeitzone manuell.
- Das gewählte Zeitintervall bleibt unverändert, unabhängig davon, ob Sie Metriken in einem Dashboard anzeigen oder Entdeckungen untersuchen, bis Sie das Intervall ändern oder zu einer Seite mit einem voreingestellten Zeitintervall navigieren, z. B. Erkennungsdetails oder Bedrohungsinformationen.
- Wenn beim Abmelden ein relatives Zeitintervall ausgewählt wird, verwendet das ExtraHop-System standardmäßig dieses relative Zeitintervall, wenn Sie sich wieder anmelden.
- Wenn beim Abmelden ein benutzerdefinierter Zeitraum ausgewählt wird, verwendet das ExtraHop-System standardmäßig das letzte relative Zeitintervall, das Sie während der vorherigen Anmeldesitzung angesehen haben.
- Sie können auf die fünf letzten eindeutigen Zeitintervalle zugreifen über **Geschichte** Registerkarte der Zeitselektor.
- Das Zeitintervall ist am Ende der URL in Ihrem Browser enthalten. Um einen Link mit anderen zu teilen, der ein bestimmtes Zeitintervall einhält, kopieren Sie die gesamte URL. Um nach dem Abmelden vom ExtraHop-System ein bestimmtes Zeitintervall einzuhalten, setzen Sie ein Lesezeichen für die URL.

Ändern Sie das Zeitintervall

Dieses Verfahren zeigt Ihnen, wie Sie das globale Zeitintervall einstellen. Sie können ein Zeitintervall auch per Dashboard anwenden oder nach Region.

1. Klicken Sie auf das Zeitintervall in der oberen linken Ecke der Seite (zum Beispiel **Letzte 30 Minuten**).
2. Wählen Sie aus den folgenden Intervall-Optionen:
   - Ein voreingestelltes Zeitintervall (z. B. **Letzte 30 Minuten**, **Letzte 6 Stunden**, **Letzter Tag**, oder **Letzte Woche**).
   - Eine benutzerdefinierte Zeiteinheit.
   - Ein benutzerdefinierter Zeitraum. Klicken Sie auf einen Tag, um das Startdatum für den Bereich anzugeben. Mit einem Klick wird ein einzelner Tag angegeben. Wenn Sie auf einen anderen Tag klicken, wird das Enddatum für den Bereich angegeben.
   - Metrik Deltas vergleichen aus zwei verschiedenen Zeitintervallen.
3. klicken **Speichern**.

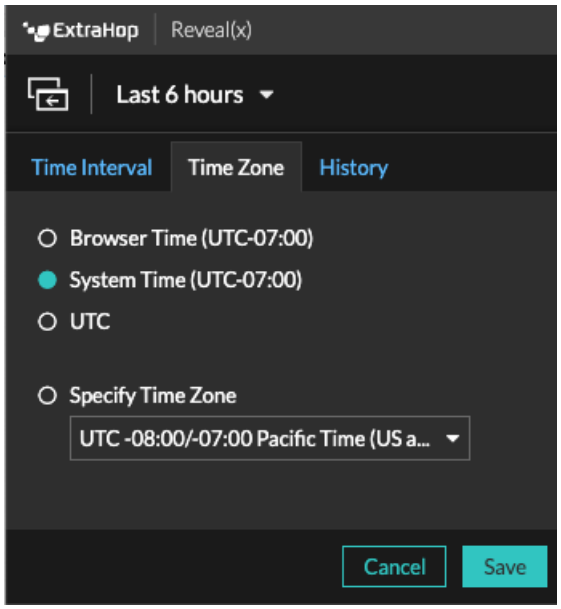
Hinweis: Sie können das Zeitintervall auch über den **Geschichte** Klicken Sie auf die Registerkarte, indem Sie aus bis zu fünf aktuellen Zeitintervallen auswählen, die in einer vorherigen Anmeldesitzung festgelegt wurden.

Ändern Sie die angezeigte Zeitzone

Mit dem Zeitselektor können Sie die im ExtraHop-System angezeigte Zeitzone ändern. Dies bietet mehr Flexibilität bei der Anzeige zeitbasierter Daten wie Metriken, Erkennungen und Aufzeichnungen in Umgebungen, die sich über mehrere Zeitzonen erstrecken.

Hier sind einige Überlegungen zur Anzeige von Zeiteinstellungen in RevealX 360 :

- Die Änderung Ihrer angezeigten Zeitzone wirkt sich auf die Datums- und Zeitstempel aus, die Sie im ExtraHop-System sehen, gilt jedoch nicht für geplante Berichte oder exportierte Dashboards.
- Wenn Sie Ihre Zeitzone ändern, wird die in den Administrationseinstellungen konfigurierte Standardanzeigezeit überschrieben. siehe Systemzeit (für ExtraHop Performance und RevealX Enterprise) oder Konfigurieren Sie die Systemzeit (für RevealX 360) für weitere Informationen.

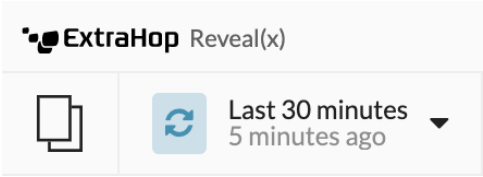


1. <extrahop-hostname-or-IP-address>Loggen Sie sich über https://in das ExtraHop-System ein.
2. Klicken Sie in der oberen linken Ecke der Seite auf die Zeitselektor.
3. Klicken Sie **Zeitzone**.
4. Wählen Sie eine der folgenden Optionen aus:
   - **Uhrzeit des Browsers**
   - **Systemzeit**
   - **UTC**
   - **Zeitzone angeben** und wählen Sie dann eine Zeitzone aus der Dropdownliste aus.
5. Klicken Sie **Speichern**.

Die neuesten Daten für ein Zeitintervall anzeigen

Seiten, auf denen überwachte Metrikdaten angezeigt werden, wie Dashboards und Protokollseiten, werden kontinuierlich aktualisiert, um die neuesten Daten für das ausgewählte Zeitintervall anzuzeigen.

Seiten mit detaillierten Metriken, Erkennungen, Datensätze, Pakete und Warnungen werden auf Anfrage neu geladen, indem Sie auf das Symbol „Daten aktualisieren“ in der oberen linken Ecke der Seite klicken.



Granularität der Diagrammdaten ändern

Das ExtraHop-System speichert Metriken in Zeitabständen von 30 Sekunden. Metrische Daten werden dann aggregiert oder in weitere Zeiträume von fünf Minuten und einer Stunde zusammengefasst. Durch das Aggregieren von Daten kann die Anzahl der in einem Zeitreihendiagramm gerenderten Datenpunkte begrenzt werden, sodass die Granularität der Daten einfacher zu interpretieren ist. Das von Ihnen gewählte Zeitintervall bestimmt die beste Aggregation oder Zusammenfassung von Daten, die für den betrachteten Zeitraum in einem Diagramm angezeigt werden sollen.

Wenn Sie beispielsweise ein großes Zeitintervall auswählen, z. B. eine Woche, werden die Metrikdaten zu einstündigen Rollups zusammengefasst. Auf der X-Achse eines Liniendiagramm sehen Sie einen Datenpunkt für jede Stunde statt eines Datenpunkts für alle 30 Sekunden. Wenn Sie die Granularität erhöhen möchten, können Sie ein Diagramm vergrößern oder das Zeitintervall ändern.

Das ExtraHop-System umfasst integrierte hochpräzise Metriken mit 1-Sekunden-Rollups, bei denen es sich um die Netzwerk-Bytes- und Netzwerk-Paket-Metriken handelt. Diese Metriken sind mit einem Gerät oder einer Netzwerkerfassungsquelle verknüpft. Weitere Informationen zum Anzeigen dieser Metriken in einem Diagramm finden Sie unter Zeigen Sie die maximale Rate in einem Diagramm an.

Das ExtraHop-System enthält auch integrierte Metriken zur Identifizierung der einzelnen Millisekunde des Datenverkehrs mit dem höchsten Verkehrsaufkommen innerhalb von 1 Sekunde. Diese Metriken, d. h. Maximale Netzwerk-Bytes pro Millisekunde und Maximale Anzahl an Paketen pro Millisekunde, sind mit einer Netzwerk-Capture-Quelle verknüpft und helfen Ihnen dabei, Microbursts zu erkennen. Microbursts sind schnelle Datenverkehrsschübe, die innerhalb von Millisekunden auftreten .

Die folgende Tabelle enthält Informationen darüber, wie Daten basierend auf dem Zeitintervall aggregiert werden.

Zeitintervall	Aggregations-Rollup (falls verfügbar)	Hinweise

Weniger als sechs Minuten	1 Sekunde	Ein 1-Sekunden-Rollup ist nur für benutzerdefinierte Metriken und für die folgenden integrierten Metriken verfügbar:
		• Netzwerkquelle:
		  • Netzwerk-Bytes (Gesamtdurchsatz)
		  • Netzwerkpakete (Gesamtpakete)
		  • Maximale Netzwerk-Bytes pro Millisekunde
		  • Maximale Netzwerkpakete pro Millisekunde
		• Gerätequelle:
		  • Netzwerk-Bytes (kombinierter

Zeitintervall	Aggregations-Rollup (falls verfügbar)	Hinweise
		eingehender und ausgehender Durchsatz pro Gerät) • Eingehende Netzwerk-Bytes (eingehender Durchsatz pro Gerät) • Netzwerk-Bytes Out (ausgehender Durchsatz pro Gerät) • Netzwerkpakete (kombinierte eingehende und ausgehende Pakete pro Gerät) • Eingehende Netzwerkpakete (eingehende Pakete pro Gerät) • Ausgehende Netzwerkpakete (ausgehende Pakete pro Gerät)
120 Minuten oder weniger	30 Sekunden	Wenn kein 30-Sekunden-Roll-Up verfügbar ist, wird ein 5-minütiges oder 60-minütiges Roll-Up angezeigt.
Zwischen 121 Minuten und 24 Stunden	5 Minuten	Wenn das 5-minütige Roll-Up nicht verfügbar ist, wird ein 60-minütiges Roll-Up angezeigt.
Mehr als 24 Stunden	60 Minuten	—

Hinweis: Wenn Sie über einen erweiterten Datenspeicher verfügen, der für 24-Stunden-Metriken konfiguriert ist, zeigt ein bestimmtes Zeitintervall von 30 Tagen oder länger einen 24-Stunden-Aggregations-Rollup an.

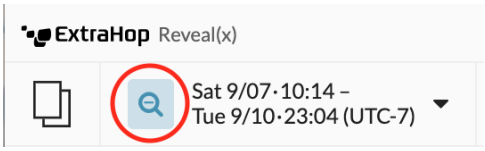
Vergrößern Sie einen benutzerdefinierten Zeitraum

Sie können über ein Diagramm klicken und ziehen, um interessante Metrikaktivitäten zu vergrößern. Dieser benutzerdefinierte Zeitraum wird dann auf das gesamte ExtraHop-System angewendet. Dies ist nützlich, um andere Metrik Aktivitäten zu untersuchen, die gleichzeitig aufgetreten sind.

Das Vergrößern eines Zeitbereichs ist nur in Diagrammen mit einer X- und Y-Achse verfügbar, z. B. in Linien-, Flächen-, Candlestick- und Histogrammdiagrammen.

1. Klicken und ziehen Sie die Maus über das Diagramm, um einen Zeitraum auszuwählen. Wenn der Zeitbereich weniger als eine Minute beträgt, wird der Zeitbereich rot angezeigt. Ziehen Sie die Maus, bis der Zeitbereich grün erscheint.
2. Lassen Sie die Maustaste los. Das Diagramm wird im benutzerdefinierten Zeitraum neu gezeichnet und das Zeitintervall in der oberen rechten Ecke der Navigationsleiste wird aktualisiert.

3. Um vom benutzerdefinierten Zeitintervall zum ursprünglichen Zeitintervall zurückzukehren, klicken Sie auf das Rückgängig-Symbol — eine Lupe mit einem Minuszeichen —, das neben dem Zeitintervall in der oberen rechten Ecke der Navigationsleiste angezeigt wird.

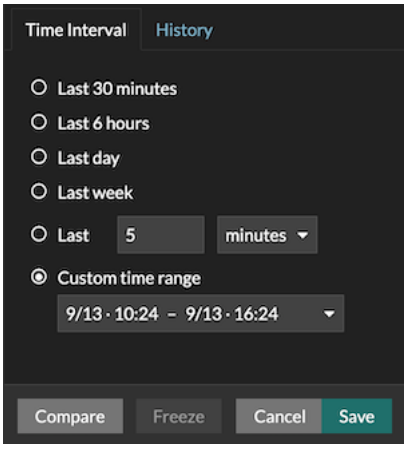


Hinweis: Auf einer Dashboard-Seite können Sie den benutzerdefinierten Zeitbereich für das Zoomen auf eine bestimmte Region beschränken. Klicken Sie auf die Kopfzeile der Region und wählen Sie **Region Zeitselektor verwenden**, und vergrößern Sie dann ein Diagramm. Jedes Diagramm oder Widget in dieser Region wird auf den benutzerdefinierten Zeitraum aktualisiert.

Frieren Sie das Zeitintervall ein, um einen benutzerdefinierten Zeitraum zu erstellen

Wenn Sie interessante Daten auf einer Aktivitätsdiagramm, einem Dashboard oder einer Protokollseite sehen, können Sie das Zeitintervall einfrieren, um sofort einen benutzerdefinierten Zeitraum zu erstellen. Das Einfrieren des Zeitintervalls ist nützlich, um Links zu erstellen, die Sie mit anderen teilen können, und um verwandte Metrikaktivitäten zu untersuchen, die gleichzeitig aufgetreten sind.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf die Zeitauswahl in der oberen linken Ecke der Seite.
3. Wählen Sie ein voreingestelltes Zeitintervall.
4. klicken **Einfrieren**.
   Der benutzerdefinierte Zeitraum wird automatisch aktualisiert, wie in der Abbildung unten dargestellt. Der Bereich beginnt mit dem frühesten Zeitpunkt aus dem vorherigen Zeitintervall und endet mit dem Zeitpunkt, zu dem Sie geklickt haben **Einfrieren**.



5. klicken **Speichern**.
   Der neue benutzerdefinierte Zeitraum ändert sich nicht, wenn Sie durch das ExtraHop-System navigieren. Sie können die URL in Ihrem Browser teilen oder mit einem Lesezeichen versehen.

   Hinweis: Das Zeitintervall ist am Ende der URL in Ihrem Browser enthalten. Um einen Link mit anderen zu teilen, der ein bestimmtes Zeitintervall einhält, kopieren Sie die gesamte URL. Durch das Erstellen eines Lesezeichens für die URL wird der benutzerdefinierte Zeitraum auch nach dem Abmelden vom ExtraHop-System beibehalten.
6. Um den benutzerdefinierten Zeitraum zu entfernen, das Zeitintervall ändern.

Übersichtsseiten

Auf Übersichtsseiten können Sie schnell den Umfang verdächtiger Aktivitäten in Ihrem Netzwerk einschätzen, sich über Protokollaktivitäten und Geräteverbindungen informieren und eingehenden und ausgehender Datenverkehr in Ihrem Netzwerk untersuchen.

- Sehen Sie sich das an Überblick über die Sicherheit für Informationen über Sicherheitserkennungen in Ihrem Netzwerk.
- Sehen Sie sich das an Überblick über das Netzwerk für Informationen über aktive Geräte in Ihrem Netzwerk.
- Sehen Sie sich das an Überblick über den Perimeter für Informationen über den Verkehr, der in und aus Ihrem Netzwerk fließt.

Überblick über die Sicherheit

In der Sicherheitsübersicht werden mehrere Diagramme angezeigt, in denen Daten zu Erkennungen aus unterschiedlichen Perspektiven dargestellt werden. Mithilfe dieser Diagramme können Sie den Umfang der Sicherheitsrisiken einschätzen, Untersuchungen zu ungewöhnlichen Aktivitäten einleiten und Sicherheitsbedrohungen eindämmen. Erkennungen werden je nach Metrik alle 30 Sekunden oder jede Stunde analysiert.

Video: Sehen Sie sich die entsprechende Schulung an: Überblick über Sicherheit, Netzwerk und Perimeter

Für Triage empfohlen

Dieses Diagramm zeigt Ihnen eine Liste von Erkennungen, die ExtraHop auf der Grundlage einer kontextbezogenen Analyse Ihrer Umgebung, auch bekannt als Smart Triage, empfiehlt. Klicken Sie auf eine Erkennung, um die Erkennungskarte in Triage-Ansicht auf der Seite „Erkennungen“.

Ermittlungen

Dieses Diagramm zeigt die Anzahl der Untersuchungen, die während des ausgewählten Zeitintervalls erstellt wurden. Die Zählung beinhaltet Untersuchungen, die von ExtraHop empfohlen oder von Benutzern erstellt wurden. Klicken Sie auf das Diagramm, um das zu sehen Tabelle der Untersuchungen auf der Seite „ Erkennungen“.

Erkennungen nach Angriffskategorie

Dieses Diagramm bietet einen schnellen Überblick über die Arten von Angriffen, für die Ihr Netzwerk möglicherweise gefährdet ist, und zeigt die Anzahl der Erkennungen an, die in jeder Kategorie während des ausgewählten Zeitintervalls aufgetreten sind. Die Aktionen bei objektiven Erkennungen sind nach Typ aufgelistet, damit Sie die schwerwiegendsten Erkennungen priorisieren können. Klicken Sie auf eine beliebige Zahl, um eine gefilterte Ansicht der Erkennungen zu öffnen, die den ausgewählten entsprechen Kategorie des Angriffs.

Häufige Straftäter

Dieses Diagramm zeigt die 20 Geräte oder Endgeräte, die bei einer oder mehreren Erkennungen als Straftäter fungierten. Das ExtraHop-System berücksichtigt die Anzahl der verschiedenen Angriffskategorien und Erkennungstypen sowie die Risikobewertung der mit jedem Gerät verbundenen Erkennungen, um festzustellen, welche Geräte als häufige Straftäter gelten.

Die Größe des Geräterollensymbols gibt die Anzahl der verschiedenen Erkennungstypen an, und die Position des Symbols gibt die Anzahl der verschiedenen Angriffskategorien an. Klicken Sie auf ein Rollensymbol, um weitere Informationen zu den Angriffskategorien und Erkennungstypen anzuzeigen, die dem Gerät zugeordnet sind. Klicken Sie auf den Gerätenamen, um ihn anzuzeigen Eigenschaften Gerät.

Erfahren Sie mehr über Netzwerksicherheit mit dem Dashboard zur Erhöhung der Sicherheit.

Bedrohungsinformationen

Threat Briefings bieten in der Cloud aktualisierte Hinweise zu branchenweiten Sicherheitsereignissen. Erfahren Sie mehr über Bedrohungsinformationen.

Standortauswahl und Bericht über Sicherheitsoperationen

Auf dieser Seite können Sie die Websites angeben, von denen Sie Daten anzeigen möchten. Benutzer mit Zugriff auf das NDR-Modul können einen Security Operations Report erstellen, um die Ergebnisse zu teilen.

Seitenauswahl

Klicken Sie oben auf der Seite auf die Seitenauswahl, um Daten für eine oder mehrere Websites in Ihrer Umgebung anzuzeigen. Sehen Sie sich den kombinierten Traffic in Ihren Netzwerken an oder konzentrieren Sie sich auf einen einzelnen Standort, um Gerätedaten schnell zu finden. Die Seitenauswahl zeigt an, wann alle oder einige Websites offline sind. Da Daten von Offline-Websites nicht verfügbar sind, werden in den Diagrammen und Geräteseiten, die Offlineseiten zugeordnet sind, möglicherweise keine oder nur begrenzte Daten angezeigt. Der Site-Selector ist nur von einem verfügbar Konsole.

(nur NDR-Modul) Sicherheitsbetriebsbericht

Der Security Operations Report enthält eine Zusammenfassung der wichtigsten Erkennungen und Risiken für Ihr Netzwerk. klicken **Bericht generieren** um den Berichtsinhalt, das Zeitintervall und die Websites anzugeben, die in den Bericht aufgenommen werden sollen, klicken Sie dann auf **Generieren** um eine PDF-Datei zu erstellen. klicken **Bericht planen** um einen Security Operations Report zu erstellen, der per E-Mail an die Empfänger gesendet wird gemäß die konfigurierte Frequenz.

Überblick über das Netzwerk

In der Netzwerkübersicht werden eine Übersicht der Funde in Ihrem Netzwerk sowie eine Liste der Straftäter nach Anzahl der Entdeckungen angezeigt. Die Netzwerkübersicht aktualisiert die Erkennungskarte und die Täterdaten jede Minute.

Video: Sehen Sie sich die entsprechende Schulung an: Überblick über Sicherheit, Netzwerk und Perimeter

Erkennungskategorie umschalten

Sie können zwischen Ansichten wechseln, die angezeigt werden **Alle Angriffserkennungen** oder **Alle Leistungserkennungen**, abhängig von den aktivierten Modulen und Ihrem Modulzugriff.

Straftäter bei Feststellungen

Diese Liste zeigt die Täter, sortiert nach der Anzahl der Erkennungen, bei denen das Gerät oder der Endpunkt als Täter fungierte.

Hier sind einige Möglichkeiten, wie Sie mit der Liste der Straftäter interagieren können:

- Klicken Sie in der Liste auf ein Gerät oder einen Endpunkt, um die zugehörigen Funde in der Erkennungsübersicht hervorzuheben und die Geräteeigenschaften sowie die Links zum Zugriff auf Endpunktsuche Websites, Erkennungen, Aufzeichnungen oder Pakete.
- Abhängig von der ausgewählten Erkennungskategorie und Ihrem Systemmodul klicken Sie auf **Alle Angriffserkennungen anzeigen** oder **Alle Leistungserkennungen anzeigen** Link zum Erkennungen seite, nach Erkennungskategorie gefiltert und nach Quelle gruppiert.
- Wählen Sie die **Erkennungen ohne Opfer anzeigen** Kontrollkästchen, um Erkennungen anzuzeigen, an denen kein Opferteilnehmer Teilnehmer ist. TLS-Scans und bestimmte Warnmeldungen bei verdächtigen Aktivitäten schließen beispielsweise nur einen Täter ein.

Erkennungskarte

In der Erkennungsübersicht werden der Täter und das Opfer für alle Erkennungen angezeigt, die im Umschalter für die Erkennungskategorie ausgewählt wurden.

Kreise werden rot hervorgehoben, wenn das Gerät während des ausgewählten Zeitintervalls bei mindestens einer Erkennung als Täter aufgetreten ist, und blaugrün hervorgehoben, wenn es sich bei dem Gerät um ein Opfer handelt.

Die Teilnehmer sind durch Leitungen miteinander verbunden, die mit dem Erkennungstyp oder der Anzahl der mit der Verbindung verbundenen Erkennungen gekennzeichnet sind, und Geräterollen werden durch ein Symbol dargestellt.

Hier sind einige Möglichkeiten, wie Sie mit der Erkennungskarte interagieren können:

- Klicken Sie auf einen Kreis, um die Geräteeigenschaften anzuzeigen und auf Links zuzugreifen Endpunktsuche Websites, Erkennungen, Aufzeichnungen oder Pakete.
- Klicken Sie auf eine Verbindung, um die zugehörigen Erkennungen anzuzeigen.
- Bewegen Sie den Mauszeiger über einen Kreis, um Gerätebeschriftungen zu sehen und Geräteanschlüsse hervorzuheben.

Erfahre mehr über Erkennungen.

Standortauswahl und Bericht über Sicherheitsoperationen

Auf dieser Seite können Sie die Websites angeben, von denen Sie Daten anzeigen möchten. Benutzer mit Zugriff auf das NDR-Modul können einen Security Operations Report erstellen, um die Ergebnisse zu teilen.

Seitenauswahl

Klicken Sie oben auf der Seite auf die Seitenauswahl, um Daten für eine oder mehrere Websites in Ihrer Umgebung anzuzeigen. Sehen Sie sich den kombinierten Traffic in Ihren Netzwerken an oder konzentrieren Sie sich auf einen einzelnen Standort, um Gerätedaten schnell zu finden. Die Seitenauswahl zeigt an, wann alle oder einige Websites offline sind. Da Daten von Offline-Websites nicht verfügbar sind, werden in den Diagrammen und Geräteseiten, die Offlineseiten zugeordnet sind, möglicherweise keine oder nur begrenzte Daten angezeigt. Der Site-Selector ist nur von einem verfügbar Konsole.

(nur NDR-Modul) Sicherheitsbetriebsbericht

Der Security Operations Report enthält eine Zusammenfassung der wichtigsten Erkennungen und Risiken für Ihr Netzwerk. klicken **Bericht generieren** um den Berichtsinhalt, das Zeitintervall und die Websites anzugeben, die in den Bericht aufgenommen werden sollen, klicken Sie dann auf **Generieren** um eine PDF-Datei zu erstellen. klicken **Bericht planen** um einen Security Operations Report zu erstellen, der per E-Mail an die Empfänger gesendet wird gemäß die konfigurierte Frequenz.

Perimeter im Überblick

In der Perimeterübersicht werden Diagramme und interaktive Visualisierungen angezeigt, mit denen Sie den Datenverkehr überwachen können, der über Verbindungen mit externen Endpunkten in Ihr Netzwerk ein- und ausströmt.

Video: Sehen Sie sich die entsprechende Schulung an: Überblick über Sicherheit, Netzwerk und Perimeter

Perimeterverkehr

Die Perimeter-Traffic-Diagramme bieten einen Überblick über den Geräteverkehr mit externen Verbindungen.

Eingehender Verkehr

Diese Anzahl zeigt die Gesamtmenge des eingehender Datenverkehr während des ausgewählten Zeitintervalls. Klicken Sie auf die Anzahl, um die Geschwindigkeit anzuzeigen, mit der Daten von externen Endpunkten eintreffen, und eine Aufschlüsselung nach Standort oder Konversation.

Ausgehender Verkehr

Diese Anzahl zeigt die Gesamtmenge des ausgehender Datenverkehr während des ausgewählten Zeitintervalls. Klicken Sie auf die Anzahl, um die Rate anzuzeigen, mit der Daten an externe Endpunkte übertragen werden, und eine Aufschlüsselung nach Standort oder Konversation.

Geräte, die eingehende Verbindungen akzeptieren

Diese Anzahl zeigt die Anzahl der Geräte an, die während des ausgewählten Zeitintervalls eingehende Verbindungen von externen Endpunkten akzeptiert haben. Klicken Sie auf die Anzahl, um eine Übersichtsseite für Gerätegruppe zu öffnen, auf der eine Liste der Geräte, Verkehrsdaten und Protokollaktivitäten angezeigt wird.

Eingehende Verbindungen

Diese Anzahl zeigt die Anzahl der eingehenden Verbindungen an, die von externen Endpunkten initiiert wurden. Klicken Sie auf die Anzahl, um eine detaillierte Ansicht dieser Konversationen zu öffnen.

Verdächtige eingehende Verbindungen

Dieses Zähldiagramm zeigt die Anzahl der Verbindungen an, die von verdächtigen externen Endpunkten initiiert wurden. ExtraHop identifiziert verdächtige Endpunkte durch Bedrohungsinformationen Daten. Klicken Sie auf das Diagramm, um eine gefilterte Ansicht dieser Konversationen zu öffnen.

Verdächtige ausgehende Verbindungen

Diese Anzahl zeigt die Anzahl der Verbindungen an, die interne Endpunkte mit verdächtigen externen Endpunkten initiiert haben. ExtraHop identifiziert verdächtige Endpunkte durch Bedrohungsinformationen Daten. Klicken Sie auf das Diagramm, um eine gefilterte Ansicht dieser Konversationen zu öffnen.

Ungewöhnliche Verbindungen

(Nur RevealX 360) Diese Anzahl zeigt die Anzahl der ausgehenden Verbindungen von Ihrem Netzwerk zu IP-Adressen an, die normalerweise nicht besucht werden oder in der Vergangenheit nicht besucht wurden. Klicken Sie auf das Diagramm, um eine gefilterte Ansicht dieser Konversationen zu öffnen.

Halo-Visualisierung

Die Halo-Visualisierung bietet zwei Ansichten Ihrer Netzwerkverbindungen zu externen Endpunkten: Cloud Services und Large Uploads.

Externe Endpunkte erscheinen auf dem äußeren Ring mit Verbindungen zu internen Endpunkten und erscheinen als Kreise in der Mitte der Visualisierung. Diese Visualisierungen ermöglichen es Ihnen, Ihre Prioritäten zu setzen Untersuchung für Verbindungen, bei denen ein hohes Risiko erkannt wurde, oder für hochwertige Geräte.

Um die Identifizierung von Endpunkten mit hohem Traffic zu erleichtern, nehmen innere und äußere Ringe mit steigendem Verkehrsaufkommen an Größe zu. In einigen Fällen kann die Größe der inneren Kreise und der äußeren Ringsegmente aus Gründen der Lesbarkeit erhöht werden. Klicken Sie auf einen Endpunkt, um genaue Verkehrsinformationen anzuzeigen.

Klicken Sie **Cloud-Dienste** um Verbindungen zwischen internen Endpunkten und Cloud-Dienstanbietern anzuzeigen. Cloud-Dienstanbieter und die Menge der gesendeten oder empfangenen Daten werden im Informationsfeld auf der rechten Seite angezeigt. Sie können zwischen Ansichten wechseln , die angezeigt werden **Ausgehende Bytes** an Anbieter und **Eingehende Byte** zu Ihrem Netzwerk.

Klicken Sie **Große Uploads** um Verbindungen zwischen internen und externen Endpunkten anzuzeigen, bei denen über 1 MB an Daten in einer einzigen Übertragung von Ihrem Netzwerk zu einem Externer

Endpunkt übertragen wurden. Externe Endpunkte und die Menge der hochgeladenen Daten werden im Informationsfeld auf der rechten Seite angezeigt.

Hier sind einige Möglichkeiten, wie Sie mit diesen Halo-Visualisierungen interagieren können:

- Zeigen Sie mit der Maus auf Endpunkte oder Verbindungen, um die verfügbaren Hostnamen und IP-Adressen anzuzeigen.
- Zeigen Sie mit der Maus auf Endpunkte oder Verbindungen, um die entsprechenden Listenelemente auf der rechten Seite hervorzuheben. Zeigen Sie ebenfalls mit der Maus auf Listenelemente, um die entsprechenden Endpunkte und Verbindungen in der Halo-Visualisierung hervorzuheben.
- Klicken Sie in der Halo-Visualisierung auf Endpunkte oder Verbindungen, um den Fokus zu behalten und auf der rechten Seite präzise Verkehrsinformationen und Links für Ihre Auswahl anzuzeigen.
- Klicken Sie in der Halo-Visualisierung oder -Liste auf einen Externer Endpunkt, um die Gesamtmenge des eingehenden oder ausgehender Datenverkehr anzuzeigen, der mit dem Endpunkt und den verbundenen internen Endpunkten verknüpft ist .
- Klicken Sie in der Liste auf einen internen Endpunkt, um Geräteeigenschaften anzuzeigen und auf Links zu zugehörigen Informationen wie Erkennungen, Aufzeichnungen oder Paketen zuzugreifen.
- Klicken Sie in der Liste auf die Lupe neben einem Endpunkt, um die mit dem Endpunkt verknüpften Datensätze anzuzeigen.
- Wechseln Sie am Ende der Liste für Cloud-Dienste zwischen Ansichten, die Bytes Out und Bytes In für Ihr Netzwerk anzeigen.
- Passen Sie das Zeitintervall an, um Verbindungen zu bestimmten Zeiten anzuzeigen, z. B. unerwartete Aktivitäten am Abend oder am Wochenende.

Kartenvisualisierung

Die Registerkarte Geolocation bietet eine Weltkarte des Verkehrs zwischen internen Endpunkten und geografischen Standorten, die auf der Karte in einer kontrastierenden Farbe hervorgehoben sind. Die Intensität der kontrastierenden Farbe steht für das Verkehrsaufkommen an dieser Geolokation. Auf der Karte dargestellte Geolokationen werden auch im rechten Bereich aufgeführt.

Klicken Sie auf eine hervorgehobene Geolokalisierung auf der Karte oder der Liste, um die Gesamtmenge des eingehenden oder ausgehender Datenverkehr im Zusammenhang mit verbundenen internen Endpunkten anzuzeigen.

Hier sind einige Möglichkeiten, wie Sie mit den Geolokalisierungsdetails und der Kartenvisualisierung interagieren können:

- Klicken Sie in der Liste auf einen internen Endpunkt, um Geräteeigenschaften anzuzeigen und auf Links zu zugehörigen Informationen wie Erkennungen, Aufzeichnungen oder Paketen zuzugreifen.
- Klicken Sie auf die Lupe neben einem Endpunkt in der Liste, um die mit dem Endpunkt verknüpften Datensätze anzuzeigen.
- Wechseln Sie am Ende der Liste zwischen Ansichten, in denen Bytes Out und Bytes In to your Netzwerk angezeigt werden.
- Klicken Sie auf die Steuerelemente in der unteren rechten Ecke der Karte, um die Karte zu vergrößern und zu verkleinern oder die Karte an die ursprüngliche Position zurückzubringen, oder Sie können das Mausrad drehen.
- Klicken und ziehen Sie mit der Maus auf die Karte oder drücken Sie die Pfeiltasten auf Ihrer Tastatur, um die Kartenansicht neu zu positionieren.
- Passen Sie das Zeitintervall an, um den Verkehr zu bestimmten Zeiten anzuzeigen, z. B. unerwartete Aktivitäten am Abend oder am Wochenende.

Standortauswahl und Bericht über Sicherheitsoperationen

Auf dieser Seite können Sie die Websites angeben, von denen Sie Daten anzeigen möchten. Benutzer mit Zugriff auf das NDR-Modul können einen Security Operations Report erstellen, um die Ergebnisse zu teilen.

Seitenauswahl

Klicken Sie oben auf der Seite auf die Seitenauswahl, um Daten für eine oder mehrere Websites in Ihrer Umgebung anzuzeigen. Sehen Sie sich den kombinierten Traffic in Ihren Netzwerken an oder konzentrieren Sie sich auf einen einzelnen Standort, um Gerätedaten schnell zu finden. Die Seitenauswahl zeigt an, wann alle oder einige Websites offline sind. Da Daten von Offline-Websites nicht verfügbar sind, werden in den Diagrammen und Geräteseiten, die Offlineseiten zugeordnet sind, möglicherweise keine oder nur begrenzte Daten angezeigt. Der Site-Selector ist nur von einem verfügbar Konsole.

(nur NDR-Modul) Sicherheitsbetriebsbericht

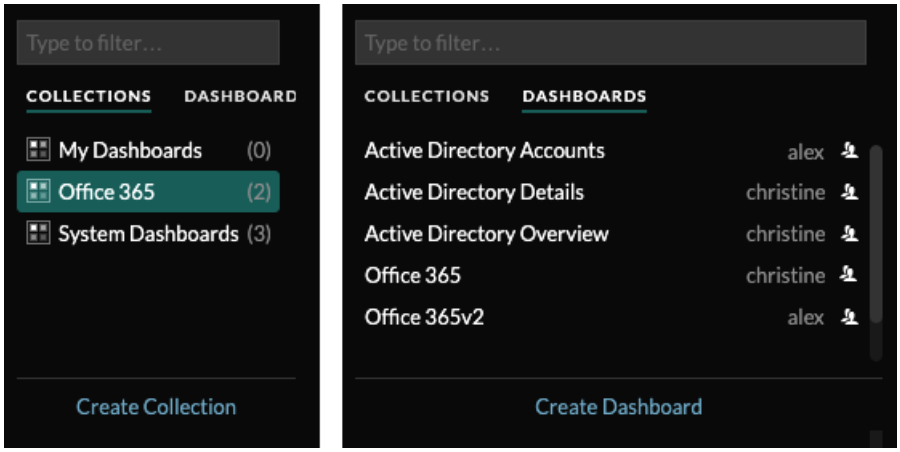
Der Security Operations Report enthält eine Zusammenfassung der wichtigsten Erkennungen und Risiken für Ihr Netzwerk. klicken **Bericht generieren** um den Berichtsinhalt, das Zeitintervall und die Websites anzugeben, die in den Bericht aufgenommen werden sollen, klicken Sie dann auf **Generieren** um eine PDF-Datei zu erstellen. klicken **Bericht planen** um einen Security Operations Report zu erstellen, der per E-Mail an die Empfänger gesendet wird gemäß die konfigurierte Frequenz.

Dashboards

Dashboards sind ein effektives Tool zur Überwachung des Netzwerkverkehrs mit hoher Priorität oder zur Behebung von Problemen, da sie mehrere Metrikdiagramme an einem zentralen Ort konsolidieren, an dem Sie Daten untersuchen und austauschen können. Sie können auch Textfelder hinzufügen, die mit Markdown formatiert sind, um Inhalte für Stakeholder bereitzustellen.

Video: Sehen Sie sich die entsprechende Schulung an: Dashboard-Konzepte

Dashboards und Sammlungen befinden sich im Dashboard-Dock.



Klicken Sie **Sammlungen** um alle Dashboard-Sammlungen anzuzeigen, die Sie besitzen oder die mit Ihnen geteilt wurden. Die Anzahl der Dashboards in jeder Sammlung wird angezeigt. Klicken Sie auf den Namen der Sammlung, um den Besitzer, mit dem die Sammlung geteilt wurde, und die Liste der Dashboards in der Sammlung anzuzeigen.

Nur der Sammlungsbesitzer kann eine Sammlung ändern oder löschen. Da Dashboards jedoch zu mehreren Sammlungen hinzugefügt werden können, können Sie eine Sammlung erstellen und teile es mit anderen Benutzern und Gruppen.

Klicken Sie **Dashboards** um eine alphabetische Liste aller Dashboards anzuzeigen, die Ihnen gehören oder die mit Ihnen geteilt wurden, einschließlich Dashboards, die über eine Sammlung geteilt wurden. Der Besitzer jedes Dashboard wird angezeigt. Ein Symbol neben dem Namen des Besitzers weist darauf hin, dass das Dashboard mit Ihnen geteilt wurde.

Dashboards erstellen

Wenn Sie bestimmte oder benutzerdefinierte Metriken überwachen möchten, können Sie ein benutzerdefiniertes Dashboard erstellen. Sie benötigen persönliche Schreibrechte oder höher und müssen über NPM-Modulzugriff verfügen, um Dashboards zu erstellen und zu bearbeiten.

Benutzerdefinierte Dashboards werden für jeden Benutzer, der auf das ExtraHop-System zugreift, separat gespeichert. Nachdem Sie ein benutzerdefiniertes Dashboard erstellt haben, können Sie es mit anderen ExtraHop-Benutzern teilen.

Es gibt mehrere Möglichkeiten, ein eigenes Dashboard zu erstellen:

- Erstellen Sie ein benutzerdefiniertes Dashboard oder ein Dashboard mit dynamischen Quellen erstellen von Grund auf
- Ein vorhandenes Dashboard kopieren, und passen Sie es dann an
- Ein vorhandenes Diagramm kopieren, und speichern Sie es dann in einem neuen Dashboard

Neue Dashboards werden im Modus „Layout bearbeiten“ geöffnet, in dem Sie Komponenten innerhalb des Dashboard hinzufügen, anordnen und löschen können. Nachdem Sie ein Dashboard erstellt haben, können Sie die folgenden Aufgaben ausführen:

- Widgets und Regionen hinzufügen oder löschen
- Eine Region bearbeiten
- Ein Diagramm bearbeiten
- Ein Textfeld bearbeiten

Klicken Sie auf das Befehlsmenü ⋮ in der oberen rechten Ecke der Seite, um die Dashboard-Eigenschaften zu bearbeiten oder das Dashboard zu löschen.

Hinweis: Sie können ein gelöschtes Dashboard nicht wiederherstellen. Beim Löschen von Benutzerkonten können ExtraHop-Administratoren den Besitz des Dashboard auf einen anderen Systembenutzer übertragen. Andernfalls werden auch alle mit dem Benutzerkonto verknüpften benutzerdefinierten Dashboards gelöscht. Um Dashboards beizubehalten, eine Kopie erstellen bevor das Konto gelöscht wird.

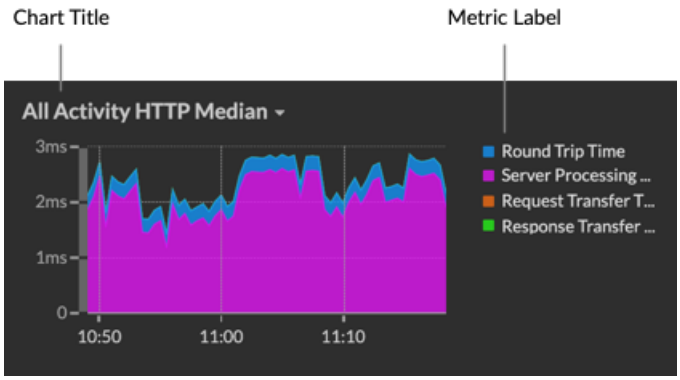
Erfahren Sie, wie Sie Ihr Netzwerk überwachen können, indem Sie Durchführen einer Dashboard-Komplettlösung.

Dashboards anzeigen

Dashboards bestehen aus Diagramm-Widgets, Warnungs-Widgets und Textfeld-Widgets, die einen übersichtlichen Überblick über kritische Systeme oder über Systeme bieten können, die von einem bestimmten Team verwaltet werden.

Klicken Sie in ein Diagramm, um mit den Metrikdaten zu interagieren:

- Klicken Sie auf einen Diagrammtitel, um eine Liste von anzuzeigen Metrik Quellen und Menüoptionen.
- Klicken Sie auf eine Metrikbezeichnung, um bohren und untersuchen durch ein Metrik Detail.
- Klicken Sie auf eine Metrikbezeichnung und dann auf Fokus halten, um nur diese Metrik im Diagramm anzuzeigen.
- Klicken Sie auf einen Diagrammtitel oder eine Metrikbezeichnung und dann auf Beschreibung, um mehr über die Quellmetrik zu erfahren.
- Klicken Sie auf eine Erkennungsmarkierung, um zur Seite mit den Erkennungsdetails zu gelangen



Ändern Sie die Zeitauswahl, um Datenänderungen im Laufe der Zeit zu beobachten:

- Ändern Sie das Zeitintervall für das gesamte Dashboard
- Ändern Sie das Zeitintervall nach Region
- Vergrößern Sie ein Zeitintervall innerhalb eines Diagramms
- Vergleichen Sie das Metrik Delta aus zwei Zeitintervallen in einem Diagramm

Dashboard-Daten exportieren und teilen

Standardmäßig sind alle benutzerdefinierten Dashboards privat und keine anderen ExtraHop-Benutzer können Ihr Dashboard anzeigen oder bearbeiten.

Teilen Sie Ihr Dashboard um anderen ExtraHop-Benutzern und -Gruppen Anzeige- oder Bearbeitungsberechtigungen zu gewähren, oder eine Sammlung teilen um mehreren Dashboards nur Leseberechtigungen zu gewähren.

Sie können ein geteiltes Dashboard nur ändern, wenn der Eigentümer Ihnen die Bearbeitungsberechtigung erteilt hat. Sie können jedoch kopieren und anpassen ein geteiltes Dashboard ohne Bearbeitungsberechtigung.

Exportieren Sie Daten nach einzelnen Diagrammen oder nach dem gesamten Dashboard:

- Um einzelne Diagrammdaten zu exportieren, klicken Sie auf den Diagrammtitel und wählen Sie eine der folgenden Optionen aus dem Drop-down-Menü aus: In CSV exportieren oder Nach Excel exportieren.
- Um das gesamte Dashboard zu präsentieren oder zu exportieren, klicken Sie auf das Befehlsmenü ⋮ in der oberen rechten Ecke der Seite und wählen Sie eine der folgenden Optionen: Präsentationsmodus, Als PDF exportieren oder Geplante Berichte (nur Konsolen).

System-Dashboards

Das ExtraHop-System bietet die folgenden integrierten Dashboards, die allgemeine Protokollaktivitäten zum allgemeinen Verhalten und zur Integrität Ihres Netzwerk anzeigen.

System-Dashboards befinden sich in der Standardsammlung System-Dashboards im Dashboard-Dock und können nicht zu einer anderen Sammlung hinzugefügt werden, die mit anderen Benutzern geteilt wird.

System-Dashboards können von jedem Benutzer angezeigt werden, mit Ausnahme von eingeschränkte Benutzer Das Systemnutzungs-Dashboard kann nur von Benutzern mit System- und Zugriffsverwaltung angezeigt werden. Privilegien.

Netzwerkaktivitäts-Dashboard (NPM-Modulzugriff erforderlich)

Finden Sie Top-Talker nach Anwendungsprotokollen (L7) und sehen Sie sich aktuelle Benachrichtigungen an. Weitere Informationen zu Diagrammen in diesem Dashboard finden Sie unter Dashboard zur Netzwerkaktivität.

Dashboard zur Netzwerkleistung (Zugriff auf das NPM-Modul erforderlich)

Identifizieren Sie Verkehrslatenz und Engpässe auf den Ebenen Datenverbindung (L2), Netzwerk (L3) und Transport (L4). Weitere Informationen zu den Diagrammen in diesem Dashboard finden Sie unter Dashboard zur Netzwerkleistung.

Security Hardening-Dashboard (Zugriff auf das NDR-Modul erforderlich)

Überwachen Sie allgemeine Informationen über potenzielle Sicherheitsbedrohungen in Ihrem Netzwerk. Weitere Informationen zu Diagrammen in diesem Dashboard finden Sie unter Dashboard „Sicherheitshärtung“.

Dashboard mit generativen KI-Tools

Prüfen Sie den OpenAI-Verkehr in Ihrem Netzwerk und von internen Endpunkten, die über OpenAI kommunizieren. Weitere Informationen zu den Diagrammen in diesem Dashboard finden Sie unter Dashboard mit generativen KI-Tools.

Active Directory Directory-Dashboard

Verfolgen Sie die Kerberos-Serveraktivität für Active Directory Directory-Benutzer- und Computerkonten sowie für Dienste wie globale Kataloge und Gruppenrichtlinien. Weitere Informationen zu Diagrammen in diesem Dashboard finden Sie unter Active Directory Directory-Dashboard.

Systemintegritäts-Dashboard

Stellen Sie sicher, dass Ihr ExtraHop-System wie erwartet läuft, beheben Sie Probleme und bewerten Sie Bereiche, die die Leistung beeinträchtigen. Weitere Informationen zu Diagrammen in diesem Dashboard finden Sie unter Systemstatus-Dashboard.

Dashboard zur Systemnutzung (System- und Zugriffsadministrationsrechte erforderlich)

Überwachen Sie, wie Benutzer mit Erkennungen, Untersuchungen und Dashboards im ExtraHop-System interagieren. Weitere Informationen zu den Diagrammen in diesem Dashboard finden Sie unter Dashboard zur Systemnutzung.

Dashboard zur Netzwerkaktivität

Mit dem Netzwerkaktivitäts-Dashboard können Sie allgemeine Informationen zur Anwendungsaktivität und -leistung vom Transport über die Anwendungsebenen (L4 bis L7) in Ihrem Netzwerk überwachen.

Jedes Diagramm im Netzwerkaktivitäts-Dashboard enthält Visualisierungen von Netzwerk- und Protokollmetrikdaten, die über ausgewähltes Zeitintervall, nach Region organisiert.

Hinweis: Von einer Konsole aus können Sie das Netzwerkaktivitäts-Dashboard für jede verbundene Standort anzeigen. Der Site-Name wird in der Navigationsleiste angezeigt. Klicken Sie auf den Abwärtspfeil neben dem Namen, um die Anzeige auf andere Sites auszurichten.

Das Netzwerkaktivitäts-Dashboard ist ein integriertes System-Dashboard, das Sie nicht bearbeiten, löschen oder zu einer geteilten Sammlung hinzufügen können. Sie können jedoch ein Diagramm kopieren aus dem Netzwerkaktivitäts-Dashboard und füge es zu einem benutzerdefiniertes Dashboard, oder du kannst eine Kopie des Dashboard erstellen und bearbeiten Sie es, um für Sie relevante Kennzahlen zu überwachen.

Die folgenden Informationen fassen jede Region und ihre Diagramme zusammen.

Überblick über den Verkehr

Beobachten Sie, ob Datenverkehrsengpässe mit einem bestimmten Anwendungsprotokoll oder mit der Netzwerklatenz zusammenhängen. Die Region „Verkehrsübersicht“ enthält die folgenden Diagramme:

- **Diagramm der durchschnittlichen Rate von Netzwerkpaketen nach L7-Protokoll:** Finden Sie das Protokoll mit dem höchsten Volumen an Paketübertragungen über die Anwendungsschicht (L7) während des ausgewählten Zeitintervalls.
- **Rundreisezeit für alle Aktivitäten im Netzwerk:** Die 95. Perzentillinie zeigt Ihnen den oberen Bereich der Zeit, die Pakete benötigt haben, um das Netzwerk zu durchqueren. Wenn dieser Wert über 250 ms liegt, können Netzwerkprobleme die Anwendungsleistung beeinträchtigen. Die Roundtrip-Zeit ist ein Maß für die Zeit zwischen dem Senden eines Paket durch einen Client oder Server und dem Empfang einer Bestätigung.
- **Alerts:** Sehen Sie sich bis zu 40 der zuletzt generierten Warnmeldungen und deren Schweregrad an. Warnungen sind vom Benutzer konfigurierte Bedingungen, die Basiswerte für bestimmte Protokollmetriken festlegen.

Aktive Protokolle

Beobachten Sie, wie die Protokolle, die aktiv auf dem ExtraHop-System kommunizieren, auf die Anwendungsleistung auswirken. Sie können beispielsweise schnell einen Blick auf Diagramme werfen, in denen die Serververarbeitungszeiten und das Verhältnis von Fehlern zu Antworten pro Protokoll angezeigt werden.

Für jedes aktive Protokoll gibt es ein Diagramm. Wenn Sie kein erwartetes Protokoll sehen, kommunizieren Anwendungen möglicherweise nicht über dieses Protokoll für ausgewähltes Zeitintervall.

Weitere Informationen zu Protokollen und zum Anzeigen von Metrikdefinitionen finden Sie in der Referenz zu ExtraHop-Protokollmetriken.

Dashboard zur Netzwerkleistung

Mit dem Network Performance Dashboard können Sie überwachen, wie effektiv Daten über die Datenverbindungs-, Netzwerk- und Transportebenen (L2 — L4) übertragen werden.

Jedes Diagramm im Netzwerk Performance Dashboard enthält Visualisierungen von Netzwerkleistungsdaten, die generiert wurden über ausgewähltes Zeitintervall, nach Region organisiert.

Hinweis: Von einer Konsole aus können Sie das Netzwerkleistungs-Dashboard für jeden verbundenen Standort anzeigen. Der Site-Name wird in der Navigationsleiste angezeigt. Klicken Sie auf den Abwärtspfeil neben dem Namen, um die Anzeige auf andere Sites auszurichten.

Das Netzwerkleistungs-Dashboard ist ein integriertes System-Dashboard, das Sie nicht bearbeiten, löschen oder zu einer gemeinsamen Sammlung hinzufügen können. Sie können jedoch ein Diagramm kopieren aus dem Network Performance Dashboard und füge das Diagramm zu einem benutzerdefiniertes Dashboard, oder du kannst eine Kopie des Dashboard erstellen und bearbeiten Sie das Dashboard, um für Sie relevante Kennzahlen zu überwachen.

Die folgenden Informationen fassen die einzelnen Region zusammen.

Netzwerk-L2-Metriken

Überwachen Sie die Durchsatzraten über die Datenverbindungsschicht (L2) anhand von Bits und Paketen und überwachen Sie die Arten der übertragenen Frames. Sie können auch festlegen, wie viele Daten per Unicast-, Broadcast- oder Multicast-Verteilung an Empfänger gesendet werden.

Netzwerk-L4-Metriken

Überwachen Sie die Latenz der Datenübertragung über die Transportschicht (L4). Zeigen Sie die TCP-Aktivität anhand von Verbindungs-, Anfrage- und Antwortmetriken an. Diese Daten können Aufschluss darüber geben, wie effektiv Daten über die Transportschicht in Ihrem Netzwerk gesendet und empfangen werden.

Leistung des Netzwerks

Überwachen Sie, wie sich die Netzwerkleistung auf Anwendungen auswirkt. Sehen Sie sich den gesamten Netzwerkdurchsatz an, indem Sie den Durchsatz pro Anwendungsprotokoll und das Ausmaß der hohen TCP-Roundtrip-Zeiten überprüfen.

Netzwerk-L3-Metriken

Zeigen Sie den Datendurchsatz auf der Netzwerkebene (L3) an und sehen Sie sich Pakete und Verkehr nach TCP/IP-Protokollen an.

DSCP

Sehen Sie sich eine Aufschlüsselung der Pakete und des Datenverkehrs nach Differentiated Services-Codepunkten an, die Teil der DiffServ-Netzwerkarchitektur sind. Jedes IP-Paket enthält ein Feld, in dem die Priorität angegeben wird, wie das Paket behandelt werden soll. Dies wird als differenzierte Dienste bezeichnet. Die Werte für die Prioritäten werden Codepunkte genannt.

Multicast-Gruppen

Zeigen Sie den Verkehr an, der in einer einzigen Übertragung an mehrere Empfänger gesendet wird, und sehen Sie sich Pakete und Verkehr jeder Empfängergruppe an. Der Multicast-Verkehr in einem Netzwerk ist auf der Grundlage von Zieladressen in Gruppen organisiert.

Dashboard zur Erhöhung der Sicherheit

Mit dem Security Hardening-Dashboard können Sie allgemeine Informationen über potenzielle Sicherheitsbedrohungen in Ihrem Netzwerk überwachen.

Jedes Diagramm im Security Hardening-Dashboard enthält Visualisierungen von Sicherheitsdaten, die über den ausgewähltes Zeitintervall, nach Region organisiert.

Video: Sehen Sie sich die entsprechende Schulung an: Sicherheits-Dashboard

Hinweis: Von einer Konsole aus können Sie das Security Hardening-Dashboard für jeden Paketsensor anzeigen. Klicken Sie in der Navigationsleiste neben dem Namen des Sensor auf den Abwärtspfeil, um das Security Hardening-Dashboard für andere Sensoren anzuzeigen.

Das Security Hardening-Dashboard ist ein integriertes System-Dashboard, das Sie nicht bearbeiten, löschen oder einer gemeinsamen Sammlung hinzufügen können. Sie können jedoch ein Diagramm kopieren aus dem Security Hardening-Dashboard und füge es zu einem benutzerdefiniertes Dashboard, oder du kannst eine Kopie des Dashboard erstellen und bearbeiten Sie es, um Kennzahlen zu überwachen, die für Sie relevant sind.

Die folgenden Informationen fassen jede Region und ihre Diagramme zusammen.

Bedrohungsinformationen

Beobachten Sie die Anzahl der Verbindungen und Transaktionen, die verdächtige Hostnamen, IP-Adressen oder URIs enthalten, die in Bedrohungsinformationen. Klicken Sie in der Legende auf einen blauen Metrikwert oder einen Metriknamen, um nach einer verdächtigen Metrik zu suchen. Eine Detailseite mit einem roten Kamerasymbol wird angezeigt. neben dem verdächtigen Objekt. Klicken Sie auf das rote Kamerasymbol, um mehr über die Quelle der Bedrohungsinformationen zu erfahren.

Hinweis: Bedrohungsanalyse-Metriken zeigen aus einem oder mehreren der folgenden Gründe einen Nullwert an:

- Ihr ExtraHop RevealX-Abonnement beinhaltet keine Bedrohungsinformationen.
- Sie haben Bedrohungsinformationen für Ihr ExtraHop RevealX-System nicht aktiviert.
- Sie haben benutzerdefinierte Bedrohungssammlungen nicht direkt in Ihre hochgeladen Sensoren. Wenden Sie sich an den ExtraHop-Support, wenn Sie Hilfe beim Hochladen einer benutzerdefinierten Bedrohungssammlung auf Ihre von ExtraHop verwaltete Sammlung benötigen Sensoren.
- Es wurden keine verdächtigen Gegenstände gefunden.

TLS - Sitzungen

Beobachten Sie die Anzahl der aktiven TLS-Sitzungen mit Schwache Verschlüsselung Verschlüsselungssammlungen in Ihrem Netzwerk. Sie können sehen, welche Clients und Server an diesen Sitzungen teilnehmen und mit welchen Verschlüsselungssammlungen diese Sitzungen verschlüsselt sind. DES-, 3DES-, MD5-, RC4-, Null-, Anonym- und Export-Cipher Suites gelten als schwach, da sie einen Verschlüsselungsalgorithmus enthalten, der bekanntermaßen anfällig ist. Daten, die mit einer Schwache Verschlüsselung Verschlüsselungssuite verschlüsselt wurden, sind potenziell unsicher.

Sie können auch die Anzahl der TLS-Sitzungen beobachten, die mit TLS v1.0 eingerichtet wurden, und welche Clients an diesen Sitzungen teilnehmen. Bekannte Sicherheitslücken stehen im Zusammenhang mit TLS v1.0. Wenn Sie eine hohe Anzahl von TLS v1.0-Sitzungen haben, sollten Sie erwägen, Server so zu konfigurieren, dass sie die neueste Version von TLS unterstützen.

TLS - Zertifikate

Beobachten Sie, welche TLS-Zertifikate in Ihrem Netzwerk selbstsigniert sind, Platzhalter sind, abgelaufen sind und bald ablaufen. Selbstsignierte Zertifikate werden von der Entität signiert, die das Zertifikat ausstellt, und nicht von einer vertrauenswürdigen Zertifizierungsstelle. Selbstsignierte Zertifikate sind zwar günstiger als Zertifikate, die von einer Zertifizierungsstelle ausgestellt wurden, aber sie sind auch anfällig für Man-in-the-Middle-Angriffe.

Ein Platzhalterzertifikat gilt für alle Subdomains der ersten Ebene eines bestimmten Domänenname. Das Platzhalterzertifikat *.company.com schützt beispielsweise www.company.com, docs.company.com und customer.company.com. Wildcard-Zertifikate sind zwar günstiger als Einzelzertifikate, aber Wildcard-Zertifikate bergen ein höheres Risiko, wenn sie kompromittiert werden, da sie für eine beliebige Anzahl von Domänen gelten können.

Schwachstellen-Scans

Beobachten Sie, welche Geräte Anwendungen und Systeme in Ihrem Netzwerk scannen, um nach Schwachstellen und potenziellen Zielen, wie z. B. hoher Wert Geräten, zu suchen. In der linken Tabelle können Sie erkennen, welche Geräte die meisten Scananfragen senden. Dabei handelt es sich um HTTP-Anfragen, die mit bekannten Scanneraktivitäten verknüpft sind. Im rechten Diagramm können Sie sehen, welche Benutzeragenten mit den Scananfragen verknüpft sind. Der User-Agent kann Ihnen dabei helfen, festzustellen, ob Scananfragen mit bekannten Schwachstellenscannern wie Nessus und Qualys verknüpft sind.

DNS

Beobachten Sie, welche DNS-Server in Ihrem Netzwerk am aktivsten sind und wie viele Reverse-DNS-Lookup-Fehler auf diesen Servern insgesamt aufgetreten sind. Ein Reverse-DNS-Lookup-Fehler tritt auf, wenn ein Server als Antwort auf eine Client-Anfrage nach einem Pointer-Record (PTR) einen Fehler ausgibt. Fehler bei Reverse-DNS-Lookups sind normal, aber eine plötzliche oder stetige Zunahme von Ausfällen auf einem bestimmten Host kann darauf hindeuten, dass ein Angreifer Ihr Netzwerk scannt.

Sie können auch die Anzahl der Adresszuordnungs- und Textdatensatzabfragen in Ihrem Netzwerk beobachten. Ein starker oder plötzlicher Anstieg dieser Arten von Abfragen kann ein Indikator für einen potenziellen DNS-Tunnel sein.

Dashboard mit generativen KI-Tools

Mit dem Generative AI-Dashboard können Sie den Datenverkehr von OpenAI-Tools in Ihrem Netzwerk überwachen.

Jedes Diagramm im Generative AI Tools-Dashboard enthält Visualisierungen des Datenverkehrs im Zusammenhang mit dem OpenAI-Cloud-Dienst für Tools wie ChatGPT. Traffic anzeigen, der während eines generiert wurde ausgewähltes Zeitintervall, nach Region organisiert.

Hinweis: Von einer Konsole aus können Sie das Generative AI Tools-Dashboard für jede verbundene Standort anzeigen. Der Site-Name wird in der Navigationsleiste angezeigt. Klicken Sie auf den Abwärtspfeil neben dem Namen, um die Anzeige auf andere Sites auszurichten.

Das Generative AI Tools-Dashboard ist ein integriertes System-Dashboard, und Sie können System-Dashboards nicht bearbeiten, löschen oder zu einer Sammlung hinzufügen. Sie können jedoch ein Diagramm kopieren aus dem Generative AI Tools-Dashboard und füge das Diagramm zu einem benutzerdefiniertes Dashboard, oder du kannst eine Kopie des Dashboard erstellen und bearbeiten Sie das Dashboard, um für Sie relevante Kennzahlen zu überwachen.

Die folgenden Informationen fassen jede Region und ihre Diagramme zusammen.

Generative KI-Tools

Überwachen Sie den in Ihrem Netzwerk beobachteten Datenverkehr zu OpenAI-basierten Tools. Erfahren Sie, wann der Verkehr auftrat, wie viele Daten übertragen wurden und welche internen Endpunkte beteiligt waren.

Active Directory Directory-Dashboard

Mit dem Active Directory Directory-Dashboard können Sie die Kerberos-Serveraktivität für Active Directory Directory-Benutzer- und Computerkonten sowie für Dienste wie globale Katalog- und Gruppenrichtlinien verfolgen.

Jedes Diagramm im Active Directory Directory-Dashboard enthält Visualisierungen von Active Directory-Kontodaten, die über den ausgewähltes Zeitintervall, nach Region organisiert.

Das Active Directory Directory-Dashboard ist ein integriertes System-Dashboard, das Sie nicht bearbeiten, löschen oder einer gemeinsamen Sammlung hinzufügen können. Sie können jedoch ein Diagramm kopieren aus dem Active Directory Directory-Dashboard und fügen Sie es zu einem benutzerdefiniertes Dashboard, oder du kannst eine Kopie des Dashboard erstellen und bearbeiten Sie es, um Kennzahlen zu überwachen, die für Sie relevant sind.

Hinweis: Von einer Konsole aus können Sie das Active Directory Directory-Dashboard für jeden verbundenen Standort anzeigen. Der Name der Standort wird in der Navigationsleiste angezeigt. Klicken Sie auf den Abwärtspfeil neben dem Namen, um die Anzeige auf andere Websites zu lenken.

Die folgenden Informationen fassen jede Region und ihre Diagramme zusammen.

Zusammenfassung des Kontos

Beachten Sie die Anzahl der Active Directory Directory-Konten in Ihrer Umgebung in den folgenden Diagrammen:

- **Konten insgesamt:** Gesamtzahl der Benutzerkonten und Computerkonten.
- **Privilegierte Konten:** Gesamtzahl der privilegierten Konten, die sich erfolgreich angemeldet haben, bei denen ein Anmeldefehler aufgetreten ist und die eine Servicezugriffsanforderung gesendet haben.

Fehler bei der Authentifizierung

Beachten Sie die Anzahl der Active Directory Directory-Konten mit Authentifizierungsfehlern in den folgenden Diagrammen:

- **Fehler im Benutzerkonto:** Gesamtzahl der Anmeldefehler Benutzerkonto aufgrund ungültiger Passwörter, abgelaufener Passwörter und deaktivierter Konten. Wird als Liniendiagramm und Listendiagramm angezeigt.
- **Fehler beim Computerkonto:** Gesamtzahl der Fehler bei der Anmeldung bei Computerkonten aufgrund ungültiger Passwörter, abgelaufener Passwörter und deaktivierter Konten. Wird als Liniendiagramm und Listendiagramm angezeigt.
- **Kontofehler:** Gesamtzahl der Fehler für jeden Kontotyp aufgrund von Kontosperrungen und Zeitfehlern. Wird als Liniendiagramm und Listendiagramm angezeigt.

Details zum Authentifizierungsfehler

Beachten Sie die Details zu Active Directory Directory-Konten, bei denen Authentifizierungsfehler aufgetreten sind, in den folgenden Diagrammen:

- **Benutzerkonten:** Benutzernamen, die mit Benutzerkonten verknüpft sind, bei denen die Anmeldung fehlgeschlagen ist. In diesem Diagramm wird auch angezeigt, wie oft bei jedem Benutzerkonto ein Fehler aufgrund eines ungültigen Kennworts oder eines abgelaufenen Kontos aufgetreten ist.
- **Computerkonten:** Client-IP-Adressen und Hostnamen, die mit Benutzerkonten verknüpft sind, die sich nicht anmelden konnten. In diesem Diagramm wird auch angezeigt, wie oft bei jedem Benutzerkonto ein Fehler aufgrund eines ungültigen Kennworts oder eines abgelaufenen Kontos aufgetreten ist.

Service zur Ticketgewährung

Beachten Sie die Transaktionsdaten, die mit dem Kerberos-Ticketgewährungsdienst verknüpft sind, in den folgenden Diagrammen:

- **Transaktionen:** Gesamtzahl der Serviceticket-Anfragen und Anzahl unbekannter SPN-Fehler (Service Principal Name).
- **Transaktionen:** Gesamtzahl der Serviceticket-Anfragen.
- **Unbekannte SPN-Fehler von SPN:** Anzahl der unbekannten SPN-Fehler, die vom SPN aufgeführt werden, der den Fehler gesendet hat.
- **Unbekannte SPN-Fehler vom Client:** Anzahl der unbekannten SPN-Fehler, die von dem Client aufgeführt wurden, der den Fehler erhalten hat.
- **Gesamtzahl unbekannter SPN-Fehler:** Gesamtzahl unbekannter SPN-Fehler.

Gruppenrichtlinie

Beachten Sie die SMB-Transaktionsdaten, die der Gruppenrichtlinie zugeordnet sind, in den folgenden Diagrammen:

- **Transaktionen:** Gesamtzahl der Gruppenrichtlinienantworten und der Gruppenrichtlinienfehler.
- **Transaktionen:** Gesamtzahl der Gruppenrichtlinienantworten und der Gruppenrichtlinienfehler, zusätzlich zur Serververarbeitungszeit, die benötigt wurde, um das erste Paket als Antwort auf das letzte Paket der Gruppenrichtlinienanforderung zu senden.

LDAP

Beobachten Sie die LDAP-Transaktionsdaten anhand der folgenden Diagramme:

- **Transaktionen:** Gesamtzahl der LDAP-Antworten und -Fehler.
- **Transaktionen:** Gesamtzahl der LDAP-Antworten und -Fehler, zusätzlich zur Serververarbeitungszeit, die benötigt wurde, um das erste Paket als Antwort nach dem Empfang des letzten Paket der Anfrage zu senden.
- **Unsichere LDAP-Anmeldeinformationen :** Gesamtzahl der Klartext-Bindungsanforderungen. Wird als Liniendiagramm und Listendiagramm angezeigt.

Globaler Katalog

Beachten Sie die Transaktionsdaten, die dem globalen Katalog zugeordnet sind, in den folgenden Diagrammen:

- **Transaktionen:** Gesamtzahl der Antworten und Fehler im globalen Katalog.
- **Transaktionen:** Gesamtzahl der globalen Katalogantworten und Fehler, zusätzlich zu der Serververarbeitungszeit, die benötigt wurde, um das erste Paket als Antwort nach dem Empfang des letzten Paket der globalen Kataloganforderung zu senden.

DNS-Dienstaufzeichnungen

Beachten Sie die Transaktionsdaten der DNS-Dienstdatensätze in den folgenden Diagrammen:

- **Transaktionen:** Gesamtzahl der Antworten und Fehler im Servicedatensatz.
- **Transaktionen:** Gesamtzahl der Antworten und Fehler im Servicedatensatz, zusätzlich zu der Serververarbeitungszeit, die benötigt wurde, um das erste Paket als Antwort nach dem Empfang des letzten Paket der Anfrage zu senden.

Systemstatus-Dashboard

Das Systemstatus-Dashboard bietet eine große Sammlung von Diagrammen, mit denen Sie sicherstellen können, dass Ihr ExtraHop-System wie erwartet läuft, Probleme zu beheben und Bereiche zu bewerten, die die Leistung beeinträchtigen. Sie können beispielsweise die Anzahl der vom ExtraHop-System verarbeiteten Pakete überwachen, um sicherzustellen, dass Pakete kontinuierlich erfasst werden.

Jedes Diagramm im Network Performance Dashboard enthält Visualisierungen der Systemleistungsdaten, die über den ausgewähltes Zeitintervall, nach Region organisiert.

Das Systemstatus-Dashboard ist ein integriertes System-Dashboard, das Sie nicht bearbeiten, löschen oder einer gemeinsamen Sammlung hinzufügen können. Sie können jedoch ein Diagramm kopieren aus dem Systemstatus-Dashboard und füge es zu einem benutzerdefiniertes Dashboard, oder du kannst eine Kopie des Dashboard erstellen und bearbeiten Sie es, um Kennzahlen zu überwachen, die für Sie relevant sind.

Hinweis: Auf der Seite mit den Administrationseinstellungen finden Sie auch Statusinformationen und Diagnosetools für alle ExtraHop-Systeme.

Navigieren Sie zum Systemstatus-Dashboard

Rufen Sie die Seite Systemstatus auf, indem Sie auf das Symbol Systemeinstellungen klicken oder durch Anklicken **Armaturenbretter** von oben auf der Seite. Das Systemstatus-Dashboard zeigt automatisch Informationen über das ExtraHop-System an, mit dem Sie verbunden sind. Wenn Sie das Systemstatus-Dashboard von einer Konsole aus aufrufen, können Sie oben auf der Seite auf die Site-Auswahl klicken, um Daten für eine bestimmte Standort oder für alle Sites in Ihrer Umgebung anzuzeigen.

Die Diagramme auf dem Systemstatus-Dashboard sind in die folgenden Abschnitte unterteilt:

Gerätesuche

Sehen Sie sich die Gesamtzahl der Geräte in Ihrem Netzwerk an. Sehen Sie, welche Geräte erkannt wurden und wie viele dieser Geräte derzeit aktiv sind.

Datenfeed

Beurteilen Sie die Effizienz des Datenerfassungsprozesses über Kabel anhand von Diagrammen zu Durchsatz, Paketrate, Desynchronisierungen und Erfassungsausfällen.

Rekorde

Zeigt die Gesamtanzahl der Datensätze an, die an einen angehängten Recordstore gesendet werden..

Auslöser

Überwachen Sie die Auswirkungen von Triggern auf Ihr ExtraHop-System. Sehen Sie, wie oft Trigger ausgeführt werden, wie oft sie ausfallen und welche Trigger Ihre CPU am stärksten belasten.

Öffnen Sie Data Stream und Recordstore

Verfolgen Sie die Aktivität von Open-Data-Stream-Übertragungen (ODS) zu und von Ihrem System. Zeigen Sie die Gesamtzahl der Remote-Verbindungen, den Nachrichtendurchsatz und Details zu bestimmten Remote-Zielen an.

TLS-Zertifikate

Überprüfen Sie die Statusinformationen für alle TLS-Zertifikate auf Ihrem ExtraHop-System.

Paketerfassung aus der Ferne (RPCAP)

Zeigen Sie die Anzahl der Pakete und Frames an, die von RPCAP-Peers gesendet und empfangen werden.

Fortgeschrittene Gesundheitsmetriken

Verfolgen Sie die Heap-Zuweisung im Zusammenhang mit der Datenerfassung, dem Systemdatenspeicher, Triggern und Fernübertragungen. Überwachen Sie den Schreibdurchsatz, die Größe des Arbeitssatzes und Auslöser Sie Aktivitäten im Systemdatenspeicher aus.

Gerätesuche

Das Gerätesuche Der Abschnitt des Systemstatus-Dashboards bietet einen Überblick über die Gesamtzahl der Geräte in Ihrem Netzwerk. Sehen Sie, welche Gerätetypen angeschlossen sind und wie viele dieser Geräte derzeit aktiv sind.

Das Gerätesuche Abschnitt enthält die folgenden Diagramme:

- Aktive Geräte

Aktive Geräte

Ein Flächendiagramm, das die Anzahl der L2-, L3-, Gateway- und benutzerdefinierten Geräte anzeigt, die während des ausgewählten Zeitintervalls aktiv im Netzwerk kommuniziert haben. Neben dem Flächendiagramm zeigt ein Wertdiagramm die Anzahl der L2-, L3-, Gateway- und benutzerdefinierten Geräte an, die im ausgewählten Zeitintervall aktiv waren.

Wie diese Informationen Ihnen helfen können

Überwachen Sie dieses Diagramm, nachdem Sie Änderungen an der SPAN-Konfiguration vorgenommen haben, um sicherzustellen, dass keine unbeabsichtigten Folgen auftreten, die das ExtraHop-System in einen schlechten Zustand versetzen könnten. Beispielsweise kann die versehentliche Einbindung eines Netzwerk die Kapazität der ExtraHop-Systemfunktionen belasten, da mehr Ressourcen verbraucht und mehr Paketverarbeitung erforderlich ist, was zu einer schlechten Leistung führt. Vergewissern Sie sich, dass das ExtraHop-System die erwartete Anzahl aktiver Geräte überwacht.

Datenfeed

Das Datenfeed In einem Abschnitt des Systemstatus-Dashboards können Sie anhand von Diagrammen zu Durchsatz, Paketrate, Desynchronisierungen und Erfassungsabbrüchen die Effizienz des Datenerfassungsprozesses über Kabel beobachten.

Das Datenfeed Abschnitt enthält die folgenden Diagramme:

- Durchsatz
- Durchsatz nach Schnittstelle
- Paket-Rate
- Paketrate nach Schnittstelle
- Paketfehler nach Schnittstelle
- Analysierte Ströme
- Desynchronisierungen
- Drop-Rate erfassen
- Auf die Festplatte geschriebene Metriken (Log-Skala)
- Lookback-Schätzungen für metrische Daten

Durchsatz
Ein Flächendiagramm, das den Durchsatz eingehender Pakete im ausgewählten Zeitintervall darstellt, ausgedrückt in Byte pro Sekunde. Das Diagramm zeigt Durchsatzinformationen für analysierte und gefilterte Pakete sowie L2- und L3-Duplikate an.

Wie diese Informationen Ihnen helfen können

Das Überschreiten der Produktgrenzwerte kann zu Datenverlust führen. Eine hohe Durchsatzrate kann beispielsweise dazu führen, dass Pakete an der Span-Quelle oder an einem Span-Aggregator verworfen werden. In ähnlicher Weise kann eine große Anzahl von L2- oder L3-Duplikaten auch auf ein Problem an der Span-Quelle oder dem Span-Aggregator hinweisen und zu verzerrten oder falschen Metriken führen.

Die akzeptable Rate von Byte pro Sekunde hängt von Ihrem Produkt ab. Beziehen Sie sich auf die Datenblatt für ExtraHop-Sensoren um herauszufinden, welche Grenzwerte für Ihr ExtraHop-System gelten, und um festzustellen, ob die Byte-Rate pro Sekunde zu hoch ist.

Durchsatz nach Schnittstelle
Ein Liniendiagramm, das den Durchsatz eingehender Pakete darstellt und von jeder auf dem Sensor konfigurierten Schnittstelle aufgeführt ist. Der Durchsatz wird während des ausgewählten Zeitintervalls in Byte pro Sekunde ausgedrückt. Das Diagramm zeigt Durchsatzinformationen für analysierte und gefilterte Pakete sowie L2- und L3-Duplikate an.

Wenn Sie mehrere Sensoren von einer ExtraHop-Konsole aus betrachten, zeigt das Diagramm die aggregierte durchschnittliche Übertragungsrate von Schnittstellen mit derselben Nummer.

Wie diese Informationen Ihnen helfen können

Das Überschreiten der Produktschwellenwerte kann zu Datenverlust führen. Beispielsweise kann eine hohe Durchsatzrate dazu führen, dass Pakete an der Span-Quelle oder an einem Span-Aggregator verloren gehen. In ähnlicher Weise können große Mengen an L2- oder L3-Duplikaten auch auf ein Problem an der Span-Quelle oder am Span-Aggregator hinweisen und zu verzerrten oder falschen Metriken führen.

Die akzeptable Rate von Paket pro Sekunde hängt von Ihrem Produkt ab. Beziehen Sie sich auf die Datenblatt für ExtraHop-Sensoren um herauszufinden, welche Grenzwerte für Ihr ExtraHop-System gelten und um festzustellen, ob die Rate der Pakete pro Sekunde zu hoch ist.

Überwachen Sie dieses Diagramm, um Probleme mit dem Paketdurchsatz auf detaillierter Ebene zu beheben und bei Bedarf Anpassungen der Schnittstellenkonfiguration vorzunehmen.

Paket-Rate
Ein Flächendiagramm, das die Rate eingehender Pakete, ausgedrückt in Paketen pro Sekunde, anzeigt. In der Tabelle werden Informationen zur Paketrate für analysierte und gefilterte Pakete sowie für L2- und L3-Duplikate angezeigt.

Wie diese Informationen Ihnen helfen können
Das Überschreiten der Produktgrenzwerte kann zu Datenverlust führen. Eine hohe Paketrate kann beispielsweise dazu führen, dass Pakete an der Span-Quelle oder an einem Span-Aggregator verworfen

werden. In ähnlicher Weise können große Mengen von L2- oder L3-Duplikaten auch auf ein Problem an der Span-Quelle oder dem Span-Aggregator hinweisen und zu verzerrten oder falschen Metriken führen.

Die akzeptable Paketrate pro Sekunde hängt von Ihrem Produkt ab. Weitere Informationen finden Sie in Datenblatt für ExtraHop-Sensoren um herauszufinden, welche Grenzwerte für Ihr ExtraHop-System gelten, und um festzustellen, ob die Rate der Pakete pro Sekunde zu hoch ist.

Paketrate nach Schnittstelle
Ein Liniendiagramm, das die Rate eingehender Pakete anzeigt, und ein Säulendiagramm, das die Anzahl der verworfenen Pakete anzeigt, aufgeführt nach jeder auf dem Sensor konfigurierten Schnittstelle. Die Paketrate wird in Paketen ausgedrückt, die während des ausgewählten Zeitintervalls pro Sekunde empfangen wurden. Das Diagramm zeigt Paketrateninformationen für analysierte und gefilterte Pakete sowie L2 - und L3-Duplikate an.

Wenn Sie mehrere Sensoren von einer ExtraHop-Konsole aus betrachten, zeigt das Diagramm die aggregierte Paketrate und die Anzahl der Pakete, die von Schnittstellen mit derselben Nummer verworfen wurden.

Wie diese Informationen Ihnen helfen können

Das Überschreiten der Produktschwellenwerte kann zu Datenverlust führen. Beispielsweise kann eine hohe Paketrate dazu führen, dass Pakete an der Span-Quelle oder an einem Span-Aggregator verloren gehen. In ähnlicher Weise können große Mengen an L2- oder L3-Duplikaten auch auf ein Problem an der Span-Quelle oder am Span-Aggregator hinweisen und zu verzerrten oder falschen Metriken führen.

Die akzeptable Rate von Paket pro Sekunde hängt von Ihrem Produkt ab. Beziehen Sie sich auf die Datenblatt für ExtraHop-Sensoren um herauszufinden, welche Grenzwerte für Ihr ExtraHop-System gelten und um festzustellen, ob die Rate der Pakete pro Sekunde zu hoch ist.

Überwachen Sie dieses Diagramm, um Probleme mit der Paketrate auf detaillierter Ebene zu beheben und bei Bedarf Anpassungen der Schnittstellenkonfiguration vorzunehmen.

Paketfehler nach Schnittstelle
Ein Liniendiagramm, das die Anzahl der während des ausgewählten Zeitintervalls empfangenen Paketfehler anzeigt und von jeder auf dem Sensor konfigurierten Schnittstelle aufgeführt wird. Das Diagramm zeigt Paketfehlerinformationen für analysierte und gefilterte Pakete sowie L2- und L3-Duplikate an.

Wenn Sie mehrere Sensoren von einer ExtraHop-Konsole aus betrachten, zeigt das Diagramm die aggregierte Anzahl von Paketfehlern, die auf Schnittstellen mit derselben Anzahl aufgetreten sind.

Wie diese Informationen Ihnen helfen können

Überwachen Sie dieses Diagramm, um Paketfehler auf granularer Ebene zu beheben. Vermehrte Paketfehler können zu Datenverlust führen. Stellen Sie sicher, dass Pakete wie erwartet gesendet werden, und nehmen Sie bei Bedarf Anpassungen der Schnittstellenkonfiguration vor.

Analysierte Ströme
Ein Liniendiagramm, das die Anzahl der Flows anzeigt, die das ExtraHop-System im ausgewählten Zeitintervall analysiert hat. Das Diagramm zeigt auch, wie viele unidirektionale Flüsse im gleichen Zeitraum aufgetreten sind. Neben dem Liniendiagramm wird in einem Wertdiagramm die Gesamtzahl der analysierten und unidirektionalen Flüsse angezeigt, die im ausgewählten Zeitintervall aufgetreten sind. Ein Fluss ist ein Satz von Paketen, die Teil einer Transaktion zwischen zwei Endpunkten über ein Protokoll wie TCP, UDP oder ICMP sind.

Wie diese Informationen Ihnen helfen können
Das Überschreiten der Produktgrenzwerte kann zu Datenverlust führen. Beispielsweise könnte eine hohe Anzahl analysierter Datenflüsse dazu führen, dass Pakete an der Span-Quelle oder an einem Span-Aggregator verworfen werden.

Desynchronisierungen
Ein Liniendiagramm, das das Auftreten systemweiter Desynchronisierungen auf dem ExtraHop-System im ausgewählten Zeitintervall anzeigt. Neben dem Liniendiagramm wird in einem Wertdiagramm die Gesamtzahl der Desynchronisierungen angezeigt, die im ausgewählten Zeitintervall aufgetreten sind. Eine Desynchronisierung liegt vor, wenn der ExtraHop-Datenfeed ein TCP-Paket verwirft und daher nicht mehr mit einer TCP-Verbindung synchronisiert wird.

Wie diese Informationen Ihnen helfen können
Eine große Anzahl von Desynchronisierungen kann auf verworfene Pakete auf der Überwachungsschnittstelle, dem SPAN oder dem Netzwerk-Tap hinweisen.

Wenn Anpassungen an Ihrem SPAN eine große Anzahl von Desynchronisierungen nicht reduzieren, wenden Sie sich an ExtraHop-Unterstützung.

Verkürzte Pakete
Ein Liniendiagramm, das das Auftreten von gekürzten Paketen auf dem ExtraHop-System im ausgewählten Zeitintervall anzeigt. Neben dem Liniendiagramm wird in einem Wertdiagramm die Gesamtzahl der gekürzten Pakete angezeigt, die im ausgewählten Zeitintervall aufgetreten sind. Ein abgeschnittenes Paket liegt vor, wenn die tatsächliche Gesamtlänge des Paket geringer ist als die Gesamtlänge, die im IP-Header angegeben ist.

Wie diese Informationen Ihnen helfen können
Verkürzte Pakete deuten möglicherweise auf Paket Slicing hin. Ein Sensor verwirft alle abgeschnittenen Pakete, die er empfängt, was dazu führen kann Desynchronisierungen auftreten.
Drop-Rate erfassen
Ein Liniendiagramm, das den Prozentsatz der Pakete anzeigt, die während des ausgewählten Zeitintervalls an der Netzwerkkartenschnittstelle eines ExtraHop-Systems verworfen wurden.

Wie diese Informationen Ihnen helfen können
Paketverluste treten häufig auf, wenn Sensorschwellenwerte überschritten werden. Beziehen Sie sich auf die Datenblatt für ExtraHop-Sensoren um herauszufinden, wo die Grenzen Ihres ExtraHop-Systems liegen.
Ladung erfassen
Ein Liniendiagramm, das den Prozentsatz der Zyklen auf dem ExtraHop-System anzeigt, die von aktiven Capture-Threads im ausgewählten Zeitintervall verbraucht wurden, basierend auf der gesamten Capture-Thread-Zeit. Klicken Sie auf das zugehörige Durchschnittliche Aufnahmelast Diagramm, um nach Threads aufzuschlüsseln und festzustellen, welche Threads die meisten Ressourcen verbrauchen.

Wie diese Informationen Ihnen helfen können
Achten Sie auf Spitzen oder ein steigendes Wachstum der Fanglast, um zu überwachen, ob Sie sich den Sensorgrenzwerten nähern. Beziehen Sie sich auf die Datenblatt für ExtraHop-Sensoren um die Grenzen Ihres ExtraHop-Systems zu entdecken.
Auf die Festplatte geschriebene Metriken (Log-Skala)
Ein Liniendiagramm, das den Speicherverbrauch von Messwerten, die während des ausgewählten Zeitintervalls auf die Festplatte geschrieben wurden, in Byte pro Sekunde anzeigt. Da zwischen den Datenpunkten ein großer Bereich besteht, wird die Festplattennutzung in logarithmischer Skala angezeigt.

Wie diese Informationen Ihnen helfen können
Es ist wichtig, dass Sie sich darüber im Klaren sind, wie viel Speicherplatz die Metriken in Ihrem Datenspeicher beanspruchen. Die Größe des Speicherplatzes in Ihrem Datenspeicher wirkt sich auf die Menge des verfügbaren Lookbacks aus. Wenn einige Metriken zu viel Speicherplatz beanspruchen, können Sie die zugehörigen Trigger untersuchen, um zu sehen, ob Sie den Auslöser ändern können, um ihn effizienter zu gestalten.

Lookback-Schätzungen für metrische Daten
Zeigt die geschätzten Datenspeicher-Lookback-Metriken auf dem ExtraHop-System an. Lookback-Metriken sind in Zeitintervallen von 24 Stunden, 1 Stunde, 5 Minuten und 30 Sekunden verfügbar, basierend auf der Schreibdurchsatzrate, die in Byte pro Sekunde ausgedrückt wird.

Wie diese Informationen Ihnen helfen können

Anhand dieser Tabelle können Sie ermitteln, wie weit Sie historische Daten für bestimmte Zeitintervalle zurückverfolgen können. Beispielsweise können Sie Daten in Intervallen von 1 Stunde bis zu 9 Tagen nachschlagen.

Rekorde
Die Rekorde In einem Bereich des Systemstatus-Dashboards können Sie die Effizienz der Kabeldatenerfassung anhand von Diagrammen zur Anzahl der Datensatz und zum Durchsatz beobachten.

Die Datenfeed Dieser Abschnitt enthält die folgenden Diagramme:

- Anzahl der Datensätze
- Durchsatz aufzeichnen

Anzahl der Datensätze
Ein Liniendiagramm, das die Anzahl der Datensätze anzeigt, die im ausgewählten Zeitintervall an einen Recordstore gesendet wurden. Neben dem Liniendiagramm wird in einem Wertdiagramm die Gesamtzahl der im ausgewählten Zeitintervall gesendeten Datensätze angezeigt.

Wie diese Informationen Ihnen helfen können

Eine extrem hohe Anzahl von Datensätzen, die an einen Recordstore gesendet werden, kann zu langen Nachrichtenwarteschlangen und verworfenen Nachrichten im Recordstore führen. Sehen Sie sich Diagramme in der Öffnen Sie Data Stream und Recordstore Im Abschnitt Systemintegritäts-Dashboard finden Sie weitere Informationen zu Recordstore-Übertragungen.

Durchsatz aufzeichnen
Ein Liniendiagramm, das die Anzahl der Datensätze in Byte anzeigt, die an einen Recordstore gesendet wurden. Neben dem Liniendiagramm wird in einem Wertdiagramm die Gesamtmenge der im ausgewählten Zeitintervall gesendeten Datensätze in Byte angezeigt.

Wie diese Informationen Ihnen helfen können

Dieses Diagramm spiegelt keine Größenanpassungen auf der Grundlage von Komprimierung oder Datendeduplikation wider und sollte nicht zur Schätzung der Recordstore-Kosten verwendet werden. Ein extrem hoher Datensatzdurchsatz kann zu langen Warteschlangenlängen und verworfenen Nachrichten im Recordstore führen. Sehen Sie sich Diagramme in der Öffnen Sie Data Stream und Recordstore Im Abschnitt Systemintegritäts-Dashboard finden Sie weitere Informationen zu Recordstore-Übertragungen.

Auslöser
Die Auslöser In einem Bereich des Systemstatus-Dashboards können Sie die Auswirkungen von Triggern auf Ihr System überwachen. Sehen Sie, wie oft Trigger ausgeführt werden, wie oft sie ausfallen und welche Trigger Ihre CPU am stärksten belasten.

Die Auslöser Dieser Abschnitt enthält die folgenden Diagramme:

- Last auslösen
- Triggerverzögerung
- Trigger wird ausgeführt und gelöscht
- Einzelheiten zum Auslöser
- Laden nach Trigger auslösen
- Trigger wird von Trigger ausgeführt
- Ausnahmen nach Trigger auslösen

- Zyklen nach Thread auslösen

Last auslösen
Ein Liniendiagramm, das den Prozentsatz der CPU-Zyklen anzeigt , die Triggerprozessen zugewiesen wurden und während des ausgewählten Zeitintervalls von Triggern verbraucht wurden.

Wie diese Informationen Ihnen helfen können
Achten Sie auf Spitzen oder ein steigendes Wachstum der Triggerlast, insbesondere nach dem Erstellen eines neuen Auslöser oder dem Ändern eines vorhandenen Auslöser. Wenn Sie eine der beiden Bedingungen bemerken, sehen Sie sich die Laden nach Trigger auslösen Diagramm, um zu sehen, welche Trigger die meisten Ressourcen verbrauchen.
Triggerverzögerung
Ein Säulendiagramm, das die maximalen Triggerverzögerungen, die während des ausgewählten Zeitintervalls aufgetreten sind, in Millisekunden anzeigt. Neben dem Säulendiagramm wird in einem Wertdiagramm die längste Triggerverzögerung angezeigt, die im ausgewählten Zeitintervall aufgetreten ist. Eine Triggerverzögerung ist die Zeitspanne zwischen der Erfassung eines Triggerereignisses und der Erstellung eines Trigger-Threads für das Ereignis.

Wie diese Informationen Ihnen helfen können

Lange Auslöseverzögerungen können auf Verarbeitungsprobleme hinweisen. Sehen Sie sich die Ausnahmen nach Trigger auslösenund Laden nach Trigger auslösen Diagramme, um zu sehen, welcher Auslöser die meisten unbehandelten Ausnahmen auslöst und welcher die meisten Ressourcen verbraucht.

Trigger wird ausgeführt und gelöscht
Ein Linien- und Säulendiagramm, in dem das Liniendiagramm anzeigt, wie oft Trigger ausgeführt wurden, und das dazugehörige Säulendiagramm zeigt, wie oft Trigger im ausgewählten Zeitintervall gelöscht wurden. Neben dem Linien- und Säulendiagramm zeigt ein Wertdiagramm die Gesamtzahl der Triggerausführungen und Drops an, die im ausgewählten Zeitintervall aufgetreten sind. Diese Diagramme bieten einen allgemeinen Überblick über alle Trigger, die derzeit auf dem ExtraHop-System ausgeführt werden.

Wie diese Informationen Ihnen helfen können
Suchen Sie im Linien- und Säulendiagramm nach Spitzen und untersuchen Sie alle Auslöser, die zu dem Anstieg geführt haben. Möglicherweise stellen Sie beispielsweise eine erhöhte Aktivität fest, wenn ein Auslöser geändert oder ein neuer Auslöser aktiviert wurde. Sehen Sie sich das an Trigger wird von Trigger ausgeführt Diagramm, um zu sehen , welche Trigger am häufigsten ausgeführt werden.
Einzelheiten zum Auslöser
Ein Listendiagramm, das einzelne Trigger und die Anzahl der Zyklen, Ausführungen und Ausnahmen anzeigt, die den einzelnen Triggern im ausgewählten Zeitintervall zugewiesen wurden. Standardmäßig ist die Liste der Trigger in absteigender Reihenfolge nach Triggerzyklen sortiert.

Wie diese Informationen Ihnen helfen können
Identifizieren Sie, welche Auslöser die meisten Zyklen verbrauchen. Trigger, die zu häufig ausgeführt werden oder auf andere Weise mehr Zyklen verbrauchen, als sie sollten, können mehr Quellen als nötig zugewiesen werden. Stellen Sie sicher, dass jeder überaktive Auslöser nur der spezifischen Quelle zugewiesen ist, aus der Sie Daten sammeln müssen.
Laden nach Trigger auslösen
Ein Liniendiagramm, das den Prozentsatz der CPU-Zyklen anzeigt , die Triggerprozessen zugewiesen sind und während des ausgewählten Zeitintervalls von Triggern verbraucht wurden, aufgelistet nach Triggernamen.

Wie diese Informationen Ihnen helfen können
Identifizieren Sie, welche Auslöser die meisten Zyklen verbrauchen. Trigger, die mehr Zyklen verbrauchen, als sie sollten, können mehr Quellen als nötig zugewiesen werden. Stellen Sie sicher, dass jeder überaktive Auslöser nur der spezifischen Quelle zugewiesen ist, aus der Sie Daten sammeln müssen.

Trigger wird von Trigger ausgeführt
Ein Liniendiagramm, das anzeigt, wie oft jeder aktive Auslöser im ausgewählten Zeitintervall ausgeführt wurde.

Wie diese Informationen Ihnen helfen können
Suchen Sie nach Triggern, die häufiger als erwartet ausgeführt werden, was darauf hindeuten könnte, dass der Auslöser zu breit zugewiesen ist. Ein Auslöser, der allen Anwendungen oder allen Geräten zugewiesen ist, kann hohe Leistungseinbußen nach sich ziehen. Ein Auslöser, der einer erweiterten Gerätegruppe zugewiesen ist, sammelt möglicherweise Messwerte, die Sie nicht möchten. Um die Auswirkungen auf die Leistung zu minimieren, sollte ein Auslöser nur den spezifischen Quellen zugewiesen werden, aus denen Sie Daten sammeln müssen.

Eine hohe Aktivität kann auch darauf hindeuten, dass ein Auslöser härter arbeitet, als er muss. Beispielsweise kann ein Auslöser bei mehreren Ereignissen ausgeführt werden, bei denen es effizienter wäre, separate Trigger zu erstellen, oder ein Trigger-Skript entspricht möglicherweise nicht den empfohlenen Skriptrichtlinien, wie in der Leitfaden mit bewährten Methoden für Trigger.

Ausnahmen nach Trigger auslösen
Ein Liniendiagramm, das die Anzahl der unbehandelten Ausnahmen, sortiert nach Auslöser, anzeigt, die im ausgewählten Zeitintervall auf dem ExtraHop-System aufgetreten sind.

Wie diese Informationen Ihnen helfen können
Trigger-Ausnahmen sind die Hauptursache für Leistungsprobleme bei Triggern. Wenn dieses Diagramm darauf hinweist, dass eine Trigger-Ausnahme aufgetreten ist, sollten Sie den Auslöser sofort untersuchen.
Zyklen nach Thread auslösen
Ein Liniendiagramm, das die Anzahl der Triggerzyklen anzeigt, die von Triggern für einen Thread verbraucht wurden.

Wie diese Informationen Ihnen helfen können
Triggerverluste können auftreten, wenn der Verbrauch eines Threads erheblich höher ist als der der anderen, auch wenn der Thread-Verbrauch gering ist. Achten Sie auf einen gleichmäßigen Zyklusverbrauch zwischen den Threads.

Öffnen Sie Data Stream und Recordstore
Im Bereich Open Data Stream (ODS) und Recordstore des Systems Health Dashboard können Sie die Aktivitäten von ODS- und Recordstore-Übertragungen zu und von Ihrem System verfolgen. Sie können auch die Gesamtzahl der Remoteverbindungen, den Nachrichtendurchsatz und Details zu bestimmten Remote-Zielen anzeigen.

Die Open Data Stream (ODS) und Recordstore Dieser Abschnitt enthält die folgenden Diagramme:

- Nachrichtendurchsatz
- Gesendete Nachrichten
- Nach Remotetyp verworfene Nachrichten
- Fehler beim Senden von Nachrichten
- Verbindungen
- Länge der Exremote-Nachrichtenwarteschlange nach Ziel
- Länge der Nachrichtenwarteschlange nach Remote-Typ ausschließen
- Einzelheiten zum Ziel

Nachrichtendurchsatz
Ein Liniendiagramm, das den Durchsatz von Fernmeldungsdaten in Byte anzeigt. Neben dem Liniendiagramm zeigt ein Wertdiagramm die durchschnittliche Durchsatzrate von Fernmeldungsdaten über das ausgewählte Zeitintervall an. Fernnachrichten sind Übertragungen, die vom ExtraHop-System über einen offenen Datenstrom (ODS) an einen Recordstore oder an Systeme von Drittanbietern gesendet werden.

Wie diese Informationen Ihnen helfen können
Überwachen Sie dieses Diagramm, um sicherzustellen, dass die Byte wie erwartet übertragen werden. Wenn Sie niedrige Durchsatzzahlen feststellen, liegt möglicherweise ein Problem mit der Konfiguration eines ODS oder eines angeschlossenen Recordstore vor. Signifikante Durchsatzeinbrüche können auf Probleme mit Ihren Datenströmen hinweisen.
Gesendete Nachrichten
Ein Liniendiagramm, das die durchschnittliche Rate anzeigt, mit der Remote-Nachrichten vom ExtraHop-System an ein Recordstore- oder ODS-Ziel (Open Data Stream) gesendet wurden. Neben dem Liniendiagramm zeigt ein Wertdiagramm die Gesamtzahl der Nachrichten an, die im ausgewählten Zeitintervall gesendet wurden.

Wie diese Informationen Ihnen helfen können
Überwachen Sie dieses Diagramm, um sicherzustellen, dass Pakete wie erwartet gesendet werden. Wenn keine Pakete gesendet werden, liegt möglicherweise ein Problem mit der Konfiguration eines ODS oder eines angehängten Recordstore vor.
Nach Remotetyp verworfene Nachrichten
Ein Liniendiagramm, das die durchschnittliche Rate von Remotenachrichten anzeigt, die gelöscht wurden, bevor sie einen Recordstore oder ein ODS-Ziel erreichten.

Wie diese Informationen Ihnen helfen können
Verworfene Nachrichten weisen auf Verbindungsprobleme mit dem Remote-Ziel hin. Eine hohe Anzahl von Drops könnte auch darauf hinweisen, dass der Nachrichtendurchsatz zu hoch ist, um vom ExtraHop-System oder dem Zielserver verarbeitet zu werden.
Fehler beim Senden von Nachrichten
Ein Liniendiagramm, das die Anzahl der Fehler anzeigt, die beim Senden einer Remote-Nachricht an einen Recordstore oder ein ODS-Ziel aufgetreten sind. Überwachen Sie dieses Diagramm, um sicherzustellen, dass Pakete wie erwartet gesendet werden. Übertragungsfehler können Folgendes beinhalten:

Fehler auf dem Zielserver

Die Anzahl der Fehler, die von Recordstores oder ODS-Zielen an das ExtraHop-System zurückgegeben werden. Diese Fehler sind auf dem Zielserver aufgetreten und deuten nicht auf ein Problem mit dem ExtraHop-System hin.

Verworfene Nachrichten in voller Warteschlange

Die Anzahl der an Datensatzspeicher und ODS-Ziele gesendeten Nachrichten, die gelöscht wurden, weil die Nachrichtenwarteschlange auf dem Zielserver voll war. Eine hohe Anzahl verworfener Nachrichten kann darauf hindeuten, dass der Nachrichtendurchsatz zu hoch ist, um vom ExtraHop-System oder dem Zielserver verarbeitet zu werden. Schau dir das an Länge der Exremote-Nachrichtenwarteschlange nach Ziel und der Einzelheiten zum Ziel Diagramme, um festzustellen, ob Ihre Übertragungsfehler möglicherweise auf eine lange Nachrichtenwarteschlange zurückzuführen sind.

Nicht übereinstimmende Zielmeldungen

Die Anzahl der gelöschten Remote-Nachrichten, weil das im Open Data Stream (ODS) -Triggerskript angegebene Remotesystem nicht mit dem Namen übereinstimmt, der auf der Seite Open Data Streams in den Administrationseinstellungen konfiguriert wurde. Stellen Sie sicher, dass die Namen der Remotesysteme in den Triggerskripten und den Administrationseinstellungen konsistent sind.

Fehler beim Dekodieren gelöschter Nachrichten

Die Anzahl der Nachrichten, die aufgrund interner Kodierungsprobleme zwischen ExtraHop Capture (excap) und ExtraHop Remote (exremote) verloren gegangen sind.

Verbindungen
Ein Linien- und Säulendiagramm, in dem das Liniendiagramm die Anzahl der Versuche anzeigt, die das System unternommen hat, eine Verbindung zu einem Remote-Zielserver herzustellen, und das dazugehörige Säulendiagramm die Anzahl der Fehler anzeigt, die als Ergebnis dieser Versuche aufgetreten sind. Neben dem Linien- und Säulendiagramm zeigt ein Wertdiagramm die Gesamtzahl der Verbindungsversuche und Verbindungsfehler an, die im ausgewählten Zeitintervall aufgetreten sind.

Wie diese Informationen Ihnen helfen können
Identifizieren Sie Zielserver, die ungewöhnlich viele Verbindungsversuche erfordern oder unverhältnismäßig viele Verbindungsfehler verursachen. Ein Anstieg der Verbindungsversuche könnte darauf hindeuten, dass der Zielserver nicht verfügbar ist.
Länge der Exremote-Nachrichtenwarteschlange nach Ziel
Ein Liniendiagramm, das die Anzahl der Nachrichten in der ExtraHop Remote (exremote) -Warteschlange anzeigt, die darauf warten, vom ExtraHop-System verarbeitet zu werden.

Wie diese Informationen Ihnen helfen können

Eine hohe Anzahl von Nachrichten in der Warteschlange kann darauf hindeuten, dass der Nachrichtendurchsatz zu hoch ist, um vom ExtraHop-System oder dem Zielserver verarbeitet zu werden. Beziehen Sie sich auf den Wert Exremote Full Queue Dropped Messages in der Fehler beim Senden von Nachrichten Diagramm, um festzustellen, ob Nachrichtenabbrüche aufgetreten sind.
Länge der Nachrichtenwarteschlange nach Remote-Typ ausschließen
Ein Liniendiagramm, das die Anzahl der Remote-Zielnachrichten in der ExtraHop Capture (Excap) -Warteschlange anzeigt, die darauf warten, vom ExtraHop-System verarbeitet zu werden.

Wie diese Informationen Ihnen helfen können
Eine hohe Anzahl von Nachrichten in der Warteschlange kann darauf hindeuten, dass der Nachrichtendurchsatz zu hoch ist, um vom ExtraHop-System oder dem Zielserver verarbeitet zu werden.

Beziehen Sie sich auf die Nach Remotetyp verworfene Nachrichten Diagramm, um festzustellen, ob Nachrichtenabbrüche aufgetreten sind.

Einzelheiten zum Ziel
Ein Listendiagramm, das die folgenden Metriken zu Recordstore- oder ODS-Remote-Zielen im ausgewählten Zeitintervall anzeigt: Zielname, Zielnachrichten-Bytes out, gesendete Zielnachrichten, Zielserverfehler, gelöschte Nachrichten in voller Warteschlange, Dekodierungsfehler, gelöschte Nachrichten, Zielserver-Verbindungsversuche und Zielserver-Verbindungsfehler.

Wie diese Informationen Ihnen helfen können
Wenn Sie Nachrichtenfehler sehen, die in der Gesendete Nachrichten Diagramm, die Details in diesem Diagramm können Ihnen helfen, die Hauptursache von Fernmeldungsfehlern zu ermitteln.

TLS-Zertifikate
Im Abschnitt TLS-Zertifikate des Systemstatus-Dashboards können Sie die Statusinformationen für alle TLS-Zertifikate auf Ihrem System überprüfen.

Das TLS-Zertifikate Abschnitt enthält das folgende Diagramm:

- Angaben zum Zertifikat

Angaben zum Zertifikat
Ein Listendiagramm, das die folgenden Informationen für jedes Zertifikat anzeigt:

Entschlüsselte Sitzungen
Die Anzahl der Sitzungen, die erfolgreich entschlüsselt wurden.

Nicht unterstützte Sitzungen
Die Anzahl der Sitzungen, die mit passiver Analyse, z. B. beim DHE-Schlüsselaustausch, nicht entschlüsselt werden konnten.

Getrennte Sessions
Die Anzahl der Sitzungen, die aufgrund von Desynchronisierungen nicht oder nur teilweise entschlüsselt wurden.

Passthrough-Sitzungen
Die Anzahl der Sitzungen, die aufgrund von Hardwarefehlern nicht entschlüsselt wurden, z. B. weil die Spezifikationen der TLS-Beschleunigungshardware überschritten wurden.

Mit Shared Secret entschlüsselte Sitzungen

Die Anzahl der Sitzungen, die mit einem gemeinsamen geheimen Schlüssel entschlüsselt wurden.

Wie diese Informationen Ihnen helfen können
Überwachen Sie dieses Diagramm, um sicherzustellen, dass die richtigen TLS-Zertifikate auf dem ExtraHop-System installiert sind und die Entschlüsselung wie erwartet durchgeführt wird.

Paketerfassung aus der Ferne (RPCAP)
Im Bereich Remote Packet Capture (RPCAP) des Systemstatus-Dashboards können Sie die Anzahl der Pakete und Frames anzeigen, die von RPCAP-Peers gesendet und vom ExtraHop-System empfangen wurden.

Die Paketerfassung aus der Ferne (RPCAP) Dieser Abschnitt enthält die folgenden Diagramme:

- Weitergeleitet von Peer
- Vom ExtraHop-System empfangen

Weitergeleitet von Peer
Ein Listendiagramm, das die folgenden Informationen zu Paketen und Frames anzeigt, die von einem RPCAP-Peer weitergeleitet werden:

Weitergeleitete Pakete

Die Anzahl der Pakete, die ein RPCAP-Peer versucht hat, an ein ExtraHop-System weiterzuleiten.

Forwarder-Schnittstellenpakete

Die Gesamtzahl der Pakete, die vom Forwarder angesehen wurden. Forwarder auf RPCAP-Geräten koordinieren sich miteinander, um zu verhindern, dass mehrere Geräte dasselbe Paket senden. Dies ist die Anzahl der Pakete, die angesehen wurden, bevor Frames entfernt wurden, um den weitergeleiteten Verkehr zu reduzieren, und bevor Frames durch benutzerdefinierte Filter entfernt wurden.

Forwarder-Kernel-Frame-Drops

Die Anzahl der Frames, die gelöscht wurden, weil der Kernel des RPCAP-Peers mit dem Stream ungefilterter Frames überlastet war. Ungefilterte Frames wurden vom Kernel nicht gefiltert, um doppelte Pakete oder Pakete zu entfernen, die aufgrund benutzerdefinierter Regeln nicht weitergeleitet werden sollten.

Die Forwarder-Schnittstelle wird unterbrochen

Die Anzahl der Pakete, die verworfen wurden, weil der RPCAP-Forwarder mit dem Stream ungefilterter Frames überlastet war. Ungefilterte Frames wurden nicht gefiltert, um doppelte Pakete oder Pakete zu entfernen, die aufgrund benutzerdefinierter Regeln nicht weitergeleitet werden sollten.

Wie diese Informationen Ihnen helfen können
Jedes Mal, wenn Sie Pakete sehen, die vom RPCAP-Peer verworfen wurden, deutet dies darauf hin, dass ein Problem mit der RPCAP-Software vorliegt.

Vom ExtraHop-System empfangen
Ein Listendiagramm, das die folgenden Informationen zu Paketen und Frames anzeigt, die von einem ExtraHop-System von einem Remote Packet Capture (RPCAP) -Peer empfangen werden:

Gekapselte Bytes

Die Gesamtgröße aller Pakete, die sich auf den UDP-Fluss vom RPCAP-Gerät zum ExtraHop-System beziehen, in Byte. Diese Information zeigt Ihnen, wie viel Traffic der RPCAP-Forwarder Ihrem Netzwerk hinzufügt.

Gekapselte Pakete

Die Anzahl der Pakete, die sich auf den UDP-Fluss vom RPCAP-Gerät zum ExtraHop-System beziehen.

Tunnel-Bytes

Die Gesamtgröße der Pakete, ohne Kapselungsheader, die das ExtraHop-System von einem RPCAP-Gerät empfangen hat, in Byte.

Tunnel-Pakete

Die Anzahl der Pakete, die das ExtraHop-System von einem RPCAP-Peer empfangen hat. Diese Zahl sollte der Zahl der weitergeleiteten Pakete in der Tabelle Vom Remote-Gerät gesendet sehr ähnlich sein. Wenn zwischen diesen beiden Zahlen eine große Lücke besteht, fallen Pakete zwischen dem RPCAP-Gerät und dem ExtraHop-System ab.

Wie diese Informationen Ihnen helfen können

Die Verfolgung der gekapselten Pakete und Bytes ist eine gute Methode, um sicherzustellen, dass RPCAP-Forwarder Ihr Netzwerk nicht unnötig belasten. Sie können Tunnelpakete und Bytes überwachen, um sicherzustellen, dass das ExtraHop-System alles empfängt, was das RPCAP-Gerät sendet.

Fortgeschrittene Gesundheitsmetriken
Im Bereich Advanced Health Metrics des Systems Health Dashboard können Sie die Heap-Zuweisung im Zusammenhang mit der Datenerfassung, dem Systemdatenspeicher, Triggern und Fernübertragungen verfolgen. Überwachen Sie den Schreibdurchsatz, die Größe des Arbeitssets und die Triggeraktivität im Systemdatenspeicher.

Die Fortgeschrittene Gesundheitsmetriken Dieser Abschnitt enthält die folgenden Diagramme:

- Erfassung und Datenspeicher-Heap-Zuweisung
- Trigger- und Remote-Heap-Zuweisung
- Schreibdurchsatz speichern
- Größe des Arbeitssets
- Laden des Datenspeicher-Triggers
- Der Datenspeicher-Trigger wird ausgeführt und gelöscht
- Datenspeicherauslöserausnahmen nach Trigger

Erfassung und Datenspeicher-Heap-Zuweisung
Ein Liniendiagramm, das die Speichermenge anzeigt, die das ExtraHop-System für die Erfassung von Netzwerkpaketen und für den Datenspeicher reserviert.

Wie diese Informationen Ihnen helfen können
Die Daten in dieser Tabelle dienen internen Zwecken und können angefordert werden von ExtraHop-Unterstützung um Ihnen bei der Diagnose eines Problems zu helfen.
Trigger- und Remote-Heap-Zuweisung
Ein Liniendiagramm, das die Speichermenge, ausgedrückt in Byte, anzeigt, die das ExtraHop-System der Verarbeitung von Capture-Triggern und Open Data Streams (ODS) widmet.

Wie diese Informationen Ihnen helfen können
Die Daten in dieser Tabelle dienen internen Zwecken und können angefordert werden von ExtraHop-Unterstützung um Ihnen bei der Diagnose eines Problems zu helfen.
Schreibdurchsatz speichern
Ein Flächendiagramm, das den Datenspeicher-Schreibdurchsatz, ausgedrückt in Byte, auf dem ExtraHop-System anzeigt. Das Diagramm zeigt Daten für das ausgewählte Zeitintervall und für Intervalle von 24 Stunden, 1 Stunde, 5 Minuten und 30 Sekunden an.

Wie diese Informationen Ihnen helfen können
Die Daten in dieser Tabelle dienen internen Zwecken und können angefordert werden von ExtraHop-Unterstützung um Ihnen bei der Diagnose eines Problems zu helfen.

Größe des Arbeitssets
Ein Flächendiagramm, das die Größe des Schreib-Cache-Arbeitssets für Metriken auf dem ExtraHop-System anzeigt. Die Größe des Arbeitssets gibt an, wie viele Metriken für das ausgewählte Zeitintervall und für Intervalle von 24 Stunden, 1 Stunde, 5 Minuten und 30 Sekunden in den Cache geschrieben werden können.

Wie diese Informationen Ihnen helfen können
Die Daten in diesem Diagramm können nach der Erstellung oder Änderung des Auslöser stark ansteigen, wenn das Trigger-Skript Metriken nicht effizient sammelt.
Laden des Datenspeicher-Triggers
Ein Liniendiagramm, das den Prozentsatz der Zyklen anzeigt, die von datenspeicherspezifischen Triggern auf dem ExtraHop-System verbraucht wurden, basierend auf der gesamten Capture-Thread-Zeit.

Wie diese Informationen Ihnen helfen können
Achten Sie auf Spitzen oder ein steigendes Wachstum der Datenspeicher-Triggerlast, insbesondere nach dem Erstellen eines neuen Datenspeicher-Triggers oder dem Ändern eines vorhandenen Datenspeicher-Triggers. Wenn Sie beides bemerken, klicken Sie auf **Last auslösen** Metriklabel, um eine Aufschlüsselung durchzuführen und zu sehen, welche Datenspeicher-Trigger die meisten Ressourcen verbrauchen.
Der Datenspeicher-Trigger wird ausgeführt und gelöscht
Ein Linien- und Säulendiagramm, in dem das Liniendiagramm anzeigt, wie oft datenspeicherspezifische Trigger auf dem ExtraHop-System während des ausgewählten Zeitintervalls ausgeführt wurden, und das dazugehörige Säulendiagramm die Anzahl der datenspeicherspezifischen Trigger anzeigt, die während des ausgewählten Zeitintervalls aus der Warteschlange der Trigger gelöscht wurden, die darauf warten, auf dem ExtraHop-System ausgeführt zu werden.

Wie diese Informationen Ihnen helfen können
Ein einzelner Datenspeicher-Trigger, der häufig ausgeführt wird, kann darauf hinweisen, dass der Auslöser allen Quellen zugewiesen wurde, z. B. Anwendungen oder Geräten. Um die Auswirkungen auf die Leistung zu minimieren, sollte ein Auslöser nur den spezifischen Quellen zugewiesen werden, aus denen Sie Daten sammeln müssen.

Aus dem Laden des Datenspeicher-Triggers Diagramm, klicken Sie auf **Last auslösen** Metriklabel, um eine Aufschlüsselung durchzuführen und zu sehen, welche Datenspeicher-Trigger am häufigsten ausgeführt werden.

Alle Drop-Daten, die im Säulendiagramm angezeigt werden, weisen darauf hin, dass es zu Drops von Datenspeicher-Triggern kommt und dass Trigger-Warteschlangen gesichert werden .

Das System stellt Triggeroperationen in die Warteschlange, wenn ein Trigger-Thread überlastet ist. Wenn die Datenspeicher-Trigger-Warteschlange zu lang wird, beendet das System das Hinzufügen von Trigger-Vorgängen zur Warteschlange und löscht die Trigger. Aktuell ausgeführte Trigger sind davon nicht betroffen.

Die Hauptursache für lange Warteschlangen und nachfolgende Triggerausfälle ist ein Trigger mit langer Laufzeit im Datenspeicher.

Datenspeicherauslöserausnahmen nach Trigger
Ein Listendiagramm, das die Anzahl der unbehandelten Ausnahmen anzeigt, die durch datenspeicherspezifische Trigger im ExtraHop-System verursacht wurden.

Wie diese Informationen Ihnen helfen können
Ausnahmen für Datenspeicher-Trigger sind die Hauptursache für Leistungsprobleme bei Auslöser. Wenn dieses Diagramm darauf hinweist, dass eine Trigger-Ausnahme aufgetreten ist, sollte der Datenspeicher-Trigger sofort korrigiert werden.

Status- und Diagnosetools in den Administrationseinstellungen
Die Administrationseinstellungen sind eine weitere Quelle für Systeminformationen und Diagnosen.

Für weitere Messwerte zum allgemeinen Zustand des ExtraHop-Systems und für Diagnosetools, die ExtraHop-Unterstützung um Systemfehler zu beheben, schauen Sie sich die Status und Diagnose Abschnitt der Administrationseinstellungen.

Dashboard zur Systemnutzung

Mit dem Dashboard zur Systemnutzung können Sie überwachen, wie Benutzer mit dem ExtraHop-System interagieren.

Jedes Diagramm im Systemnutzungs-Dashboard enthält Visualisierungen der Benutzerinteraktionen mit dem ExtraHop-System und der Erkennungen, die über das ausgewähltes Zeitintervall, nach Region organisiert.

Hinweis: Das Systemnutzungs-Dashboard ist ein integriertes System-Dashboard, das Sie nicht bearbeiten, löschen oder einer gemeinsamen Sammlung hinzufügen können. Sie können keine Kopie des Systemnutzungs-Dashboards erstellen oder Diagramme in benutzerdefinierte Dashboards kopieren.

Bevor Sie beginnen
Das Systemnutzungs-Dashboard kann nur von Benutzern mit System- und Zugriffsadministration von einer Konsole aus angezeigt werden Privilegien.

Die folgenden Informationen fassen jede Region und ihre Diagramme zusammen.

ExtraHop Nutzer

Beobachten Sie die Anmeldeaktivitäten der Benutzer und die aktuelle Anzahl der aktiven Benutzer im ExtraHop-System.

- **Aktive Benutzer und Logins:** Die Häufigkeit, mit der sich Benutzer beim ExtraHop-System angemeldet haben, und aktuelle Schnappschüsse der aktiven Benutzer. Das Liniendiagramm zeigt die aktuellen aktiven Benutzer an, und das Säulendiagramm zeigt die Anzahl der Benutzeranmeldungen im Laufe der Zeit an. Eine Anmeldung wird jedes Mal gezählt, wenn sich ein Benutzer am System anmeldet, einschließlich mehrerer Anmeldungen durch einen einzelnen Benutzer.
- **Die häufigsten Benutzeranmeldungen:** Benutzer mit den meisten Logins im ExtraHop-System im ausgewählten Zeitintervall.
- **Aktive Benutzer und Logins:** Die Anzahl der Benutzer, die derzeit auf dem ExtraHop-System aktiv sind, und die Gesamtzahl der Benutzeranmeldungen im ausgewählten Zeitintervall.

Armaturenbretter

Beobachten Sie, wie oft Benutzer zuschauen Dashboards und welche Dashboards am häufigsten angesehen werden.

- **Dashboard-Ansichten:** Gesamtzahl der Dashboard-Ansichten im Laufe der Zeit. Eine Dashboard-Ansicht wird gezählt, wenn ein Dashboard nach einer Benutzeranmeldung, einem Klick oder einer direkten Navigation über eine geteilte URL angezeigt wird.
- **Am häufigsten angesehene Dashboards:** Dashboards mit der höchsten Anzahl von Ansichten.
- **Gesamtzahl der Dashboard-Ansichten:** Die Gesamtzahl der Dashboard-Ansichten im ausgewählten Zeitintervall.

Erkennungen

Beachten Sie Informationen über Erkennungen die vom ExtraHop-System generiert werden und wie die Benutzer sie betrachten und Verfolgung Erkennungen.

- **Erkennungsansichten:** In diesem Liniendiagramm werden zwei Werte angezeigt: Erkennungslistenansichten zählen die Anzahl der Klicks auf die Erkennungsliste, wenn gruppiert nach Erkennungstyp, und Detection Detail Views zählt, wie oft a Entdeckungsdetailseite erscheint nach einer Benutzeranmeldung, einem Klick oder einer direkten Navigation über eine geteilte URL. Klicken Sie in der Legende auf einen der Metriknamen, um eine Aufschlüsselung nach Erkennungstyp durchzuführen.

• **Am häufigsten angesehene Erkennungen:** Die Erkennungstypen, die im ausgewählten Zeitintervall am häufigsten angesehen wurden.

• **Gesamtzahl der Entdeckungsansichten:** Die Gesamtwerte für Erkennungslistenansichten und Erkennungsdetailansichten im ausgewählten Zeitintervall.

• **Erkennungsverfolgung (Liniendiagramm):** Die Anzahl der Funde, die mit und ohne ergriffene Maßnahmen geschlossen wurden, und die Anzahl der Funde, die im Laufe der Zeit bestätigt wurden.

• **Erkennungsverfolgung (Listendiagramm):** Die Gesamtzahl der Entdeckungen, die mit und ohne ergriffene Maßnahmen abgeschlossen wurden, die Anzahl der erstellten Untersuchungen und die Gesamtzahl der Entdeckungen, die im ausgewählten Zeitintervall auf den Status Bestätigt gesetzt wurden. Die Liste enthält auch die Anzahl der Erkennungen, für die derzeit der Status In Bearbeitung festgelegt ist.

• **Gesamtzahl geschlossener Erkennungen:** Die Gesamtzahl der Funde, die im ausgewählten Zeitintervall mit und ohne ergriffene Maßnahmen geschlossen wurden. Die Werte für Gesamtzahl geschlossener Entdeckungen beinhalten Entdeckungen, die ausgeblendet wurden, nachdem der Erkennungsstatus festgelegt wurde.

• **Empfohlene Erkennungen:** Die Anzahl der Erkennungen, die für die Triage, auch bekannt als Smart Triage, während des ausgewählten Zeitintervalls empfohlen wurden.

• **Die am häufigsten empfohlenen Erkennungen:** Die Erkennungstypen, die während des ausgewählten Zeitintervalls am häufigsten für die Triage empfohlen wurden.

• **Gesamtzahl geschlossener empfohlener Erkennungen:** Die Gesamtzahl der empfohlenen Erkennungen, die während des ausgewählten Zeitintervalls mit und ohne ergriffene Maßnahmen geschlossen wurden.

Erkennungsarten

Beobachten Sie, welche Erkennungstypen am häufigsten vom ExtraHop-System generiert wurden und wie Benutzer mit diesen Erkennungen interagieren.

• **Am häufigsten angesehene Erkennungstypen:** Die Anzahl der Erkennungslistenansichten und Erkennungsdetailansichten für die Erkennungstypen, die im ausgewählten Zeitintervall aufgetreten sind.

Ermittlungen

Beachten Sie die Informationen über von Benutzern erstellte Untersuchungen, die vom ExtraHop-System empfohlenen Untersuchungen und die Art und Weise, wie Benutzer Untersuchungen ansehen und mit ihnen interagieren .

• **Ansichten zur Untersuchung:** Die Anzahl der vom Benutzer erstellten und empfohlenen Untersuchungsansichten im Laufe der Zeit. Eine Untersuchungsansicht wird gezählt, wenn eine Untersuchung nach einer Benutzeranmeldung, einem Klick oder einer direkten Navigation über eine geteilte URL angezeigt wird.

• **Am häufigsten angesehene Untersuchungen:** Die Typen von vom Benutzer erstellten und empfohlenen Untersuchungen, die während des ausgewählten Zeitintervalls am häufigsten angesehen wurden.

• **Gesamtzahl der Ermittlungsansichten:** Die Gesamtzahl der vom Benutzer erstellten und empfohlenen Untersuchungsansichten während des ausgewählten Zeitintervalls.

• **Ermittlungen eingeleitet:** Die Anzahl der Untersuchungen, die im Laufe der Zeit erstellt wurden, aufgeführt nach Untersuchungen, die von Benutzern erstellt wurden, und nach Untersuchungen, die vom ExtraHop-System empfohlen wurden.

• **Die am häufigsten empfohlenen Untersuchungen:** Die Untersuchungstypen, die vom ExtraHop-System während des ausgewählten Zeitintervalls am häufigsten empfohlen wurden.

• **Gesamtzahl der eingeleiteten Ermittlungen:** Die Gesamtzahl der von Benutzern erstellten Untersuchungen und die Gesamtzahl der Untersuchungen, die vom ExtraHop-System während des ausgewählten Zeitintervalls empfohlen wurden.

Bedrohungsinformationen

Beachten Sie die Informationen zu Bedrohungsinformationen, die Hinweise zu potenziellen Bedrohungen für Ihr Netzwerk geben und darüber, wie Benutzer sie betrachten.

• **Einblicke in die Bedrohungslage:** Die Anzahl der Aufrufe von Bedrohungsübersicht im Laufe der Zeit. Eine Bedrohungs-Briefing-Ansicht wird gezählt, wenn eine Detailseite der Bedrohungsinformationen angezeigt wird, nachdem ein Benutzer auf eine geteilte URL geklickt oder direkt durch eine geteilte URL navigiert hat.

• **Die am häufigsten angesehenen Bedrohungsinformationen:** Die Bedrohungsinformationen, die während des ausgewählten Zeitintervalls am häufigsten angesehen wurden.

• **Gesamtansichten zur Bedrohungslage:** Die Gesamtzahl der Bedrohungsinformationen, die während des ausgewählten Zeitintervalls angesehen wurden.

Erstellen Sie ein Dashboard

Dashboards bieten einen zentralen Ort für wichtige Kennzahlen, die Ihnen wichtig sind. Wenn Sie ein benutzerdefiniertes Dashboard erstellen, wird ein Dashboard-Layout geöffnet, das eine einzelne Region mit einem leeren Diagramm-Widget und einem leeren Textfeld-Widget enthält. Bearbeiten Sie ein Diagramm, um Echtzeitmetriken in Ihr Dashboard zu integrieren, und bearbeiten Sie ein Textfeld, um Informationen bereitzustellen. Passen Sie abschließend das Layout an und fügen Sie weitere Widgets hinzu, um Ihr Dashboard zu vervollständigen und mit der Überwachung Ihres Netzwerk zu beginnen.

Bevor Sie beginnen
Bestimmen Sie, welche Metriken Sie auf Ihrem Dashboard überwachen möchten. Stellen Sie sich die folgenden Fragen:

- Möchte ich nachverfolgen, ob mein Server offline oder nicht verfügbar ist? Fügen Sie Verfügbarkeitsmetriken wie Anfragen und Antworten zu Ihren Dashboard-Diagrammen hinzu.
- Funktioniert mein Server richtig? Fügen Sie Zuverlässigkeitsmetriken wie Fehler zu Ihren Dashboard-Diagrammen hinzu.
- Ist mein Server richtig ausgestattet? Fügen Sie Leistungskennzahlen wie die Serververarbeitungszeit zu Ihren Dashboard-Diagrammen hinzu.

Erstellen Sie das Dashboard-Layout

Die folgenden Schritte zeigen Ihnen, wie Sie das Framework für Ihr Dashboard erstellen, das zwei leere Widget-Typen umfasst: ein Diagramm und ein Textfeld. Ihr neues Dashboard wird im Modus „ Layout bearbeiten“ geöffnet (der in der oberen rechten Ecke angezeigt wird). Im Modus „Layout bearbeiten“ können Sie Ihr Diagramm und Ihr Textfeld schnell bearbeiten und die Platzierung von Widgets und Bereichen auf einem Dashboard anordnen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Armaturenbretter**.
3. Führen Sie auf der Seite Dashboards einen der folgenden Schritte aus:
   - klicken **Armaturenbretter** im Dashboard-Dock und dann klicken **Dashboard erstellen** am unteren Rand des Docks.
   - Klicken Sie auf das Befehlsmenü ⋮ in der oberen rechten Ecke der Seite und wählen **Neues Dashboard**.
4. Geben Sie im Fenster Dashboard-Eigenschaften einen Namen für Ihr Dashboard ein.
5. Geben Sie weitere Metadaten für Ihr Dashboard ein, z. B. einen Namen für den Autor oder eine Beschreibung. Beachten Sie, dass der Permalink eine direkte URL zu Ihrem Dashboard für alle Benutzer bereitstellt, die Freigabeberechtigungen für dein Dashboard.
6. klicken **Erstellen**.

Bearbeiten Sie ein einfaches Diagramm

Die folgenden Schritte zeigen den allgemeinen Fluss für die Bearbeitung eines Diagramm-Widgets im Metric Explorer-Tool. Geben Sie zunächst Quellen und Metriken an, um Daten zu Ihrem Diagramm hinzuzufügen. Sie können jetzt beispielsweise die Verfügbarkeits-, Zuverlässigkeits- oder Leistungskennzahlen, die Sie zu Beginn dieses Verfahrens berücksichtigt haben, zu Ihrem Dashboard hinzufügen. Wählen Sie dann einen Diagrammtyp aus, um die Daten zu visualisieren.

1. Klicken Sie auf das Diagramm, um das zu starten Metric Explorer.
2. klicken **Quelle hinzufügen**.
3. Geben Sie im Quellensuchfeld den Namen einer Quelle ein und wählen Sie dann Quelle aus den Suchergebnissen.
4. Geben Sie in das Metrik-Suchfeld das Protokoll und den Metriknamen ein und wählen Sie dann aus den Suchergebnissen die Metrik aus, die Sie dem Diagramm hinzufügen möchten. Um beispielsweise die Zuverlässigkeit von Webtransaktionen zu überwachen, geben Sie `HTTP-Fehler` und wählen Sie dann **HTTP-Fehler** aus den Suchergebnissen.
5. Wählen Sie unten im Metric Explorer einen Diagrammtyp aus.

   Einige Diagramme sind möglicherweise nicht mit den von Ihnen ausgewählten Kennzahlen kompatibel. Das Heatmap-Diagramm kann beispielsweise nur angezeigt werden Datensatz Metrikdaten, z. B. Serververarbeitungszeit. Weitere Informationen zu Diagrammen und kompatiblen Messwerten finden Sie unter Diagrammtypen.
6. Optional: Wählen Sie einen Drilldown-Schlüssel aus, um detaillierte Metriken anzuzeigen. klicken **Drilldown nach <None>**, wo *<None>* ist der Name des Detailmetrikschlüssels, der derzeit in Ihrem Diagramm angezeigt wird. Sie können bis zu 20 Top-Keywerte in einem Diagramm für ein bestimmtes Zeitintervall anzeigen.
7. klicken **Speichern**.

Nächste Schritte

- Erfahren Sie mehr über Charts von der Häufig gestellte Fragen zu Grafiken.
- Üben Sie das Erstellen von Diagrammen, indem Sie die folgenden exemplarischen Vorgehensweisen ausführen:
  - Überwachen Sie DNS-Fehler in einem Dashboard
  - Überwachen Sie den Zustand der Datenbank in einem Dashboard
  - Überwachen Sie die Webleistung in einem Dashboard

Bearbeiten Sie ein einfaches Textfeld-Widget

Die folgenden Schritte zeigen Ihnen, wie Sie benutzerdefinierten Text in einem Dashboard-Bereich anzeigen. Dies ist ein hilfreiches Tool zum Hinzufügen von Notizen zu einem Diagramm oder Daten in einem Dashboard. Das Textfeld-Widget unterstützt die Markdown-Syntax. Ein neues Textfeld-Widget enthält Beispieltext, der bereits in Markdown formatiert ist, um Ihnen grundlegende Beispiele zu bieten.

1. Klicken Sie auf das Textfeld.
2. Text auf der linken Seite eingeben und bearbeiten Herausgeber Fensterscheibe. Der HTML-Ausgabetext wird dynamisch im rechten Vorschaufenster angezeigt. Weitere Formatierungsbeispiele finden Sie unter Text in Markdown formatieren.
3. klicken **Speichern**.

Fügen Sie Ihrem Dashboard weitere Widgets und Regionen hinzu

Fügen Sie Regionen und Widgets hinzu und ordnen Sie deren Platzierung auf Ihren Dashboards an.

1. Klicken Sie auf Dashboard-Komponenten, wie z. B. eine Region oder Widgets, und ziehen Sie sie vom unteren Seitenrand in den Arbeitsbereich.
2. Um Dashboard-Komponenten anzuordnen, klicken Sie auf den Rand einer Region oder eines Widget und ziehen Sie sie, um deren Größe zu ändern. Wenn sich Dashboard-Komponenten überschneiden,

werden sie rot umrandet. Sie müssen die Seiten der Widgets und Regionen anklicken und ziehen, um Platz zu schaffen.

3. Optional: klicken **Überflüssigen Speicherplatz entfernen** um den leeren vertikalen weißen Bereich um Widgets zu entfernen. Leerer vertikaler Leerraum wird aus allen Bereichen des Dashboard entfernt.
4. Nachdem Sie Ihre Änderungen vorgenommen haben, klicken Sie **Layoutmodus verlassen**.

Hinweis: Wenn eine Fehlermeldung angezeigt wird, nimmt ein anderer Benutzer möglicherweise Änderungen vor. Es hat sich bewährt, dass jeder ExtraHop-Benutzer über ein eigenes Konto verfügt.

Nächste Schritte

Jetzt, da Ihr Dashboard fertig ist, können Sie die folgenden Schritte ausführen:

- Teilen Sie Ihr Dashboard
- Aktualisiere dein Dashboard:
  - Ein Dashboard-Layout bearbeiten
  - Dashboard-Eigenschaften bearbeiten
  - Eine Dashboard-Region bearbeiten
  - Ein Diagramm mit dem Metric Explorer bearbeiten

Tipps zur Bearbeitung von Diagrammen

Die folgenden Tipps helfen Ihnen bei der Erstellung eines Diagramms bei der Suche nach Metriken und deren Auswahl.

- Filtern Sie die Suchergebnisse nach einem bestimmten Quelltyp oder Protokoll, indem Sie auf **Beliebiger Typ** oder **Beliebiges Protokoll** unter den Suchfeldern.
- Sie können nur denselben Quelltyp auswählen, der derzeit in Ihrem Metriksatz enthalten ist. Ein Metriksatz enthält einen Quelltyp und Metriken. Wenn Sie beispielsweise die Anwendung „Alle Aktivitäten“ als Quelle auswählen, können Sie diesem Metriksatz nur weitere Anwendungen hinzufügen.
- Erstellen Sie eine Ad-hoc-Gruppe mit mehr als einer Quelle in Ihrem Diagramm, indem Sie **Quellen kombinieren**. Sie können beispielsweise zwei Anwendungen kombinieren und dann einen einzelnen Metrikwert im Diagramm für diese beiden Anwendungen anzeigen.
- Wenn Sie eine Gerätegruppe als Quelle auswählen, können Sie **Aufschlüsselung nach Gruppenmitglied** um einzelne Metriken für bis zu 20 Geräte innerhalb der Gruppe anzuzeigen.

Erstellen Sie ein Dashboard mit dynamischen Quellen

Sie können ein Dashboard mit dynamischen Quellen erstellen, damit Benutzer die Quelle des Dashboard jederzeit ändern können. Wenn Sie eine große Anzahl von Dashboards erstellt haben , die alle dieselben Metriken, aber unterschiedliche Quellen haben, sollten Sie erwägen, diese Dashboards durch ein einzelnes Dashboard mit dynamischen Quelle zu ersetzen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Armaturenbretter**.
3. Wählen Sie im Dashboard-Dock ein Dashboard aus, das Sie bearbeiten möchten.
4. Stellen Sie die Quelle jedes Diagramms auf eine Quelltypvariable ein.
   a) Klicken Sie auf den Namen eines Diagramms und dann auf **Bearbeiten**.
   b) In der **Quellen** Feld, Typ $.
   Die Variablen des Quelltyps Liste wird angezeigt.
   c) Aus dem Variablen des Quelltyps Liste, wählen Sie den Quelltyp aus, den Sie ersetzen möchten. Wenn Sie beispielsweise eine Gerätequelle austauschen, wählen Sie `$device`.

5. klicken **Speichern**.
   Am oberen Rand des Dashboard befindet sich der Quelltext ansehen Ein Drop-down-Menü wird angezeigt.
6. Aus dem Quelltext ansehen Wählen Sie im Dropdownmenü die Quelle aus, für die Sie Kennzahlen anzeigen möchten.
   Wenn in den Dashboard-Diagrammen keine Daten angezeigt werden, versuchen Sie, die Seite zu aktualisieren.

Hinweis: Wenn Sie das dynamische Quellmenü in Ihrem Dashboard ausblenden möchten, fügen Sie den folgenden Parameter an das Ende der URL der Dashboard-Seite an: `&hideTemplatePanel=true`.

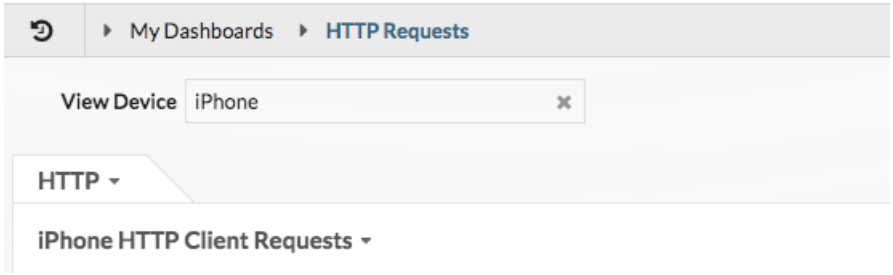


Abbildung 3: Vorher

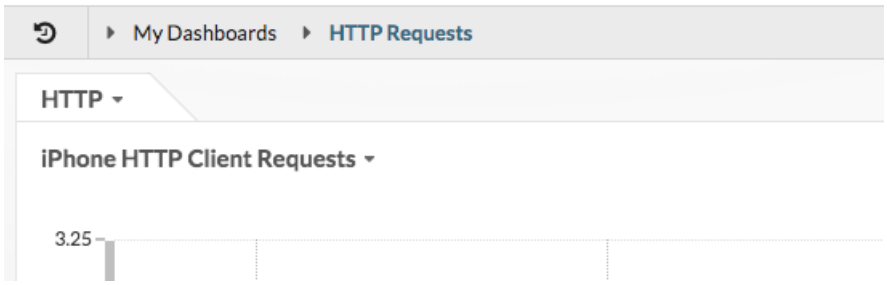


Abbildung 4: Nach

Zum Beispiel:

```
https://eda/extrahop/#/Dashboard/XYFwM/?
$device=16&from=30&interval_type=MIN&until=0&hideTemplatePanel=true
```

Nächste Schritte

- Ein Dashboard kopieren

Ein Dashboard kopieren

Wenn Sie ein nützliches Dashboard duplizieren möchten, können Sie ein Dashboard kopieren und dann Quellen ersetzen oder ändern, um andere Anwendung-, Gerät- oder Netzwerkdaten anzuzeigen. Sie können jeweils nur ein Dashboard kopieren.

Hinweis: Wenn Sie nur ein Dashboard kopieren möchten, damit Sie die Quelle im gesamten Dashboard ändern können, sollten Sie Folgendes in Betracht ziehen Erstellen eines Dashboard mit dynamischen Quellen anstatt mehrere Kopien eines einzelnen Dashboard zu erstellen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Armaturenbretter**.

3. Wählen Sie im Dashboard-Dock ein Dashboard aus, das Sie kopieren möchten.
4. Klicken Sie auf das Befehlsmenü ⋮ in der oberen rechten Ecke der Dashboard-Seite.
5. klicken **Kopieren** und führen Sie einen der folgenden Schritte aus:
   - klicken **Quellen behalten** um die ursprünglichen Datenkonfigurationen im neuen Dashboard beizubehalten.

     Hinweis: Wenn Sie ein Dashboard mit dynamischen Quellen kopieren, werden die ursprünglichen Datenkonfigurationen automatisch beibehalten.
   - klicken **Quellen ändern**, was Ihnen hilft, jede Region, jedes Diagramm und jedes Widget innerhalb des kopierten Dashboard sofort mit einer anderen Quelle zu aktualisieren und dann die folgenden Schritte durchzuführen:
     1. Im rechten Bereich des Quellen ändern Fenster, klicken Sie auf einen Quellnamen. Ein Suchfeld öffnet sich.
     2. Geben Sie den Namen einer neuen Quelle ein und wählen Sie dann die Quelle aus der Dropdownliste aus. Wiederholen Sie diesen Schritt, wenn das Dashboard mehr als eine Quelle enthält, die Sie ersetzen möchten.
     3. klicken **Dashboard erstellen**.

   Ein kopiertes Dashboard mit einer geänderten Version des Originaltitels wird erstellt.
6. Gehen Sie wie folgt vor, um das kopierte Dashboard umzubenennen:
   a) Klicken Sie auf das Befehlsmenü ⋮ in der oberen rechten Ecke und auf der Seite.
   b) Wählen **Dashboard-Eigenschaften**.
   c) Geben Sie im Feld Titel einen neuen Namen ein.
   d) klicken **Speichern**.

Nächste Schritte

- Eine Dashboard-Region bearbeiten
- Ein Diagramm mit dem Metric Explorer bearbeiten
- Dashboard-Layout bearbeiten

Ein Dashboard-Layout bearbeiten

Versetzen Sie Ihr Dashboard in den Modus „Layout bearbeiten“, um Widgets und Bereiche in Ihrem Dashboard-Layout hinzuzufügen, zu löschen oder neu anzuordnen. Sie können Widgets oder Regionen nur hinzufügen oder löschen, wenn sich das Dashboard im Modus „Layout bearbeiten“ befindet.

Wenn Sie ein neues Dashboard erstellen, wird das Dashboard automatisch in den Layoutbearbeitungsmodus versetzt. Gehen Sie wie folgt vor, um das Layout eines vorhandenen Dashboard zu bearbeiten:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Armaturenbretter**.
3. Wählen Sie im Dashboard-Dock ein Dashboard aus, das Sie bearbeiten möchten.
4. Klicken Sie auf das Befehlsmenü ⋮ in der oberen rechten Ecke der Seite, und wählen Sie dann **Layout bearbeiten**.
5. Wählen Sie im Modus „Layout bearbeiten“ aus den folgenden Optionen:

   Widgets und Regionen hinzufügen

   Klicken und ziehen Sie ein Widget oder eine Region vom unteren Rand der Seite und platzieren Sie sie auf dem Dashboard.

   Widgets sind konfigurierbare Dashboard-Komponenten, die die folgenden Funktionen bieten:

- **Diagramm :** Fügen Sie Metriken hinzu und wählen Sie Diagrammtypen aus, um Daten zu visualisieren
- **Textfeld :** Fügen Sie Ihrem Dashboard Erklärungen, Links und Bilder hinzu
- **Alerts :** scannt bis zu 40 aktuelle Warnmeldungen, sortiert nach Schweregrad
- **Aktivitätsgruppe:** Geräte überwachen, die im ExtraHop-System automatisch nach Protokollaktivitäten gruppiert sind

Regionen enthalten Widgets und gruppieren sie logisch. Klicken Sie auf Widgets und ziehen Sie sie in eine Region. Die Breite einer Region kann maximal sechs Widgets enthalten. Die Länge einer Region und eines Dashboard ist unbegrenzt.

Widgets und Regionen löschen

Um eine Region zu löschen, klicken Sie auf **Löschen** in der Kopfzeile der Region. Um ein Widget zu löschen, klicken Sie auf den Titel und wählen Sie dann **Löschen** aus dem Drop-down-Menü.

Ordnen Sie die Platzierung von Widgets und Regionen an

Klicken Sie auf die Kopfzeile einer Region oder eines Widget, um sie an eine andere Position zu ziehen. Klicken und ziehen Sie den Rand einer Region oder eines Widget, um deren Größe zu ändern.

Wenn sich Dashboard-Komponenten überschneiden, werden sie rot umrandet. Sie müssen die Seiten der Widgets und Regionen anklicken und ziehen, um Platz zu schaffen.

Diagramme duplizieren

klicken **Duplizieren** um eine Kopie eines Diagramms oder Textfeldes in derselben Region zu erstellen.

6. Optional: klicken **Überflüssigen Speicherplatz entfernen** um den leeren vertikalen weißen Bereich um Widgets zu entfernen. Leere vertikale Leerräume werden aus allen Bereichen Region Dashboard entfernt.
7. klicken **Layoutmodus verlassen** in der oberen rechten Ecke der Seite, um Ihre Änderungen zu speichern.

Hinweis: Wenn eine Fehlermeldung angezeigt wird, nimmt ein anderer Benutzer möglicherweise Änderungen vor. Es hat sich bewährt, dass jeder ExtraHop-Benutzer über ein eigenes Konto verfügt.

Nächste Schritte

- Eine Region bearbeiten
- Bearbeiten Sie ein Diagramm mit dem Metric Explorer
- Ein Textfeld bearbeiten

Ein Diagramm mit dem Metric Explorer bearbeiten

Der Metric Explorer ist ein Tool zum Erstellen und Bearbeiten von Diagrammen, mit dem Sie dynamische Visualisierungen des Gerät- und Netzwerkverhaltens erstellen können.

Sie müssen ein persönliches Schreiben haben Privilegien oder höher und NPM-Modulzugriff zum Erstellen und Bearbeiten von Diagrammen in einem Dashboard.

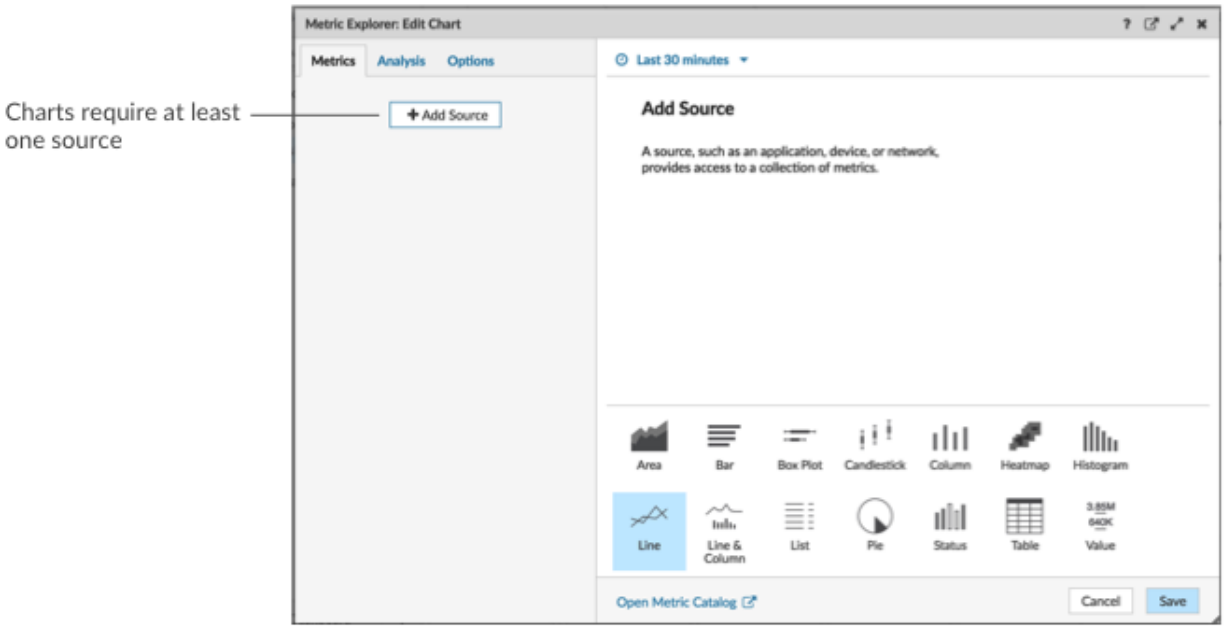
Video: Sehen Sie sich die entsprechende Schulung an: Eine Metrik auswählen

Erstellen und bearbeiten Sie ein Basisdiagramm

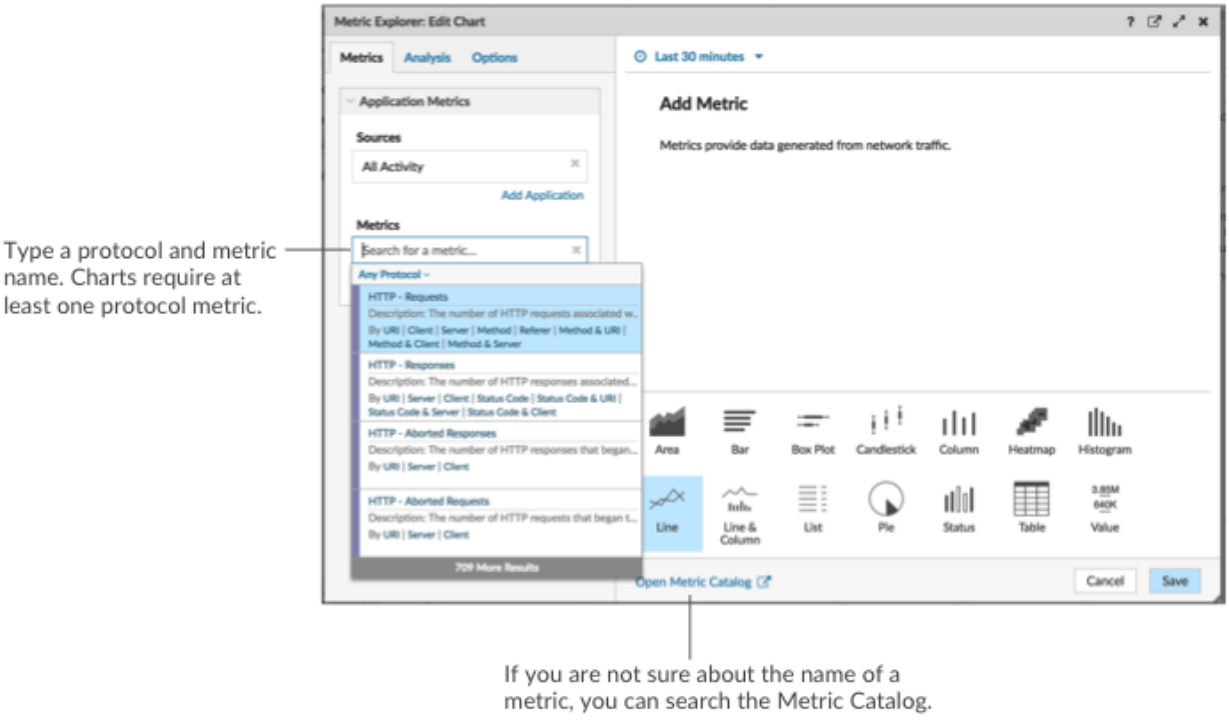
Mit dem Metric Explorer können Sie Diagrammkomponenten wie Quellen, Metriken und Datenberechnungen bearbeiten und dann eine Vorschau anzeigen, wie Metrikdaten in verschiedenen Diagrammtypen angezeigt werden. Wenn Sie mit Ihrer Auswahl zufrieden sind, speichern Sie Ihr Diagramm in einem Dashboard.

Die folgenden Schritte zeigen Ihnen den grundlegenden Arbeitsablauf und die Mindestanforderungen für das Ausfüllen eines neuen Diagramms.

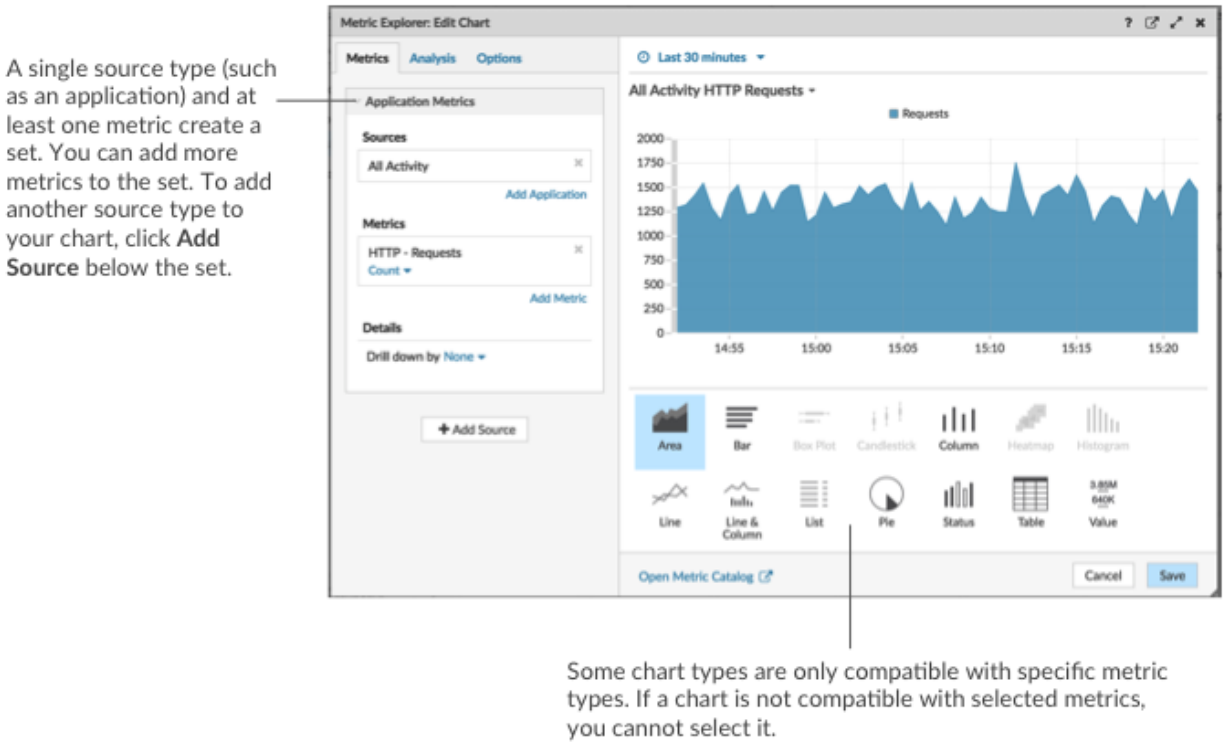
1. klicken **Quelle hinzufügen** und wählen Sie dann eine Quelle aus.



   - Sie können eine statische Quelle für das Diagramm auswählen, indem Sie den Namen einer Anwendung, eines Gerät oder eines Netzwerk eingeben.
   - Sie können auch eine dynamische Quelle auswählen, die von Dashboard-Viewern dynamisch geändert werden kann, indem Sie Folgendes eingeben $ und Auswahl einer Variablen aus dem Quelltyp: Variable Liste. Weitere Informationen zu Quelltypvariablen und Dashboard-Vorlagen finden Sie unter Erstellen Sie ein Dashboard mit dynamischen Quellen.
2. Wählen Sie die Quelle aus der Ergebnisliste aus.
3. Geben Sie im Feld Metriken ein Protokoll und einen Metriknamen ein. Wählen Sie dann die Metrik aus der Ergebnisliste aus, wie in der folgenden Abbildung dargestellt.



4. Wählen Sie unten im Metric Explorer ein Diagramm aus, wie in der folgenden Abbildung dargestellt.

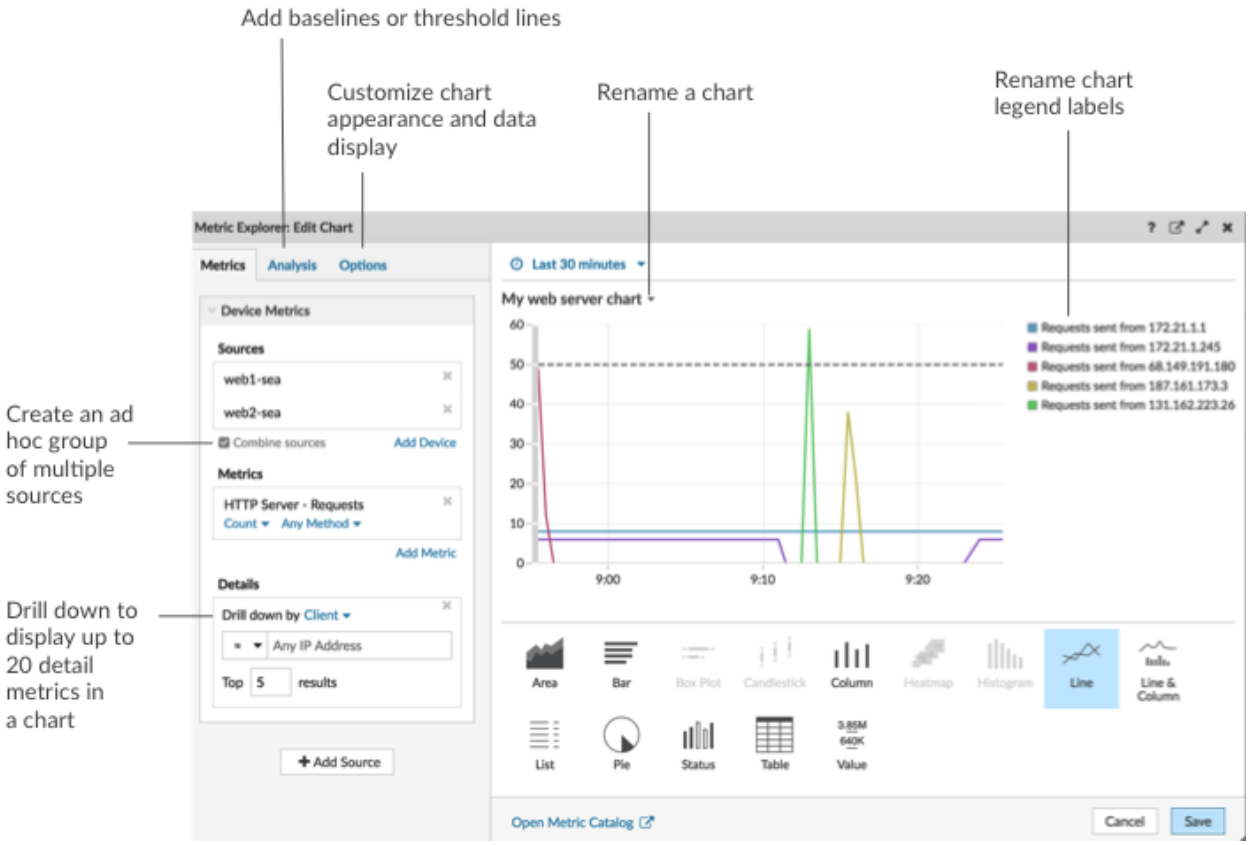


5. Optional: Klicken Sie auf den Dropdown-Link unter dem Metriknamen, um eine Zählung oder Rate anzeigen oder Perzentil.
6. Führen Sie einen der folgenden Schritte aus:
   - klicken **Speichern** beim Erstellen oder Bearbeiten eines Diagramms von einem Dashboard aus. Ihr Dashboard wird mit Ihrem Basisdiagramm aktualisiert.

- klicken **Zum Dashboard hinzufügen** wenn Sie ein Diagramm von einer Protokollseite aus erstellen oder bearbeiten. Wählen Sie dann ein vorhandenes Dashboard aus der Liste aus, oder wählen Sie **Dashboard erstellen**.

Konfigurieren Sie erweiterte Optionen für die Datenanalyse und Diagrammanpassung

Je nach den ausgewählten Metriken und dem Diagrammtyp können Sie erweiterte Optionen für die Erstellung anspruchsvoller Visualisierungen mit dem Metric Explorer konfigurieren, wie in der folgenden Abbildung dargestellt.



Drilldown zu Metrik Daten und Quellen, um Details anzuzeigen
Im Abschnitt „ Details“ auf der Registerkarte „Metriken“ können Sie Drilldown zur Anzeige detaillierter Metriken oder Drilldown für eine Gerätegruppe um einzelne Geräte in der Tabelle anzuzeigen. Sie können auch Detailmetriken nach exakten Übereinstimmungen filtern oder eine erstellen Regex-Filter .

Fügen Sie auf der Registerkarte „Analyse“ eine Basislinie oder eine Schwellenwertlinie hinzu
Du eine Dynamische Basislinie hinzufügen oder statische Schwellenlinie zu deinem Diagramm. Basislinien werden berechnet, nachdem das Diagramm gespeichert wurde. Um eine Linie zu sehen, die einen Schwellenwert darstellt, z. B. einen SLA-Wert (Service Level Agreement), fügen Sie Ihrem Diagramm eine statische Schwellenwertlinie hinzu.

Benennen Sie Legendenbeschriftungen und den Diagrammtitel um
Bei Diagrammen, die eine Legende anzeigen, können Sie einen Metriknamen in der Diagrammlegende mit einem benutzerdefiniertes Etikett. Klicken Sie im Metric Explorer auf das Label im Vorschaufenster und wählen Sie **Umbenennen**. Um ein Diagramm umzubenennen, klicken Sie auf den Diagrammtitel und wählen Sie **Umbenennen**.

Passen Sie Ihr Diagramm auf der Registerkarte Optionen an
Sie können auf die folgenden Optionen zugreifen, um die Diagrammeigenschaften und die Anzeige von Metrikdaten in Ihrem Diagramm anzupassen:

- Metrikdaten von Byte in Bits umwandeln
- Metrik Daten von Basis 2 (Ki=1024) nach Basis 10 (K = 1000) umrechnen
- Ändern Sie die Y-Achse in einem Zeitreihendiagramm von der linearen zur logarithmischen Skala
- Metrikwerte in einem Diagramm abkürzen (z. B. 16.130.542 Byte auf 16,1 MB abkürzen)
- Sortieren Sie Metrikdaten in aufsteigender oder absteigender Reihenfolge in einem Balken-, Listen- oder Wertdiagramm
- Ändern Sie die Perzentilgenauigkeit in einem Tortendiagramm
- Eine Diagrammlegende ein- oder ausblenden
- Blenden Sie inaktive Metriken mit einem Nullwert aus, sodass diese Metriken im Diagramm, einschließlich der Legende und der Bezeichnung, nicht sichtbar sind
- Sparkline in eine Liste oder ein Wertdiagramm aufnehmen
- Den Warnstatus für Daten anzeigen, die in Listen- oder Wertdiagrammen angezeigt werden (weitere Informationen finden Sie unter Warnmeldungen)
- Schalten Sie die Farbdarstellung für Metrikdaten auf Graustufen um (mit Ausnahme von Diagrammen , die einen Warnstatus anzeigen)
- Zeigen Sie für IP-Adressbezeichnungen den Hostnamen (falls er anhand des DNS-Datenverkehrs in wire data erkannt wurde) oder die ursprüngliche IP-Adresse (wenn ein Proxy anhand von wire data erkannt wird) an
- Zeigt die relative Zeit für ein Ablaufdatum an, z. B. die Anzahl der Tage, bis ein TLS-Zertifikat abläuft.

Hinweis: Einige Optionen sind nur für bestimmte Diagrammtypen verfügbar. Beispielsweise erscheint die Option, eine Sparkline einzuschließen, nur auf der Registerkarte „Optionen“ für Listen- und Wertdiagramme.

Erstellen Sie eine Ad-hoc-Gruppe, um Daten aus mehreren Quellen zu kombinieren
Auf der Registerkarte „ Metrik“ können Sie eine Ad-hoc-Gruppe mit mehreren Quellen innerhalb eines Sets erstellen, indem Sie **Quellen kombinieren**. Sie können beispielsweise zwei Anwendungen kombinieren und dann einen einzelnen Metrikwert im Diagramm für beide Anwendungen anzeigen.

Nächste Schritte
Üben Sie das Erstellen von Diagrammen, indem Sie die folgenden exemplarischen Vorgehensweisen ausführen:

- Überwachen Sie DNS-Fehler in einem Dashboard
- Überwachen Sie den Zustand der Datenbank in einem Dashboard
- Überwachen Sie die Webleistung in einem Dashboard

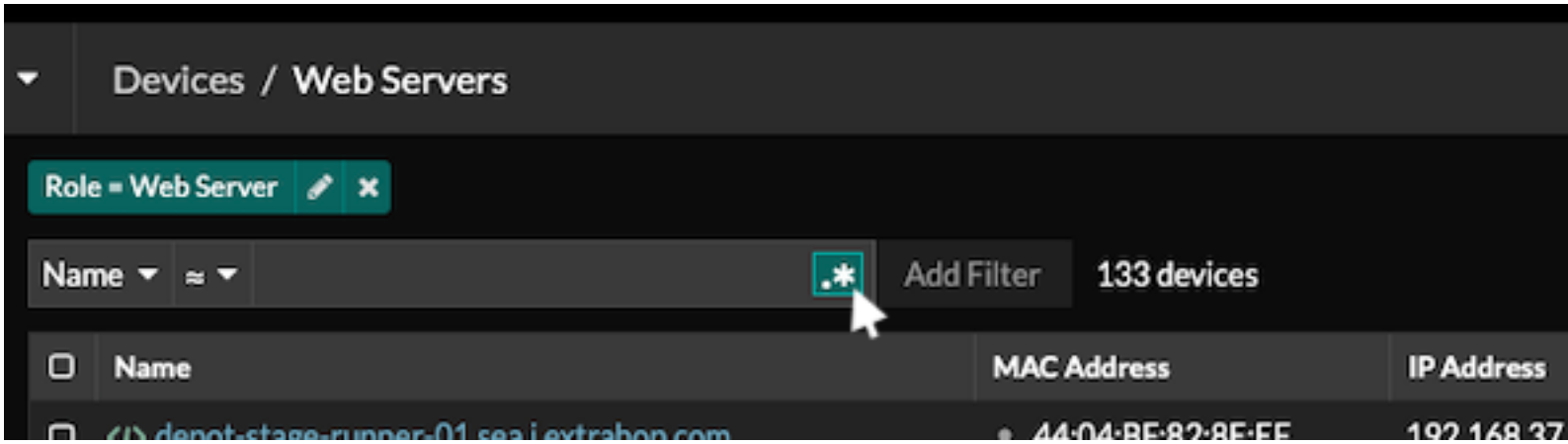
Filter für reguläre Ausdrücke

Filtern Sie Ihre Suchergebnisse, indem Sie in bestimmte Suchfelder im gesamten ExtraHop-System Zeichenketten mit regulären Ausdrücken (Regex) schreiben. Sie können beispielsweise nach Parametern in einem Detail-Metrik Metrikschlüssel filtern, z. B. nach einer Zahl innerhalb einer IP-Adresse. Sie können auch filtern, indem Sie bestimmte Schlüssel oder eine Kombination von Schlüsseln aus Diagrammen ausschließen.

Regex-fähige Suchfelder verfügen über visuelle Indikatoren im gesamten System und akzeptieren die Standardsyntax.

Suchfelder mit einem Sternchen

Klicken Sie auf das Sternchen, um Regex-Zeichenfolgen zu aktivieren.

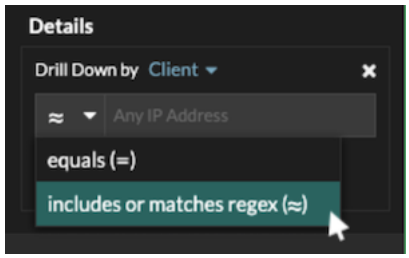


Dieser Feldtyp ist auf den folgenden Systemseiten verfügbar:

- Eine Tabelle mit Geräten filtern
- Filterkriterien für eine dynamische Gerätegruppe erstellen

Bestimmte Suchfelder mit einem Dreifeld-Operator

Klicken Sie auf das Operator-Dropdown-Menü, um die Regex-Option auszuwählen.

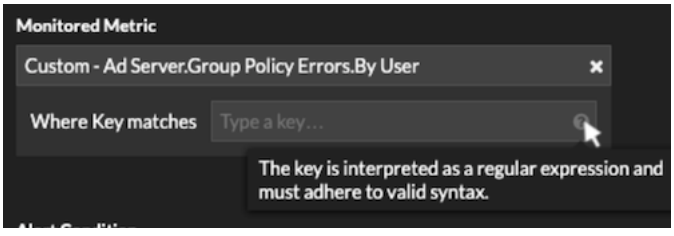


Dieser Feldtyp ist auf der folgenden Systemseite verfügbar:

- Ein Diagramm im Metric Explorer bearbeiten

Bestimmte Suchfelder mit einem Tooltip

Zeigen Sie mit der Maus auf den Tooltip im Feld, um zu sehen, wann Regex erforderlich ist.



Dieser Feldtyp ist auf der folgenden Systemseite verfügbar:

- Hinzufügen von Datensatzbeziehungen zu einer benutzerdefinierten Metrik

Die folgende Tabelle enthält Beispiele für die Standard-Regex-Syntax.

Diagrammszenario	Regex-Filter	So funktioniert's
Vergleichen Sie HTTP-Statuscodes `200` zu `404`.	`(200|404)`	Das vertikale Balkensymbol (|) ist der OR-Operator. Dieser Filter entspricht `200`, oder `404`, oder beide Statuscodes.

Diagrammszenario	Regex-Filter	So funktioniert's
Zeigt jeden HTTP-Statuscode an, der einen enthält `4`.	`[41]`	Eckige Klammern ([und]) bezeichnen eine Reihe von Zeichen. Der Filter sucht nach jedem Zeichen innerhalb der Klammern, unabhängig von der Reihenfolge. Dieser Filter entspricht jedem Wert, der einen enthält `4` oder ein `1`. Zum Beispiel kann dieser Filter zurückkehren `204`, `400`, `101`, oder `201` Statuscodes.
Alles anzeigen `500`HTTP-Statuscodes auf -Ebene.	`^ [5]`	Das Caret-Symbol (^) außerhalb der eckigen Klammern ([und]) bedeutet „beginnt mit“. Dieser Filter entspricht jedem Wert, der mit einem beginnt `5`. Dieser Filter kann beispielsweise zurückkehren `500` und `502` Statuscodes.
Alles anzeigen `400` und `500` HTTP-Statuscodes auf -Ebene.	`^ [45]`	Mehrere Werte in eckigen Klammern ([und]) werden einzeln durchsucht, auch wenn ihnen das Caret-Symbol (^) vorangestellt ist. Dieser Filter sucht nicht nach Werten, die beginnen mit `45`, entspricht aber allen Werten, die mit einem beginnen `4` oder `5`. Zum Beispiel kann dieser Filter zurückkehren `400`, `403`, und `500` Statuscodes.
Zeigt alle HTTP-Statuscodes an, außer `200` Statuscodes auf -Ebene.	`^ (?! 2)`	Ein Fragezeichen (?) und Ausrufezeichen (!) geben Sie in Klammern einen auszuschließenden Wert an. Dieser Filter entspricht allen Werten außer Werten, die mit einem beginnen `2`. Zum Beispiel kann dieser Filter zurückkehren `400`, `500`, und `302` Statuscodes.
Zeigen Sie eine beliebige IP-Adresse mit einem `187`.	`187.`	Spiele `1`, `8`, und `7` Zeichen in der IP-Adresse. Dieser Filter gibt keine IP-Adressen zurück, die auf 187 enden, da der letzte Punkt angibt, dass nach den Werten etwas stehen muss. Wenn Sie den Punkt als Literalwert durchsuchen möchten, müssen Sie ihm einen umgekehrten Schrägstrich (\) voranstellen.
Überprüfen Sie alle IP-Adressen, die enthalten `187.18.`	`187\ .18.`	Spiele `187.18` und alles, was folgt. Die erste Periode wird wörtlich behandelt, da ihr ein

Diagrammszenario	Regex-Filter	So funktioniert's
		umgekehrter Schrägstrich (\) vorausgeht. Die zweite Periode wird als Platzhalter behandelt. Dieser Filter gibt beispielsweise Ergebnisse für `187.18.0.0`, `180.187.0.0`, oder `187.180.0.0/16`. Dieser Filter gibt keine Adresse zurück, die endet mit `187.18`, weil der Platzhalter erfordert, dass Zeichen den angegebenen Werten folgen.
Zeigt eine beliebige IP-Adresse an, außer `187.18.197.150`.	`^ (?! 187\ .18\ .197\ .150)`	Stimmt mit allem überein, außer `187.18.197.150`, wo `^(?!)` gibt den auszuschließenden Wert an.
Schließt eine Liste bestimmter IP-Adressen aus.	`^(?! 187\.18\.197\.15[012])`	Stimmt mit allem überein, außer `187.18.197.150`, `187.18.197.151`, und `187.18.197.152`, wo `^(?!)` gibt den auszuschließenden Wert an und die eckigen Klammern ([und]) geben mehrere Werte an.

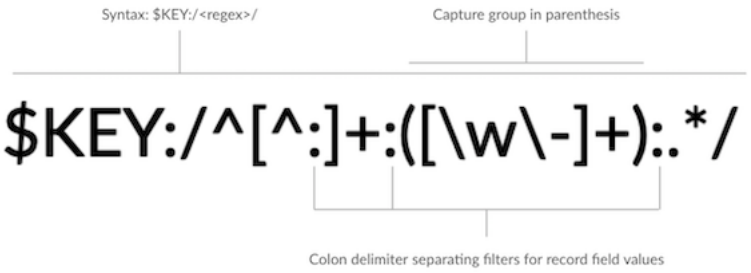
Zusätzliche Filter

Wenn du eine benutzerdefinierte Detail-Metrik erstellen Im Metrikkatalog können Sie dem Suchfeld Zusätzliche Filter im Abschnitt Datensatzbeziehungen eine erweiterte Regex-Syntax hinzufügen.

Der Tooltip wird angezeigt, nachdem Sie ausgewählt haben **Detailmetrik** und ist nicht verfügbar, wenn **Basismetrik** ist ausgewählt.

Die Regex-Syntax in diesem Feld muss die folgenden Anforderungen erfüllen:

- Wenn Ihr Schlüssel mehrere Werte enthält, muss Ihre Regex-Syntax eine einzelne Erfassungsgruppe enthalten. Eine Erfassungsgruppe wird durch Klammern gekennzeichnet. Ihre Capture-Gruppe bestimmt den Filterwert.



- Wenn Sie einen bestimmten Wert aus einem Detailmetrikschlüssel zurückgeben möchten, der mehrere Datensatzfeldwerte enthält, muss die Regex dieser Syntax folgen:

  `$SCHLÜSSEL:/ <regex> /`

  Wenn Ihr Detailmetrikschlüssel beispielsweise ipaddr:host:cipher lautet und Sie nur den IP-Adresswert zurückgeben möchten, geben Sie Folgendes ein:

  `$SCHLÜSSEL: /^ ([^:] +): . +/`
- Wenn Ihr Schlüssel mehrere Datensatzfeldwerte enthält, werden die Werte durch ein Trennzeichen getrennt, das in dem Auslöser angegeben ist, der den Schlüssel generiert. Die Platzierung der Trennzeichen in Ihrer Regex-Syntax muss mit den Trennzeichen im Detailschlüssel übereinstimmen. Wenn Sie beispielsweise einen Schlüssel mit drei Werten haben, die durch ein Trennzeichen getrennt sind, das ein Doppelpunkt ist, müssen die drei Werte für den Schlüssel in Ihrer Regex-Syntax durch zwei Doppelpunkte getrennt werden.

Hinweis: Wenn Sie alle Datensatzfeldwerte in einem detaillierten Metrikschlüssel zurückgeben möchten, geben Sie ein `$SCHLÜSSEL`. Wenn Ihr Detailmetrikschlüssel beispielsweise ipaddr:host:cipher lautet, geben Sie Folgendes ein `$SCHLÜSSEL` im Suchfeld , um alle drei dieser Felddatensatzwerte (IP-Adresse, Hostname und TLS Verschlüsselungssuite) zurückzugeben.

Ein Textfeld-Widget bearbeiten

Wenn Sie erläuternden Text neben Ihren Dashboard-Diagrammen einfügen oder ein Firmenlogo in Ihrem Dashboard anzeigen möchten, können Sie ein Textfeld-Widget bearbeiten. Mit dem Textfeld-Widget können Sie Text, Links, Bilder oder Beispielmetriken in Ihrem Dashboard anzeigen.

Video: Sehen Sie sich die entsprechende Schulung an: Kontext mit Textfeld-Widgets bereitstellen

Das Textfeld-Widget unterstützt Markdown, eine einfache Formatierungssyntax, die einfachen Text in HTML mit nicht alphabetischen Zeichen wie „#“ oder „*“ konvertiert. Neue Textfeld-Widgets enthalten Markdown-Beispiele. Jedes Mal wird automatisch ein Textfeld-Widget bereitgestellt ein Dashboard erstellen. Du kannst auch fügen Sie Ihrem Dashboard-Layout ein Textfeld-Widget Widget.

Gehen Sie wie folgt vor, um ein vorhandenes Textfeld-Widget zu bearbeiten:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Armaturenbretter**.
3. Wählen Sie im Dashboard-Dock ein Dashboard aus, das das Textfeld enthält, das Sie bearbeiten möchten.
4. Klicken Sie auf das Befehlsmenü ⋮ in der oberen rechten Ecke und wähle **Layout bearbeiten**.
5. Klicken Sie auf das Textfeld.
6. Geben Sie links Text ein und bearbeiten Sie ihn Redakteur Scheibe.

Der HTML-Ausgabetext wird dynamisch rechts angezeigt Vorschau Scheibe. Mit Markdown können Sie die folgenden Arten von Inhalten formatieren:

- Text formatieren
- Bilder hinzufügen
- Beispiele für Metrik hinzufügen

7. Klicken Sie **Speichern** um den Metric Explorer zu schließen.

Text in Markdown formatieren

Die folgende Tabelle zeigt gängige Markdown-Formate, die im Textfeld-Widget unterstützt werden.

Hinweis: Weitere Beispiele für das Markdown-Format finden Sie im GitHub-Anleitungen: Markdown beherrschen und in der CommonMark-Spezifikation.

Format	Beschreibung	Beispiel
Überschriften	Platzieren Sie ein Nummernzeichen (#) und ein Leerzeichen vor Ihrem Text, um Überschriften zu formatieren. Die Ebene der Überschrift wird durch die Anzahl der Nummernzeichen bestimmt.	`#### Example H4 heading`
Ungeordnete Listen	Platzieren Sie ein einzelnes Sternchen (*) vor Ihrem Text. Wenn möglich, fügen Sie jedes Listenelement in eine separate Zeile ein.	`* First example` `* Second example`
Geordnete Listen	Platzieren Sie für jeden Zeileneintrag eine Zahl 1 und einen Punkt (1.) vor Ihrem Text. Markdown erhöht automatisch die Listennummer. Wenn möglich, fügen Sie jedes Listenelement in eine separate Zeile ein.	`1. First example` `1. Second example`
Mutig	Platzieren Sie doppelte Sternchen vor und nach Ihrem Text.	`**bold text**`
Kursivschrift	Platzieren Sie einen Unterstrich vor und nach Ihrem Text.	`_italicized text_`
Hyperlinks	Platzieren Sie den Linktext in Klammern vor der URL in Klammern. Oder geben Sie Ihre URL ein. Links zu externen Websites werden in einem neuen Browser-Tab geöffnet. Links innerhalb des ExtraHop-Systems, wie z. B. Dashboards, werden im aktuellen Browser-Tab geöffnet.	`[Visit our home page](https://www.extrahop.com)` `https://www.extrahop.com`
Anführungszeichen blockieren	Platzieren Sie eine rechtwinklige Klammer und ein Leerzeichen vor Ihrem Text.	`On the ExtraHop website:`

Format	Beschreibung	Beispiel
		`> Access the live demo and review case studies.`
Monospace-Schrift	Platziere einen Backtick (`) vor und nach deinem Text.	`` `example code block` ``
Emojis	Kopieren Sie ein Emoji-Bild und fügen Sie es in das Textfeld ein. Sehen Sie die Unicode-Emoji-Diagramm Website für Bilder. Die Markdown-Syntax unterstützt keine Emoji-Shortcodes.	

Bilder in Markdown hinzufügen

Sie können dem Textfeld-Widget Bilder hinzufügen, indem Sie auf sie verlinken. Stellen Sie sicher, dass Ihr Bild in einem Netzwerk gehostet wird, auf das das ExtraHop-System zugreifen kann.

Links zu Bildern müssen im folgenden Format angegeben werden:

```
![<alt_text>](<file_path>)
```

Wo *<alt_text>* ist der alternative Text für den Bildnamen und *<file_path>* ist der Pfad des Bildes. Zum Beispiel:

```
![Graph](/images/graph_1.jpg)
```

Hinweis: Sie können Bilder auch hinzufügen, indem Sie sie in Base64 kodieren. Weitere Informationen finden Sie im folgenden Beitrag im ExtraHop-Forum:"Kodieren Sie ein Bild für die Aufnahme in ein Textfeld".

Fügen Sie Metrikbeispiele in Markdown hinzu

Sie können eine Metrikabfrage schreiben, um einen Metrikwert in das Textfeld-Widget einzubeziehen. Um beispielsweise zu zeigen, wie viele Webserver einen 404-Fehler zurückgegeben haben, können Sie einem Satz eine Metrikabfrage hinzufügen und der Wert wird im Text aktualisiert.

Das folgende Beispiel zeigt das grundlegende Format für das Schreiben von Metrikabfragen:

```
%%metric:{
    "metric_category": "<metric_category>",
    "object_type": "<object_type>",
    "object_ids": [object_id],
    "metric_specs": [
        {
            "name": "<metric_spec>"
        }
    ]
}%%
```

Um das zu finden `object_type`, `metric_spec`, und `metric_category` Werte für eine Metrik, führen Sie die folgenden Schritte aus:

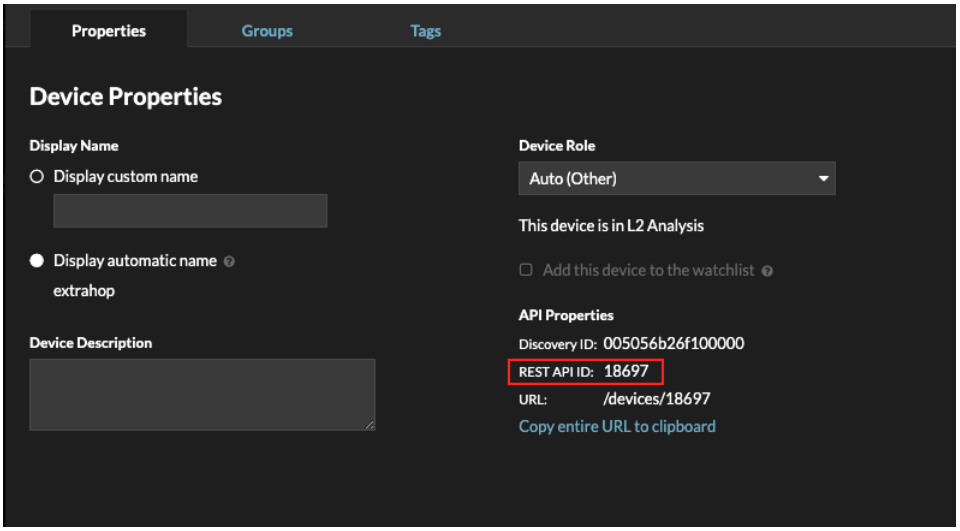
1. klicken **Einstellungen**
2. klicken **Metrischer Katalog**.
3. Geben Sie den Metriknamen in das Suchfeld Feld.
4. Wählen Sie die Metrik aus und notieren Sie sich die Werte für `metric_category`, `object_type`, und `metric_spec` in der REST-API-Parameter Abschnitt.

Die folgende Abbildung zeigt Werte für NFS-Server — TCP-Anfragen nach Client.

Um das zu finden `object_id` Führen Sie für ein Gerät, eine Gerätegruppe oder ein anderes Asset die folgenden Schritte aus:

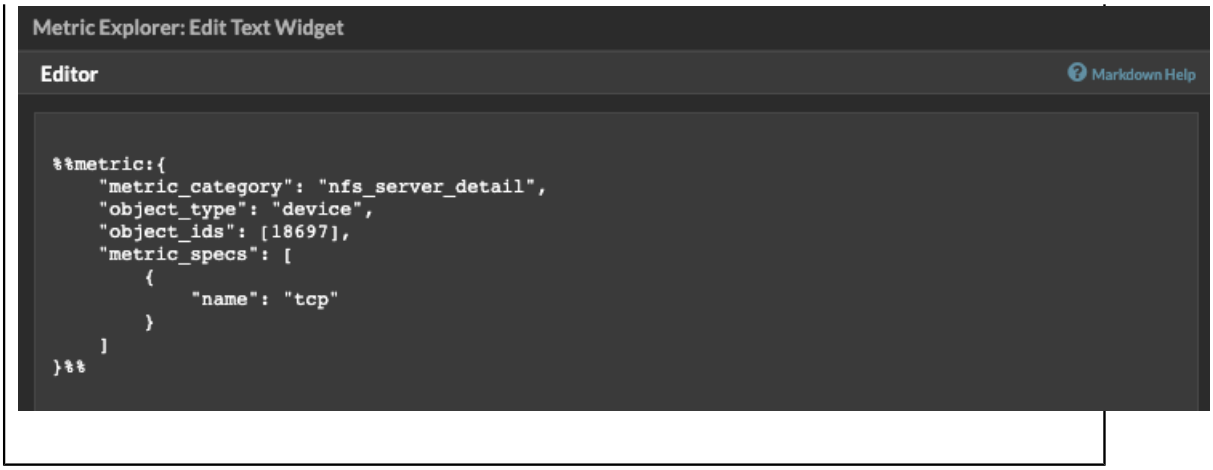
1. klicken **Vermögenswerte**, und klicken Sie dann im linken Bereich auf einen Asset-Typ.
2. Klicken Sie auf den Namen des gewünschten Asset, und öffnen Sie dann das Eigenschaftenfenster.
3. Notieren Sie sich den Wert, der für die REST-API-ID angezeigt wird.

Die folgende Abbildung zeigt die Eigenschaften für ein Gerät mit der ID 18697.



Nachdem Sie die Werte für die Metrik gefunden haben, die Sie anzeigen möchten, fügen Sie sie der Metrikabfrage im Texteditor hinzu. Der Wert wird im Text-Widget angezeigt.

Das folgende Beispiel-Markup zeigt die Anzahl der empfangenen TCP-Anfragen, aufgelistet nach Client-IP-Adresse, für einen NFS-Server mit der Objekt-ID 18697 an.



Hinweis: Die folgenden Metrikabfragen werden im Textfeld-Widget nicht unterstützt:

- Zeitreihenabfragen
- Mittelwertberechnungen
- Mehrere object_ids
- Mehrere metric_spec
- Mehrere Perzentile

Beispiele für metrische Abfragen für das Textfeld-Widget
Die folgenden Beispiele zeigen Ihnen, wie Sie Metrikabfragen der obersten Ebene oder Basis für Anwendung-, Gerät- und Netzwerkobjekte schreiben. Sie können auch eine Abfrage für Detailmetriken schreiben.

Anwendungsmetriken

Um das Objekt All Activity zu spezifizieren, `object_ids` ist "`0`".

Diese Beispielabfrage zeigt, wie Sie HTTP-Metriken aus dem Anwendungsobjekt All Activity abrufen können, und zeigt die folgende Ausgabe an:"`Getting [value] HTTP requests and [value] HTTP responses from All Activity.`"

```
Getting
%%metric:{
"object_type": "application",
"object_ids": [0],
"metric_category": "http",
"metric_specs": [{"name":"req"}]
}%%HTTP requests and
%%metric:{
"object_type": "application",
"object_ids": [0],
"metric_category": "http",
"metric_specs": [{"name":"rsp"}]
}%%
HTTP responses from All Activity.
```

Geräte-Metriken

Sie müssen entweder einen Client angeben ("`_client`") oder Server ("`_server`") in der `metric_category`. Um Metriken für ein bestimmtes Gerät abzurufen, geben Sie die Geräteobjekt-ID-Nummer in `object_ids`. Um die Geräteobjekt-ID abzurufen (`deviceOid`), suchen Sie in der globalen ExtraHop-Suche nach dem Geräteobjekt. Wählen Sie das Gerät aus Ihren Suchergebnissen aus. Das "`deviceOid=`" Der Wert wird in die URL-Abfragezeichenfolge eingebettet.

Diese Beispielabfrage zeigt, wie Metriken von einem Geräteclient-Objekt abgerufen werden, und zeigt die folgende Ausgabe an:“`Getting [value] CLIENT DNS response errors from a specific device.`“

```
Getting
%%metric:{"object_type": "device",
"object_ids": [8],
"metric_category": "dns_client",
"metric_specs": [{"name":"rsp_error"}]
}%%
CLIENT DNS response errors from a specific device.
```

Diese Beispielabfrage zeigt, wie Metriken von einem Geräteserverobjekt abgerufen werden, und zeigt die folgende Ausgabe an:“`Getting [value] SERVER DNS response errors from a specific device.`“

```
Getting
%%metric:{
"object_type": "device",
"object_ids": [156],
"metric_category": "dns_server",
"metric_specs": [{"name":"rsp_error"}]
}%%
SERVER DNS response errors from a specific device.
```

Netzwerk-Metriken

Um Alle Netzwerke anzugeben, `object_type` ist“`capture`“ und die `object_ids` ist“`0`.“ Um ein bestimmtes VLAN anzugeben, `object_type` ist“`vlan`“ und die `object_ids` ist die VLAN-Nummer.

Diese Beispielabfrage zeigt, wie Metriken für alle Netzwerke abgerufen werden, und zeigt die folgende Ausgabe an:“`Getting [value] broadcast packets from all networks.`“

```
Getting
%%metric:{
"object_type": "capture",
"object_ids": [0],
"metric_category": "net","metric_specs":
 [{"name":"frame_cast_broadcast_pkts"}]
}%%
broadcast packets from all networks.
```

Diese Beispielabfrage zeigt, wie Metriken für ein bestimmtes VLAN abgerufen werden, und zeigt die folgende Ausgabe an:“`Getting [value] broadcast packets from VLAN 3.`“

```
Getting
%%metric:{
"object_type": "vlan",
"object_ids": [3],
"metric_category": "net",
"metric_specs": [{"name":"frame_cast_broadcast_pkts"}]
}%%
broadcast packets from VLAN 3.
```

Kennzahlen für Gruppen

Um eine Gruppe anzugeben, `object_type` ist“`device_group`.“ Sie müssen entweder einen Client angeben (“`_client`“) oder Server (“`_server`“) in der `metric_category`. Die `object_ids` für die spezifische Gruppe muss aus dem REST API Explorer abgerufen werden.

Diese Beispielabfrage zeigt, wie Metriken für alle Netzwerke abgerufen werden, und zeigt die folgende Ausgabe an:“`Getting [value] HTTP responses from the HTTP Client Device Group.`“

```
Getting
%%metric:{
"object_type": "device_group",
"object_ids": [17],
"metric_category": "http_client",
"metric_specs": [{"name":"req"}]
}%%
HTTP responses from the HTTP Client Device Group.
```

Metriken im Detail

Wenn Sie Detailmetriken abrufen möchten, sollte Ihre Metrikabfrage zusätzliche Schlüsselparameter wie Schlüssel1 und Schlüssel2 enthalten:

- Objekttyp
- Objekt-IDs
- metrik_kategorie
- metrische Spezifikation
  - Name
  - Schlüssel 1
  - Schlüssel 2

Die Schlüsselparameter dienen als Filter für die Anzeige Detail-Metrik Ergebnisse. Für nicht benutzerdefinierte Detailmetriken können Sie Detail-Metrik Metrikparameter aus dem Metrikkatalog abrufen. Geben Sie beispielsweise `HTTP-Antworten nach URI`, und schauen Sie sich dann die Parameterwerte im Abschnitt REST-API-Parameter an.

Wichtig: Sie müssen die liefern `object_ids` in Ihrer Anfrage.

Dieses Beispiel zeigt, wie HTTP-Anfragen per URI für die All Activity-Anwendung abgerufen werden (`object_ids` ist“`0`“):

```
%%metric:{
"object_type": "application",
"object_ids": [0],
"metric_category": "http_uri_detail",
"metric_specs": [{"name":"req"}]
}%%
```

Diese Beispielabfrage zeigt Ihnen, wie Sie HTTP-Anfragen anhand von URIs abrufen, die einen Schlüsselwert für“`pagead2`“ für die All Activity-Anwendung (`object_ids` ist“`0`“):

```
%%metric:{
"metric_category": "http_uri_detail",
"object_type": "application",
"object_ids": [0],
"metric_specs": [
{
"name": "req",
"key1": "/pagead2/"
}
]
}%%
```

Diese Beispielabfrage zeigt, wie Zählmetriken für alle Netzwerke abgerufen werden, und zeigt die folgende Ausgabe an:“`Getting [value] detail ICA metrics on all networks.`“

```
Getting
%%metric:{
"object_type": "capture",
"object_ids": [0],
"metric_category": "custom_detail",
"metric_specs": [{
"name":"custom_count",
"key1":"network-app-byte-detail-ICA"
}]
}%%
detail ICA metrics on all networks.
```

Diese Beispielabfrage zeigt, wie eine benutzerdefinierte Datensatzstatistik mit Topn-Schlüsseln und Perzentilen abgerufen wird, und zeigt die folgende Ausgabe an:“`The fifth percentile is: [value].`“

```
The fifth percentile is:
%%metric:{
"object_type": "vlan",
"object_ids": [1],
"metric_category": "custom_detail",
"metric_specs": [{
"name": "custom_dset",
"key1": "myCustomDatasetDetail",
"key2": "/10.10.7/",
"calc_type": "percentiles",
"percentiles": [5]
}]
}%%
.
```

Hinweis Beispielsatz-Metriken werden im Textfeld-Widget nicht unterstützt. Zum Beispiel das Hinzufügen von `"calc_type": "mean"` Der Parameter für Ihre Textfeld-Abfrage wird nicht unterstützt.

Eine Dashboard-Region bearbeiten

Dashboard-Bereiche, die Diagramme und Widgets enthalten, sind hochgradig anpassbar. Bei der Arbeit mit Dashboards müssen Sie eine Region möglicherweise häufig ändern oder kopieren. Sie können einen Region nur löschen, seine Größe ändern oder neu anordnen, indem Sie das Dashboard-Layout bearbeiten.

Gehen Sie wie folgt vor, um grundlegende Eigenschaften einer Region in einem Dashboard zu bearbeiten:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Armaturenbretter**.
3. Wählen Sie im Dashboard-Dock ein Dashboard mit der Region aus, die Sie bearbeiten möchten.
4. Klicken Sie auf die Kopfzeile der Region, um auf die folgenden Optionen zuzugreifen:

   Eine Region umbenennen

   Fügen Sie der Region einen benutzerdefinierten Namen hinzu.

   Quellen ändern

   Ersetzen Sie danach schnell die Datenquellen für jedes Diagramm in einer Region durch eine andere Quelle Diagramm kopieren, Region oder Dashboards.

Eine Region kopieren

Bewegen Sie den Mauszeiger darüber **Kopieren nach...** und treffen Sie eine der folgenden Auswahlen:

- Wählen Sie den Namen eines vorhandenen Dashboard aus der Liste aus. Die Dashboard-Seite wird geöffnet und zeigt den Speicherort der kopierten Region an.

  Hinweis: Die Dashboard-Liste ist von den zuletzt erstellten Dashboards (unten) bis zu den ältesten Dashboards (oben) geordnet.
- Wählen **Dashboard erstellen**. Geben Sie im Fenster Dashboard-Eigenschaften einen Namen für das neue Dashboard ein.

Ändern Sie das Zeitintervall der Region

Wenden Sie ein Zeitintervall an für die gesamte Region, indem Sie den Region Zeitselektor aktivieren.

Vollbild

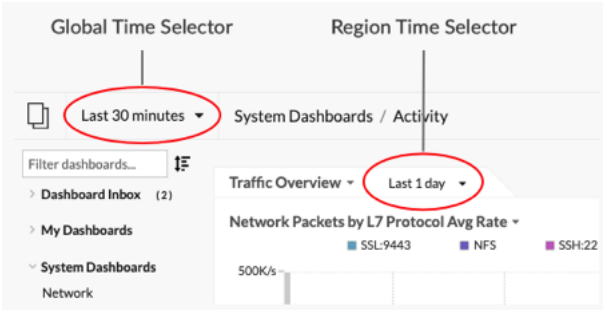
Erweitern Sie den Inhalt der Region zu einer Vollbildanzeige.

Nächste Schritte

- Ein Dashboard-Layout bearbeiten
- Bearbeiten Sie ein Diagramm mit dem Metric Explorer

Ändern Sie das Zeitintervall für eine Dashboard-Region

In einem Dashboard können Sie mit der Global Time Selector ein Zeitintervall auf ein ganzes Dashboard anwenden oder mit der Region Zeitselektor ein anderes Zeitintervall pro Region anwenden.



1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Armaturenbretter**.
3. Wählen Sie ein Dashboard aus.
4. Klicken Sie auf die Kopfzeile der Region und wählen Sie dann **Region Time Selector verwenden**.
5. klicken **Letzte 30 Minuten** und führen Sie einen der folgenden Schritte aus:
   - Wählen Sie auf der Registerkarte Zeitintervall eine der folgenden Optionen aus:
     - Wählen Sie ein anderes Zeitintervall (z. B. **Letzte 30 Minuten**, **Letzte 6 Stunden**, **Letzter Tag**, oder **Letzte Woche**).
     - Geben Sie eine benutzerdefinierte Zeiteinheit an.
     - Wählen Sie einen benutzerdefinierten Zeitraum aus. Klicken Sie auf einen Tag, um das Startdatum für den Bereich anzugeben. Mit einem Klick wird ein einzelner Tag angegeben. Klicken Sie auf einen anderen Tag, um das Enddatum für den Bereich anzugeben.
     - Metrik Deltas vergleichen aus zwei verschiedenen Zeitintervallen.
   - Wählen Sie auf der Registerkarte Verlauf aus bis zu fünf aktuellen Zeitintervallen aus, die in einer vorherigen Anmeldesitzung ausgewählt wurden.
6. klicken **Speichern** um den Region Zeitselektor zu schließen.

Das neue Zeitintervall wird auf alle Diagramme und Widgets innerhalb der Region angewendet.

7. Um das Zeitintervall für die Region zu entfernen, klicken Sie auf die Überschrift der Region und wählen Sie **Verwenden Sie Global Zeitselektor**.
   Wenn das Zeitintervall aus dem Region-Header verschwindet, wird das globale Zeitintervall auf die Region angewendet.

Dashboard-Eigenschaften bearbeiten

Um ein Dashboard umzubenennen, das Design zu ändern oder die URL zu ändern, müssen Sie die Dashboard-Eigenschaften bearbeiten. Wenn Sie ein Dashboard erstellen, haben Sie die Möglichkeit, Dashboard-Eigenschaften anzugeben. Sie können die Dashboard-Eigenschaften jedoch jederzeit ändern.

Sie können jeweils nur die Eigenschaften für ein Dashboard ändern. Sie können Dashboards nicht mehrfach auswählen und eine Eigenschaft ändern, z. B. den Dashboard-Autor.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Dashboards**.
3. Wählen Sie im Dashboard-Dock das Dashboard aus, das Sie bearbeiten möchten.
4. Klicken Sie auf das Befehlsmenü ⋮ in der oberen rechten Ecke der Seite und wählen Sie dann **Eigenschaften des Dashboards**.
5. In der Eigenschaften des Dashboards In diesem Fenster können Sie die folgenden Felder ändern:

   Titel

   Benennen Sie das Dashboard um.

   Autor

   Ändern Sie den Namen des Autors.

   Beschreibung

   Ändern Sie die Beschreibung des Dashboard. Beachten Sie, dass die Beschreibung nur angezeigt wird , wenn Sie die Dashboard-Eigenschaften bearbeiten.

   Permalink

   Ändern Sie die URL für das Dashboard. Standardmäßig ist der Permalink, auch Kurzcode genannt, ein fünfstelliger eindeutiger Bezeichner, der danach angezeigt wird `/Dashboard` in der URL. Sie können den Permalink in einen benutzerfreundlicheren Namen ändern.

   Hinweis: Der Permalink kann aus bis zu 100 Zeichen bestehen, die Buchstaben, Zahlen und die folgenden Symbole kombinieren: Punkt (.), Unterstrich (_), Bindestrich (-), Pluszeichen (+), Klammern () und Klammern ([]). Andere alphanumerische Zeichen werden nicht unterstützt. Der Permalink darf keine Leerzeichen enthalten.

   Teilen

   Um ein Dashboard mit Benutzern zu teilen, die es anzeigen und bearbeiten können, klicken Sie auf den Link. Weitere Informationen finden Sie unter Ein Dashboard teilen.

   Redakteure

   Sehen Sie sich die Liste der ExtraHop-Benutzer mit Bearbeitungszugriff auf das Dashboard an. Um die Benutzer zu ändern, klicken Sie auf **Teilen**.

6. klicken **Speichern**.

Präsentieren Sie ein Dashboard

Sie können Ihr Dashboard so einrichten, dass es für Präsentationen oder für die Bildschirme Ihres Netzwerk Operation Centers im Vollbildmodus angezeigt wird.

Der Vollbildmodus bietet die folgenden Anzeigeoptionen:

- Im Präsentationsmodus können Sie das gesamte Dashboard anzeigen und mit ihm interagieren.
- Sie können einen kontinuierlichen Zyklus jedes Diagramms im Dashboard in einer Widget-Diashow anzeigen.
- Sie können eine ansehen einzelne Region in der Vollbildanzeige.

Gehen Sie wie folgt vor, um ein ganzes Dashboard im Vollbildmodus anzuzeigen:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Armaturenbretter**.
3. Wählen Sie im Dashboard-Dock das Dashboard aus, das Sie präsentieren möchten.
4. Klicken Sie in der oberen rechten Ecke der Seite auf das Befehlsmenü ⋮ und wählen Sie eine der folgenden Optionen:

   Präsentationsmodus

   Das Dashboard-Dock und die oberen Navigationsmenüs werden zusammengeklappt. Im Präsentationsmodus können Sie mit den Komponenten Zeitintervall und Dashboard interagieren.

   Widget-Diashow

   Ein kontinuierlicher Zyklus von Diagrammen und Widgets in der Vollbildanzeige beginnt. Wählen Sie aus, wie lange jedes Widget angezeigt werden soll (z. B. **20 Sekunden**, **15 Sekunden**usw.). Klicken Sie auf **x** Symbol in der oberen rechten Ecke des Bildschirms, um zum Dashboard zurückzukehren.

   Hinweis: Um ein Dashboard im Präsentationsmodus zu öffnen, fügen Sie hinzu `/presentation` an das Ende der URL und dann bookmarken . Zum Beispiel:

   ```
   https://<extrahop_ip>/extrahop/#/Dashboard/437/presentation
   ```

Ein Dashboard teilen

Standardmäßig sind alle benutzerdefinierten Dashboards, die Sie erstellen, privat, was bedeutet, dass keine ExtraHop-Benutzer Ihr Dashboard anzeigen oder bearbeiten können. Sie können Ihr Dashboard jedoch teilen, indem Sie anderen ExtraHop-Benutzern und -Gruppen Ansichts- oder Bearbeitungszugriff gewähren.

Hier sind einige wichtige Überlegungen zum Teilen von Dashboards:

- Wie ein Benutzer mit einem gemeinsam genutzten Dashboard interagiert und welche Informationen er im ExtraHop-System einsehen kann, hängt von den Benutzerrechten ab. Sie können zum Beispiel einen Benutzer mit eingeschränktem Nur-Lese-Recht hinzufügen, wodurch dieser Benutzer nur die Dashboards sehen kann, die Sie mit ihm im ExtraHop-System teilen. Weitere Informationen finden Sie in der Benutzerrechte Abschnitt im ExtraHop-Administratorhandbuch.
- Wenn Sie einem Benutzer die Bearbeitungsberechtigung gewähren, kann dieser Benutzer das Dashboard ändern und mit anderen teilen und es einer Sammlung hinzufügen. Andere Benutzer können das Dashboard jedoch nicht löschen. Nur der Dashboard-Besitzer kann ein Dashboard löschen.
- Gruppeninformationen werden aus LDAP (wie OpenLDAP oder Active Directory) in das ExtraHop-System importiert. Benutzerinformationen sind verfügbar, nachdem sich ein ExtraHop-Benutzer bei seinem Konto angemeldet hat.
- Um ein Dashboard mit einem Nicht-ExtraHop-Benutzer zu teilen, können Sie eine PDF-Datei des Dashboard erstellen.
- Du kannst einen geplanten Dashboard-Bericht erstellen, das die PDF-Datei des Dashboard regelmäßig an jeden E-Mail-Empfänger sendet. (Nur Konsolen.)

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.

2. Klicken Sie oben auf der Seite auf **Armaturenbretter**.
3. Wählen Sie im Dashboard-Dock ein Dashboard aus, das Sie teilen möchten.

   Sie können keine System-Dashboards oder Dashboards teilen, für die Sie keinen Bearbeitungszugriff haben.
4. Klicken Sie auf das Befehlsmenü ⋮ in der oberen rechten Ecke der Dashboard-Seite und wählen Sie **Teilen**.
5. Um jedem Benutzer die Leseberechtigung zu gewähren, wählen Sie **Allen Benutzern erlauben, dieses Dashboard zu sehen**.
6. Gehen Sie wie folgt vor, um bestimmten Benutzern und Gruppen Anzeige- oder Bearbeitungsberechtigungen zu erteilen:
   a) Geben Sie den Namen eines Benutzers oder einer Gruppe ein, und wählen Sie dann den Namen aus der Dropdownliste aus.
   b) Wählen Sie neben dem Namen **Kann ansehen** oder wählen **Kann bearbeiten**.
7. klicken **Speichern**.
   Wenn du dein Dashboard geteilt hast, erscheint ein kleines graues Symbol neben deinem Dashboard im Dock.

Zugriff auf ein Dashboard entfernen

Sie können den Dashboard-Zugriff, den Sie Benutzern und Gruppen gewährt haben, entfernen oder ändern.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Armaturenbretter**.
3. Wählen Sie im Dashboard-Dock das benutzerdefinierte Dashboard aus, das Sie ändern möchten.
4. Klicken Sie auf das Befehlsmenü ⋮ in der oberen rechten Ecke der Seite und wählen **Teilen**.
5. Entfernen Sie den Zugriff für Benutzer oder Gruppen, indem Sie einen der folgenden Schritte ausführen:
   - Entfernen Sie den gesamten Zugriff für einen Benutzer oder eine Gruppe, indem Sie auf das rote Löschen klicken **(x)** Symbol neben dem Benutzer- oder Gruppennamen.
   - Entfernen Sie den Bearbeitungszugriff, indem Sie **Kann ansehen** aus der Dropdownliste neben dem Benutzer- oder Gruppennamen.
6. klicken **Speichern**.

Eine Dashboard-Sammlung erstellen

Sie können eine Sammlung erstellen, um Dashboards zu organisieren, die Ihnen gehören und die mit Ihnen geteilt wurden.

Im Folgenden finden Sie einige wichtige Überlegungen zu Dashboard-Sammlungen:

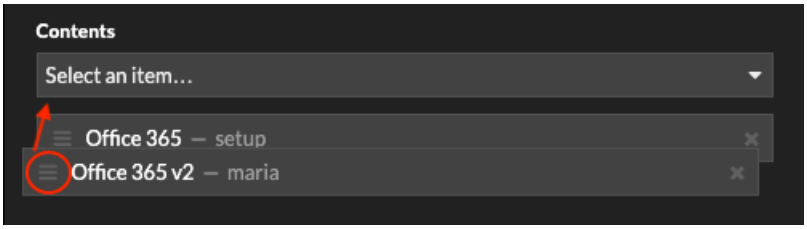
- Ihr Benutzerrechte bestimmen Sie , ob Sie Sammlungen erstellen und teilen können.
- Sie können einer Sammlung jedes Dashboard hinzufügen, das Ihnen gehört oder das Sie anzeigen oder bearbeiten dürfen.
- Sie können ein Dashboard zu mehreren Sammlungen hinzufügen.
- Sie können eine Sammlung teilen, wenn Sie Eigentümer aller Dashboards in dieser Sammlung sind oder über Bearbeitungsberechtigungen verfügen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Dashboards**.
3. klicken **Sammlungen** oben im Dashboard-Dock und dann klicken **Sammlung erstellen** am unteren Rand des Docks.

4. In der **Name** Feld, geben Sie einen eindeutigen Namen für die Sammlung ein.
5. Optional: In der **Beschreibung** Feld, füge Informationen über die Sammlung hinzu.
6. Optional: Geben Sie den Namen eines Benutzers oder einer Gruppe in das **Teilen** Dropdownliste, wählen Sie aus den Suchergebnissen aus, und klicken Sie dann auf **Hinzufügen**.
7. Geben Sie den Namen eines Dashboard in das **Inhalt** Drop-down-Liste und wählen Sie dann aus den Suchergebnissen aus.

   Der Name des Besitzers wird für jedes hinzugefügte Dashboard angezeigt.

   Hinweis: Das Dashboard oben in der Liste wird standardmäßig angezeigt, wenn die Sammlung im Dashboard-Dock ausgewählt wird. Klicken Sie auf das Symbol neben einem Dashboard-Namen und ziehen Sie es, um die Liste neu zu ordnen.



8. klicken **Speichern**.
   Die Sammlung wird dem Dashboard-Dock hinzugefügt.

Eine Dashboard-Sammlung teilen

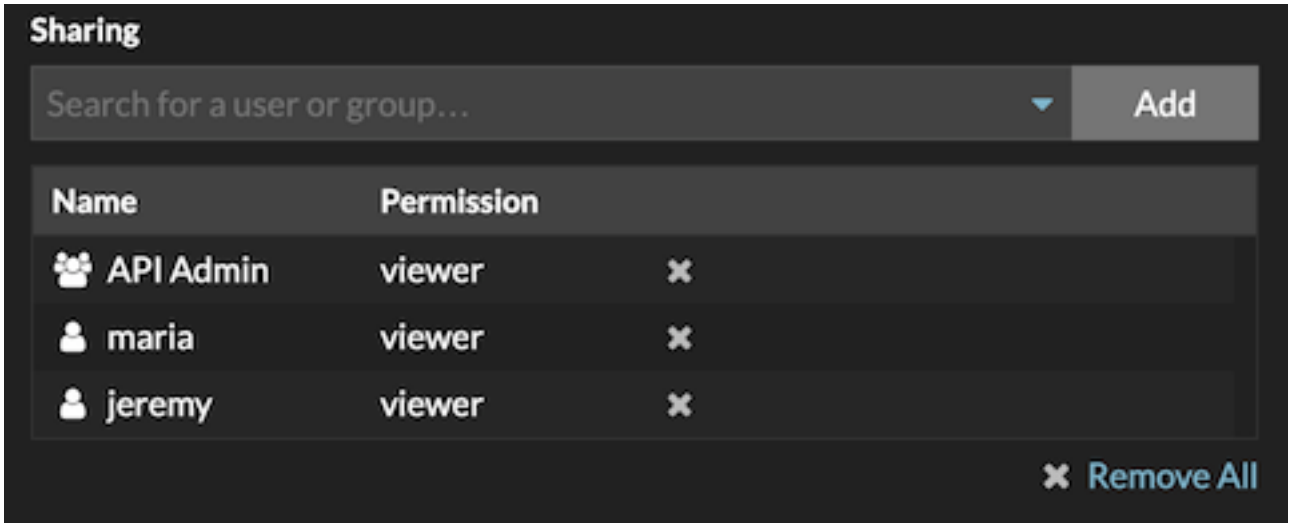
Standardmäßig sind alle Dashboard-Sammlungen privat, was bedeutet, dass keine anderen Benutzer Ihre Sammlung ansehen oder bearbeiten können. Sie können Ihre Sammlung jedoch mit anderen Benutzern und Gruppen teilen.

Hier sind einige wichtige Überlegungen zum Teilen von Dashboard-Sammlungen:

- Sie können eine Sammlung nur teilen, wenn Sie Eigentümer aller Dashboards in der Sammlung sind oder die Berechtigung haben, sie zu bearbeiten.
- Benutzer können nur die Dashboards in einer geteilten Sammlung anzeigen; sie können keine Sammlungseigenschaften bearbeiten.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Armaturenbretter**.
3. klicken **Sammlungen** oben im Armaturenbrett-Dock.
4. Klicken Sie auf die Sammlung, die Sie teilen möchten, und klicken Sie dann auf **Bearbeiten**.
5. Geben Sie den Namen eines Benutzers oder einer Gruppe in das **Teilen** Drop-down-Liste und wählen Sie dann aus den Suchergebnissen aus.
6. klicken **Hinzufügen**.

   Der Benutzer oder die Gruppe wird in einer Liste von gemeinsam genutzten Benutzern angezeigt.



Hinweis: Entfernen Sie einen Benutzer oder eine Gruppe, indem Sie auf das Entfernen-Symbol (X) neben dem Namen klicken.

7. klicken **Speichern**.
   Die Sammlung wird für jeden geteilten Benutzer im Dashboard-Dock angezeigt.

Daten exportieren

Sie können Diagrammdaten aus dem ExtraHop-System in den Formaten CSV und XLSX exportieren.

Du kannst auch PDFs erstellen von ExtraHop-Diagrammen, Seiten und Dashboards.

Daten nach Excel exportieren

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Navigieren Sie zu einem Dashboard oder Protokollseite.
3. Klicken Sie mit der rechten Maustaste auf ein Diagramm, eine Tabelle oder eine Metrik und wählen Sie **Nach Excel exportieren**.

Daten nach CSV exportieren

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Navigieren Sie zu einem Dashboard oder Protokollseite.
3. Klicken Sie mit der rechten Maustaste auf ein Diagramm, eine Tabelle oder eine Metrik und wählen Sie **In CSV exportieren**.

Erstellen Sie eine PDF-Datei

Sie können Daten aus einem Dashboard, einer Protokollseite oder einem einzelnen Diagramm als PDF-Datei exportieren.

1. Suchen Sie das Dashboard oder die Protokollseite, die die Daten enthält, die Sie exportieren möchten, und führen Sie einen der folgenden Schritte aus:

- Um eine PDF-Datei der gesamten Seite zu erstellen, klicken Sie auf das Befehlsmenü ⋮ in der oberen rechten Ecke der Seite und wählen **Drucken** von einem Sensor oder **Als PDF exportieren** von einer Konsole aus.
- Um eine PDF-Datei eines einzelnen Diagramms oder Widget zu erstellen, klicken Sie auf den Diagrammtitel und wählen Sie **Drucken** von einem Sensor oder wählen **Als PDF exportieren** aus dem Drop-down-Menü auf einer Konsole.

2. Ein PDF-Vorschaufenster wird geöffnet. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie **Seite drucken** und wählen Sie dann **PDF** als Ziel aus den Druckeinstellungen in Ihrem Browser.
   - Klicken Sie von einem Sensor aus auf **Widget drucken** und wähle **PDF** als Ziel aus den Druckeinstellungen in Ihrem Browser.
   - Wählen Sie auf einer Konsole Anpassungen im PDF-Format und klicken Sie dann **Als PDF exportieren**. Das Generieren einer PDF-Datei kann mehrere Sekunden dauern.

Passen Sie das Format einer PDF-Datei an

Beim Erstellen einer PDF-Datei einer Dashboard- oder Protokollseite aus einem Konsole, haben Sie mehrere Möglichkeiten, das Erscheinungsbild Ihrer PDF-Datei anzupassen.

1. Geben Sie einen benutzerdefinierten Namen für Ihre PDF-Datei ein oder akzeptieren Sie den Standardnamen.
2. Wählen Sie eine der folgenden Optionen für die Seitenbreite:

   Schmal

   Zeigt großen Text in Diagrammtiteln und Beschriftungen an, bietet jedoch weniger Platz für die Anzeige von Diagrammdaten. Lange Diagrammtitel und Beschriftungen werden möglicherweise gekürzt.

   Mittel

   (Empfohlen) Zeigt eine Ansicht von Diagrammtiteln, Legenden und Daten an, die für die Seitenausrichtung im Hochformat optimiert ist.

   Breit

   Zeigt kleinen Text in Diagrammtiteln und Beschriftungen an, bietet jedoch mehr Platz für die Anzeige von Diagrammdaten.
3. Wählen Sie eine der folgenden Optionen für den Seitenumbruch:

   Einzelne Seite

   Zeigt das gesamte Dashboard oder die Protokollseite auf einer einzigen, fortlaufenden Seite an. Mit dieser Einstellung wird möglicherweise eine PDF-Datei generiert, die größer als die Standardseitenformate für Drucker ist.

   Seitenumbruch pro Region

   Zeigt jeden Diagrammbereich auf einer einzelnen Seite an.
4. Wählen Sie eines der folgenden Themen:

   Licht

   Weißer Hintergrund mit dunklem Text.

   Dunkel

   Schwarzer Hintergrund mit weißem Text.

   Weltall

   Dunkler Hintergrund mit stilisiertem Hintergrundbild und Text.
5. klicken **Als PDF exportieren**.

   Das Generieren einer PDF-Datei kann mehrere Sekunden dauern.

Nächste Schritte

Die PDF-Datei wird auf Ihren lokalen Computer heruntergeladen. Jede PDF-Datei enthält den Titel und das Zeitintervall des Dashboard. klicken **Bericht auf ExtraHop ansehen** um das ursprüngliche Dashboard zu öffnen, das auf das in der PDF-Datei angegebene Zeitintervall eingestellt ist.

Einen geplanten Bericht erstellen

Von einem Konsole, können Sie festlegen, dass Berichte, die Informationen über Aktivitäten auf Ihrem ExtraHop-System enthalten, per E-Mail an bestimmte Empfänger gesendet werden. Erstellen Sie einen geplanten Dashboard-Bericht, um eine PDF-Datei mit ausgewählten Dashboard-Informationen, einschließlich Diagrammen und Metriken, per E-Mail zu senden. Erstellen Sie einen geplanten Sicherheitsbetriebsbericht, um eine PDF-Datei mit einer Zusammenfassung der wichtigsten Erkennungen und Risiken für Ihr Netzwerk per E-Mail zu versenden.

Erstellen Sie einen geplanten Dashboard-Bericht

Wenn Sie einen geplanten Dashboard-Bericht erstellen, können Sie angeben, wie oft der Bericht per E-Mail gesendet wird und in welchem Zeitintervall die Dashboard-Daten in der PDF-Datei enthalten sind.

Bevor Sie beginnen

- Ihr Benutzerkonto muss über eine beschränkte Schreibfähigkeit oder mehr verfügen Privilegien.
- Ihr ExtraHop-System muss konfiguriert für den Versand von E-Mails. (Nur RevealX Enterprise)
- Sie müssen sich an einer Konsole auf dem ExtraHop-System anmelden.
- Sie können einen Bericht nur für Dashboards erstellen, die Sie besitzen oder auf die Sie gemeinsamen Zugriff haben.
- Wenn Sie einen Bericht für ein Dashboard erstellen, das später gelöscht wird oder auf das Sie nicht mehr zugreifen können, wird trotzdem eine E-Mail an die Empfänger gesendet. Die E-Mail enthält jedoch nicht die PDF-Datei und einen Hinweis, dass das Dashboard für den Berichtsbesitzer nicht verfügbar ist.

Gehen Sie wie folgt vor, um einen geplanten Dashboard-Bericht zu erstellen:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Geplante Berichte**.
3. Klicken Sie **Erstellen**.
4. Geben Sie einen eindeutigen Namen für den Bericht in das **Name des Berichts** Feld.
5. Optional: In der **Beschreibung** Feld, geben Sie Informationen zum Bericht ein. Die Beschreibung erscheint nicht im Abschlussbericht, sondern nur in den Berichtseinstellungen.
6. Wählen Sie im Abschnitt Berichtstyp **Armaturenbrett**.
7. Aus dem **Inhalt des Berichts** Drop-down-Liste, wählen Sie ein Dashboard aus.
   - Wenn Ihre Umgebung mehrere Standorte hat, müssen Sie eine Standort auswählen.
   - Wenn das Dashboard, das Sie auswählen, eine dynamische Quelle hat, müssen Sie eine Quelle auswählen.
8. Optional: Aus dem **Inhalt des Berichts** Wählen Sie in der Dropdownliste zusätzliche Dashboards aus, die Sie dem Bericht hinzufügen möchten.
9. Aus dem Zeitplan Führen Sie im Abschnitt die folgenden Schritte aus, um einen Zeitplan für den Bericht zu konfigurieren:
   a) Aus dem Zeitintervall Abschnitt, wählen Sie den Zeitraum der Daten aus, die Sie in den Bericht aufnehmen möchten.

Letzte...	Geben Sie ein Zeitintervall relativ zu dem Zeitpunkt an, zu dem Sie den Bericht angeben, der per E-Mail gesendet werden soll.

Vorige Kalenderwoche	Wählen Sie diese Option, um Daten aus der gesamten Kalenderwoche vor dem Zeitpunkt zu senden, zu dem Sie den Bericht angeben, der per E-Mail gesendet werden soll. Eine volle Kalenderwoche beginnt am Sonntag und endet am Samstag. Wenn Ihr Bericht beispielsweise an einem Mittwoch per E-Mail gesendet wird, enthält der Bericht Daten vom vorherigen Sonntag bis Samstag und nicht vom vorherigen Mittwoch bis Dienstag.
Voriger Kalendermonat	Wählen Sie diese Option, um Daten aus dem gesamten Kalendermonat vor dem Zeitpunkt zu senden, zu dem Sie den Bericht angeben, der per E-Mail gesendet werden soll. Wenn Ihr Bericht beispielsweise am 15. eines jeden Monats per E-Mail versendet wird, enthält der Bericht Daten vom 1. bis zum letzten Tag des Vormonats und nicht vom 15. des Vormonats bis zum 15. des aktuellen Monats.

b) Aus dem Häufigkeit melden Abschnitt, legen Sie den Zeitplan für die E-Mail-Zustellung fest, indem Sie eine der folgenden Optionen auswählen:

Hinweis: Die verfügbaren Optionen hängen von den angegebenen ab **Zeitintervall**. Wenn Sie beispielsweise Daten aus der vorherigen Kalenderwoche angegeben haben, können Sie keine tägliche Häufigkeit auswählen.

Die Häufigkeit der Berichte basiert auf Standardsystemzeit von Ihrem ExtraHop-Administrator festgelegt.

Stündlich	Senden Sie den Bericht jede Stunde per E-Mail.
täglich	Geben Sie die Uhrzeit an, zu der der Bericht per E-Mail versendet werden soll. klicken **Zeitplan hinzufügen** um den Bericht mehrmals täglich per E-Mail zu versenden.
Wöchentlich	Geben Sie einen oder mehrere Wochentage sowie die Uhrzeit an, zu der der Bericht per E-Mail versendet werden soll. Klicken Sie **Zeitplan hinzufügen** um Berichts-E-Mails mehrmals täglich oder zu unterschiedlichen Zeiten pro Woche zu versenden.
Monatlich	Geben Sie den Tag des Monats an, an dem der Bericht per E-Mail gesendet werden soll. klicken **Zeitplan hinzufügen** um Berichts-E-Mails mehrmals pro Monat zu senden.

10. Aus dem Format Führen Sie im Abschnitt die folgenden Schritte aus, um das Berichtsformat zu konfigurieren:
    a) Legen Sie das Inhaltslayout fest, indem Sie eine der folgenden Optionen aus der ersten auswählen Stil Dropdownliste:

Schmal	Zeigt großen Text in Diagrammtiteln und Beschriftungen an, bietet jedoch weniger Platz für die Anzeige von Diagrammdaten. Lange Diagrammtitel und Beschriftungen werden möglicherweise gekürzt.
Mittel	(Standard) Zeigt eine Ansicht von Diagrammtiteln, Legenden und Daten an, die für die Seitenausrichtung im Hochformat optimiert ist.
Breit	Zeigt kleinen Text in Diagrammtiteln und Beschriftungen an, bietet jedoch mehr Platz für die Anzeige von Diagrammdaten.

    b) Stellen Sie die Anzahl der Seitenumbrüche in der PDF-Datei ein, indem Sie eine der folgenden Optionen aus der zweiten auswählen Stil Dropdownliste:

Einzelne Seite	(Standard) Zeigt das gesamte Dashboard oder die gesamte Protokollseite auf einer einzigen, fortlaufenden Seite an. Diese

	Einstellung generiert möglicherweise eine PDF-Datei, die größer als die Standarddruckerseitengrößen ist.
Seitenumbruch pro Region	Zeigt jeden Diagrammbereich auf einer einzelnen Seite an. Wählen Sie diese Option, wenn Ihr Dashboard eine Tabelle oder Liste enthält, in der mehr als 20 Detailmetrikwerte angezeigt werden.

c) Stellen Sie das Anzeigedesign ein, indem Sie eine der folgenden Optionen auswählen Thema Optionen:

Licht	(Standard) Zeigt Dashboard-Daten als dunklen Text vor hellem Hintergrund an.
Dunkel oder Weltraum	Zeigt Dashboard-Daten als hellen Text vor dunklem Hintergrund an.
Kontrast	Zeigt Dashboard-Daten mit einer begrenzten Farbpalette und kontrastierenden Farben an.

11. Aus dem E-Mail senden Führen Sie im Abschnitt die folgenden Schritte aus , um E-Mail-Benachrichtigungen zu konfigurieren:
    a) Optional: (Nur RevealX Enterprise-Benutzer) Aus dem Benachrichtigungsgruppen Wählen Sie in der Dropdownliste eine Gruppe von Empfängern aus.

    Wenn Sie die E-Mail-Gruppe, nach der Sie suchen, nicht finden, können Sie E-Mail-Gruppen in den ExtraHop-Administrationseinstellungen oder über die REST-API konfigurieren. Wenden Sie sich an Ihren ExtraHop RevealX Enterprise-Administrator, um einen hinzuzufügen E-Mail-Benachrichtigungsgruppe.
    b) In der **Empfänger** In diesem Feld geben Sie die E-Mail-Adresse für jeden Empfänger ein, getrennt durch ein Komma.
    c) Aus dem Betreff Abschnitt, klicken **Benutzerdefiniert** um Ihre eigene Betreffzeile für die E-Mail zu schreiben. Die automatische Betreffzeile ist der Berichtsname.
    d) Optional: In der **Nachricht** Feld, geben Sie die Informationen, die Sie senden möchten, in den Text der Berichts-E-Mail ein.
12. Führen Sie einen der folgenden Schritte aus, um Ihren Bericht zu speichern:
    - klicken **Jetzt senden** um eine Testbericht-E-Mail an die E-Mail-Adressen zu senden, und klicken Sie dann auf **Erledigt**. Ihr Bericht wurde gespeichert und geplant.
    - klicken **Speichern**. Ihr Bericht ist geplant und wird entsprechend der von Ihnen angegebenen Berichtshäufigkeit an die Empfänger gesendet.

Nächste Schritte

- Um das Senden eines geplanten Berichts zu beenden, löschen Sie das **Bericht aktivieren** Markieren oder löschen Sie den Bericht.

Einen Bericht über geplante Sicherheitsoperationen erstellen

Wenn Sie einen geplanten Sicherheitsbetriebsbericht erstellen, können Sie angeben, wie oft eine PDF-Datei des Berichts per E-Mail gesendet wird und in welchem Zeitintervall die im Bericht enthaltenen Daten verwendet werden sollen.

Bevor Sie beginnen

- Ihr Benutzerkonto muss über eine beschränkte Schreibrechte oder mehr verfügen Privilegien.
- Ihr ExtraHop-System muss das Network Detection and Response (NDR) -Modul enthalten.
- Sie müssen sich an einer Konsole auf dem ExtraHop-System anmelden.
- Ihr ExtraHop-System muss konfiguriert für den Versand von E-Mails. (Nur RevealX Enterprise)

Gehen Sie wie folgt vor, um einen geplanten Sicherheitsbetriebsbericht zu erstellen:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Geplante Berichte**.
3. Klicken Sie **Erstellen**.
4. Geben Sie einen eindeutigen Namen für den Bericht in das **Name des Berichts** Feld.
5. Optional: In der **Beschreibung** Feld, geben Sie Informationen zum Bericht ein. Die Beschreibung erscheint nicht im Abschlussbericht, sondern nur in den Berichtseinstellungen.
6. Wählen Sie im Abschnitt Berichtstyp **Sicherheitsoperationen**.
7. Aus dem **Websites** Wählen Sie im Dropdownmenü die Websites aus, die Sie in den Bericht aufnehmen möchten.
8. Aus dem Zeitplan Führen Sie im Abschnitt die folgenden Schritte aus, um einen Zeitplan für den Bericht zu konfigurieren:
   a) Aus dem Zeitintervall Abschnitt, wählen Sie den Zeitraum der Daten aus, die Sie in den Bericht aufnehmen möchten.

Letzte N Tage	Wählen Sie diese Option, um Daten aus einem Zeitintervall zu senden, das sich auf die Uhrzeit bezieht, zu der Sie den Bericht als E-Mail angeben.
Vorige Kalenderwoche	Wählen Sie diese Option, um Daten aus der gesamten Kalenderwoche vor dem Zeitpunkt zu senden, zu dem Sie den Bericht angeben, der per E-Mail gesendet werden soll. Eine volle Kalenderwoche beginnt am Sonntag und endet am Samstag. Wenn Ihr Bericht beispielsweise an einem Mittwoch per E-Mail gesendet wird, enthält der Bericht Daten vom vorherigen Sonntag bis Samstag und nicht vom vorherigen Mittwoch bis Dienstag.
Voriger Kalendermonat	Wählen Sie diese Option, um Daten aus dem gesamten Kalendermonat vor dem Zeitpunkt zu senden, zu dem Sie den Bericht angeben, der per E-Mail gesendet werden soll. Wenn Ihr Bericht beispielsweise am 15. eines jeden Monats per E-Mail versendet wird, enthält der Bericht Daten vom 1. bis zum letzten Tag des Vormonats und nicht vom 15. des Vormonats bis zum 15. des aktuellen Monats.

   b) Aus dem Häufigkeit melden Abschnitt, legen Sie den Zeitplan für die E-Mail-Zustellung fest, indem Sie eine der folgenden Optionen auswählen:

> **Hinweis:** Die verfügbaren Optionen hängen von den angegebenen ab **Zeitintervall**. Wenn Sie beispielsweise Daten aus der vorherigen Kalenderwoche angegeben haben, können Sie keine tägliche Häufigkeit auswählen.
>
> Die Häufigkeit der Berichte basiert auf Standardsystemzeit von Ihrem ExtraHop-Administrator festgelegt.

Stündlich	Senden Sie den Bericht jede Stunde per E-Mail.
täglich	Geben Sie die Uhrzeit an, zu der der Bericht per E-Mail versendet werden soll. klicken **Zeitplan hinzufügen** um den Bericht mehrmals täglich per E-Mail zu versenden.
Wöchentlich	Geben Sie einen oder mehrere Wochentage sowie die Uhrzeit an, zu der der Bericht per E-Mail versendet werden soll. Klicken Sie **Zeitplan hinzufügen** um Berichts-E-Mails mehrmals täglich oder zu unterschiedlichen Zeiten pro Woche zu versenden.

Monatlich	Geben Sie den Tag des Monats an, an dem der Bericht per E-Mail gesendet werden soll. klicken **Zeitplan hinzufügen** um Berichts-E-Mails mehrmals pro Monat zu senden.

9. Aus dem E-Mail senden Führen Sie im Abschnitt die folgenden Schritte aus , um E-Mail-Benachrichtigungen zu konfigurieren:
   a) Optional: (Nur RevealX Enterprise-Benutzer) Aus dem Benachrichtigungsgruppen Wählen Sie in der Dropdownliste eine Gruppe von Empfängern aus.

      Wenn Sie die E-Mail-Gruppe, nach der Sie suchen, nicht finden, können Sie E-Mail-Gruppen in den ExtraHop-Administrationseinstellungen oder über die REST-API konfigurieren. Wenden Sie sich an Ihren ExtraHop RevealX Enterprise-Administrator, um einen hinzuzufügen E-Mail-Benachrichtigungsgruppe.
   b) In der **Empfänger** In diesem Feld geben Sie die E-Mail-Adresse für jeden Empfänger ein, getrennt durch ein Komma.
   c) Aus dem Betreff Abschnitt, klicken **Benutzerdefiniert** um Ihre eigene Betreffzeile für die E-Mail zu schreiben. Die automatische Betreffzeile ist der Berichtsname.
   d) Optional: In der **Nachricht** Feld, geben Sie die Informationen, die Sie senden möchten, in den Text der Berichts-E-Mail ein.
10. Führen Sie einen der folgenden Schritte aus, um Ihren Bericht zu speichern:
    - klicken **Jetzt senden** um eine Testbericht-E-Mail an die E-Mail-Adressen zu senden, und klicken Sie dann auf **Erledigt**. Ihr Bericht wurde gespeichert und geplant.
    - klicken **Speichern**. Ihr Bericht ist geplant und wird entsprechend der von Ihnen angegebenen Berichtshäufigkeit an die Empfänger gesendet.

Nächste Schritte

- Um das Senden eines geplanten Berichts zu beenden, löschen Sie das **Bericht aktivieren** Markieren oder löschen Sie den Bericht.

Diagrammtypen

Dashboard-Diagramme im ExtraHop-System bieten mehrere Möglichkeiten, Metrik Daten zu visualisieren, was Ihnen bei der Beantwortung von Fragen zu Ihrem Netzwerkverhalten helfen kann.

Sie wählen einen Diagrammtyp aus, wenn Sie Bearbeiten Sie ein Diagramm im Metric Explorer. Aber woher wissen Sie , welches Diagramm Sie auswählen müssen? Es hilft, zunächst zu entscheiden, welche Frage Sie beantworten möchten:

- Um zu erfahren, wie sich eine Metrik im Laufe der Zeit ändert, wählen Sie ein Zeitreihendiagramm aus, z. B. das Flächen-, Säulen-, Linien-, Zeilen- und Säulendiagramm oder das Statusdiagramm.
- Um zu erfahren, wie ein Metrikwert im Vergleich zu einem vollständigen Datensatz abschneidet, wählen Sie ein Verteilungsdiagramm aus, z. B. Boxplot, Candlestick, Heatmap oder Histogramm-Diagramm.
- Um den genauen Metrikwert für einen Zeitraum zu ermitteln, wählen Sie ein Gesamtwertdiagramm aus, z. B. ein Balken-, Listen-, Kreis-, Tabellen- oder Wertdiagramm.
- Um den Warnstatus dieser Metrik zu erfahren, wählen Sie die Liste, den Status oder das Wertdiagramm aus.

Weitere Antworten finden Sie in der Häufig gestellte Fragen zu Grafiken.

Die folgende Tabelle enthält eine Liste der Diagrammtypen und Beschreibungen. Klicken Sie auf den Diagrammtyp, um weitere Details und Beispiele zu sehen.

Diagrammtyp	Beschreibung	Typ
Flächendiagramm	Zeigt Metrik Werte als Linie an, die Datenpunkte im Laufe der Zeit verbindet, wobei der Bereich zwischen der Linie und der Achse farbig ausgefüllt ist.	Zeitreihen
Säulendiagramm	Zeigt Metrikdaten als vertikale Spalten über ein ausgewähltes Zeitintervall an.	Zeitreihen
Liniendiagramm	Zeigt Metrikwerte als Datenpunkte in einer Linie im Zeitverlauf an.	Zeitreihen
Linien- und Säulendiagramm	Zeigt Metrikwerte als Linie an, die eine Reihe von Datenpunkten im Laufe der Zeit verbindet, mit der Option, eine weitere Metrik als Säulendiagramm unter dem Liniendiagramm anzuzeigen.	Zeitreihen
Status-Diagramm	Zeigt Metrikwerte in einem Säulendiagramm und den Status einer Alarm an, die sowohl der Quelle als auch der Metrik im Diagramm zugewiesen ist.	Zeitreihen
Boxplot-Diagramm	Zeigt die Variabilität für eine Verteilung metrischer Daten an. Jede horizontale Linie im Boxplot umfasst drei oder fünf Datenpunkte.	Vertrieb

Diagrammtyp	Beschreibung	Typ
Candlestick-Diagramm	Zeigt die Variabilität für eine Verteilung metrischer Daten über die Zeit an.	Vertrieb
Heatmap-Diagramm	Zeigt eine Verteilung metrischer Daten über die Zeit an, wobei Farbe für eine Datenkonzentration steht.	Vertrieb
Histogramm-Diagramm	Zeigt eine Verteilung metrischer Daten als vertikale Balken oder Fächer an.	Vertrieb
Balkendiagramm	Zeigt den Gesamtwert der Metrik Daten als horizontale Balken an.	Gesamtwert
Diagramm auflisten	Zeigt Metrik Daten als Liste mit optionalen Sparklines an, die Datenänderungen im Laufe der Zeit darstellen.	Gesamtwert
Kreisdiagramm	Zeigt Metrik Daten als Teil oder Prozentsatz eines Ganzen an.	Gesamtwert
Tabellen-Diagramm	Zeigt mehrere Metrikwerte in einer Tabelle an, die einfach sortiert werden können.	Gesamtwert
Wertetabelle	Zeigt den Gesamtwert für eine oder mehrere Metriken an.	Gesamtwert

Flächendiagramm

Metrische Daten werden als Datenpunkte im Zeitverlauf angezeigt, die durch eine Linie verbunden sind, wobei der Bereich zwischen der Linie und der X-Achse farbig ausgefüllt ist.

Wenn Ihr Diagramm mehr als eine Metrik enthält, werden die Daten für jede Metrik als einzelne Linie oder als Reihe angezeigt. Jede Reihe ist zusammengestapelt, um den kumulativen Wert der Daten zu veranschaulichen.

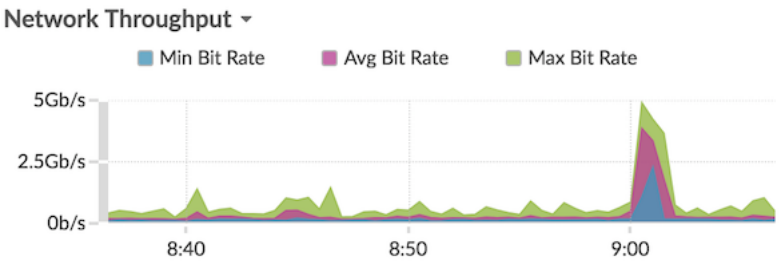
Wählen Sie das Flächendiagramm aus, um zu sehen, wie die Akkumulation mehrerer Metrik Datenpunkte im Laufe der Zeit zu einem Gesamtwert beiträgt. Ein Flächendiagramm kann beispielsweise aufzeigen, wie verschiedene Protokolle zur gesamten Protokollaktivität beitragen.

Weitere Informationen zur Anzeige von Raten in Ihrem Diagramm finden Sie in der Tarife anzeigen Abschnitt.

Hinweis: Dieses Diagramm unterstützt Erkennungsmarker, die auf Erkennungen hinweisen, die mit Diagrammdaten verknüpft sind.

Hinweis: Erkennungen durch maschinelles Lernen erfordern eine Verbindung zu ExtraHop Cloud Services.

Die folgende Abbildung zeigt ein Beispiel für ein Flächendiagramm.

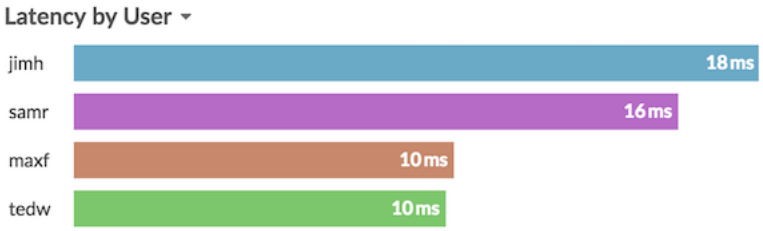


Balkendiagramm

Der Gesamtwert der Metrik Daten wird als horizontale Balken angezeigt.

Wählen Sie das Balkendiagramm aus, wenn Sie die Daten für mehr als eine Metrik für ein ausgewähltes Zeitintervall vergleichen möchten.

Die folgende Abbildung zeigt ein Beispiel für ein Balkendiagramm.

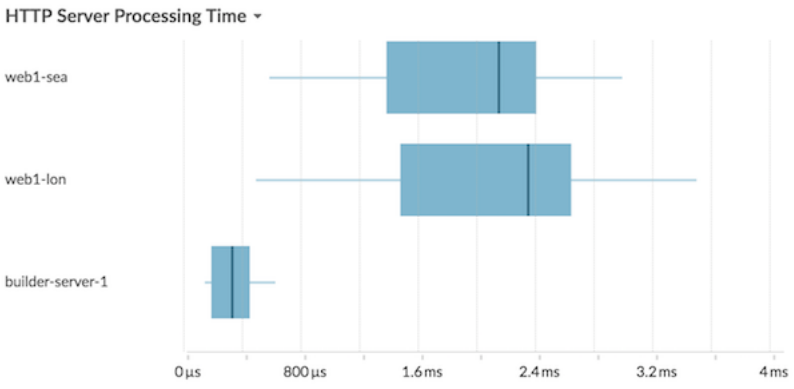


Boxplot-Diagramm

Das Boxplot-Diagramm zeigt die Variabilität für eine Verteilung Metrik Daten. In diesem Diagramm können Sie nur Daten aus Datensatzmetriken anzeigen, z. B. die Serververarbeitungszeit.

Jede horizontale Linie im Boxplot umfasst drei oder fünf Datenpunkte. Bei fünf Datenpunkten enthält die Linie einen Textbalken, ein vertikales Häkchen, eine obere Schattenlinie und eine untere Schattenlinie. Bei drei Datenpunkten enthält die Linie ein vertikales Häkchen, einen oberen Schatten und einen unteren Schatten. Weitere Informationen zur Anzeige bestimmter Perzentilwerte in Ihrem Diagramm finden Sie unter Perzentile anzeigen.

Die folgende Abbildung zeigt ein Beispiel für ein Boxplot-Diagramm.



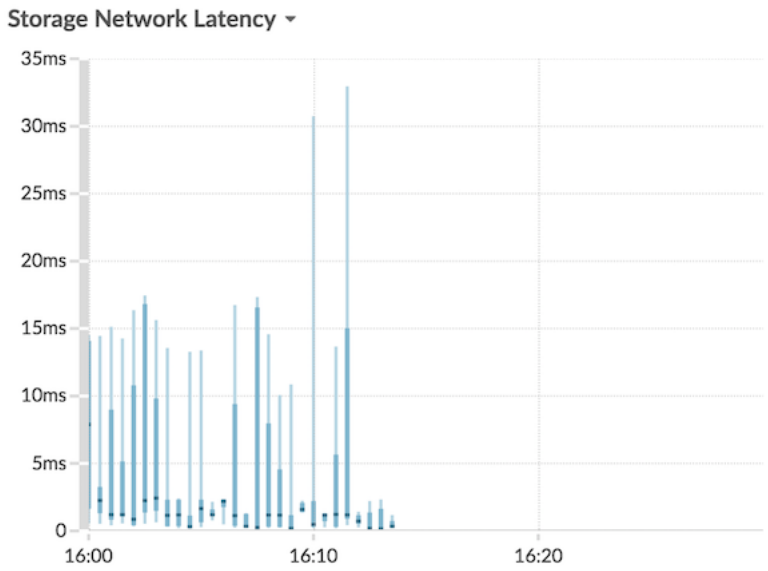
Kerzendiagramm

Das Kerzen-Chart zeigt die Variabilität einer Verteilung metrischer Daten über die Zeit. Sie können nur Daten aus Datensatzmetriken oder hochpräzisen Netzwerk-Byte- und Paketmetriken (L2) anzeigen.

Vertikale Linien in jedem Zeitintervall zeigen drei oder fünf Datenpunkte an. Wenn die Linie fünf Datenpunkte hat, enthält sie einen Körper, ein mittleres Häkchen, eine obere Schattenlinie und eine untere Schattenlinie. Wenn die Linie drei Datenpunkte hat, enthält sie ein mittleres Häkchen. Weitere Informationen zur Anzeige bestimmter Perzentilwerte in Ihrem Diagramm finden Sie unter Perzentile anzeigen.

Wählen Sie das Kerzen-Chart aus, um die Variabilität der Datenberechnungen für einen bestimmten Zeitraum anzuzeigen.

Die folgende Abbildung zeigt ein Beispiel für ein Kerzen-Chart.



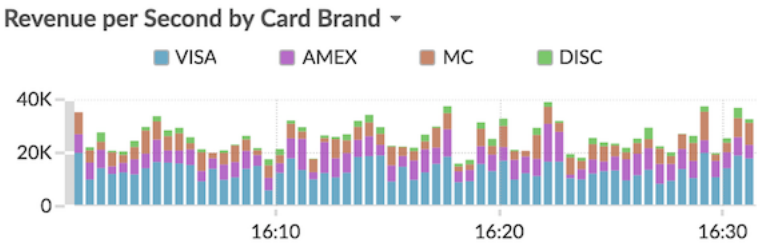
Säulendiagramm

Metrische Daten werden im Zeitverlauf als vertikale Spalten angezeigt. Wenn Ihr Diagramm mehr als eine Metrik enthält, werden die Daten für jede Metrik als einzelne Spalte oder als Reihe angezeigt. Jede Reihe ist zusammengestapelt, um den kumulativen Wert der Daten zu veranschaulichen.

Wählen Sie das Säulendiagramm aus, um zu vergleichen, wie die Akkumulation mehrerer Metrik Datenpunkte zu einem bestimmten Zeitpunkt zum Gesamtwert beiträgt.

Hinweis: Dieses Diagramm unterstützt Erkennungsmarker, die auf Erkennungen hinweisen, die mit Diagrammdaten verknüpft sind.

Die folgende Abbildung zeigt ein Beispiel für ein Säulendiagramm.



Heatmap-Diagramm

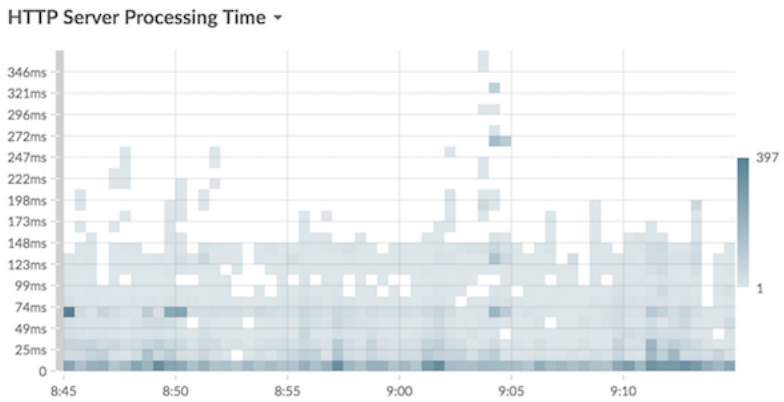
Das Heatmap-Diagramm zeigt eine Verteilung der Metrik Daten über die Zeit, wobei die Farbe eine Datenkonzentration darstellt. Sie können nur eine Dataset-Metrik auswählen, die im Diagramm angezeigt werden soll, z. B. Serververarbeitungszeit oder Roundtrip-Zeit.

Wählen Sie die Heatmap aus, wenn Sie Muster in der Datenverteilung identifizieren möchten.

Hier sind einige wichtige Überlegungen zum Heatmap-Diagramm:

- Die Heatmap-Legende zeigt den Farbverlauf an, der dem Datenbereich im Diagramm entspricht. Beispielsweise weist die dunklere Farbe auf der Heatmap auf eine höhere Konzentration von Datenpunkten hin.
- Der Standarddatenbereich liegt zwischen dem 5. und 95. Perzentil, wodurch Ausreißer aus der Verteilung herausgefiltert werden. Ausreißer können den Maßstab der in Ihrem Diagramm angezeigten Daten verzerren, wodurch es schwieriger wird, Trends und Muster für den Großteil Ihrer Daten zu erkennen. Sie können sich jedoch dafür entscheiden, den gesamten Datenbereich anzuzeigen, indem Sie den Standardfilter in der **Optionen** Registerkarte. Weitere Informationen finden Sie unter Ausreißer filtern.
- Das ausgewählte Thema, z. B. Hell, Dunkel oder Raum, beeinflusst, ob eine dunkle oder helle Farbe auf eine höhere Konzentration von Datenpunkten hinweist.

Die folgende Abbildung zeigt ein Beispiel für ein Heatmap-Diagramm.



Histogramm-Diagramm

Das Histogramm-Diagramm zeigt eine Verteilung der Metrik Daten als vertikale Balken oder Abschnitte an. Sie können nur eine Dataset-Metrik auswählen, die in diesem Diagramm angezeigt werden soll, z. B. Serververarbeitungszeit oder Roundtrip-Zeit.

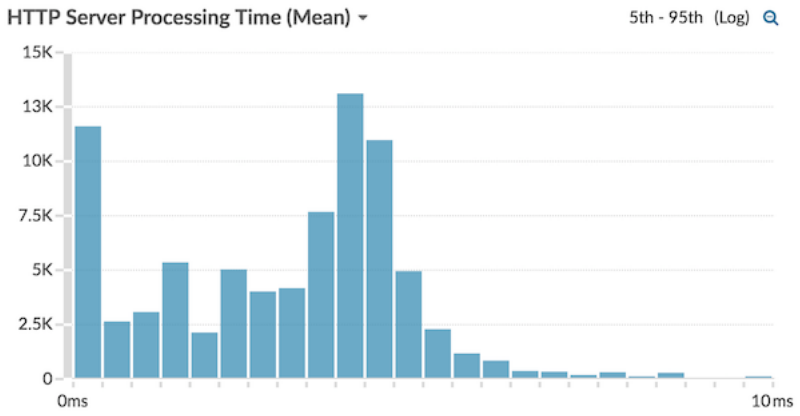
Wählen Sie das Histogramm-Diagramm aus, um die Form der Datenverteilung zu sehen.

Hier sind einige wichtige Überlegungen zum Histogramm-Diagramm:

- Der Standarddatenbereich reicht vom 5. bis zum 95. Perzentil (5. bis 95), wodurch Ausreißer aus der Verteilung herausgefiltert werden. In der Ansicht Minimum bis Maximum (Min-Max) wird der gesamte Datenbereich angezeigt. Klicken Sie auf die Lupe in der oberen rechten Ecke des Diagramms, um zwischen den beiden Ansichten umzuschalten.
- Die Daten werden je nach Datenbereich automatisch entweder auf linearer oder logarithmischer Skala in Fächer verteilt. Wenn sich der Datenbereich beispielsweise über mehrere Größenordnungen erstreckt, werden die Daten auf einer logarithmischen Skala in Abschnitte eingeteilt. Min-Max (log) wird in der oberen rechten Ecke des Diagramms angezeigt.
- Klicken und ziehen Sie, um mehrere Fächer oder eine bestimmte Ablage zu vergrößern. Klicken Sie erneut auf die Lupe in der oberen rechten Ecke des Diagramms, um die ursprüngliche Ansicht zu verkleinern (entweder 5—95. oder Min bis Max).

  Hinweis Durch das Heranzoomen, um ein benutzerdefiniertes Zeitintervall anzuzeigen, wird das globale oder Region Zeitintervall nicht geändert.
- Ihre Umschaltoption (zwischen der 5. und 95. Ansicht und der Min-Max-Ansicht) bleibt für Ihr Diagramm bestehen, jedoch nicht für die Benutzer, mit denen Sie Ihr Dashboard und Ihr Diagramm geteilt haben. Informationen zum Festlegen einer dauerhaften Umschaltoption vor dem Teilen eines Dashboard finden Sie unter Ausreißer filtern.

Die folgende Abbildung zeigt ein Beispiel für ein Histogramm-Diagramm.



Hinweis Dieses Diagramm unterstützt keine Grundlinien oder Schwellenwerte.

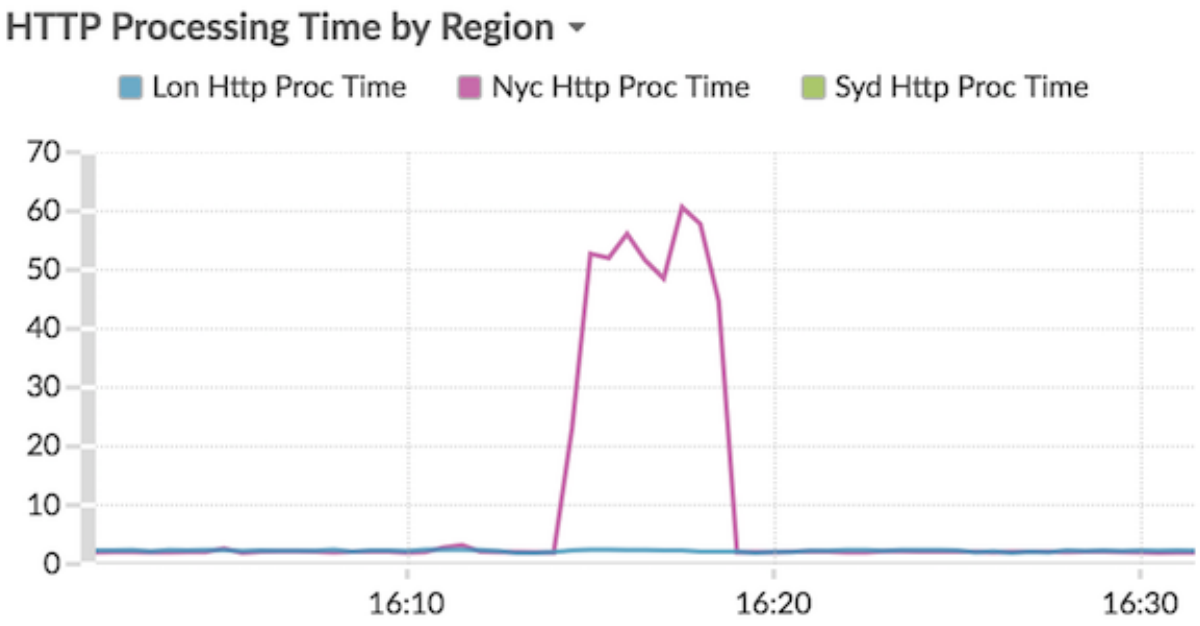
Liniendiagramm

Metrische Daten werden als Datenpunkte im Zeitverlauf angezeigt, die in einer Linie verbunden sind. Wenn Ihr Diagramm mehr als eine Metrik enthält, werden die Daten für jede Metrik als einzelne Linie oder als Reihe angezeigt. Jede Serie überschneidet sich.

Wählen Sie das Liniendiagramm aus, um Änderungen im Laufe der Zeit zu vergleichen.

Hinweis Dieses Diagramm unterstützt Erkennungsmarker, die auf Erkennungen hinweisen, die mit Diagrammdaten verknüpft sind.

Die folgende Abbildung zeigt ein Beispiel für ein Liniendiagramm.



Linien- und Säulendiagramm

Metrische Daten werden als Datenpunkte im Zeitverlauf angezeigt, die durch eine Linie miteinander verbunden sind. Es besteht die Möglichkeit, ein Säulendiagramm unter dem Liniendiagramm anzuzeigen. Wenn Ihr Diagramm beispielsweise mehr als eine Metrik enthält (z. B. HTTP-Anfragen und HTTP-Fehler), können Sie auswählen **Als Spalten anzeigen** um eine der Metriken als Säulendiagramm unter dem Liniendiagramm anzuzeigen.

Spalten werden standardmäßig in der Farbe Rot angezeigt. Um die rote Farbe zu entfernen, klicken Sie auf **Optionen** und abwählen **Spalten rot anzeigen**.

Wählen Sie das Linien- und Säulendiagramm aus, um verschiedene Metriken auf verschiedenen Skalen in einem Diagramm zu vergleichen. Sie können beispielsweise die Fehlerraten und die Gesamtzahl der HTTP-Antworten in einem Diagramm anzeigen.

Hinweis: Dieses Diagramm unterstützt Erkennungsmarker, die auf Erkennungen hinweisen, die mit Diagrammdaten verknüpft sind.

Die folgende Abbildung zeigt ein Beispiel für ein Linien- und Säulendiagramm.

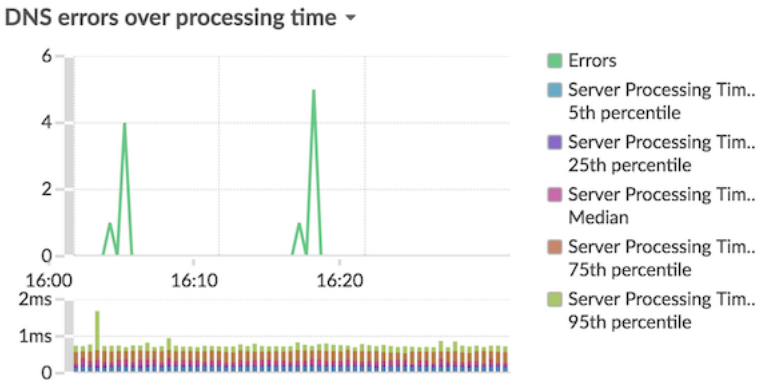


Diagramm auflisten

Metrische Daten werden als Liste angezeigt. Wählen Sie das Listendiagramm aus, um lange Listen mit Metrikwerten, z. B. Detailmetriken, anzuzeigen.

Dieses Diagramm enthält die folgenden Optionen:

- Fügen Sie eine Sparkline hinzu, bei der es sich um ein einfaches Flächendiagramm handelt, das direkt neben dem Namen und Wert der Metrik platziert wird. Eine Sparkline zeigt, wie sich Daten im Laufe der Zeit verändert haben. Klicken Sie auf **Optionen** Tabulatortaste und wählen **Sparklines einbeziehen**.
- Zeigt den Metrikwert in einer Farbe für den Warnstatus an. Verschiedene Farben geben den Schweregrad der konfigurierten Alarm an. Wenn beispielsweise ein Warnschwellenwert für eine Metrik überschritten wird, die im Listendiagramm angezeigt wird, wird der Wert für diese Metrik rot angezeigt. Klicken Sie auf **Optionen** Tabulatortaste und wählen **Farbe zeigt den Alarmstatus an**.

Hinweis Dieses Diagramm unterstützt keine Grundlinien oder Schwellenwerte.

Die folgende Abbildung zeigt ein Beispiel für ein Listendiagramm.

Kreisdiagramm

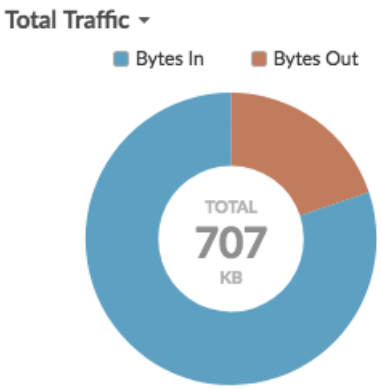
Metrische Daten werden als Teil oder Prozentsatz eines Ganzen angezeigt. Wenn Ihr Diagramm mehr als eine Metrik enthält, werden die Daten für jede Metrik im Kreisdiagramm als einzelnes Segment oder Reihe dargestellt.

Wählen Sie das Tortendiagramm aus, um die Metrikwerte zu vergleichen, die sich gegenseitig ausschließen, z. B. Statuscode-Detailmetriken für die HTTP-Antwortmetrik der obersten Ebene.

Dieses Diagramm enthält die folgenden Optionen:

- Als Ringdiagramm anzeigen. Klicken Sie auf **Wahl** Tabulatortaste und wählen **Gesamtwert anzeigen**.
- Geben Sie die Dezimalgenauigkeit oder die Anzahl der Ziffern an, die in Ihrem Diagramm angezeigt werden. Die Perzentilgenauigkeit ist nützlich für die Darstellung von Datenverhältnissen, insbesondere für Service Level Agreements (SLAs), für die möglicherweise genaue Daten für die Berichterstattung erforderlich sind. Klicken Sie auf **Optionen** Registerkarte, und wählen Sie im Abschnitt Einheiten **Prozentzahlen statt Zählungen anzeigen**. Wählen Sie dann **0,00%** oder **0,000%** aus der Drop-down-Liste.

Die folgende Abbildung zeigt ein Beispiel für ein Tortendiagramm.



Status-Diagramm

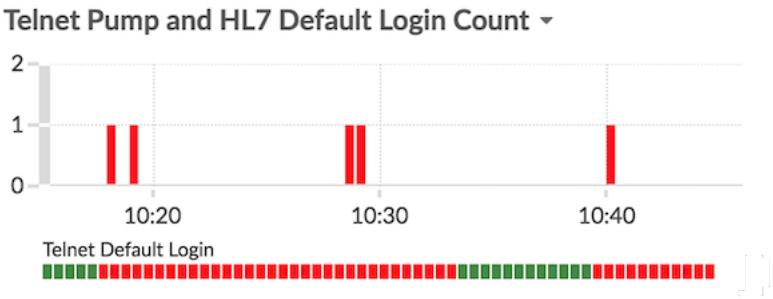
Metrische Daten werden in einem Säulendiagramm angezeigt. Die Farbe jeder Spalte steht für den schwerwiegendsten Warnstatus der konfigurierten Alarm für die Metrik. Sie können nur eine Quelle und Metrik für die Anzeige in diesem Diagramm auswählen.

Um den Status aller Alerts anzuzeigen, die mit der ausgewählten Metrikkategorie verknüpft sind, klicken Sie auf **Verwandte Benachrichtigungen anzeigen**. Eine Liste von Warnungen wird dann unter dem Säulendiagramm angezeigt.

Wählen Sie das Statusdiagramm aus, um zu sehen, wie sich die Daten und der Warnstatus für Ihre Metrik im Laufe der Zeit ändern.

Hinweis Dieses Diagramm unterstützt keine Basislinien.

Die folgende Abbildung zeigt ein Beispiel für ein Statusdiagramm.



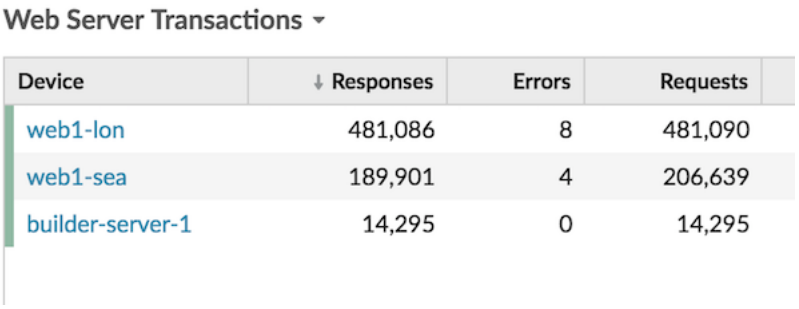
Tabellen-Diagramm

Metrische Daten werden zeilen- und spaltenübergreifend in einer Tabelle angezeigt. Jede Zeile steht für eine Quelle. Jede Spalte steht für eine Metrik. Sie können einer Tabelle mehrere Quellen (desselben Typs) und Metriken hinzufügen.

Wählen Sie das Tabellendiagramm aus, wenn Sie Metrikdaten in einem Raster anzeigen und Werte einfach nach mehreren Metriken sortieren möchten.

Hinweis Dieses Diagramm unterstützt keine Grundlinien oder Schwellenwerte .

Die folgende Abbildung zeigt ein Beispiel für ein Tabellendiagramm.



Wertetabelle

Der Gesamtwert für eine oder mehrere Metriken wird als Einzelwert angezeigt. Wenn Sie mehr als eine Metrik auswählen, werden die Metrikwerte nebeneinander angezeigt.

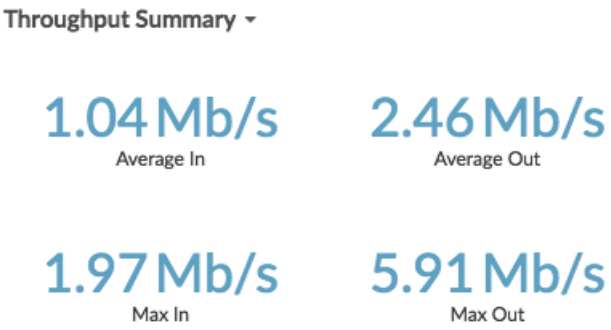
Wählen Sie das Wertdiagramm aus, um den Gesamtwert wichtiger Metriken anzuzeigen, z. B. die Gesamtzahl der in Ihrem Netzwerk aufgetretenen HTTP-Fehler.

Dieses Diagramm enthält die folgenden Optionen:

- Fügen Sie Sparklines hinzu. Dabei handelt es sich um ein einfaches Flächendiagramm, das unter dem Metrikwert platziert wird. Eine Sparkline zeigt, wie sich Daten im Laufe der Zeit verändert haben. Klicken Sie auf **Optionen** Tabulatortaste und wählen **Sparklines einbeziehen**.
- Zeigt den Metrikwert in einer Farbe für den Warnstatus an. Verschiedene Farben geben den Schweregrad der konfigurierten Alarm an. Wenn beispielsweise ein Warnschwellenwert für eine Metrik überschritten wird, wird der Wert rot angezeigt. Klicken Sie auf **Optionen** Tabulatortaste und wählen **Farbe zeigt den Alarmstatus an**.

Hinweis: Dieses Diagramm unterstützt keine Grundlinien oder Schwellenwerte.

Die folgende Abbildung zeigt ein Beispiel für ein Wertdiagramm.



Erstellen Sie ein Diagramm

Diagramme sind ein unverzichtbares Werkzeug zur Visualisierung, Analyse und zum Verständnis des Netzwerkverhaltens. Sie können von einem Dashboard oder einer Protokollseite aus ein benutzerdefiniertes Diagramm erstellen, um Daten aus den über 4.000 integrierten oder benutzerdefinierten Metriken zu visualisieren, die im ExtraHop-System verfügbar sind. Wenn Sie beispielsweise bei der Problembehandlung eine interessante Servermetrik beobachten, können Sie ein

Diagramm erstellen, um diese Metrik zu visualisieren und weiter zu analysieren. Benutzerdefinierte Diagramme werden dann in Dashboards gespeichert.

Die folgenden Schritte zeigen Ihnen, wie Sie schnell ein leeres benutzerdefiniertes Diagramm erstellen können:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Führen Sie einen der folgenden Schritte aus:
   - klicken **Dashboards** oben auf der Seite.
   - klicken **Vermögenswerte** oben auf der Seite. Wählen Sie im linken Bereich eine Quelle aus, und klicken Sie dann im mittleren Bereich auf den Namen einer Anwendung, eines Geräts, einer Gerätegruppe oder eines Netzwerk. Eine Protokollseite für die Quelle wird angezeigt.
3. Klicken Sie auf das Befehlsmenü ⋮ in der oberen rechten Ecke der Seite und wählen Sie dann **Diagramm erstellen**.
4. Bearbeiten Sie das Diagramm im Metric Explorer.
5. Um Ihr Diagramm zu speichern, klicken Sie auf **Zum Dashboard hinzufügen** und führen Sie einen der folgenden Schritte aus:
   - Wählen Sie den Namen eines vorhandenen Dashboard aus der Liste aus. Die Dashboard-Liste ist von den zuletzt erstellten Dashboards (unten) bis zu den ältesten Dashboards (oben) geordnet.
   - Wählen **Dashboard erstellen**. In der Eigenschaften des Dashboards Fenster, geben Sie einen Namen für das neue Dashboard ein und klicken Sie dann auf **Erstellen**.

Hinweis: Hier sind einige andere Möglichkeiten, ein Diagramm zu erstellen:

- Wenn Sie auf einer Protokollseite oder einem Dashboard ein Diagramm finden, das Ihnen gefällt, können Sie dieses Diagramm neu erstellen und in Ihrem Dashboard speichern. Klicken Sie auf den Diagrammtitel und wählen Sie dann **Diagramm erstellen aus...**.
- Du kannst ein Dashboard-Layout bearbeiten und klicken und ziehen Sie ein neues Diagramm-Widget auf das Dashboard.

Nächste Schritte

Nachdem Sie ein Diagramm erstellt haben, erfahren Sie mehr über die Arbeit mit Dashboards:

- Ein Dashboard-Layout bearbeiten
- Ein Dashboard teilen

Ein Diagramm kopieren

Sie können ein Diagramm von einer Dashboard- oder Protokollseite kopieren und das kopierte Diagramm dann in einem Dashboard speichern. Kopierte Widgets werden immer in einem neuen Region auf dem Dashboard platziert, den Sie später ändern können.

Hinweis: Wenn Sie ein Dashboard-Diagramm oder ein Textfeld kopieren möchten, ohne einen neuen Region zu erstellen, klicken Sie auf das Befehlsmenü ⋮ in der oberen rechten Ecke der Dashboard-Seite und klicken Sie auf **Layout bearbeiten**. Suchen Sie das Diagramm, das Sie kopieren möchten, und klicken Sie dann auf **Duplizieren**.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Armaturenbretter**.
3. Wählen Sie ein Dashboard aus, das das Diagramm oder Widget enthält, das Sie kopieren möchten.
4. Klicken Sie auf den Titel.

Hinweis Sie können nicht auf den Titel eines Textfeld-Widgets klicken. Um ein Text-Widget zu kopieren, müssen Sie zuerst das Dashboard-Layout bearbeiten. Klicken Sie auf das Befehlsmenü ⋮ in der oberen rechten Ecke des Textfeld-Widgets, und führen Sie dann Schritt 4 aus.

5. Bewegen Sie den Mauszeiger darüber **Kopieren nach...** um eine Dropdownliste zu erweitern und dann eine der folgenden Auswahlen zu treffen:
   - Wählen Sie den Namen eines vorhandenen Dashboard aus der Liste aus. Die Dashboard-Liste ist von den zuletzt erstellten Dashboards (unten) bis zu den ältesten Dashboards (oben) geordnet.
   - Wählen **Dashboard erstellen**. In der Eigenschaften des Dashboards Fenster, geben Sie einen Namen für das neue Dashboard ein und klicken Sie dann auf **Erstellen**.

Nächste Schritte
Das Diagramm wird in einen neuen Region auf dem Dashboard kopiert, der sich im Modus „Layout bearbeiten“ befindet. Sie können Ihr Dashboard oder Diagramm jetzt auf folgende Weise bearbeiten:

- Eine Dashboard-Region bearbeiten
- Ein Dashboard-Layout bearbeiten
- Ein Diagramm mit dem Metric Explorer bearbeiten

Drilldown

Eine interessante Metrik führt natürlich zu Fragen zu den Faktoren, die mit diesem Metrikwert verbunden sind. Wenn Sie beispielsweise in Ihrem Netzwerk eine große Anzahl von DNS-Anforderungs-Timeouts feststellen, fragen Sie sich möglicherweise, bei welchen DNS-Clients diese Timeouts auftreten. Im ExtraHop-System können Sie ganz einfach einen Drilldown von einer Top-Level-Metrik aus durchführen, um die Geräte, Methoden oder Ressourcen anzuzeigen, die mit dieser Metrik verknüpft sind.

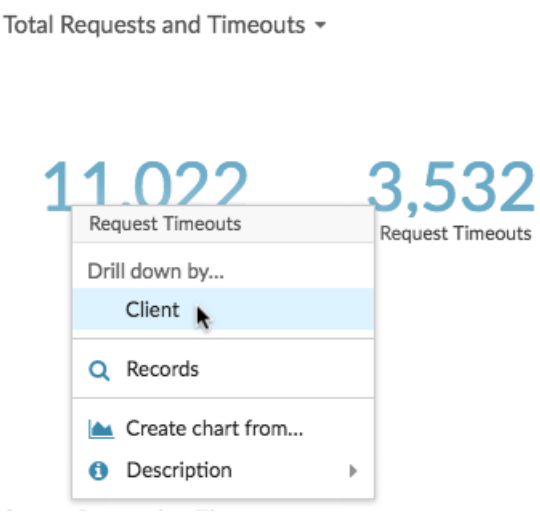
Wenn Sie eine Metrik anhand eines Schlüssels (z. B. einer Client-IP-Adresse, Methode, URI oder Ressource) aufschlüsseln, berechnet das ExtraHop-System eine Topnset von bis zu 1.000 Schlüssel-Wert-Paaren. Anschließend können Sie diese Schlüssel-Wert-Paare untersuchen, die als Metriken detailliert, um zu erfahren, welche Faktoren mit der interessanten Aktivität zusammenhängen.

Drilldown von einem Dashboard oder einer Protokollseite aus

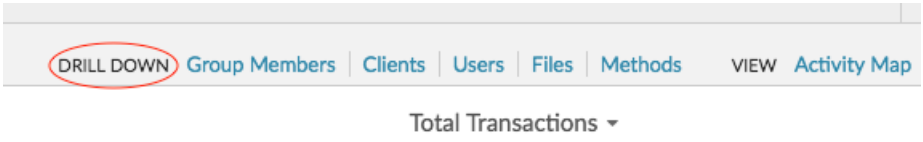
Wenn Sie in einem Diagramm oder einer Legende auf eine Metrik klicken, können Sie sehen, welcher Schlüssel, z. B. Client-IP-Adresse, Server-IP-Adresse, Methode oder Ressource, zu diesem Wert beigetragen hat.

In den folgenden Schritten erfahren Sie, wie Sie eine Metrik finden und anschließend eine Aufgliederung vornehmen können:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Finden Sie eine interessante Metrik, indem Sie einen der folgenden Schritte ausführen:
   - klicken **Armaturenbrett**, und wählen Sie dann im linken Bereich ein Dashboard aus. Ein Dashboard mit Metriken wird angezeigt.
   - klicken **Vermögenswerte**, klicken **Gerät**, **Gerätegruppe**, oder **Bewerbung** im linken Bereich. Wählen Sie dann ein Gerät, eine Gruppe oder eine Anwendung aus. Eine Protokollseite mit Metriken wird angezeigt.
   - klicken **Vermögenswerte**, klicken **Netzwerke** im linken Bereich, und wählen Sie dann ein Flow-Netzwerk aus. Eine Protokollseite mit Metriken wird angezeigt.
3. Klicken Sie in der Diagrammlegende auf einen Metrikwert oder eine Metrikbezeichnung, wie in der folgenden Abbildung dargestellt. Es erscheint ein Menü.



Hinweis: Auf einer Protokollseite können Sie auch auf eine Drilldown-Schaltfläche in der Drilldown Abschnitt, der sich in der oberen rechten Ecke der Seite befindet. Die Art der Tastenkombinationen variiert je nach Protokoll.



4. In der Drilldown nach... Abschnitt, wählen Sie einen Schlüssel aus. Eine Seite mit detaillierten Metriken mit Topnset Es wird eine Liste der Metrikwerte nach Schlüssel angezeigt. Auf dieser Seite können Sie bis zu 1.000 Schlüssel-Werte-Paare anzeigen.

Hinweis: Falls verfügbar, klicken Sie auf **Mehr ansehen** Link am unteren Rand eines Diagramms, um die im Diagramm angezeigte Metrik genauer zu untersuchen.

Nächste Schritte

- Untersuchen Sie detaillierte Metriken

Detaillierter Überblick über Netzwerkerfassung und VLAN-Metriken

Klicken Sie auf eine interessante Top-Level-Metrik zur Netzwerkaktivität auf einem Netzwerk einfangen oder VLAN Seite, um zu ermitteln, welche Geräte mit dieser Aktivität verknüpft sind.

Hinweis: Informationen dazu, wie Sie Metriken von einer Seite mit einem Flussnetz oder einer Flow-Netzwerkschnittstelle aus aufschlüsseln können, finden Sie in Drilldown von einem Dashboard oder einer Protokollseite aus Abschnitt.

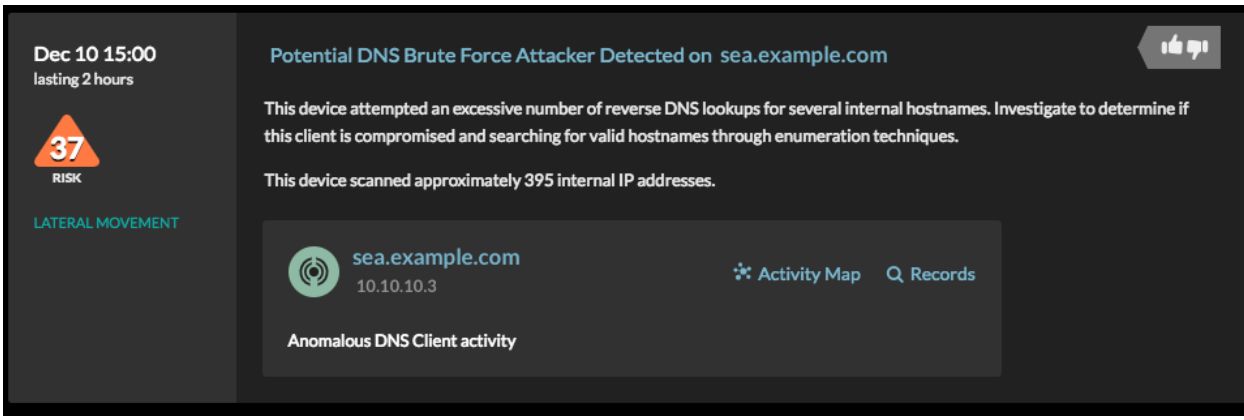
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. klicken **Vermögenswerte**.
3. klicken **Netzwerke** im linken Bereich.
4. Klicken Sie auf einen Netzwerk-Capture- oder VLAN-Schnittstellennamen.
5. Klicken Sie im linken Bereich auf einen Netzwerk-Layer, z. B. **L3** oder **L7-Protokolle**. Es werden Diagramme angezeigt, die Metrikwerte für das ausgewählte Zeitintervall anzeigen. Für die meisten Protokolle und Metriken ist ein Gerät Die Tabelle wird auch unten auf der Seite angezeigt.

6. Klicken Sie auf die Diagrammdaten, wodurch die Liste aktualisiert wird, sodass nur die Geräte angezeigt werden, die mit den Daten verknüpft sind.
7. Klicken Sie auf einen Gerätenamen. EIN Gerät Eine Seite wird angezeigt, auf der der Datenverkehr und die Protokollaktivitäten im Zusammenhang mit dem ausgewählten Gerät angezeigt werden.

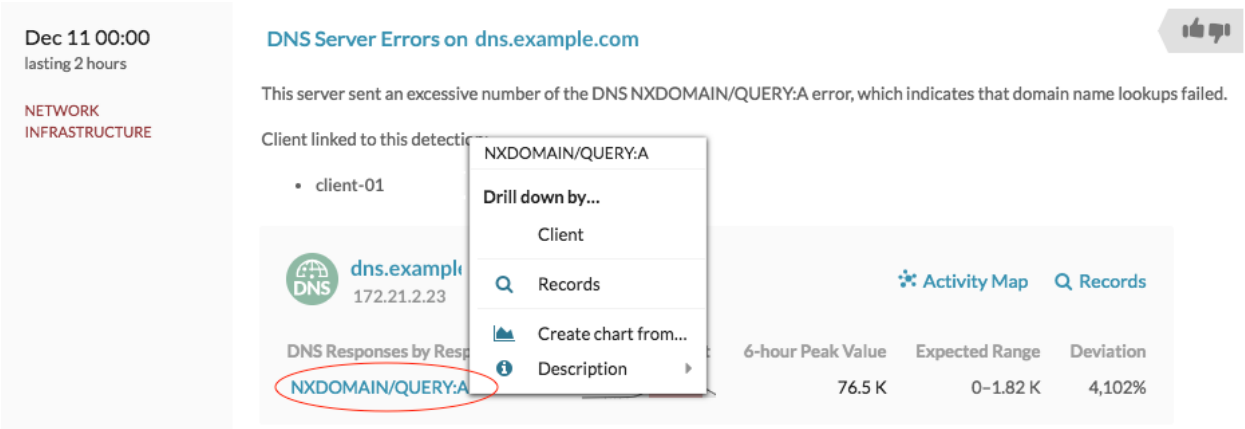
Drilldown von einer Erkennung aus

Bei bestimmten Erkennungen können Sie weitere Details zu der Metrik oder dem Schlüssel aufrufen , der zu dem ungewöhnlichen Verhalten beigetragen hat. Der Metrikname oder der Schlüssel wird als Link am Ende einer einzelnen Erkennung angezeigt.

Hinweis: Erkennungen mit Metriken oder Schlüsseln, die keine detaillierten Metriken enthalten, beinhalten keine Drilldown-Option. Erkennungen, die statt einer Metrik nur anomale Protokollaktivitäten anzeigen, beinhalten auch keine Metrik-Drilldown-Option. Sie können z. B. keinen Drilldown zu einer Erkennung von anomalen DNS-Client-Aktivitäten durchführen, wie in der Abbildung unten dargestellt. Klicken Sie stattdessen auf die Links für den Gerät- oder Anwendungsnamen. **Karte der Aktivitäten**, oder **Rekorde** um mehr über die anomale Aktivität zu erfahren.



1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. klicken **Erkennungen** oben auf der Seite.
3. Suchen Sie nach einer interessanten Erkennung, die mit einer Metrik verknüpft ist, und klicken Sie auf den Namen oder Schlüssel der Metrik. In der folgenden Abbildung können wir durch Klicken auf den Antwortcode eine Aufschlüsselung aller Clients aufrufen, die DNS-Antworten mit NXDOMAIN/QUERY:A erhalten haben.



4. In der Drilldown nach... Abschnitt, klicken Sie auf eine Taste wie **Kunde**.
   Es wird eine Seite mit Detail-Metrik angezeigt, auf der Sie nach Schlüsseln aufgelistete Metriken untersuchen.

Drilldown von einer Alarm aus

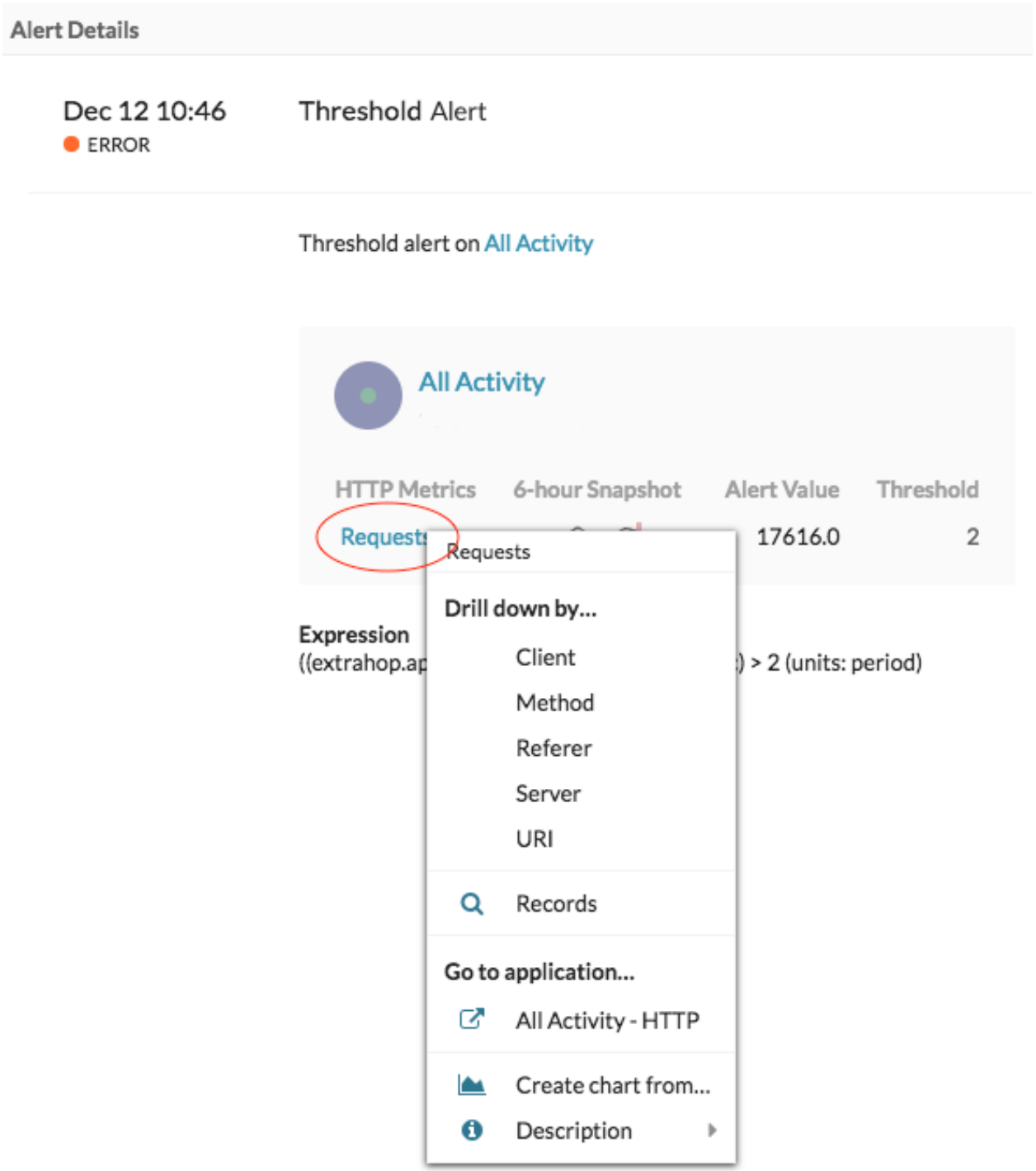
Klicken Sie in einer Schwellenwertwarnung auf den Metriknamen oder Schlüssel, um zu sehen, welcher Schlüssel, z. B. Client, Server, Methode oder Ressource, zu dem Metrikwert oder dem ungewöhnlichen Verhalten beigetragen hat.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. klicken **Alerts** oben auf der Seite.

   Hinweis: Sie können auf Benachrichtigungen auch über ein Alert-Widget in einem Dashboard oder unten auf den folgenden Protokollseiten zugreifen:

   - Seite „Anwendungsübersicht“
   - Seite „Gerätegruppen-Übersicht“
   - Seite „Netzwerkübersicht“

3. Klicken Sie auf den Namen einer Schwellenwarnung.
   Warndetails werden angezeigt.
4. Klicken Sie auf einen Metriknamen oder -schlüssel, wie in der folgenden Abbildung dargestellt.



5. In der Drilldown nach Abschnitt, klicken Sie auf eine Taste, z. B. **Kunde**, **Methode**, **Verweiser**, **Server**, oder **URI**.
   Es wird eine Seite mit Detail-Metrik angezeigt, auf der Sie nach Schlüsseln aufgelistete Metriken untersuchen.

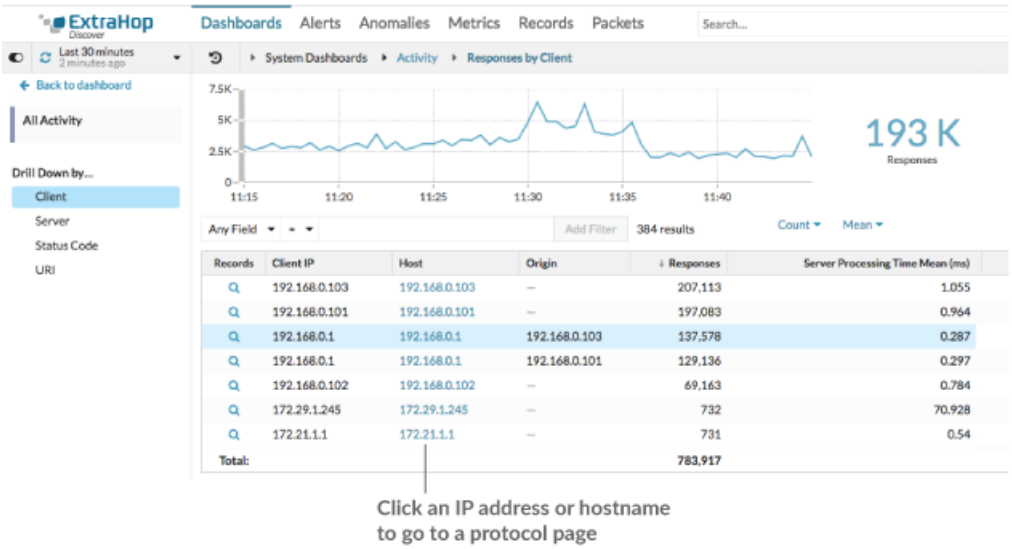
Untersuchen Sie detaillierte Metriken

Nachdem Sie eine Metrik von einem Dashboard, einer Protokollseite, einer Erkennung oder einer Alarm aus detailliert untersucht haben, können Sie die Metrikwerte anhand von Schlüsseln auf einer Seite mit den

Detail-Metrik untersuchen. Filtern Sie Metrikdaten oder wählen Sie verschiedene Schlüssel wie Statuscodes oder URIs aus, um Daten aus verschiedenen Perspektiven anzuzeigen.

Die folgende Abbildung zeigt, wie Sie Daten auf einer Seite mit Detail-Metrik Metriken filtern, pivotieren, sortieren oder exportieren.

Wenn Sie eine Metrik nach IP, Client oder Server aufgeschlüsselt haben, werden IP-Adressen und Hostnamen (sofern sie anhand des DNS-Datenverkehrs beobachtet wurden) in der Tabelle angezeigt. Zusätzliche Optionen stehen Ihnen jetzt zur Verfügung. Sie können beispielsweise direkt zu einer Client- oder Serverprotokollseite navigieren, wie in der folgenden Abbildung dargestellt.



Ergebnisse filtern

Eine Detailseite kann bis zu 1.000 Schlüssel-Wert-Paare enthalten. Es gibt zwei Möglichkeiten, bestimmte Ergebnisse aus Daten zu finden: Filterergebnisse oder klicken Sie auf eine Taste in der Tabelle, um einen weiteren Drilldown-Filter zu erstellen.

Um die Ergebnisse zu filtern, klicken Sie auf **Beliebiges Feld**, und wählen Sie dann ein Feld aus, das je nach Schlüssel variiert. Zum Beispiel können Sie wählen **Netzwerk-Lokalität** für Client- oder Serverschlüssel. Wählen Sie dann einen der folgenden Operatoren aus:

- Wählen Sie **=** um eine exakte Zeichenkettenübereinstimmung durchzuführen.
- Wählen Sie **≈** um eine ungefähre Zeichenkettenübereinstimmung durchzuführen. Der Operator ≈ unterstützt reguläre Ausdrücke.

  Hinweis: Um ein Ergebnis auszuschließen, geben Sie einen regulären Ausdruck ein. Weitere Informationen finden Sie unter Filter für reguläre Ausdrücke erstellen.
- Wählen Sie **#** um eine ungefähre Zeichenkettenübereinstimmung aus Ihren Ergebnissen auszuschließen.
- Wählen Sie **>** oder **≥** um eine Übereinstimmung mit Werten durchzuführen, die größer als (oder gleich) einem angegebenen Wert sind.
- Wählen Sie **<** oder **≤** um eine Übereinstimmung mit Werten durchzuführen, die kleiner als (oder gleich) einem bestimmten Wert sind.
- Klicken Sie **Filter hinzufügen** um die Filtereinstellungen zu speichern. Sie können mehrere Filter für eine Abfrage speichern. Gespeicherte Filter werden gelöscht, wenn Sie im Bereich Details im linken Bereich einen anderen Schlüssel auswählen.

Um den Filter abzuschließen, geben Sie einen Wert ein, nach dem Sie die Ergebnisse filtern möchten, oder wählen Sie einen Wert aus, und klicken Sie dann auf **Filter hinzufügen**.

Untersuchen Sie Bedrohungsdaten (Nur ExtraHop RevealX Premium und Ultra)

Klicken Sie auf das rote Kamerasymbol zum Ansehen Bedrohungsinformationen Details zu einem verdächtigen Host, einer IP-Adresse oder einer URI, die in Detail-Metrik Metrikdaten gefunden wurden.

Markieren Sie einen Metrikwert im oberen Diagramm

Wählen Sie eine einzelne Zeile oder mehrere Zeilen aus, um die Diagrammdaten im oberen Diagramm auf der Seite mit den Detail-Metrik zu ändern. Zeigen Sie mit der Maus auf Datenpunkte im Diagramm, um weitere Informationen zu den einzelnen Datenpunkten anzuzeigen.

Per Schlüssel zu mehr Daten wechseln

Klicken Sie auf die Schlüsselnamen in der Einzelheiten Abschnitt, um detailliertere Metrikwerte zu sehen, aufgeschlüsselt nach anderen Schlüsseln. Klicken Sie für IP-Adresse oder Hostschlüssel auf einen Gerätenamen in der Tabelle, um zu einem Gerät Protokollseite, auf der der Verkehr und die Protokollaktivitäten angezeigt werden, die mit diesem Gerät verknüpft sind.

Passen Sie das Zeitintervall an und vergleichen Sie Daten aus zwei Zeitintervallen

Durch Ändern des Zeitintervalls können Sie Metrikdaten zu verschiedenen Zeiten in derselben Tabelle anzeigen und vergleichen. Weitere Informationen finden Sie unter Vergleichen Sie Zeitintervalle, um das Metrik Delta zu ermitteln.

Hinweis: Das globale Zeitintervall in der oberen linken Ecke der Seite enthält ein blaues Aktualisierungssymbol und einen grauen Text, der angibt, wann die Drilldown-Metriken zuletzt abgefragt wurden. Um die Metriken für das angegebene Zeitintervall neu zu laden, klicken Sie auf das Aktualisierungssymbol in der Anzeige von Global Zeitselektor. Weitere Informationen finden Sie unter Die neuesten Daten für ein Zeitintervall anzeigen.

Metrikdaten in Spalten sortieren

Klicken Sie auf die Spaltenüberschrift, um nach Metriken zu sortieren und anzuzeigen, welche Schlüssel den größten oder kleinsten Metrikwerten zugeordnet sind. Sortieren Sie beispielsweise nach der Verarbeitungszeit, um zu sehen, welche Kunden die längsten Ladezeiten der Website hatten.

Datenberechnung für Metriken ändern

Ändern Sie die folgenden Berechnungen für die in der Tabelle angezeigten Metrikwerte:

- Wenn die Tabelle eine Zählmetrik enthält, klicken Sie auf **Graf** in der Optionen Abschnitt im linken Bereich und wählen Sie dann **Durchschnittliche Rate**. Erfahren Sie mehr in der Rate oder Anzahl in einem Diagramm anzeigen Thema.
- Wenn die Tabelle eine Datensatzmetrik enthält, klicken Sie auf **Gemein** in der Optionen Abschnitt im linken Bereich und wählen Sie dann **Zusammenfassung**. Wenn du auswählst **Zusammenfassung**, Sie können den Mittelwert und die Standardabweichung anzeigen.

Daten exportieren

Klicken Sie mit der rechten Maustaste auf einen Metrikwert in der Tabelle, um eine PDF-, CSV- oder Excel-Datei herunterzuladen.

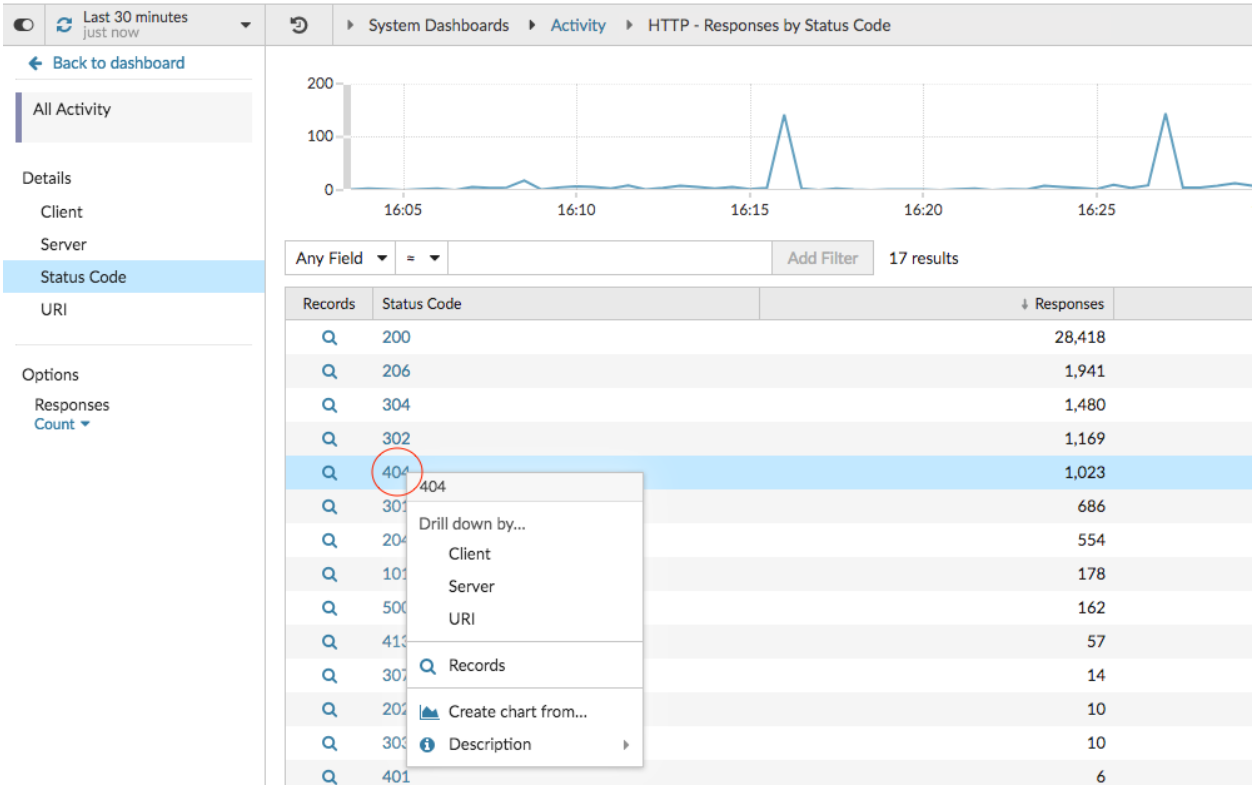
Ein zweites Mal mit einem Schlüsselfilter aufschlüsseln

Nachdem Sie eine Top-Level-Metrik zunächst nach Schlüsseln aufgeschlüsselt haben, wird eine Detailseite mit einem Topnset von Metrik Werten, aufgeschlüsselt nach diesem Schlüssel. Sie können dann einen Filter erstellen, um einen zweiten Drilldown mit einem anderen Schlüssel durchzuführen. Sie können beispielsweise HTTP-Antworten nach Statuscode aufschlüsseln und dann erneut nach dem 404-Statuscode aufschlüsseln, um weitere Informationen zu den Servern, URIs oder Clients zu finden, die mit diesem Statuscode verknüpft sind.

Hinweis: Die Option, einen zweiten Drilldown durchzuführen, ist nur für bestimmte Topnsets verfügbar.

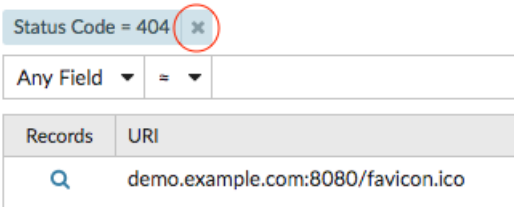
Die folgenden Schritte zeigen Ihnen, wie Sie von einem Diagramm aus einen Drilldown durchführen und dann von einer Detailseite mit Metriken aus erneut einen Drilldown durchführen:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Navigieren Sie zu einer Dashboard- oder Protokollseite.
3. Klicken Sie auf einen Metrikwert oder eine Metrikbezeichnung.
4. In der Drilldown nach... Abschnitt, wählen Sie einen Schlüssel aus.
   Eine Detailseite wird angezeigt.
5. Klicken Sie in der Tabelle auf einen Schlüssel, z. B. einen Statuscode oder eine Methode. (Der Schlüssel darf keine IP-Adresse oder kein Hostname sein.)
6. In der Drilldown nach... Wählen Sie im Abschnitt einen Schlüssel aus, wie in der folgenden Abbildung dargestellt.

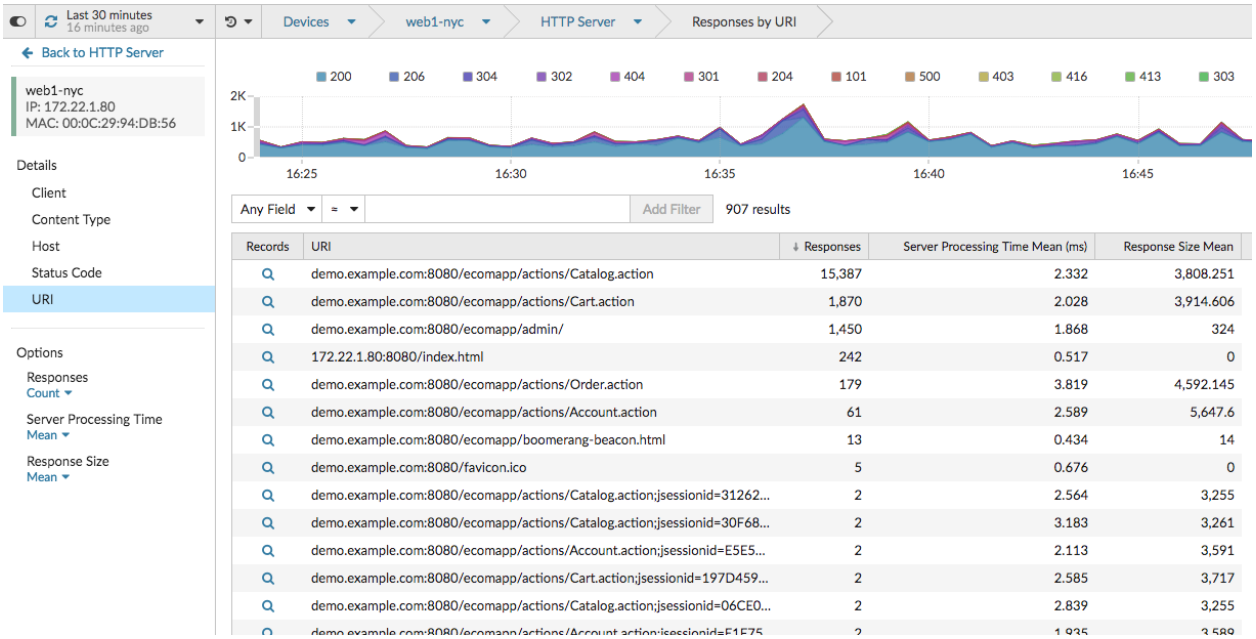


Der Schlüsselfilter wird über der Tabelle angezeigt. Sie können jetzt alle Detailmetriken anzeigen, die mit diesem einzelnen Schlüssel verknüpft sind.

7. Um diesen Filter aus der Tabelle zu entfernen und ihn dann auf das obere Diagramm anzuwenden, klicken Sie auf **x** Symbol, wie in der folgenden Abbildung dargestellt.



Der Filter im Diagramm bleibt bestehen, wenn Sie andere Schlüssel im Abschnitt Details auswählen.



Detailmetriken zu einem Diagramm hinzufügen

Wenn Sie schnell eine Reihe von Detailmetriken in einem Dashboard überwachen möchten, ohne dieselben Drilldown-Schritte wiederholt ausführen zu müssen, können Sie bei der Bearbeitung eines Diagramms in der Metric Explorer. In den meisten Diagrammen können bis zu 20 der wichtigsten Detailmetrikwerte nach Schlüsseln aufgeschlüsselt angezeigt werden. Ein Schlüssel kann eine Client-IP-Adresse, ein Hostname, eine Methode, ein URI, ein Referrer oder mehr sein. Tabellen- und Listen-Widgets können bis zu 200 Metrikwerte mit den wichtigsten Details anzeigen.

Ein Dashboard zur Überwachung des Webverkehrs kann beispielsweise ein Diagramm enthalten, in dem die Gesamtzahl der HTTP-Anfragen und -Antworten angezeigt wird. Sie können dieses Diagramm bearbeiten, um jede Metrik nach IP-Adresse aufzuschlüsseln und die Top-Talker zu sehen.

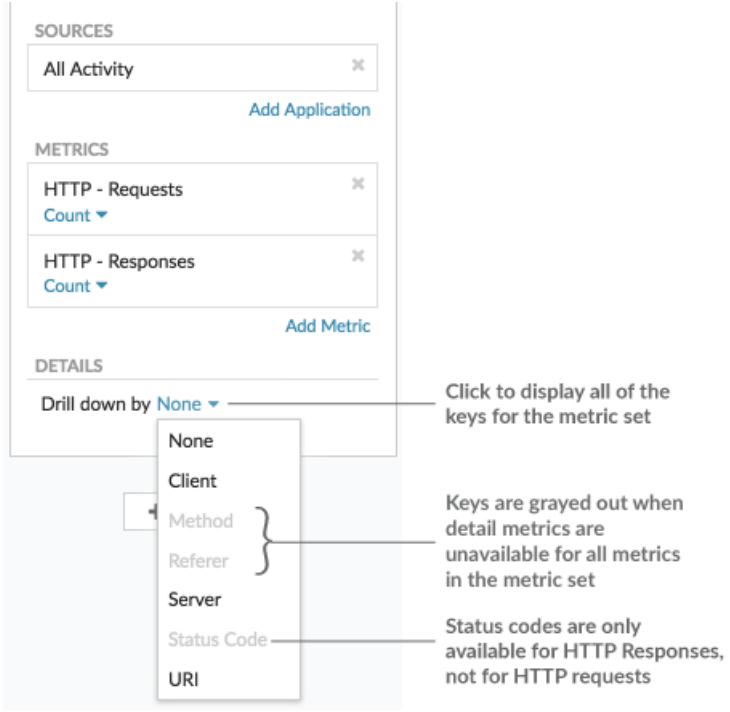
In den folgenden Schritten erfahren Sie, wie Sie ein vorhandenes Diagramm bearbeiten und anschließend Detailmetriken anzeigen können:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Navigieren Sie zu einer Dashboard- oder Protokollseite.
3. Klicken Sie auf den Diagrammtitel und wählen Sie dann **Bearbeiten**.
4. In der Einzelheiten Abschnitt, klicken **Drilldown nach *<None>*** , wo *<None>* ist der Name des Drilldown-Metrikschlüssels, der derzeit in Ihrem Diagramm angezeigt wird.
5. Wählen Sie einen Schlüssel aus der Drop-down-Liste aus.

Hinweis: Wenn Sie mehr als einen haben Quelle Die in Ihrem Metriksatz ausgewählten Quellen, z. B. zwei Geräte, werden beim Drilldown automatisch zu einer Ad-hoc-Quellengruppe zusammengefasst. Sie können die Auswahl nicht aufheben **Quellen kombinieren** Checkbox. Um Drilldown-Metriken für jede Quelle anzuzeigen, müssen Sie eine Quelle aus dem Metriksatz entfernen und dann auf **Quelle hinzufügen** um einen neuen Metriksatz zu erstellen.

Wenn detaillierte Metrikdaten für einen gemeinsamen Schlüssel für alle Metriken in einem Metriksatz verfügbar sind, wird der Schlüssel für die Detail-Metrik automatisch in der Dropdownliste angezeigt, wie in der folgenden Abbildung dargestellt. Wenn ein Schlüssel in der Liste ausgegraut ist, ist die mit diesem Schlüssel verknüpfte Detail-Metrik für alle Metriken in der oben genannten Metrik nicht

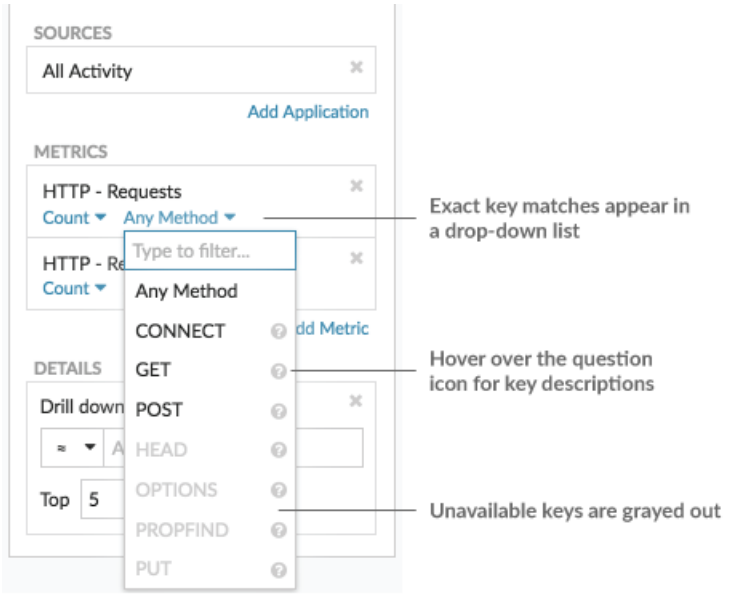
verfügbar. Beispielsweise sind Client-, Server- und URI-Daten sowohl für HTTP-Anfragen als auch für HTTP-Antwortmetriken im Metriksatz verfügbar.



6. Sie können Schlüssel mit einer ungefähren Übereinstimmung filtern, regulärer Ausdruck (Regex), oder führen Sie einen der folgenden Schritte durch, um eine exakte Übereinstimmung zu erzielen:
   - In der Filter Feld, wählen Sie **≈** Operator zur Anzeige von Schlüsseln nach ungefährer Übereinstimmung oder mit Regex. Sie müssen Schrägstriche mit Regex im Filter für ungefähre Treffer weglassen.

     Hinweis: Die **#** Die Filteroption zum Ausschließen von Ergebnissen ist nur verfügbar für Detailseiten. Wenn Sie Ergebnisse in einem Dashboard-Diagramm ausschließen möchten, erstellen Sie ein regulärer Ausdruck (Regex).
   - In der Filter Feld, wählen Sie **=** Operator zur Anzeige von Tasten nach exakter Übereinstimmung.
7. Optional: Geben Sie im oberen Ergebnisfeld die Anzahl der Schlüssel ein, die Sie anzeigen möchten. Diese Schlüssel werden die höchsten Werte haben.
8. Um eine Drilldown-Auswahl zu entfernen, klicken Sie auf **x** Ikone.

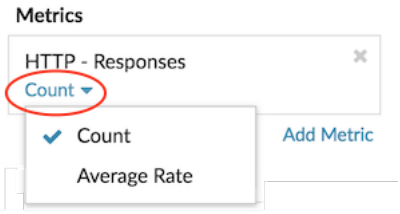
Hinweis: Sie können eine exakte Schlüsselübereinstimmung pro Metrik anzeigen, wie in der folgenden Abbildung dargestellt. Klicken Sie auf den Namen der Drilldown-Metrik (z. B. **Alle Methoden**), um einen bestimmten Metrik Drilldown-Key auszuwählen (z. B. `GET`) aus der Drop-down-Liste. Wenn ein Schlüssel grau erscheint (z. B. `PROPFIND`), sind Drilldown-Metrikdaten für diesen bestimmten Schlüssel nicht verfügbar. Sie können auch einen Schlüssel eingeben, der nicht in der Dropdownliste enthalten ist.



Rate oder Anzahl in einem Diagramm anzeigen

Sie können Fehler, Antworten, Anfragen und andere Zählmetrikdaten in einem Diagramm als Rate pro Sekunde oder als Gesamtzahl der Ereignisse im Zeitverlauf visualisieren. Für hochpräzise Metriken zu Netzwerkbytes und Netzwerkpaketen stehen Ihnen zusätzliche Optionen zur Verfügung, um die maximale, minimale und durchschnittliche Rate pro Sekunde in einem Diagramm anzuzeigen.

Wann Bearbeiten eines Diagramms im Metric Explorer, können Sie eine Anzahl oder Rate auswählen, indem Sie auf den Dropdown-Link unter dem Metriknamen klicken, wie in der folgenden Abbildung dargestellt.



Darüber hinaus können Sie aus den folgenden Optionen für die Anzeige von Tarifen und Zählungen wählen. Beachten Sie, dass der von Ihnen Metrik Metriktyp davon abhängt, welche Rate oder Anzahl automatisch angezeigt wird.

Durchschnittsrate

Berechnet den durchschnittlichen Metrikwert pro Sekunde für das ausgewählte Zeitintervall. Für netzwerkbezogene Messwerte wie Response L2 Bytes oder NetFlow Bytes wird die durchschnittliche Rate pro Sekunde automatisch angezeigt.

Zählen

Zeigt die Gesamtzahl der Ereignisse für das ausgewählte Zeitintervall an. Für die meisten Zählmetriken, wie Fehler, Anfragen und Antworten, wird die Anzahl automatisch angezeigt.

Zusammenfassung der Tarife

Berechnet den maximalen, minimalen und durchschnittlichen Metrikwert pro Sekunde. Bei hochpräzisen Metriken wie Netzwerkbytes und Netzwerkpaketen werden diese drei Raten automatisch als Zusammenfassung im Diagramm angezeigt. Sie können auch wählen, ob nur der Höchst-, Mindest- oder Durchschnittskurs in einem Diagramm angezeigt werden soll. Hochpräzise

Metriken werden mit einem erfasst Granularitätsebene von 1 Sekunde und sind nur verfügbar, wenn Sie konfiguriere dein Diagramm mit einer Netzwerk- oder Gerätequelle.

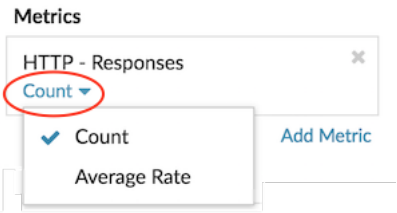
Zeigen Sie den Durchschnittskurs in einem Diagramm an

Wenn Sie ein Diagramm mit einer Fehler-, Antwort-, Anfrage- oder anderen Zählmetrik konfiguriert haben, wird automatisch die Gesamtzahl der Ereignisse im Laufe der Zeit angezeigt. Sie können das Diagramm weiter bearbeiten, um eine Durchschnittsrate pro Sekunde für Ihre Daten anzuzeigen.

Bevor Sie beginnen
Erstellen Sie ein Diagramm und wählen Sie eine Zählmetrik, z. B. Fehler, Anfragen oder Antworten, als Quelle aus. Speichern Sie Ihr Diagramm in einem Dashboard.

Die folgenden Schritte zeigen Ihnen, wie Sie einem vorhandenen Dashboard-Diagramm einen Durchschnittskurs hinzufügen:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Armaturenbretter**.
3. Starte das Metric Explorer zum Bearbeiten des Diagramms indem Sie die folgenden Schritte ausführen:
   a) Wählen Sie im Dashboard-Dock ein Dashboard aus, das das Diagramm enthält, das Sie bearbeiten möchten.
   b) Klicken Sie auf den Diagrammtitel und wählen Sie **Bearbeiten**.
4. klicken **Zählen** unter dem Metriknamen.



5. Wählen **Durchschnittliche Rate** aus der Drop-down-Liste.
   Die Einheit „/s“ wird auf Metrik Einheiten angewendet. Sie können jederzeit zur Zählung zurückkehren.
6. klicken **Speichern** um den Metric Explorer zu schließen.

Hinweis: Wenn Sie mehr als eine Zählmetrik in einem Diagramm auswählen, vermeiden Sie es, Raten und Zählungen zusammen in demselben Diagramm anzuzeigen. Es kann die Skala der Y-Achse verzerren. Die Y-Achse enthält nur dann ein „/s“ auf den Häkchenbeschriftungen, wenn alle Metriken Raten anzeigen.

Zeigen Sie die maximale Rate in einem Diagramm an

Um die maximale Rate pro Sekunde einer Metrik in einem Diagramm anzuzeigen, müssen Sie ein Diagramm mit einer hochpräzisen Metrik konfigurieren.

Die folgenden Schritte zeigen Ihnen, wie Sie ein Diagramm konfigurieren, das eine maximale Rate anzeigt:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Führen Sie einen der folgenden Schritte aus:
   - Um ein neues Diagramm zu erstellen, klicken Sie auf das Befehlsmenü ⋮ in der oberen rechten Ecke der Seite und wählen Sie dann **Diagramm erstellen**.
   - Um ein vorhandenes Diagramm zu bearbeiten, klicken Sie auf **Armaturenbretter** oben auf der Seite. Wählen Sie im Dashboard-Dock ein Dashboard aus, das das Diagramm enthält, das Sie bearbeiten möchten. Klicken Sie auf den Diagrammtitel und wählen Sie **Bearbeiten**.
3. klicken **Quelle hinzufügen** und wählen Sie eine der folgenden Quellen aus:

- Eine Netzwerkquelle, bei der es sich nicht um ein Flussnetz handelt, z. B. ein Standort.
- Ein Gerät, z. B. ein Server oder ein Client.

4. Suchen Sie nach einer der folgenden Metriken und wählen Sie sie aus:

   Für eine Netzwerkquelle

   - Netzwerk-Bytes (Gesamtdurchsatz)
   - Netzwerkpakete (Gesamtpakete)

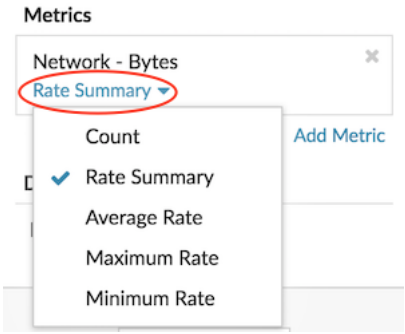
   Für eine Gerätequelle

   - Netzwerk-Bytes (kombinierter eingehender und ausgehender Durchsatz pro Gerät)
   - Eingehende Netzwerk-Bytes (eingehender Durchsatz pro Gerät)
   - Netzwerk-Bytes Out (ausgehender Durchsatz pro Gerät)
   - Netzwerkpakete (kombinierte eingehende und ausgehende Pakete pro Gerät)
   - Eingehende Netzwerkpakete (eingehende Pakete pro Gerät)
   - Ausgehende Netzwerkpakete (ausgehende Pakete pro Gerät)

5. Wählen Sie einen Diagrammtyp aus, der mit Zählmetriken kompatibel ist (einschließlich Linien-, Wert-, Säulen-, Balken-, Kreis- und Listendiagramme).

   Die Standardanzeige für eine hochpräzise Metrik ist eine Kursübersicht, in der automatisch die Höchst-, Durchschnitts- und Mindestrate angezeigt werden.

6. klicken **Zusammenfassung der Tarife** unter dem Metriknamen.



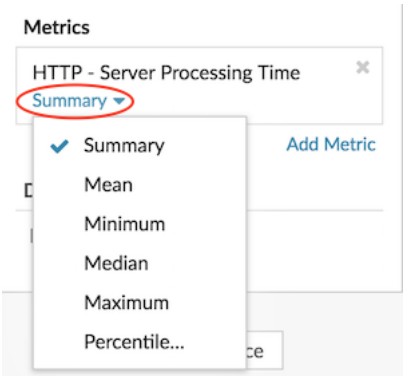
7. Wählen **Maximaler Tarif** aus dem Drop-down-Menü.
8. klicken **Speichern** um den Metric Explorer zu schließen.

Perzentile oder einen Mittelwert in einem Diagramm anzeigen

Wenn Sie über eine Reihe von Servern verfügen, die für Ihr Netzwerk von entscheidender Bedeutung sind, können Sie anhand des 95. Perzentils der Serververarbeitungszeit in einem Diagramm abschätzen, wie viele Server Probleme haben. Perzentile sind statistische Kennzahlen, die Ihnen zeigen können, wie ein Datenpunkt im Vergleich zu einer Gesamtverteilung im Laufe der Zeit abschneidet.

Sie können Perzentilwert- und Mittelwertberechnungen (Durchschnittsberechnungen) nur in Diagrammen anzeigen, die Datensatz oder Probenset Metriken. Datensatzmetriken sind mit Timing und Latenz verknüpft, z. B. Metriken zur Serververarbeitungszeit und zur Roundtrip-Zeit. Sampleset-Metriken bieten Zusammenfassungen detaillierter Timing-Metriken, wie z. B. die Serververarbeitungszeit, aufgeschlüsselt nach Server, Methode oder URI.

Wann Bearbeiten eines Diagramms im Metric Explorer, können Sie Perzentile oder den Mittelwert auswählen, indem Sie auf den Dropdown-Link unter dem Metriknamen des Datensatzes oder des Stichprobensatzes klicken, wie in der folgenden Abbildung dargestellt.



Der Metric Explorer bietet die folgenden Berechnungen für die Anzeige von Perzentilen und des Mittelwerts.

Zusammenfassung

Bei Datensatzmetriken ist die Zusammenfassung ein Bereich, der die 95., 75., 50., 25. und 5. Perzentilwerte umfasst.

Beispielsweise enthält jede Linie in einem Kerzen-Chart fünf Datenpunkte. Wenn Zusammenfassung ausgewählt ist, stellt der Hauptteil der Linie den Bereich vom 25. Perzentil bis zum 75. Perzentil dar. Das mittlere Häkchen steht für das 50. Perzentil (Median). Der obere Schatten über der Körperlinie steht für das 95. Perzentil. Der untere Schatten steht für das 5. Perzentil.

Für Stichprobenmesswerte zeigt die Zusammenfassung die +/-1 Standardabweichung und die Mittelwerte an. Im Kerzen-Chart steht das vertikale Häkchen in der Linie für den Mittelwert und die oberen und unteren Schatten für die Standardabweichungswerte.

Gemein

Der berechnete Durchschnitt der Daten.

Median

Der 50. Perzentilwert einer Datensatzmetrik.

Maximal

Der 100. Perzentilwert einer Datensatzmetrik.

Minimal

Der 0-te Perzentilwert einer Datensatzmetrik.

Perzentil

Ein benutzerdefinierter Bereich von drei oder fünf Perzentilwerten für eine Datensatzmetrik.

Einen benutzerdefinierten Perzentilbereich anzeigen

Sie können einen benutzerdefinierten Bereich von drei oder fünf Perzentilwerten für Messwerte zur Serververarbeitungszeit oder Roundtrip-Zeit anzeigen. Sie können keine benutzerdefinierten Perzentile in einem Kreis - oder Statusdiagramm anzeigen.

Die folgenden Schritte zeigen Ihnen, wie Sie einem vorhandenen Dashboard-Diagramm einen benutzerdefinierten Perzentilbereich hinzufügen:

Bevor Sie beginnen
Erstellen Sie ein Diagramm und wähle eine Datensatz oder Probenset Metrik, und speichern Sie sie in einem Dashboard.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Armaturenbretter**.
3. Starte das Metric Explorer zum Bearbeiten des Diagramms indem Sie die folgenden Schritte ausführen:

a) Wählen Sie im Dashboard-Dock ein Dashboard aus, das das Diagramm enthält, das Sie bearbeiten möchten.
b) Klicken Sie auf den Diagrammtitel und wählen Sie **Bearbeiten**.

4. klicken **Zusammenfassung** unter dem Metriknamen.
5. Wählen **Perzentil...** aus der Drop-down-Liste.
6. Geben Sie im Feld Perzentile festlegen eine Zahl für jeden Perzentilwert ein, getrennt durch ein Komma. Um beispielsweise die 10., 30. und 80. Perzentile anzuzeigen, geben Sie `10, 30, 80`.
7. klicken **Speichern**. Ihr benutzerdefinierter Bereich wird jetzt im Diagramm angezeigt. Sie können jederzeit zwischen Ihrem benutzerdefinierten Bereich und anderen Perzentilauswahlen wie Zusammenfassung oder Maximum wechseln.
8. klicken **Speichern** erneut, um den Metric Explorer zu schließen.

Ausreißer in Histogramm- oder Heatmap-Diagrammen filtern

Histogramm- und Heatmap-Diagramme zeigen eine Verteilung der Daten. Ausreißer können jedoch die Darstellung der Verteilung in Ihrem Diagramm verzerren, sodass es schwierig ist, Muster oder Durchschnittswerte zu erkennen. Die Standardfilteroption für diese Diagramme schließt Ausreißer aus dem Datenbereich aus und zeigt die Perzentile vom 5. bis 95. an. Sie können den Filter so ändern, dass der gesamte Datenbereich (Mindest- bis Höchstwerte), einschließlich Ausreißer, in Ihrem Diagramm angezeigt wird, indem Sie das folgende Verfahren ausführen.

1. Klicken Sie auf den Diagrammtitel und wählen Sie dann **Bearbeiten** um das zu starten Metric Explorer.
2. Klicken Sie auf **Optionen** Registerkarte.
3. Wählen Sie in der Dropdownliste Standardfilter im Abschnitt Filter die Option **Min bis Max**.
4. klicken **Speichern** um den Metric Explorer zu schließen.

Metrikbeschriftungen in einer Diagrammlegende bearbeiten

Sie können die standardmäßige Metrikbezeichnung in einem Diagramm in eine benutzerdefinierte Bezeichnung ändern. Sie können beispielsweise die Standardbezeichnung „Netzwerk-Bytes“ in eine benutzerdefinierte Bezeichnung wie „Durchsatz“ ändern.

Benutzerdefinierte Beschriftungen gelten nur für einzelne Diagramme. Eine benutzerdefinierte Bezeichnung für eine Metrik bleibt bestehen, wenn Sie das Diagramm in ein anderes Dashboard kopieren, ein Dashboard mit einem anderen Benutzer teilen oder Ihrem Diagramm neue Metriken hinzufügen.

Wenn Sie jedoch Änderungen an der ursprünglichen Metrik vornehmen, z. B. die Datenberechnung aktualisieren (z. B. vom Median auf das 95. Perzentil) oder die Metrik genauer untersuchen, wird die benutzerdefinierte Bezeichnung automatisch gelöscht. Das Etikett wird gelöscht, um eine falsche Kennzeichnung oder mögliche Ungenauigkeit der benutzerdefinierten Bezeichnung zu verhindern, wenn sich Metrik Daten ändern.

Im Folgenden finden Sie einige Überlegungen zum Ändern der Bezeichnung einer Diagrammlegende:

- Für detaillierte Metriken, ein benutzerdefiniertes Etikett wird automatisch an alle im Diagramm angezeigten Schlüssel angehängt. Sie können jedoch die Reihenfolge des Schlüssels in der Bezeichnung ändern, indem Sie die Variable einbeziehen *$-SCHLÜSSEL*:
  - Typ `$KEY-Fehler` zur Anzeige **Fehler 172.21.1.1**
  - Typ `[$KEY] -Fehler` anzeigen **[172.21.1.1] Fehler**
- Sie können Beschriftungen im Boxplot, im Candlestick, in der Heatmap, in der Tabelle oder in den Statusdiagrammen nicht ändern.
- Metrik Delta- oder Dynamische Basislinie Baseline-Labels können nicht umbenannt werden.

Bevor Sie beginnen
Erstellen Sie ein Diagramm und wählen Sie eine Metrik aus.

Die folgenden Schritte zeigen Ihnen, wie Sie Metrikbeschriftungen in einem vorhandenen Dashboard-Diagramm ändern können:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Armaturenbretter**.
3. Starte das Metric Explorer zum Bearbeiten des Diagramms indem Sie die folgenden Schritte ausführen:
   a) Wählen Sie im Dashboard-Dock ein Dashboard aus, das das Diagramm enthält, das Sie bearbeiten möchten.
   b) Klicken Sie auf den Diagrammtitel und wählen Sie **Bearbeiten**.
4. Klicken Sie im Vorschaufenster des Metric Explorer auf die Metrik-Bezeichnung.
5. Wählen **Umbenennen** aus dem Drop-down-Menü.
6. In der Benutzerdefiniertes Etikett anzeigen Feld, geben Sie eine neue Bezeichnung ein.
   Die Bezeichnung muss sich von anderen Beschriftungen im Diagramm unterscheiden.
7. klicken **Speichern**, und klicken Sie dann auf **Speichern** erneut, um den Metric Explorer zu schließen. Die neue Bezeichnung wird in Ihrem Diagramm angezeigt.

Hinzufügen einer Dynamische Basislinie zu einem Diagramm

Dynamische Basislinien helfen dabei, zwischen normaler und abnormaler Aktivität in Ihren Diagrammdaten zu unterscheiden. Basislinien werden nur in Flächen-, Kerzendiagrammen, Säulen-, Linien- und Linien- und Säulendiagrammen unterstützt.

Das ExtraHop-System berechnet dynamische Basislinien auf der Grundlage historischer Daten. Um einen neuen Datenpunkt auf einer Dynamische Basislinie zu generieren, berechnet das System den Medianwert für einen bestimmten Zeitraum.

Warnung: Durch das Löschen oder Ändern einer Dynamische Basislinie können Basisdaten aus dem System gelöscht werden. Wenn keine Dashboards auf eine Dynamische Basislinie verweisen, werden die Daten aus dem System gelöscht, um ungenutzte Systemressourcen freizugeben. Sie können eine Dynamische Basislinie nicht wiederherstellen, nachdem sie gelöscht wurde.

Wählen Sie einen Baseline-Typ, der am besten zu Ihrer Umgebung passt. Wenn Sie beispielsweise regelmäßig dramatische Veränderungen von einem Tag zum anderen feststellen, wählen Sie einen Basiswert für die Wochenstunden aus, der die Aktivitäten an bestimmten Wochentagen vergleicht. Wenn die HTTP-Aktivität an Samstagen stark ansteigt, können Sie anhand der Wochenstundenbasis den aktuellen Anstieg der HTTP-Aktivität mit dem Niveau vergleichen, das an anderen Samstagen zur gleichen Stunde zu beobachten ist. In der folgenden Tabelle wird beschrieben, wie die einzelnen Basislinientypen berechnet werden:

Basislinientyp	Historische Daten	Was die Baseline miteinander vergleicht	Neue Basisdatenpunkte hinzugefügt
Stunde des Tages	10 Tage	Metrische Werte für eine bestimmte Stunde eines Tages. Zum Beispiel jeden Tag um 14:00 Uhr.	Jede Stunde
Stunde der Woche	5 Wochen	Metrische Werte für eine bestimmte Stunde an einem bestimmten Wochentag. Zum Beispiel jeden Mittwoch um 14:00 Uhr.	Jede Stunde

Basislinientyp	Historische Daten	Was die Baseline miteinander vergleicht	Neue Basisdatenpunkte hinzugefügt
Kurzfristiger Trend	1 Stunde	Metrische Werte für jede Minute in einer Stunde.	Alle 30 Sekunden

Im Folgenden finden Sie einige wichtige Überlegungen zum Hinzufügen einer Basislinie zu einem Diagramm:

- Dynamische Baselines berechnen und speichern Basisdaten. Daher verbraucht das Erstellen einer Baseline Systemressourcen, und die Konfiguration zu vieler Baselines kann die Systemleistung beeinträchtigen.
- Durch das Löschen oder Ändern einer Dynamische Basislinie können Dynamische Basislinie Basisdaten aus dem System gelöscht werden.
- Detailmetriken, auch als Topnsets bezeichnet, werden nicht unterstützt. Die Metriken Sampleset, Maximal Rate und Minimal Rate werden ebenfalls nicht unterstützt. Wenn eine dieser Arten von Kennzahlen in Ihrem Diagramm ausgewählt ist, können Sie keine Dynamische Basislinie für diese Daten generieren.
- Das System kann nur dann mit dem Aufbau einer Dynamische Basislinie beginnen, wenn die erforderliche Menge an historischen Daten verfügbar ist. Zum Beispiel ein **Stunde des Tages** Für den Basisplan sind historische Daten von 10 Tagen erforderlich. Wenn das System erst seit sechs Tagen Daten sammelt, beginnt die Basislinie erst mit der Darstellung, wenn Daten für weitere vier Tage vorliegen.
- Das System zeichnet nicht rückwirkend eine Dynamische Basislinie für historische Daten auf. Das System zeichnet nur eine Dynamische Basislinie für neue Daten.
- Wenn zwei identische dynamische Baselines in separaten Dashboards existieren, verwenden die Dashboards die Basisdaten wieder. Die Baselines müssen jedoch identisch sein. Wenn Sie einen neuen Basislinientyp auswählen, teilt die neue Dynamische Basislinie keine Daten mit der vorherigen Dynamische Basislinie.

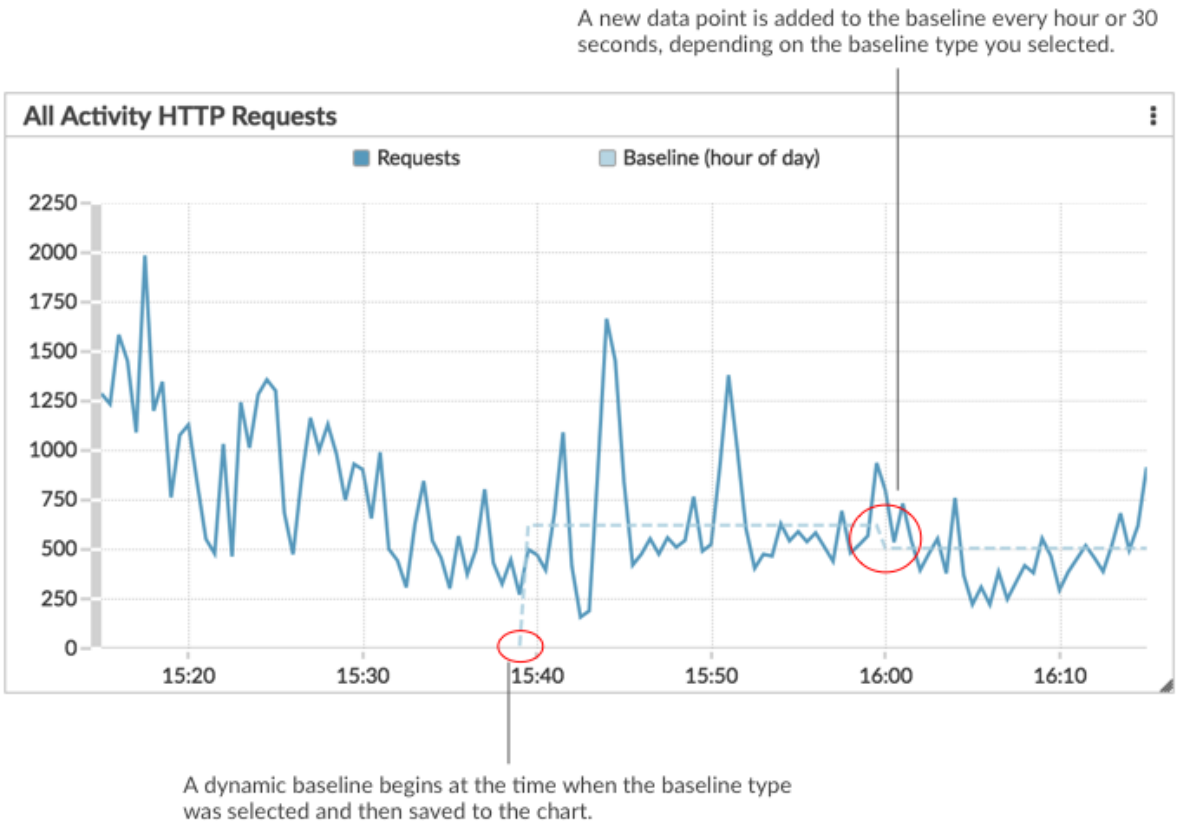
Die folgenden Schritte zeigen Ihnen, wie Sie einem vorhandenen Dashboard-Diagramm eine Dynamische Basislinie hinzufügen:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Armaturenbretter**.
3. Starte das Metric Explorer zum Bearbeiten des Diagramms indem Sie die folgenden Schritte ausführen:
   a) Wählen Sie im Dashboard-Dock ein Dashboard aus, das das Diagramm enthält, das Sie bearbeiten möchten.
   b) Klicken Sie auf den Diagrammtitel und wählen Sie dann **Bearbeiten**.
4. Klicken Sie auf **Analyse** Tabulatur.
5. In der Dynamische Baselines Wählen Sie im Abschnitt eine der folgenden Optionen für den Dynamische Basislinie Baseline-Typ aus:

Option	Description
Stunde des Tages	Zeigt den Medianwert für eine bestimmte Stunde des Tages an. Diese Option ist am nützlichsten, wenn die Aktivitäten in Ihrer Umgebung normalerweise einem konsistenten Tagesmuster folgen. Wenn Sie an verschiedenen Wochentagen regelmäßig stark unterschiedliche Aktivitätsniveaus feststellen, ist diese Option weniger nützlich, da der Basiswert normalerweise nicht mit den aktuellen Werten übereinstimmt.

Option	Description
Stunde der Woche	Zeigt den Medianwert für eine bestimmte Stunde an einem bestimmten Wochentag an. Diese Option ist am nützlichsten, wenn Sie an jedem Wochentag regelmäßig ein deutlich unterschiedliches Verkehrsaufkommen feststellen.
Kurzfristiger Trend	Zeigt den Medianwert der letzten Stunde an. Diese Option ist nützlich, um Diagrammdaten zu glätten, um kurzfristige Trends aufzudecken.

6. klicken **Speichern** um den Metric Explorer zu schließen und zum Dashboard zurückzukehren. Das ExtraHop-System beginnt mit der Berechnung der Dynamische Basislinie. Neue Basisdatenpunkte werden jede Stunde oder 30 Sekunden hinzugefügt, wie in der folgenden Abbildung dargestellt.



Hinzufügen einer statischen Schwellenwertlinie zu einem Diagramm

Durch die Anzeige einer statischen Schwellenwertlinie in einem Diagramm können Sie feststellen, welche Datenpunkte entweder unter oder über einem signifikanten Wert liegen.

Sie können beispielsweise ein Liniendiagramm für die Serververarbeitungszeit erstellen, um die Leistung einer wichtigen Datenbank in Ihrer Netzwerkumgebung zu überwachen. Durch Hinzufügen einer

Schwellenwertlinie, die eine Grenze der akzeptablen Verarbeitungszeit (Service Level Agreement, SLA) definiert, können Sie erkennen, wann sich die Datenbankleistung verlangsamt, und das Problem beheben.

Sie können nach Belieben eine oder mehrere Schwellenwertlinien hinzufügen Bearbeiten Sie ein Diagramm mit dem Metric Explorer. Diese Linien sind lokal im Diagramm und nicht mit anderen Widgets oder Benachrichtigungen verknüpft. Schwellenwertlinien sind nur für Flächen-, Kerzen-, Säulen-, Linien-, Linien- und Säulen- und Statusdiagramme verfügbar.

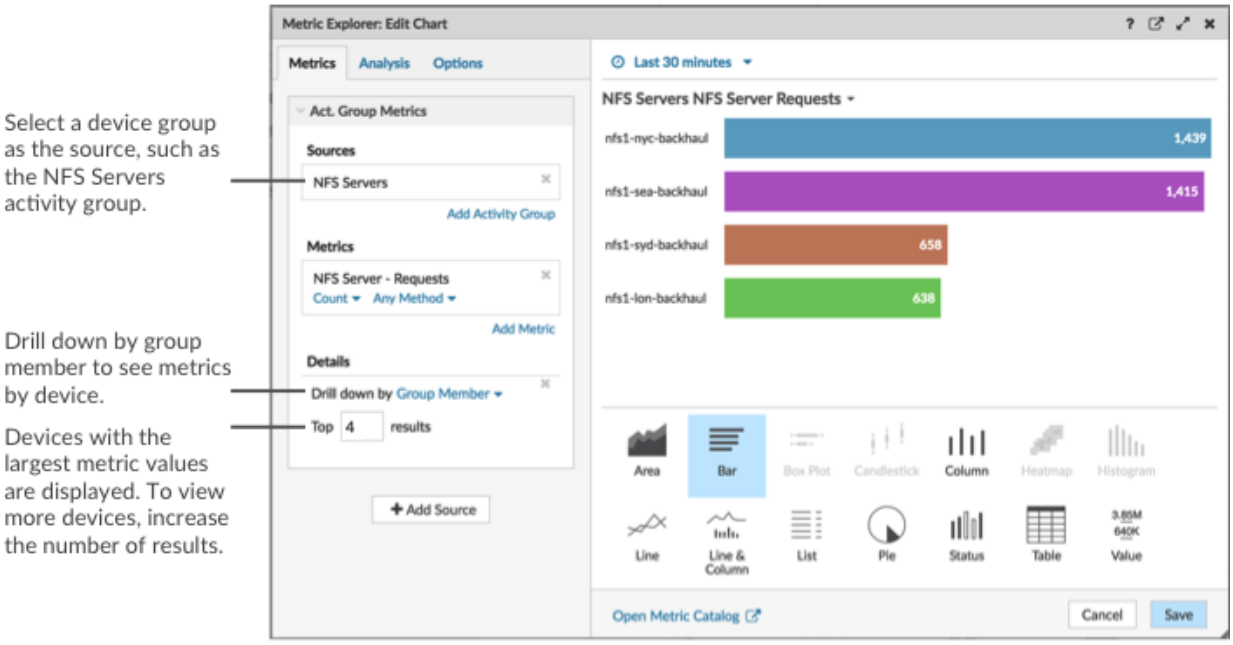
Die folgenden Schritte zeigen Ihnen, wie Sie einem vorhandenen Dashboard-Diagramm eine statische Schwellenwertlinie hinzufügen:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Dashboards**.
3. Starte das Metric Explorer zum Bearbeiten des Diagramms indem Sie die folgenden Schritte ausführen:
   a) Wählen Sie im Dashboard-Dock ein Dashboard aus, das das Diagramm enthält, das Sie bearbeiten möchten.
   b) Klicken Sie auf den Diagrammtitel und wählen Sie dann **Bearbeiten**.
4. Klicken Sie auf **Analyse** Tabulatur.
5. In der Statische Schwellenwerte Abschnitt, klicken **Schwellenlinie hinzufügen**.
6. In der Wert Feld, geben Sie eine Zahl ein, die den Schwellenwert für die Zeile angibt. Dieser Wert bestimmt, wo die Linie auf der Y-Achse Ihres Diagramms erscheint.

   Hinweis: Für Diagramme, die nur angezeigt werden Metriken zählen (wie Byte, Fehler und Antworten) wird der Wert der Schwellenwertlinie automatisch skaliert, je nachdem, ob die Daten wird als Rate oder Anzahl angezeigt. Wenn Daten nur als Anzahl angezeigt werden, passt sich der Schwellenwert der Zeile automatisch dem Rollup-Zeitraum an (entweder 30 Sekunden, 5 Minuten, 1 Stunde oder 1 Tag). Die Die Dauer des Datenaufrufs wird durch das Zeitintervall bestimmt du wählst.
7. In der Etikett Feld, geben Sie einen Namen für Ihre Schwellenwertlinie ein.
8. In der Farbe Feld, wählen Sie eine Farbe (Grau, Rot, Orange oder Gelb) für Ihre Schwellenwertlinie aus.
9. klicken **Speichern** um den Metric Explorer zu schließen.

Gerätegruppenmitglieder in einem Diagramm anzeigen

Wenn Sie über ein Diagramm verfügen, in dem eine Gerätegruppe angezeigt wird, können Sie Messwerte für die wichtigsten Geräte in der Gruppe anzeigen, anstatt einen einzelnen Wert für die gesamte Gerätegruppe anzuzeigen. Wenn Sie im Metric Explorer nach Gruppenmitgliedern aufschlüsseln, können Sie bis zu 20 Geräte im Diagramm anzeigen.



Wenn Sie in einem Diagramm weniger Gruppenmitglieder sehen als die von Ihnen angegebene Anzahl von Ergebnissen, kann dies daran liegen, dass Sie eine integrierte Gerätegruppe mit einer kleinen Anzahl von Geräten ausgewählt haben. Bei integrierten Gerätegruppen werden Geräte dynamisch einer Gruppe zugeordnet, basierend auf der Art des Protokollverkehrs, dem sie zugeordnet sind, oder der Rolle, die ihnen zugewiesen wurde.

Bevor Sie beginnen
Erstellen Sie ein Diagramm das eine Gerätegruppe als ausgewählte Quelle enthält. Speichern Sie das Diagramm in einem Dashboard.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Armaturenbretter** .
3. Starte das Metric Explorer zum Bearbeiten des Diagramms indem Sie die folgenden Schritte ausführen:
   a) Wählen Sie im Dashboard-Dock ein Dashboard aus, das das Diagramm enthält, das Sie bearbeiten möchten.
   b) Klicken Sie auf den Diagrammtitel und wählen Sie **Bearbeiten**.
4. In der Einzelheiten Feld, klicken **Drilldown nach *<None>*** , wo *<None>* ist der Name der Detail-Metrik, die derzeit in Ihrem Diagramm angezeigt wird. Wählen Sie dann **Mitglied der Gruppe**.
5. Geben Sie im Feld mit den besten Ergebnissen die Anzahl der Gruppenmitglieder ein, die Sie anzeigen möchten. Diese Geräte werden die höchsten Metrik Werte haben. Sie können bis zu 20 Gruppenmitglieder anzeigen.
6. klicken **Speichern** um den Metric Explorer zu schließen.

Hinweis: Wenn Sie einen Drilldown nach Gruppenmitgliedern durchführen, können Sie keine zusätzlichen Drilldowns durchführen, um detaillierte Metriken für jedes Gerät anhand eines Schlüssels anzuzeigen. Um detaillierte Kennzahlen für ein Gerät nach Schlüsseln anzuzeigen, empfehlen wir, ein weiteres Diagramm mit bestimmten Geräten als Quelle zu erstellen.

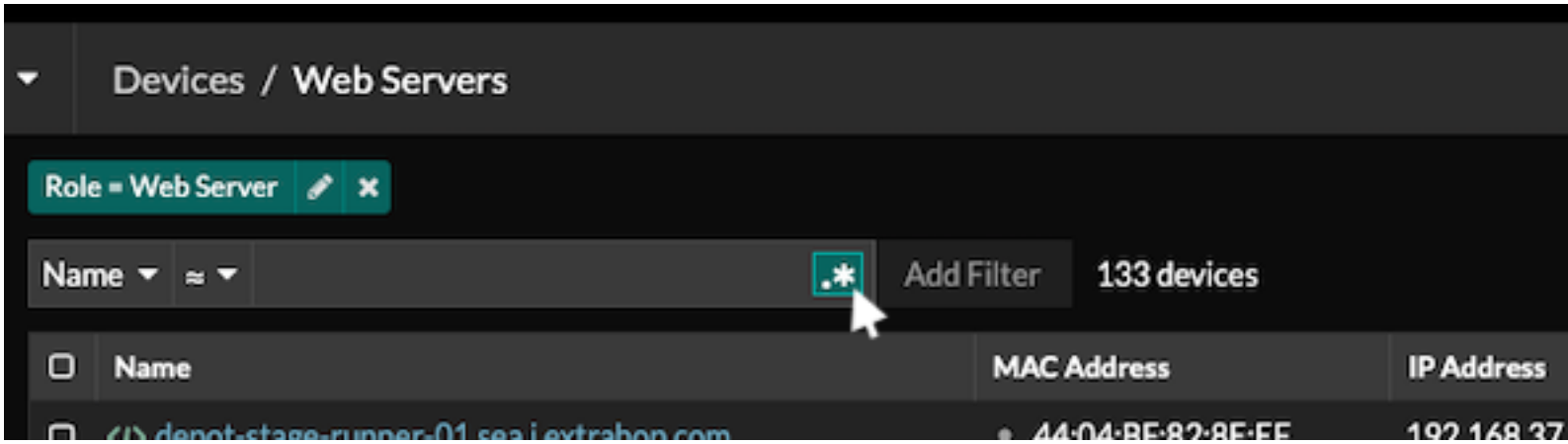
Filter für reguläre Ausdrücke

Filtern Sie Ihre Suchergebnisse, indem Sie in bestimmte Suchfelder im gesamten ExtraHop-System Zeichenketten mit regulären Ausdrücken (Regex) schreiben. Sie können beispielsweise nach Parametern in einem Detail-Metrik Metrikschlüssel filtern, z. B. nach einer Zahl innerhalb einer IP-Adresse. Sie können auch filtern, indem Sie bestimmte Schlüssel oder eine Kombination von Schlüsseln aus Diagrammen ausschließen.

Regex-fähige Suchfelder verfügen über visuelle Indikatoren im gesamten System und akzeptieren die Standardsyntax.

Suchfelder mit einem Sternchen

Klicken Sie auf das Sternchen, um Regex-Zeichenfolgen zu aktivieren.

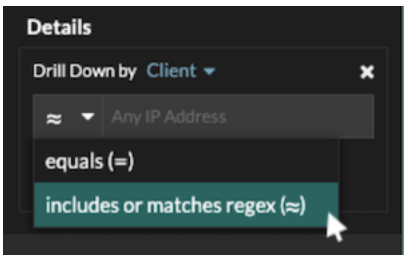


Dieser Feldtyp ist auf den folgenden Systemseiten verfügbar:

- Eine Tabelle mit Geräten filtern
- Filterkriterien für eine dynamische Gerätegruppe erstellen

Bestimmte Suchfelder mit einem Dreifeld-Operator

Klicken Sie auf das Operator-Dropdown-Menü, um die Regex-Option auszuwählen.

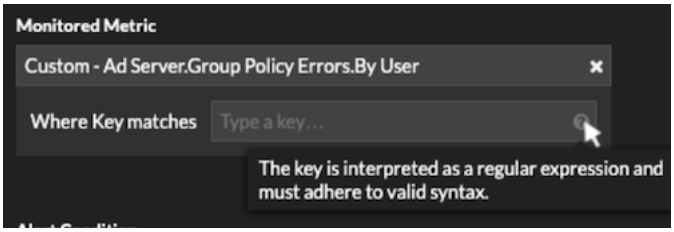


Dieser Feldtyp ist auf der folgenden Systemseite verfügbar:

- Ein Diagramm im Metric Explorer bearbeiten

Bestimmte Suchfelder mit einem Tooltip

Zeigen Sie mit der Maus auf den Tooltip im Feld, um zu sehen, wann Regex erforderlich ist.



Dieser Feldtyp ist auf der folgenden Systemseite verfügbar:

- Hinzufügen von Datensatzbeziehungen zu einer benutzerdefinierten Metrik

Die folgende Tabelle enthält Beispiele für die Standard-Regex-Syntax.

Diagrammszenario	Regex-Filter	So funktioniert's
Vergleichen Sie HTTP-Statuscodes `200` zu `404`.	`(200|404)`	Das vertikale Balkensymbol (|) ist der OR-Operator. Dieser Filter entspricht `200`, oder `404`, oder beide Statuscodes.
Zeigt jeden HTTP-Statuscode an, der einen enthält `4`.	`[41]`	Eckige Klammern ([und]) bezeichnen eine Reihe von Zeichen. Der Filter sucht nach jedem Zeichen innerhalb der Klammern, unabhängig von der Reihenfolge. Dieser Filter entspricht jedem Wert, der einen enthält `4` oder ein `1`. Zum Beispiel kann dieser Filter zurückkehren `204`, `400`, `101`, oder `201` Statuscodes.
Alles anzeigen `500`HTTP-Statuscodes auf -Ebene.	`^ [5]`	Das Caret-Symbol (^) außerhalb der eckigen Klammern ([und]) bedeutet „beginnt mit“. Dieser Filter entspricht jedem Wert, der mit einem beginnt `5`. Dieser Filter kann beispielsweise zurückkehren `500` und `502` Statuscodes.
Alles anzeigen `400` und `500` HTTP-Statuscodes auf -Ebene.	`^ [45]`	Mehrere Werte in eckigen Klammern ([und]) werden einzeln durchsucht, auch wenn ihnen das Caret-Symbol (^) vorangestellt ist. Dieser Filter sucht nicht nach Werten, die beginnen mit `45`, entspricht aber allen Werten, die mit einem beginnen `4` oder `5`. Zum Beispiel kann dieser Filter zurückkehren `400`, `403`, und `500` Statuscodes.
Zeigt alle HTTP-Statuscodes an, außer `200` Statuscodes auf -Ebene.	`^ (?! 2)`	Ein Fragezeichen (?) und Ausrufezeichen (!) geben Sie in Klammern einen auszuschließenden Wert an. Dieser Filter entspricht allen Werten außer Werten, die mit

Diagrammszenario	Regex-Filter	So funktioniert's
		einem beginnen 2. Zum Beispiel kann dieser Filter zurückkehren `400`, `500`, und `302` Statuscodes.
Zeigen Sie eine beliebige IP-Adresse mit einem `187`.	`187.`	Spiele `1`, `8`, und `7` Zeichen in der IP-Adresse. Dieser Filter gibt keine IP-Adressen zurück, die auf 187 enden, da der letzte Punkt angibt, dass nach den Werten etwas stehen muss. Wenn Sie den Punkt als Literalwert durchsuchen möchten, müssen Sie ihm einen umgekehrten Schrägstrich (\) voranstellen.
Überprüfen Sie alle IP-Adressen, die enthalten `187.18.`	`187\ .18.`	Spiele `187.18` und alles, was folgt. Die erste Periode wird wörtlich behandelt, da ihr ein umgekehrter Schrägstrich (\) vorausgeht. Die zweite Periode wird als Platzhalter behandelt. Dieser Filter gibt beispielsweise Ergebnisse für `187.18.0.0`, `180.187.0.0`, oder `187.180.0.0/16`. Dieser Filter gibt keine Adresse zurück, die endet mit `187.18`, weil der Platzhalter erfordert, dass Zeichen den angegebenen Werten folgen.
Zeigt eine beliebige IP-Adresse an, außer `187.18.197.150`.	`^ (?! 187\ .18\ .197\ .150)`	Stimmt mit allem überein, außer `187.18.197.150`, wo `^(?!)` gibt den auszuschließenden Wert an.
Schließt eine Liste bestimmter IP-Adressen aus.	`^(?! 187\.18\.197\.15[012])`	Stimmt mit allem überein, außer `187.18.197.150`, `187.18.197.151`, und `187.18.197.152`, wo `^(?!)` gibt den auszuschließenden Wert an und die eckigen Klammern ([und]) geben mehrere Werte an.

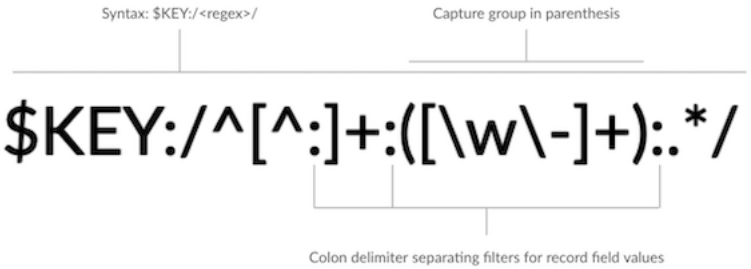
Zusätzliche Filter

Wenn du eine benutzerdefinierte Detail-Metrik erstellen Im Metrikkatalog können Sie dem Suchfeld Zusätzliche Filter im Abschnitt Datensatzbeziehungen eine erweiterte Regex-Syntax hinzufügen.

Der Tooltip wird angezeigt, nachdem Sie ausgewählt haben **Detailmetrik** und ist nicht verfügbar, wenn **Basismetrik** ist ausgewählt.

Die Regex-Syntax in diesem Feld muss die folgenden Anforderungen erfüllen:

- Wenn Ihr Schlüssel mehrere Werte enthält, muss Ihre Regex-Syntax eine einzelne Erfassungsgruppe enthalten. Eine Erfassungsgruppe wird durch Klammern gekennzeichnet. Ihre Capture-Gruppe bestimmt den Filterwert.



- Wenn Sie einen bestimmten Wert aus einem Detailmetrikschlüssel zurückgeben möchten, der mehrere Datensatzfeldwerte enthält, muss die Regex dieser Syntax folgen:

  `$SCHLÜSSEL:/ <regex> /`

  Wenn Ihr Detailmetrikschlüssel beispielsweise ipaddr:host:cipher lautet und Sie nur den IP-Adresswert zurückgeben möchten, geben Sie Folgendes ein:

  `$SCHLÜSSEL: /^ ([^:] +): . +/`
- Wenn Ihr Schlüssel mehrere Datensatzfeldwerte enthält, werden die Werte durch ein Trennzeichen getrennt, das in dem Auslöser angegeben ist, der den Schlüssel generiert. Die Platzierung der Trennzeichen in Ihrer Regex-Syntax muss mit den Trennzeichen im Detailschlüssel übereinstimmen. Wenn Sie beispielsweise einen Schlüssel mit drei Werten haben, die durch ein Trennzeichen getrennt sind, das ein Doppelpunkt ist, müssen die drei Werte für den Schlüssel in Ihrer Regex-Syntax durch zwei Doppelpunkte getrennt werden.

Hinweis: Wenn Sie alle Datensatzfeldwerte in einem detaillierten Metrikschlüssel zurückgeben möchten, geben Sie ein `$SCHLÜSSEL`. Wenn Ihr Detailmetrikschlüssel beispielsweise ipaddr:host:cipher lautet, geben Sie Folgendes ein `$SCHLÜSSEL` im Suchfeld , um alle drei dieser Felddatensatzwerte (IP-Adresse, Hostname und TLS Verschlüsselungssuite) zurückzugeben.

Finden Sie alle Geräte, die mit externen IP-Adressen kommunizieren

Die folgenden Schritte zeigen Ihnen, wie Sie alle externen IP-Adressen finden, mit denen Ihre internen Geräte kommunizieren. Sie können dann sehen, ob Geräte unbefugte Verbindungen von anderen Geräten außerhalb Ihres Netzwerk herstellen oder empfangen.

Hinweis: Standardmäßig wird jedes Gerät mit einer RFC1918-IP-Adresse (in einem 10/8-, 172.16/12- oder 192.168/16 CIDR-Block enthalten), das das ExtraHop-System automatisch erkennt, als internes Gerät klassifiziert. Da einige Netzwerkumgebungen IP-Adressen enthalten, die nicht

nach RFC1918 stammen, als Teil ihres internen Netzwerk können Sie Geben Sie den Standort einer IP-Adresse an auf der Seite Network Localities.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. klicken **Vermögenswerte** oben auf der Seite.
   Die Seite Geräte wird angezeigt, auf der alle Protokolle mit Datenverkehr im ausgewählten Zeitintervall aufgeführt sind.
3. Von Geräte nach Protokollaktivität, klicken Sie auf die Anzahl der TCP-Geräte.
   Oben auf der Seite befindet sich der Extern akzeptiert und Extern verbunden Metriken zeigen an, wie viele IP-Adressen außerhalb Ihres internen Netzwerk aktiv mit all Ihren Netzwerkgeräten verbunden sind.
4. Klicken Sie für eine der Metrik auf den blauen Metrikwert.
5. Wählen Sie im Abschnitt Drilldown nach... **Mitglied der Gruppe**. Eine Seite mit Detail-Metrik wird angezeigt, auf der alle Namen Ihrer Netzwerkgeräte und die Anzahl der Verbindungen zu externen IP-Adressen angezeigt werden.
6. Klicken Sie auf einen Gerätenamen, den Sie untersuchen möchten. Eine Protokollseite für dieses Gerät wird angezeigt, die Metriken zum Gerät enthält.

Nächste Schritte

- Finden Sie Peer-Geräte
- Überwachen Sie ein Gerät auf externe IP-Adressverbindungen

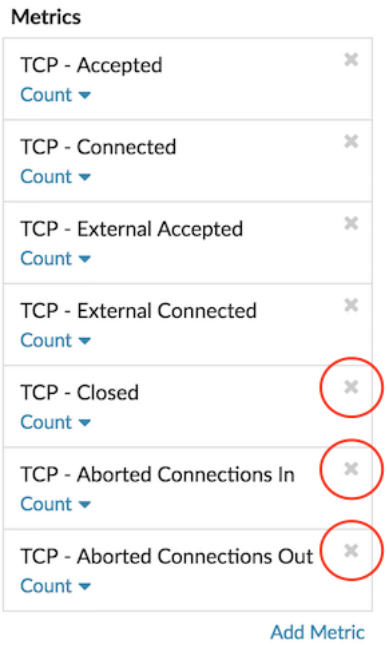
Überwachen Sie ein Gerät auf externe IP-Adressverbindungen

Wenn Sie über einen Authentifizierungsserver oder eine Datenbank verfügen, die keine Verbindung zu IP-Adressen außerhalb Ihres internen Netzwerk herstellen sollen, können Sie in einem Dashboard ein Wertdiagramm erstellen, das die Messwerte Extern Accepted und External Connected verfolgt. Von Ihrem Dashboard aus können Sie dann die Anzahl der externen Verbindungen für ein bestimmtes Gerät überwachen.

Hinweis: Standardmäßig wird jedes Gerät mit einer RFC1918-IP-Adresse (in einem 10/8-, 172.16/12- oder 192.168/16 CIDR-Block enthalten), das das ExtraHop-System automatisch erkennt, als internes Gerät klassifiziert. Da einige Netzwerkumgebungen IP-Adressen enthalten, die nicht nach RFC1918 stammen, als Teil ihres internen Netzwerk können Sie Geben Sie den Standort einer IP-Adresse an auf der Seite Network Localities.

Die folgenden Schritte zeigen Ihnen, wie Sie ein Wertdiagramm für diese TCP-Metriken erstellen und das Diagramm dann zu einem Dashboard hinzufügen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. klicken **Vermögenswerte** oben auf der Seite.
3. klicken **Geräte** im linken Bereich.
4. Finde ein Gerät und klicken Sie dann auf den Gerätenamen.
5. klicken **TCP** im linken Bereich. Im Diagramm Gesamtzahl der Verbindungen in der oberen linken Ecke zeigen die Metriken Extern Accepted und Extern Connected an, wie viele IP-Adressen außerhalb Ihres internen Netzwerk mit dem Gerät verbunden sind.
6. Klicken Sie auf **Verbindungen insgesamt** Titel des Diagramms.
7. Wählen Sie im Drop-down-Menü **Diagramm erstellen aus...**. Der Metric Explorer wird mit den bereits im Diagramm ausgewählten Gerät- und TCP-Metriken geöffnet.
8. Klicken Sie unten im Metric Explorer auf **Wert** Diagramm.
9. Klicken Sie im linken Bereich im Bereich Metrik auf **x** Symbol , um jede TCP-Metrik zu löschen, die Sie nicht im Diagramm sehen möchten, wie in der folgenden Abbildung dargestellt.



Ihr Dashboard enthält jetzt Metriken, mit denen Sie das Verhältnis aller akzeptierten Verbindungen zu externen akzeptierten Verbindungen sowie das Verhältnis aller initiierten Verbindungen zu extern initiierten Verbindungen verfolgen können.

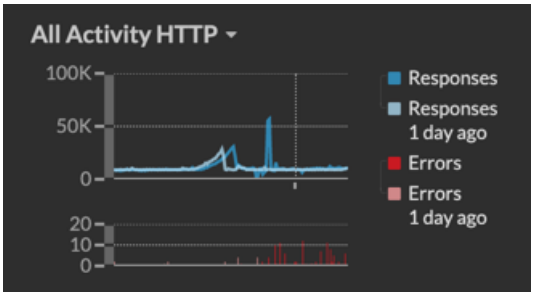
10. Optional: Nehmen Sie mit dem Metric Explorer weitere Änderungen am Diagramm vor.
11. klicken **Zum Dashboard hinzufügen** und füllen Sie eine der folgenden Optionen aus:
    - Wählen Sie den Namen eines vorhandenen Dashboard aus der Liste aus. Die Dashboard-Liste ist von den zuletzt erstellten Dashboards (unten) bis zu den ältesten Dashboards (oben) geordnet.
    - Wählen **Dashboard erstellen**. Geben Sie im Fenster Dashboard-Eigenschaften einen Namen für das neue Dashboard ein und klicken Sie dann auf **Erstellen**.
12. Optional: Nehmen Sie weitere Änderungen am Dashboard-Layout vor.
13. klicken **Layoutmodus verlassen**. Ihr Dashboard ist fertig.

Nächste Schritte
Ein Dashboard teilen

Vergleichen Sie Zeitintervalle, um das Metrik Delta zu ermitteln

Durch den Vergleich von Metrikdaten zwischen zwei Zeitintervallen können Sie den Unterschied oder das Delta in Metrik Daten nebeneinander in demselben Diagramm erkennen. Wenn Sie einen Vergleich erstellen und zu einem anderen Bereich des ExtraHop-Systems navigieren, ist der Vergleich vorübergehend deaktiviert. Wenn Sie zu Ihrer ursprünglichen Seite zurückkehren, ist der von Ihnen gespeicherte Vergleich wieder aktiviert.

1. Suchen Sie ein Diagramm mit den Kennzahlen, die Sie vergleichen möchten.
2. Klicken Sie in der oberen linken Ecke der Navigationsleiste auf das Zeitintervall.
3. In der Zeitintervall Tab, klicken **Vergleiche**.
4. In der Vorheriges Intervall (Vergleich) Wählen Sie im Abschnitt das Zeitintervall aus, das mit dem aktuellen Zeitintervall verglichen werden soll.
5. klicken **Speichern**. Neue Metrikdaten aus dem Vergleichszeitintervall werden in das Originaldiagramm eingefügt.



6. Gehen Sie wie folgt vor, um den Vergleich zu entfernen:
   a) Klicken Sie auf das Zeitintervall.
   b) klicken **Vergleich entfernen**.
   c) klicken **Speichern**.

Hinweis: Dynamische Basislinien werden nicht in einem Diagramm angezeigt, wenn Sie Zeitintervalle vergleichen.

Vermögenswerte

Alle anhand der Daten in Ihrem Netzwerk gesammelten Metrikaktivitäten sind logisch in Abschnitte auf der Seite „Ressourcen“ gruppiert, in denen Sie nach den benötigten Daten navigieren können.

Video: Sehen Sie sich die entsprechende Schulung an: Vermögenswerte

Geräte

Geräte, auch bekannt als Assets und Endpoints, sind Objekte in Ihrem Netzwerk mit einer MAC-Adresse oder IP-Adresse, die vom ExtraHop-System automatisch erkannt und klassifiziert wurden. Ordnen Sie ein beliebiges Gerät einem Diagramm, einer Alarm oder einem Auslöser als Metrikquelle zu. Erfahre mehr über Geräte.

Gerätegruppen

Gerätegruppen sind benutzerdefinierte Gruppen von Geräten, die einem Diagramm, einer Alarm oder einem Auslöser gemeinsam als Metrikquelle zugewiesen werden können. Du kannst eine dynamische Gerätegruppe erstellen das fügt Geräte hinzu, die Ihren angegebenen Kriterien entsprechen, oder Sie können eine statische Gerätegruppe erstellen und fügen Sie Geräte manuell hinzu oder entfernen Sie sie. Das ExtraHop-System enthält auch integrierte dynamische Gerätegruppen nach Rolle und Protokollaktivität, die Sie als Metrikquelle zuweisen können. Klicken Sie auf der Seite Geräte auf einen Rollen- oder Protokoll-Link, um Metriken für eine integrierte Gerätegruppe anzuzeigen.

Dateien

Das Seite „Dateien“ zeigt eine Tabelle mit Dateien an, die mit dem SHA-256-Hashing-Algorithmus gemäß den Filterkriterien gehasht wurden, die aus dem Einstellungen für die Dateianalyse. Metadaten aus Hash-Dateien sind ein wertvolles Tool zur Identifizierung von Malware und Risiken in Ihrem Netzwerk.

Nutzer

Auf der Seite Benutzer werden eine Liste aller aktiven Benutzer in Ihrem Netzwerk sowie der Geräte angezeigt, an denen sich der Benutzer angemeldet hat. Der Benutzername wird aus dem Authentifizierungsprotokoll wie LDAP oder Active Directory extrahiert. Suchen Sie nach Geräten, auf die ein bestimmter Benutzer zugegriffen hat.

Hinweis: Diese Benutzer sind nicht mit Benutzerkonten für das ExtraHop-System verknüpft.

Anwendungen

Anwendungen sind benutzerdefinierte Container, die verteilte Systeme in Ihrem Netzwerk darstellen. Erstellen Sie eine Anwendung, um die gesamte Metrikaktivität im Zusammenhang mit Ihrem Website-Traffic anzuzeigen — Webtransaktionen, DNS-Anfragen und -Antworten sowie Datenbanktransaktionen. Sehen Sie die Häufig gestellte Fragen zu Anwendungen.

Grundlegende Anwendungen, die integrierte Metriken nach Protokollaktivität filtern, können erstellt durch das ExtraHop-System. Komplexe Anwendungen, die benutzerdefinierte Metriken oder Metriken aus Nicht-L7-Verkehr sammeln, müssen durch einen Auslöser erstellt, was JavaScript-Code erfordert. Erfahre mehr über Trigger erstellen.

Netzwerke

Netzwerke sind Standorte und Flussnetzwerke, von denen das ExtraHop-System Daten sammelt und analysiert. Websites enthalten Paket Sensoren und Fluss Sensoren. Klicken Sie auf einen Eintrag, um die

mit einer Standort verknüpften VLANs anzuzeigen, oder klicken Sie auf einen Eintrag, um die mit einem Flussnetz verknüpften Schnittstellen anzuzeigen.

Geräte

Das ExtraHop-System erkennt und klassifiziert automatisch Geräte, auch Endpunkte genannt, die aktiv über Ihr Netzwerk kommunizieren, wie Clients, Server, Router, Load Balancer und Gateways. Jedes Gerät erhält die höchste verfügbare Analyseniveau, basierend auf Ihrer Systemkonfiguration.

Das ExtraHop-System kann Geräte entdecken und verfolgen nach ihrer MAC-Adresse (L2 Discovery) oder nach ihren IP-Adressen (L3 Discovery). Die Aktivierung von L2 Discovery bietet den Vorteil, dass Metriken für ein Gerät auch dann verfolgt werden, wenn die IP-Adresse durch eine DHCP-Anfrage geändert oder neu zugewiesen wird. Wenn L3 Discovery aktiviert ist, ist es wichtig zu wissen, dass Geräte möglicherweise keine Eins-zu-Eins-Beziehung zu den physischen Geräten in Ihrer Umgebung haben. Wenn beispielsweise ein einzelnes physisches Gerät über mehrere aktive Netzwerkschnittstellen verfügt, wird dieses Gerät vom ExtraHop-System als mehrere Geräte identifiziert.

Nachdem ein Gerät erkannt wurde, beginnt das ExtraHop-System mit der Erfassung von Metriken auf der Grundlage der Analyseebene für dieses Gerät konfiguriert. Die Analyseebene bestimmt, welche Arten von Metriken generiert werden und welche Funktionen für die Organisation von Metrikdaten verfügbar sind.

Navigierende Geräte

klicken **Vermögenswerte** aus dem oberen Menü, um Suchoptionen und Diagramme anzuzeigen, die einen Einblick in die aktiven Geräte geben, die während des ausgewählten Zeitintervalls in Ihrem Netzwerk entdeckt wurden:

AI Search Assistant (erfordert Zugriff auf das NDR-Modul)

Ermöglicht es Ihnen suche nach Geräten mit Fragen geschrieben in natürlicher, alltäglicher Sprache. KI-Suchassistent muss vom ExtraHop-Administrator aktiviert werden.

Standard-Suchfeld

Stellt einen Filter bereit, zu dem Kriterien hinzugefügt werden können suche nach bestimmten Geräten. Klicken Sie auf den Filter, um die Suchkriterien zu ändern.

Vorschläge für die Suche

Bietet Suchvorschläge, die die erstellten Suchfilter nutzen.

Aktive Geräte

Zeigt die Gesamtzahl der Geräte an, die vom ExtraHop-System während des ausgewählten Zeitintervalls erkannt wurden. Klicken Sie auf die Zahl, um eine Liste aller erkannten Geräte anzuzeigen. In der Liste der aktiven Geräte können Sie suche nach bestimmten Geräten oder klicken Sie auf einen Gerätenamen, um Gerätedetails auf der Seite „ Geräteübersicht“.

Neue Geräte

Zeigt die Anzahl der Geräte an, die in den letzten fünf Tagen entdeckt wurden. Klicken Sie auf die Nummer, um eine Liste all dieser Geräte anzuzeigen.

Geräte nach Rolle

Zeigt jede Geräterolle und die Anzahl der Geräte an, die jeder Rolle zugewiesen sind, die während des angegebenen Zeitintervalls aktiv ist. Klicken Sie auf eine Geräterolle, um eine integrierte Übersichtsseite für Gerätegruppen anzuzeigen, die Metrikdaten, Peer-IPs und Protokollaktivitäten für diese Gerätegruppe enthält. Sie können auch zusätzliche Filterkriterien hinzufügen und die Gruppe als neue dynamische Gerätegruppe speichern.

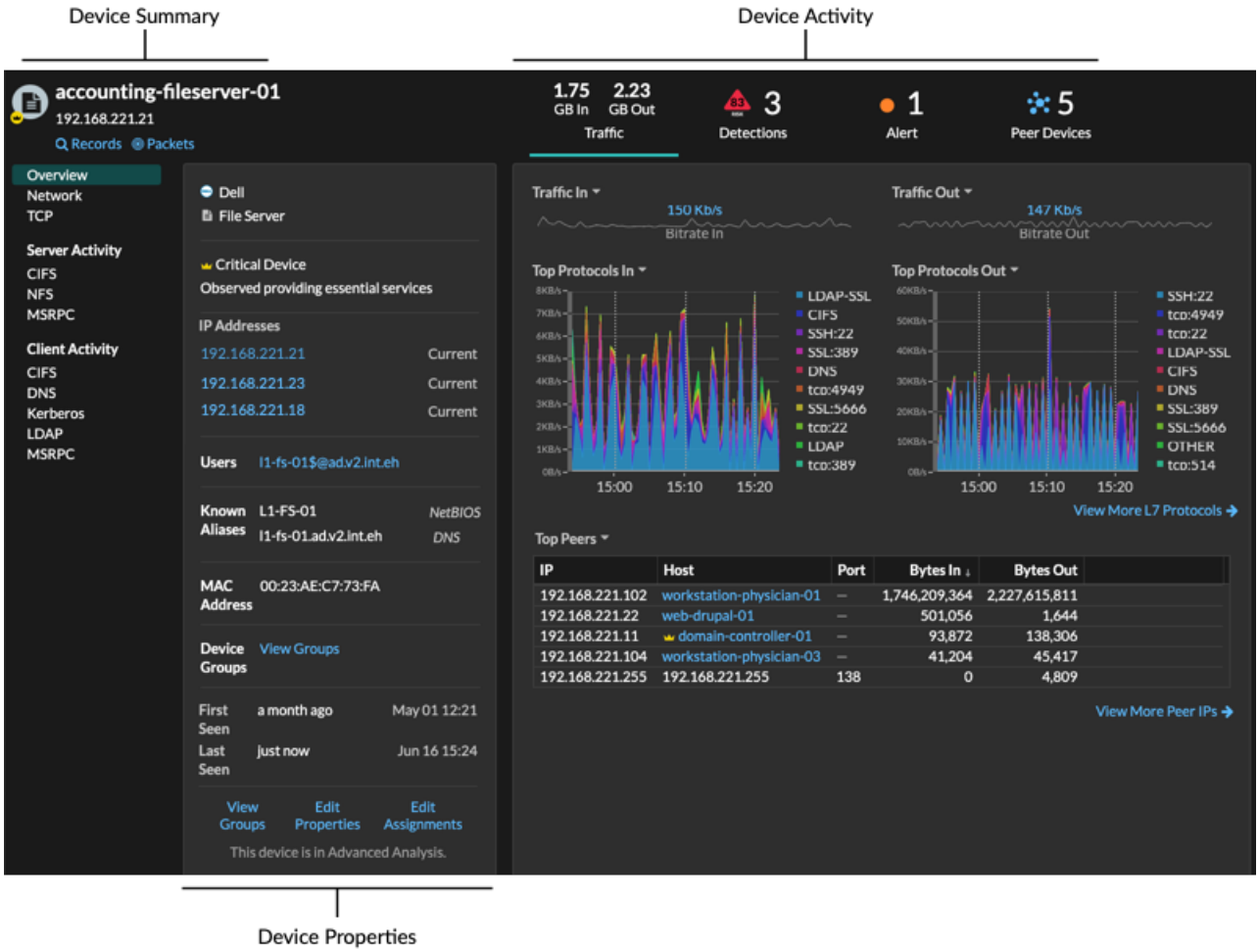
Geräte nach Protokollaktivität

Zeigt eine Liste der Protokollaktivitäten an, die in Ihrem Netzwerk gefunden wurden. Klicken Sie auf einen Protokollnamen oder eine Geräteanzahl, um eine integrierte Übersichtsseite mit bestimmten Metrikdiagrammen zu dieser Protokollaktivität anzuzeigen. Klicken Sie auf eine Aktivitätsdiagramm,

um alle Gerät-zu-Gerät-Verbindungen anzuzeigen. Sie können auch zusätzliche Filterkriterien hinzufügen und die Gruppe als neue dynamische Gerätegruppe speichern.

Seite „Geräteübersicht“

Wenn Sie auf einen Gerätenamen klicken, können Sie alle Informationen, die das ExtraHop-System über das Gerät gefunden hat, auf der Seite Geräteübersicht einsehen. Die Seite „Geräteübersicht“ ist in drei Abschnitte unterteilt: eine Zusammenfassung auf oberster Ebene, einen Eigenschaftenbereich und einen Aktivitätsbereich.



Zusammenfassung des Geräts

Die Geräteübersicht enthält Informationen wie den Gerätenamen, die aktuelle IP - oder MAC-Adresse und die dem Gerät zugewiesene Rolle. Wenn Sie von einem aus betrachten Konsole, der Name der mit dem Gerät verknüpften Standort wird ebenfalls angezeigt.

- Klicken Sie **Rekorde** um eine zu starten Datensatzabfrage das wird von diesem Gerät gefiltert.
- Klicken Sie **Pakete** um eine zu starten Paketabfrage das wird von diesem Gerät gefiltert.

Eigenschaften des Geräts

Der Abschnitt mit den Geräteeigenschaften enthält die folgenden bekannten Attribute und Zuweisungen für das Gerät.

Marke und Modell

Die Marke (oder der Hersteller) des Gerät und das Gerätemodell, falls verfügbar.

Das ExtraHop-System beobachtet den Netzwerkverkehr auf Geräten, um automatisch Marke und Modell zu ermitteln, oder Sie können Manuelles Zuweisen einer neuen Marke und eines neuen Modells.

Rolle des Geräts

Das ExtraHop-System weist automatisch eine zu Geräterolle, z. B. ein Gateway, ein Server, eine Datenbank oder ein Load Balancer, basierend auf der Art des Datenverkehrs, der mit dem Gerät oder dem Gerätemodell verknüpft ist. Sie können manuell eine Geräterolle ändern.

Hochwertiges Gerät

Eine hoher Wert Ikone erscheint, wenn das ExtraHop-System beobachtet hat, dass das Gerät die Authentifizierung oder wichtige Dienste bereitstellt; Sie können auch geben Sie manuell ein Gerät als hoher Wert. Die Risikowerte für Erkennungen auf hoher Wert Geräten werden erhöht.

Software

Das primäre Betriebssystem oder die Software, die auf dem Gerät ausgeführt wird.

Hinweis: CrowdStrike-Integration (nur auf RevealX 360) Sie können auf Links von Geräten klicken, auf denen die CrowdStrike-Software ausgeführt wird, um Gerätedetails in CrowdStrike Falcon anzuzeigen und die Eindämmung von CrowdStrike-Geräten einleiten das sind Teilnehmer an einer Sicherheitserkennung.

IP-Adressen

Eine Liste der IP-Adressen, die zu einem beliebigen Zeitpunkt während des ausgewählten Zeitintervalls auf dem Gerät beobachtet wurden. Wenn L2 Discovery aktiviert ist, werden in der Liste möglicherweise sowohl IPv4- als auch IPv6-Adressen angezeigt, die gleichzeitig auf dem Gerät beobachtet werden, oder in der Liste werden möglicherweise mehrere IP-Adressen angezeigt, die über DHCP-Anfragen zu unterschiedlichen Zeiten zugewiesen wurden. Ein Zeitstempel gibt an, wann die IP-Adresse zuletzt auf dem Gerät beobachtet wurde. Klicken Sie auf eine IP-Adresse um andere Geräte anzuzeigen, auf denen die IP-Adresse gesehen wurde.

Zugeordnete IP-Adressen

Eine Liste von IP-Adressen, normalerweise außerhalb des Netzwerk, die dem Gerät zu einem beliebigen Zeitpunkt während des ausgewählten Zeitintervalls zugeordnet sind. Beispielsweise könnte ein VPN-Client in Ihrem Netzwerk mit einer externen IP-Adresse im öffentlichen Internet verknüpft sein. Ein Zeitstempel gibt an, wann die IP-Adresse zuletzt mit dem Gerät verknüpft wurde. Klicken Sie auf eine zugehörige IP-Adresse um Details wie den geografischen Standort und andere Geräte anzuzeigen, mit denen die IP-Adresse verknüpft wurde.

Eigenschaften der Cloud-Instanz

Die folgenden Cloud-Instanzeigenschaften werden für das Gerät angezeigt, wenn Sie die Eigenschaften über die REST-API konfigurieren:

- Cloud-Konto
- Cloud-Instanztyp
- Virtuelle private Cloud (VPC)
- Subnetz
- Cloud-Instanzname (erscheint in der Eigenschaft Bekannter Alias)
- Beschreibung der Cloud-Instanz (Instanz-Metadaten werden automatisch für Geräte in Flow Analysis angezeigt)

siehe Fügen Sie Cloud-Instanz-Eigenschaften über den ExtraHop API Explorer hinzu für weitere Informationen.

Nutzer

Eine Liste der authentifizierten Benutzer, die am Gerät angemeldet sind. Klicken Sie auf einen Benutzernamen um zur Benutzerseite zu gehen und zu sehen, auf welchen anderen Geräten der Benutzer angemeldet ist.

Bekannte Aliase

Eine Liste von Alternativen Gerätenamen und das Quellprogramm oder Protokoll.

Hinweis: Es werden mehrere DNS-Namen unterstützt.

Schlagworte

Das dem Gerät zugewiesene Tags. Klicken Sie auf einen Tag-Namen, um die anderen Geräte anzuzeigen, denen das Tag zugewiesen ist.

Zuerst und zuletzt gesehen

Die Zeitstempel von dem Zeitpunkt, an dem das Gerät zum ersten Mal entdeckt wurde und wann die Aktivität zuletzt auf dem Gerät beobachtet wurde. NEU erscheint, wenn das Gerät innerhalb der letzten fünf Tage entdeckt wurde

Analyse

Das Ebene der Analyse die dieses Gerät empfängt.

Hier sind einige Möglichkeiten, wie Sie Geräteeigenschaften anzeigen und ändern können:

- Klicken Sie **Gruppen ansehen** um das zu sehen Gerätegruppe Mitgliedschaft für das Gerät.
- Klicken Sie **Eigenschaften bearbeiten** zum Anzeigen oder Ändern von Geräteeigenschaften wie Geräterolle, Gerätegruppenmitgliedschaften oder Geräte-Tags.
- Klicken Sie **Zuweisungen bearbeiten** um welche einzusehen oder zu ändern Warnungen und löst aus sind dem Gerät zugewiesen.

Aktivität des Geräts

Der Abschnitt Geräteaktivität enthält Informationen darüber, wie das Gerät mit anderen Geräten kommuniziert und welche Erkennungen und Warnungen mit dem Gerät verknüpft sind.

- Klicken Sie **Verkehr** um Diagramme für Protokoll- und Peer-Daten anzuzeigen, und dann nach unten bohren zu Metriken in Verkehrskarten.

  Hinweis: Verkehrsdiagramme sind nicht verfügbar, wenn sich die Geräteanalyseebene im Entdeckungsmodus befindet. Um Verkehrskarten für das Gerät zu aktivieren, erhöhen Sie das Gerät auf Fortgeschrittene Analyse oder Standardanalyse.
- Klicken Sie **Erkennungen** um eine Liste der Funde anzuzeigen, und klicken Sie dann auf einen Erkennungsnamen, um Erkennungsdetails anzeigen.
- Klicken Sie **Ähnliche Geräte** um eine Liste von Geräten mit ähnlichem Netzwerkverkehrsverhalten anzuzeigen, das durch maschinelle Lernanalysen beobachtet wurde. Ähnliche Geräte können Ihnen helfen, bei der Suche nach Bedrohungen einen Einblick in das normale Geräteverhalten zu erhalten. Diese Registerkarte wird nur angezeigt, wenn dem Gerät ähnliche Geräte zugeordnet sind.
- (Zugriff auf das NPM-Modul erforderlich.) Klicken Sie **Warnmeldungen** um eine Liste von Warnungen anzuzeigen, und klicken Sie dann auf einen Warnungsnamen, um Warnungsdetails anzeigen. Diese Registerkarte wird nur angezeigt, wenn dem Gerät Warnungen zugeordnet sind.
- Klicken Sie **Peer-Geräte** zu eine Aktivitätsdiagramm, das ist eine visuelle Darstellung der L4-L7-Protokollaktivität zwischen Geräten in Ihrem Netzwerk. Zu modifizieren Sie die Aktivitätsdiagramm mit zusätzlichen Filtern und Schritten klicken Sie auf **Aktivitätskarte öffnen**.

Hinweis: Sie können die Seite „Geräteübersicht“ mit einem Lesezeichen für eine bestimmte Aktivitätsansicht versehen, indem Sie die `tab` URL-Parameter für einen der folgenden Werte:

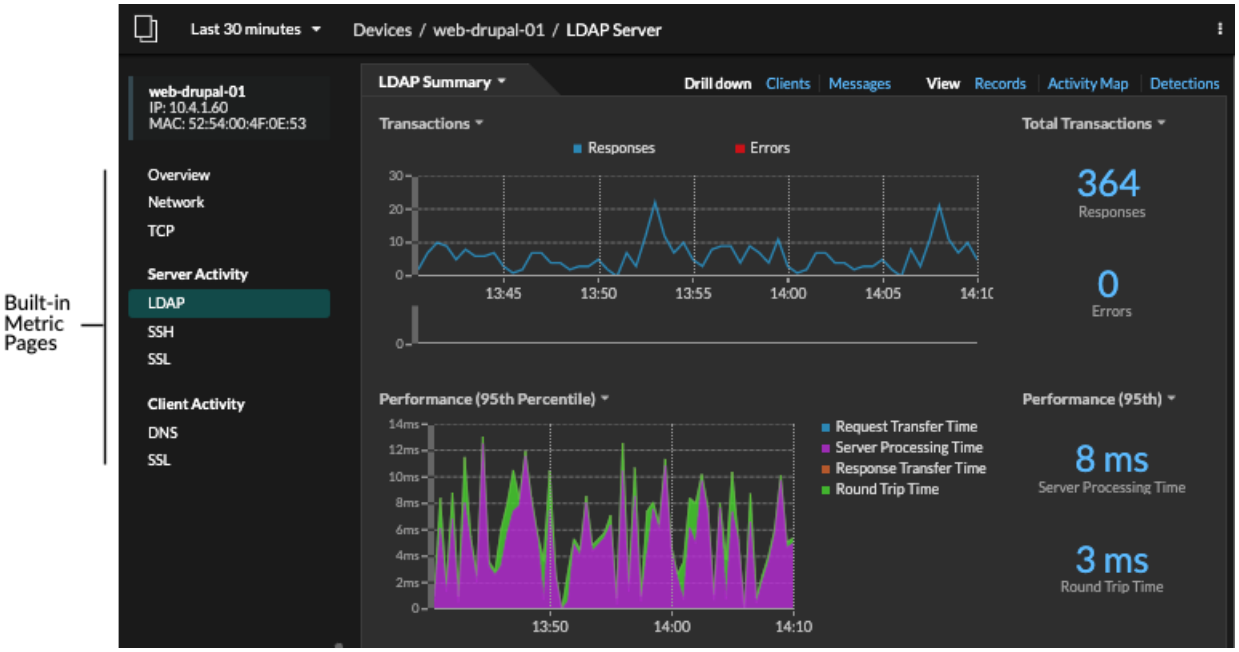
- `tab=traffic`
- `tab=detections`
- `tab=alerts`
- `tab=peers`

Beispielsweise zeigt die folgende URL immer die Erkennungsaktivität für das angegebene Gerät an:

```
https://example-eda/extrahop/#/metrics/devices//0026b94c03810000/
overview/&tab=detections
```

Geräte-Metriken

Metriken sind Echtzeitmessungen Ihres Netzwerkverkehrs, die das ExtraHop-System aus Netzwerk- oder Flussdaten berechnet. Aus dem Geräteverkehr gesammelte Messwerte können in integrierten Diagrammen und Grafiken auf einer Geräteseite angezeigt werden.



Klicken Sie im linken Bereich auf eine integrierte Metrikseite, um die oberste Ebene anzuzeigen Gerätemetriken oder Client und Server Metriken nach Protokoll. Klicken Sie auf ein Diagramm, um Detailseiten mit Metriken aufrufen, die Metrikwerte für einen bestimmten Schlüssel (z. B. eine Client- oder Server-IP-Adresse) anzeigen.

Zusätzlich zu den integrierten Netzwerk- und TCP-Seiten zeigen Geräte integrierte Metrikseiten für zugehörige Cloud-Dienste an, sofern Daten verfügbar sind. Sehen Sie die Referenz zu Protokollmetriken für weitere Informationen darüber, welche Daten auf den integrierten Geräteseiten verfügbar sind.

Das ExtraHop-System bietet Tausende von integrierten Metriken. Hier sind einige Möglichkeiten, wie Sie weitere Einblicke in Ihre Geräte gewinnen können

- Erstellen Sie ein Diagramm um bestimmte Kennzahlen zu visualisieren und das Diagramm in einem Dashboard zu speichern.
- Erstellen Sie eine Aktivitätsdiagramm um die Beziehungen zwischen Peer-Geräten über bestimmte Protokolle hinweg anzuzeigen.
- Schreiben Sie einen Auslöser erstellen benutzerdefinierte Metriken oder erstelle eine Anwendung Container zum Sammeln von Metriken für bestimmte Geräte.

Angaben zur IP-Adresse

Geben Sie eine IP-Adresse in das globale Suchfeld ein oder klicken Sie auf einer Seite mit der Geräteübersicht auf einen Link zur IP-Adresse, um Details zu einer IP-Adresse anzuzeigen.

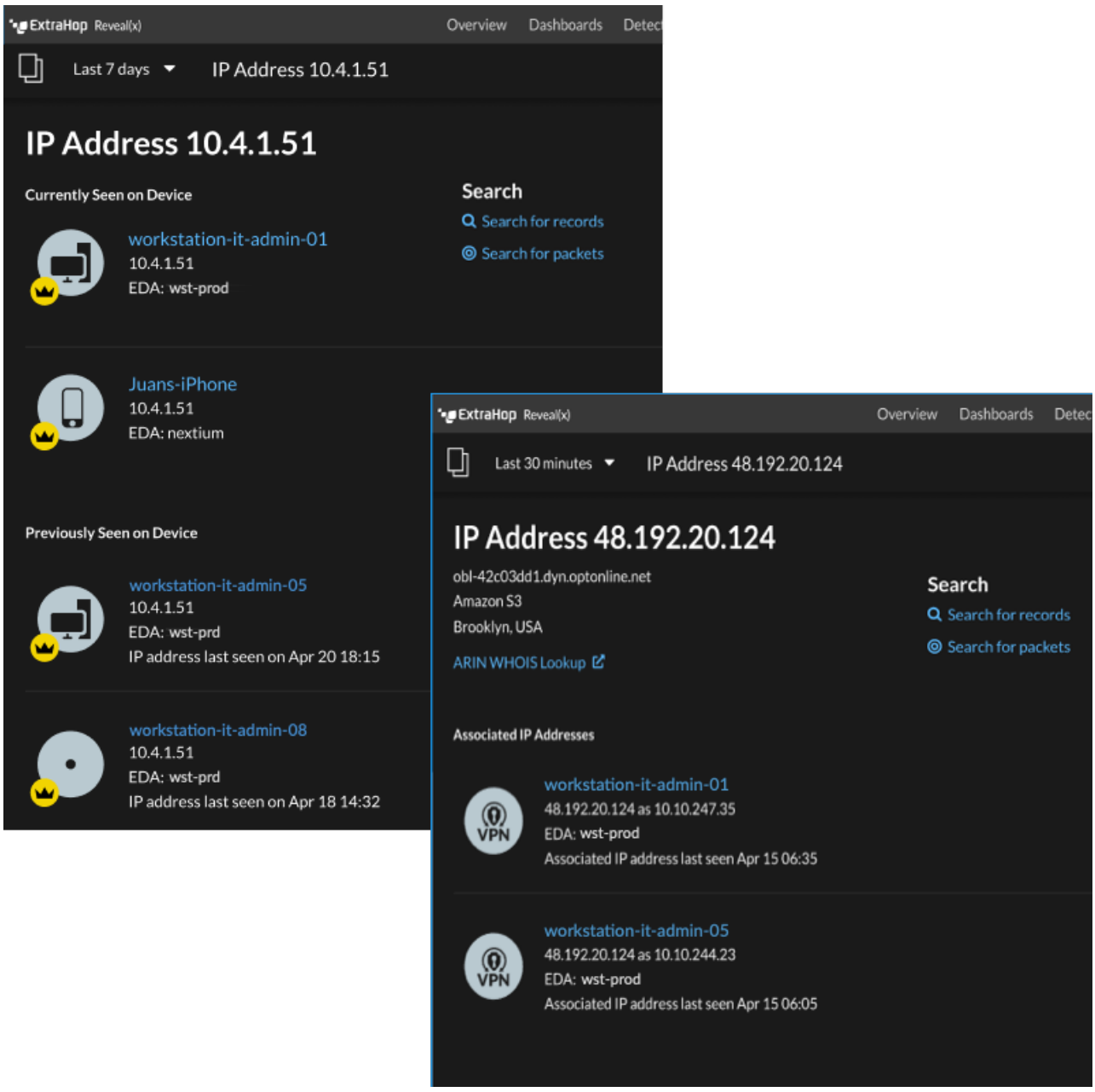
Die folgenden Informationen werden für eine IP-Adresse angezeigt, die auf einem Gerät angezeigt wird:

- Jedes Gerät, auf dem die IP-Adresse derzeit beobachtet wird, unabhängig vom ausgewählten Zeitintervall.
- Jedes Gerät, bei dem die IP-Adresse zuvor innerhalb des ausgewählten Zeitintervalls beobachtet wurde, einschließlich des Zeitstempel, ab dem die IP-Adresse zuletzt auf dem Gerät angezeigt wurde.

Wenn L2 Discovery aktiviert ist, können sowohl IPv4- als auch IPv6-Adressen gleichzeitig auf dem Gerät beobachtet werden, oder dem Gerät können im Laufe der Zeit unterschiedliche IP-Adressen per DHCP zugewiesen werden.

Die folgenden Informationen werden für eine IP-Adresse angezeigt, die einem Gerät zugeordnet ist:

- Die Geolokalisierung der IP-Adresse und Links zur ARIN Whois-Website.
- Jedes Gerät, bei dem die zugehörige IP-Adresse zu einem beliebigen Zeitpunkt während des ausgewählten Zeitintervalls außerhalb des Netzwerk gesehen wurde. Beispielsweise könnte ein VPN-Client in Ihrem Netzwerk mit einer externen IP-Adresse im öffentlichen Internet verknüpft sein.
- Alle Cloud-Dienste, die mit der IP-Adresse verknüpft sind.
- Die IP-Adresse des Gerät, wie sie vom ExtraHop-System in Ihrem Netzwerk gesehen wird.
- Der Zeitstempel, zu dem die zugehörige IP-Adresse zuletzt auf dem Gerät angezeigt wurde.



Hier sind einige Möglichkeiten, wie Sie zusätzliche IP-Adresse und Geräteinformationen anzeigen können:

- Zeigen Sie mit der Maus auf einen Gerätenamen, um die Geräteeigenschaften anzuzeigen.
- Klicken Sie auf einen Gerätenamen, um Sehen Sie sich die Seite mit der Geräteübersicht an.
- Klicken Sie **Suche nach Aufzeichnungen** um eine zu starten Abfrage Datensatz das wird durch die IP gefiltert .

- Klicken Sie **Suche nach Paketen** um eine zu starten Paketabfrage das wird von diesem Gerät gefiltert.

Geräte gruppieren

Sowohl mit benutzerdefinierten Geräten als auch mit Gerätegruppen können Sie Ihre Gerätekennzahlen aggregieren. Benutzerdefinierte Geräte sind vom Benutzer erstellte Geräte, die Metriken auf der Grundlage bestimmter Kriterien sammeln, während Gerätegruppen Metriken für alle angegebenen Geräte in einer Gruppe sammeln. Bei Gerätegruppen können Sie weiterhin Messwerte für jedes einzelne Gerät oder Gruppenmitglied anzeigen. Die Messwerte für ein benutzerdefiniertes Gerät werden wie für ein einzelnes Gerät erfasst und angezeigt — Sie können keine individuellen Gerätemetriken anzeigen.

Sowohl Gerätegruppen als auch benutzerdefinierte Geräte können Metriken basierend auf Ihren angegebenen Kriterien dynamisch aggregieren. Wir empfehlen, zuverlässige Kriterien wie Geräte-IP-Adresse, MAC-Adresse, VLAN, Tag oder Typ auszuwählen. Sie können Geräte zwar anhand ihres Namens auswählen, aber wenn der DNS-Name nicht automatisch erkannt wird, wird das Gerät nicht hinzugefügt.

	Gerätegruppen	Maßgeschneiderte Geräte
Kriterien	Beinhaltet: • Gerätenamen und Aliase • IP-Adresse, MAC-Adresse, Subnetz • Quell- und Zielport • Entdeckungszeit • Kritikalität des Geräts • Rolle „Gerät“ • Protokollaktivität • Externe Verbindungen • Anbieter, Modell, Software • Eigenschaften der Cloud-Instanz • VLAN • Geräte-Tags	• IP-Adresse • Bidirektionaler, eingehender oder ausgehender Datenverkehr • Peer-IP-Adresse • Quellport • Zielport • VLAN
Kosten der Leistung	Vergleichsweise niedrig. Da Gerätegruppen nur Metriken kombinieren, die bereits berechnet wurden, hat dies einen relativ geringen Effekt auf die Erfassung von Metrik. Die Verarbeitung einer hohen Anzahl von Gerätegruppen mit einer großen Anzahl von Geräten und komplexen Kriterien nimmt jedoch mehr Zeit in Anspruch.	Vergleichsweise hoch. Da die Metriken für benutzerdefinierte Geräte auf der Grundlage benutzerdefinierter Kriterien aggregiert werden, erfordert eine große Anzahl benutzerdefinierter Geräte oder benutzerdefinierter Geräte mit extrem breiten Kriterien mehr Verarbeitung. Benutzerdefinierte Geräte erhöhen auch die Anzahl der Systemobjekte, für die Metriken übertragen werden.
Einzelne Gerätekennzahlen anzeigen	Ja	Nein
Bearbeitungssteuerung für Benutzer mit eingeschränktem Schreibzugriff	Ja Nutzer mit eingeschränkte Schreibrechte kann Gerätegruppen erstellen und	Nein

	Gerätegruppen	Maßgeschneiderte Geräte
	bearbeiten. Diese globale Rechterichtlinie muss in den Administrationseinstellungen aktiviert werden.	
Bewährte Verfahren	Erstellen Sie für lokale Geräte, bei denen Sie die Metriken in einem einzigen Diagramm anzeigen und vergleichen möchten. Gerätegruppen können als Metrikquelle festgelegt werden.	Erstellen Sie für Geräte, die sich außerhalb Ihres lokalen Netzwerk befinden, oder für Arten von Datenverkehr, den Sie als eine einzige Quelle organisieren möchten. Beispielsweise möchten Sie möglicherweise alle physischen Schnittstellen auf einem Server als ein einziges benutzerdefiniertes Gerät definieren, um die Messobjekte für diesen Server als Ganzes besser anzeigen zu können.

Maßgeschneiderte Geräte

Mit benutzerdefinierten Geräten können Sie Messwerte für Geräte erfassen, die sich außerhalb Ihres lokalen Netzwerk befinden oder wenn Sie eine Gruppe von Geräten haben, für die Sie Metriken als einzelnes Gerät aggregieren möchten. Bei diesen Geräten kann es sich sogar um unterschiedliche physische Schnittstellen handeln, die sich auf demselben Gerät befinden. Wenn Sie die Metriken für diese Schnittstellen aggregieren, können Sie leichter nachvollziehen, wie stark Ihre physischen Ressourcen insgesamt belastet sind, und nicht nach Schnittstellen.

Du könntest ein benutzerdefiniertes Gerät erstellen um einzelne Geräte außerhalb Ihrer lokalen Broadcast-Domain zu verfolgen oder Metriken über mehrere bekannte IP-Adressen oder CIDR-Blöcke von einem Remote-Standort oder Cloud-Dienst zu sammeln. Du kannst Erfassung von Remote-Site-Metriken für benutzerdefinierte Geräte um zu erfahren, wie Dienste an entfernten Standorten genutzt werden, und um einen Einblick in den Verkehr zwischen entfernten Standorten und einem Rechenzentrum zu erhalten. Sehen Sie die Referenz zu Protokollmetriken für eine vollständige Liste der Metriken und Beschreibungen von Remote-Standorten.

Nachdem Sie ein benutzerdefiniertes Gerät erstellt haben, werden alle mit den IP-Adressen und Ports verknüpften Metriken in einem einzigen Gerät zusammengefasst, das L2-L7-Metriken erfasst. Ein einzelnes benutzerdefiniertes Gerät zählt als ein Gerät für Ihre lizenzierte Kapazität für Erweiterte Analyse oder Standardanalyse, was es Ihnen ermöglicht füge ein benutzerdefiniertes Gerät zur Beobachtungsliste. Alle Auslöser oder Warnungen werden dem benutzerdefinierten Gerät ebenfalls als einzelnes Gerät zugewiesen.

Benutzerdefinierte Geräte aggregieren zwar Metriken auf der Grundlage ihrer definierten Kriterien, die Metrikberechnungen werden jedoch nicht so behandelt wie bei erkannten Geräten. Beispielsweise könnten Sie einem benutzerdefinierten Gerät, das Datensätze an einen Recordstore überträgt, einen Auslöser zugewiesen haben. Das benutzerdefinierte Gerät wird jedoch in keinem Transaktionsdatensatz als Client oder Server angezeigt. Das ExtraHop-System füllt diese Attribute mit dem Gerät, das der Konversation auf den Wire-Daten entspricht.

Benutzerdefinierte Geräte können die Gesamtsystemleistung beeinträchtigen, daher sollten Sie die folgenden Konfigurationen vermeiden:

- Vermeiden Sie es, mehrere benutzerdefinierte Geräte für dieselben IP-Adressen oder Ports zu erstellen. Benutzerdefinierte Geräte , die mit sich überschneidenden Kriterien konfiguriert sind, können die Systemleistung beeinträchtigen.
- Vermeiden Sie es, ein benutzerdefiniertes Gerät für eine Vielzahl von IP-Adressen oder Ports zu erstellen, da dies die Systemleistung beeinträchtigen könnte.

Wenn eine große Anzahl benutzerdefinierter Geräte die Systemleistung beeinträchtigt, können Sie ein benutzerdefiniertes Gerät löschen oder deaktivieren. Die eindeutige Discovery-ID für das benutzerdefinierte Gerät verbleibt immer im System. siehe Erstellen Sie ein benutzerdefiniertes Gerät zur Überwachung des Datenverkehrs in entfernten Büros um sich mit kundenspezifischen Geräten vertraut zu machen.

Gerätegruppen

Eine Gerätegruppe ist eine benutzerdefinierte Sammlung, mit der Sie Messwerte auf mehreren Geräten verfolgen können, die in der Regel nach gemeinsamen Attributen wie Protokollaktivitäten gruppiert sind.

Du kannst eine statische Gerätegruppe erstellen das erfordert, dass Sie ein Gerät manuell zur Gruppe hinzufügen oder daraus entfernen. Oder du kannst eine dynamische Gerätegruppe erstellen das beinhaltet Kriterien, die bestimmen, welche Geräte automatisch in die Gruppe aufgenommen werden. Zum Beispiel können Sie Erstellen Sie eine dynamische Gerätegruppe auf der Grundlage der Geräteerkennungszeit das fügt Geräte hinzu , die während eines bestimmten Zeitintervalls erkannt wurden.

Standardmäßig enthält die Seite „Gerätegruppe“ die folgenden dynamischen Gerätegruppen, die Sie überschreiben oder löschen können:

Neue Geräte (letzte 24 Stunden)

Beinhaltet Assets und Endpunkte, die das ExtraHop-System in den letzten 24 Stunden zum ersten Mal gesehen hat.

Neue Geräte (letzte 7 Tage)

Beinhaltet Assets und Endpunkte, die das ExtraHop-System in den letzten 7 Tagen zum ersten Mal gesehen hat.

Das ExtraHop-System umfasst auch integrierte dynamische Gerätegruppen nach Rolle und Protokoll. Sie können integrierte Gerätegruppen als Metrikquelle für Objekte wie Diagramme, Warnungen, Auslöser und Aktivitätskarten zuweisen. Sie können eine integrierte Gerätegruppe nicht überschreiben oder löschen, aber Sie können Filterkriterien hinzufügen und sie als neue Gerätegruppe speichern.

Klicken Sie auf der Seite Geräte auf eine Geräteanzahl für eine Rolle oder ein Protokoll, z. B. Domänencontroller oder SMB-Clients, um die Seite mit der Gerätegruppenübersicht anzuzeigen. Wenn Sie oben auf der Seite auf den Filter klicken, können Sie zusätzliche Kriterien hinzufügen und die Seitendaten bei Bedarf aktualisieren, anstatt eine Gerätegruppe erstellen zu müssen.

Das Erfassen von Messwerten mit Gerätegruppen hat keine Auswirkungen auf die Leistung. Wir empfehlen Ihnen jedoch, priorisieren Sie diese Gruppen weil sie wichtig sind, um sicherzustellen, dass die richtigen Geräte ein Höchstmaß an Analyse erhalten.

Gerätegruppen sind eine gute Wahl, wenn Sie Geräte haben, die Sie gemeinsam als Quelle verwenden möchten. Sie könnten beispielsweise Metriken für alle Ihre Produktionswebserver mit hoher Priorität in einem Dashboard sammeln und anzeigen.

Indem Sie eine Gerätegruppe erstellen, können Sie all diese Geräte als eine einzige Metrikquelle verwalten, anstatt sie als einzelne Quellen zu Ihren Diagrammen hinzuzufügen. Beachten Sie jedoch, dass alle zugewiesenen Auslöser oder Warnungen jedem Gruppenmitglied (oder jedem einzelnen Gerät) zugewiesen werden.

Gerätenamen und Rollen

Nachdem ein Gerät erkannt wurde, verfolgt das ExtraHop-System den gesamten mit dem Gerät verbundenen Datenverkehr, um den Gerätenamen und die Rolle zu ermitteln.

Gerätenamen

Das ExtraHop-System erkennt Gerätenamen durch passive Überwachung von Benennungsprotokollen wie DNS, DHCP, NETBIOS und Cisco Discovery Protocol (CDP).

Wenn ein Name nicht über ein Benennungsprotokoll ermittelt wird, wird der Standardname aus Geräteattributen wie MAC-Adressen und IP-Adressen abgeleitet. Für einige Geräte, die auf Fluss entdeckt wurden Sensoren, weist das ExtraHop-System Namen basierend auf der Rolle des Gerät zu, z. B. Internet Gateway oder Amazon DNS Server. Du kannst auch einen benutzerdefinierten Namen erstellen oder einen Cloud-Instanznamen festlegen für ein Gerät.

Ein Gerät kann anhand mehrerer Namen identifiziert werden, die auf der Seite Geräteübersicht als Bekannte Aliase angezeigt werden. Wenn ein Gerät mehrere Namen hat, Die Reihenfolge der Anzeigepriorität ist in den Administrationseinstellungen festgelegt. Sie können nach einem beliebigen Namen suchen, um finde ein Gerät.

Hinweis Benutzerdefinierte Namen werden nicht zwischen verbundenen ExtraHop-Systemen synchronisiert. Beispielsweise ist ein für einen Sensor erstellter benutzerdefinierter Name nicht über eine verbundene Konsole verfügbar.

Wenn ein Gerätename keinen Hostnamen enthält, hat das ExtraHop-System noch keinen mit diesem Gerät verbundenen Verkehr mit dem Namensprotokoll beobachtet. Das ExtraHop-System führt keine DNS-Suchen nach Gerätenamen durch.

Geräterollen

Basierend auf der Art des Datenverkehrs, der mit dem Gerät oder dem Gerätemodell verknüpft ist, weist das ExtraHop-System dem Gerät automatisch eine Rolle zu, z. B. ein Gateway, einen Server, eine Datenbank oder einen Load Balancer. Die Rolle Andere wird Geräten zugewiesen, die nicht identifiziert werden können.

Einem Gerät kann jeweils nur eine Rolle zugewiesen werden. Sie können manuell eine Geräterolle ändern, oder das ExtraHop-System weist möglicherweise eine andere Rolle zu, wenn sich der beobachtete Verkehr und das Verhalten ändern. Wenn beispielsweise ein PC zu einem Server umfunktioniert wurde, können Sie die Rolle sofort ändern, oder die Änderung kann im Laufe der Zeit beobachtet werden und die Rolle wird vom System aktualisiert.

Das ExtraHop-System identifiziert die folgenden Rollen:

Ikone	Rolle	Beschreibung
	Benutzerdefiniertes Gerät	Ein vom Benutzer erstelltes Gerät, das Metriken auf der Grundlage bestimmter Kriterien erfasst. Das ExtraHop-System weist diese Rolle automatisch zu, wenn Sie ein benutzerdefiniertes Gerät erstellen. Sie können einem Gerät die benutzerdefinierte Rolle nicht manuell zuweisen.
	Angriffssimulator	Ein Gerät, auf dem eine Software zur Breach- und Angriffssimulation (BAS) ausgeführt wird, um Angriffe in einem Netzwerk zu simulieren.
	Datenbank	Ein Gerät, das hauptsächlich eine Datenbankinstanz hostet.

Ikone	Rolle	Beschreibung
	DHCP-Server	Ein Gerät, das hauptsächlich DHCP-Serveraktivitäten verarbeitet.
	DNS-Server	Ein Gerät, das hauptsächlich DNS-Serveraktivitäten verarbeitet.
	Domänencontroller	Ein Gerät, das als Domänencontroller für Kerberos-, SMB- und MSRPC-Serveraktivitäten fungiert.
	Dateiserver	Ein Gerät, das auf Lese- und Schreibanforderungen für Dateien über NFS - und SMB-Protokolle reagiert.
	Brandmauer	Ein Gerät, das den eingehenden und ausgehenden Netzwerkverkehr überwacht und den Verkehr gemäß den Sicherheitsregeln blockiert. Das ExtraHop-System weist diese Rolle Geräten nicht automatisch zu.
	Tor	Ein Gerät, das als Router oder Gateway fungiert. Das ExtraHop-System sucht bei der Identifizierung von Gateways nach Geräten, die einer großen Anzahl eindeutiger IP-Adressen zugeordnet sind (über einem bestimmten Schwellenwert). Zu den Gateway-Gerätenamen gehört der Routername wie Cisco B1B500. Im Gegensatz zu anderen L2-Elterngeräte , du kannst ein Gateway-Gerät zur Beobachtungsliste hinzufügen für erweiterte Analysen.

Ikone	Rolle	Beschreibung
	IP-Kamera	Ein Gerät, das Bild- und Videodaten über das Netzwerk sendet. Das ExtraHop-System weist diese Rolle basierend auf dem Gerätemodell zu.
	Load Balancer	Ein Gerät, das als Reverse-Proxy für die Verteilung des Datenverkehrs auf mehrere Server fungiert.
	Medizinisches Gerät	Ein Gerät, das für medizinische Bedürfnisse und medizinische Umgebungen entwickelt wurde. Das ExtraHop-System kann diese Rolle zuweisen, wenn es sich bei einem Gerät um eine bekannte medizinische Marke und ein bekanntes medizinisches Modell handelt oder wenn das Gerät DICOM-Verkehr verarbeitet.
	Mobiles Gerät	Ein Gerät, auf dem ein mobiles Betriebssystem wie iOS oder Android installiert ist.
	NAT-Gateway	Ein Gerät, das als Network Address Translation (NAT) - Gateway fungiert. Das ExtraHop-System kann diese Rolle zuweisen, wenn ein Gerät mit vier oder mehr Betriebssystem-Fingerabdruckfamilien oder mit vier oder mehr Hardware- oder Herstellermarken und -modellen verknüpft ist. Nachdem einem Gerät diese Rolle zugewiesen wurde, werden die Geräteeigenschaften für Software, Hardwaremarke und -modell sowie authentifizierte Benutzer für das Gerät nicht mehr angezeigt.
	PC	Ein Gerät wie ein Laptop, ein Desktop, eine Windows-VM oder ein macOS-Gerät, das den DNS-, HTTP- und TLS-Client-Verkehr verarbeitet.

Ikone	Rolle	Beschreibung
	Drucker	Ein Gerät, mit dem Benutzer Text und Grafiken von anderen angeschlossenen Geräten drucken können. Das ExtraHop-System weist diese Rolle auf der Grundlage des Gerätemodells oder des über mDNS (Multicast-DNS) beobachteten Datenverkehrs zu.
	VoIP-Telefon	Ein Gerät, das Voice over IP (VoIP) -Telefonanrufe verwaltet.
	VPN-Client	Ein internes Gerät, das mit einer Remote-IP-Adresse kommuniziert. Wenn VPN-Client-Erkennung ist aktiviert, das ExtraHop-System weist diese Rolle automatisch internen Geräten zu, die über ein VPN-Gateway mit Remote-IP-Adressen kommunizieren. Sie können einem Gerät die VPN-Client-Rolle nicht manuell zuweisen.
	VPN-Gateway	Ein Gerät, das zwei oder mehr VPN-Geräte oder Netzwerke miteinander verbindet , um Remoteverbindungen zu überbrücken. Das ExtraHop-System weist diese Rolle Geräten mit einer großen Anzahl externer VPN-Peers zu, wenn die automatische Klassifizierung für diese Rolle in der laufenden Konfigurationsdatei aktiviert ist.
	Schwachstellen-Scanner	Ein Gerät, auf dem Schwachstellen-Scanner-Programme ausgeführt werden.
	Web-Proxyserver	Ein Gerät, das HTTP-Anfragen zwischen einem Gerät und einem anderen Server verarbeitet.

Ikone	Rolle	Beschreibung
	Webserver	Ein Gerät, das hauptsächlich Webressourcen hostet und auf HTTP-Anfragen reagiert.
	Wi-Fi-Zugangspunkt	Ein Gerät, das ein drahtloses lokales Netzwerk erstellt und ein drahtloses Netzwerksignal an einen bestimmten Bereich projiziert. Das ExtraHop-System weist diese Rolle basierend auf dem Gerätemodell zu.

Finde ein Gerät

Das ExtraHop-System erkennt automatisch Geräte wie Clients, Server, Router, Load Balancer und Gateways, die aktiv über das Kabel mit anderen Geräten kommunizieren. Sie können auf dem System nach einem bestimmten Gerät suchen und dann die Verkehrs- und Protokollmetriken auf einer Protokollseite anzeigen.

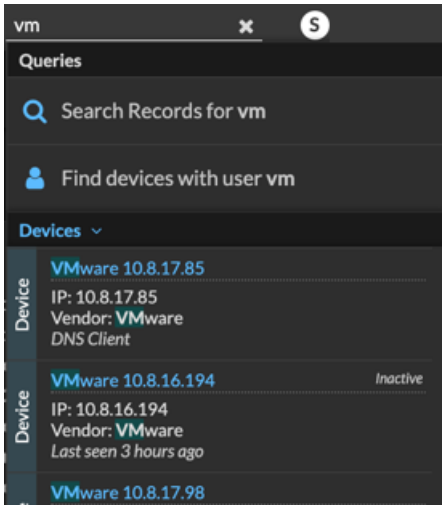
Es gibt mehrere Möglichkeiten, nach einem Gerät zu suchen:

- Finden Sie Geräte über eine globale Suche
- Geräte anhand von Details finden
- Finden Sie Geräte mit AI Search Assistant
- Finden Sie Geräte mit Suchvorschlägen
- Geräte anhand der Erkennungsaktivität finden
- Geräte anhand der Protokollaktivität finden
- Finden Sie Geräte, auf die ein bestimmter Benutzer zugegriffen hat
- Finden Sie Peer-Geräte

Finden Sie Geräte über eine globale Suche

Sie können über das globale Suchfeld oben auf der Seite nach Geräten suchen. Die globale Suche vergleicht einen Suchbegriff mit mehreren Geräteeigenschaften wie Hostname, IP-Adresse, bekanntem Alias, Anbieter, Tag, Beschreibung und Gerätegruppe. Wenn Sie beispielsweise nach dem Begriff suchen `vm`, in den Suchergebnissen werden möglicherweise Geräte angezeigt, die Folgendes enthalten `vm` im Gerätenamen, Gerätehersteller oder Geräte-Tag.

1. Geben Sie einen Suchbegriff in das globale Suchfeld oben auf der Seite ein.
2. Klicken Sie **Beliebiger Typ** und wählen Sie dann **Geräte**.
   Die Suchergebnisse werden in einer Liste unter dem Suchfeld angezeigt. Klicken Sie **Mehr Ergebnisse** um durch die Liste zu blättern.



Passende Geräte, die während des angegebenen Zeitintervalls keine Aktivität hatten, haben die Bezeichnung Inaktiv.

Hinweis: Geräte, die länger als 90 Tage inaktiv sind, werden von den globalen Suchergebnissen ausgeschlossen. Sie können jedoch sofort schließt alle Geräte aus, die seit weniger als 90 Tagen inaktiv waren über die Administrationseinstellungen.

3. Klicken Sie auf einen Gerätenamen, um das zu öffnen Seite „ Geräteübersicht“ und Geräteeigenschaften und Messwerte anzeigen.

Geräte anhand von Details finden

Sie können anhand von Informationen, die über das Kabel beobachtet wurden, wie IP-Adresse, MAC-Adresse, Hostname oder Protokollaktivität, nach Geräten suchen. Sie können auch anhand benutzerdefinierter Informationen wie Geräte-Tags nach Geräten suchen.

Mit dem Dreifeld-Suchfilter können Sie nach mehreren Kategorien gleichzeitig suchen. Sie können beispielsweise Filter für Gerätename, IP-Adresse und Rolle hinzufügen, um Ergebnisse für Geräte anzuzeigen, die alle angegebenen Kriterien erfüllen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Vermögenswerte** und klicken Sie dann auf **Aktive Geräte** Diagramm.
3. Optional: Falls angezeigt, klicken Sie auf **Standardsuche**.
4. Klicken Sie im Dreifeld-Filter auf **Name** und wählen Sie eine der folgenden Kategorien aus:

Option	Description
Name	Filtert Geräte nach dem erkannten Gerätenamen. Ein ermittelter Gerätename kann beispielsweise die IP-Adresse oder den Hostnamen enthalten.
MAC-Adresse	Filtert Geräte nach der MAC-Adresse des Gerät.
IP Adresse	Filtert Geräte nach IP-Adresse in den Blockformaten IPv4, IPv6 oder CIDR.
Standort	Filtert Geräte, die einer verbundenen Standort zugeordnet sind. Nur für die Konsole.
Zeit für Entdeckungsreisen	Filtert Geräte, die vom ExtraHop-System innerhalb des angegebenen Zeitintervalls

Option	Description
	automatisch erkannt werden. Weitere Informationen finden Sie unter Erstellen Sie eine Gerätegruppe basierend auf der Erkennungszeit.
Analyseebene	Filtert Geräte nach Analyseebene, die bestimmt, welche Daten und Metriken für ein Gerät erfasst werden. Sie können keine dynamische Gerätegruppe für Geräte erstellen, die nach Analyseebene gefiltert sind.
Modell	Filtert Geräte nach Marke, Familie oder Modellname. Die Marke steht für den Hersteller des Gerät. Eine Familie steht für eine Gruppierung, z. B. eine Produktlinie. Die folgenden Tipps können Ihnen helfen, das gewünschte Gerätemodell zu finden: • Sie können aus einer Liste von Marken auswählen, die in Ihrem ExtraHop-System gefunden wurden, und dann auf den Filter klicken, um die Ergebnisse zu verfeinern. • Sie können Hovertips neben Marken und Produktfamilien anzeigen, um zu sehen, wie viele Geräte und passende Modelle gefunden wurden. • Sie können eine Marke oder eine Familie auswählen, um alle Geräte in dieser Gruppe zu finden, unabhängig vom Modell.
Aktivität	Filtert Geräte nach Protokollaktivität, die dem Gerät zugeordnet ist. Wenn Sie beispielsweise HTTP-Server auswählen, werden Geräte mit HTTP-Server-Metriken und jedes andere Gerät zurückgegeben, dessen Geräterolle auf HTTP-Server festgelegt ist. Filtert auch Geräte, die eine externe Verbindung akzeptiert oder initiiert haben, sodass Sie feststellen können, ob Geräte verdächtige Aktivitäten ausführen.
Cloud-Konto	Filtert Geräte nach dem Cloud-Dienstkonto, das dem Gerät zugeordnet ist.
Cloud-Instanz-ID	Filtert Geräte nach der Cloud-Instanz-ID, die dem Gerät zugeordnet ist.
Cloud-Instanztyp	Filtert Geräte nach dem Cloud-Instanztyp, der dem Gerät zugeordnet ist.
SHA-256-Datei-Hash	Filtert Geräte, auf denen Dateien beobachtet wurden, die mit dem SHA-256-Hashing-Algorithmus gehasht wurden. Sie können eine Tabelle mit Hash-Dateien auf der Seite „Dateien“.

Option	Description
Hoher Wert	Filtert Geräte, die als hoher Wert eingestuft werden, weil sie Authentifizierungsdienste bereitstellen, wichtige Dienste in Ihrem Netzwerk unterstützen oder die vom Benutzer als hochwertig eingestuft wurden.
Derzeit aktiv	Filtert Geräte nach Aktivitäten, die in den letzten 30 Minuten auf einem Gerät beobachtet wurden.
Netzwerk-Lokalitätstyp	Filtert Geräte nach allen internen oder externen Netzwerkstandorten.
Name der Netzwerklokalität	Filtert Geräte nach dem Namen der Netzwerklokalität.
Rolle	Filtert Geräte nach der zugewiesenen Geräterolle wie Gateway, Firewall, Load Balancer und DNS-Server.
Software	Filtert Geräte nach der auf dem Gerät erkannten Betriebssystemsoftware.
Art der Software	Filtert Geräte nach der Art der auf dem Gerät beobachteten Software, z. B. Angriffssimulator, Fernzugriff oder Datenbankserver.
Subnetz	Filtert Geräte nach dem Subnetz, das dem Gerät zugeordnet ist.
Schlagwort	Filtert Geräte nach benutzerdefinierten Geräte-Tags.
Verkäufer	Filtert Geräte nach dem Namen des Geräteherstellers, der durch die OUI-Suche (Organizationally Unique Identifier) ermittelt wurde.
Virtuelle private Cloud	Filtert Geräte nach der VPC, die dem Gerät zugeordnet ist.
VLAN	Filtert Geräte nach dem Geräte-VLAN-Tag. VLAN-Informationen werden aus VLAN-Tags extrahiert, wenn der Datenverkehrsspiegelungsprozess sie auf dem Spiegelport beibehält. Nur verfügbar, wenn `devices_accross_vlans` Einstellung ist gesetzt auf `False` in der laufenden Konfigurationsdatei.
CDP-Name	Filtert Geräte nach dem CDP-Namen, der dem Gerät zugewiesen ist.
Name der Cloud-Instanz	Filtert Geräte nach dem Cloud-Instanznamen, der dem Gerät zugewiesen ist.
Benutzerdefinierter Name	Filtert Geräte nach dem benutzerdefinierten Namen, der dem Gerät zugewiesen wurde.
DHCP-Name	Filtert Geräte nach dem DHCP-Namen, der dem Gerät zugewiesen ist.

Option	Description
DNS-Name	Filtert Geräte nach einem beliebigen DNS-Namen, der dem Gerät zugewiesen ist.
NetBIOS-Name	Filtert Geräte nach dem NetBIOS-Namen, der dem Gerät zugewiesen ist.
Erkennungsaktivität	Filtert Geräte mit Erkennungsaktivität wo das Gerät ein Teilnehmer war. Aktiviert zusätzliche Kriterien wie Kategorie, Risikoscore und MITRE-Technik. **Hinweis** Sie können keine Gerätegruppe erstellen, die diese Kriterienoption enthält.

5. Wählen Sie einen der folgenden Operatoren aus. Die verfügbaren Operatoren hängen von der ausgewählten Kategorie ab:

Option	Description
=	Filtert Geräte, die exakt dem Suchfeld für die ausgewählte Kategorie entsprechen.
≈	Filtert Geräte, die nicht genau dem Suchfeld entsprechen.
≈	Filtert Geräte, die den Wert des Suchfelds für die ausgewählte Kategorie enthalten.
≈/	Filtert Geräte, die den Wert des Suchfelds für die ausgewählte Kategorie ausschließen.
beginnt mit	Filtert Geräte, die mit dem Wert des Suchfeldes für die ausgewählte Kategorie beginnen.
existiert	Filtert Geräte, die einen Wert für die ausgewählte Kategorie haben.
existiert nicht	Filtert Geräte, die keinen Wert für die ausgewählte Kategorie haben.
Spiel	Filtert Geräte, die den Wert des Suchfelds für die ausgewählte Kategorie enthalten.
und	Filtert Geräte, die den in zwei oder mehr Suchfeldern angegebenen Bedingungen entsprechen.
oder	Filtert Geräte, die mindestens eine in zwei oder mehr Suchfeldern angegebene Bedingung erfüllen.
nicht	Filtert Geräte, die die in einem Suchfeld angegebenen Bedingungen nicht erfüllen.

6. Geben Sie im Suchfeld die Zeichenfolge ein, die abgeglichen werden soll, oder wählen Sie einen Wert aus der Dropdownliste aus. Der Eingabetyp basiert auf der ausgewählten Kategorie.

   Wenn Sie beispielsweise Geräte anhand des Namens suchen möchten, geben Sie die Zeichenfolge, die abgeglichen werden soll, in das Suchfeld Feld. Wenn Sie Geräte anhand der Rolle suchen möchten, wählen Sie diese aus der Dropdownliste der Rollen aus.

   Hinweis Abhängig von der ausgewählten Kategorie können Sie im Textfeld auf das Regex-Symbol klicken, um den Abgleich per regulärem Ausdruck zu aktivieren.

7. Klicken Sie **Filter hinzufügen**.
   Die Geräteliste wird nach den angegebenen Kriterien gefiltert.

Nächste Schritte

- Klicken Sie auf einen Gerätenamen, um Geräteeigenschaften und Messwerte auf der Seite „ Geräteübersicht“.
- Klicken Sie **Dynamische Gruppe erstellen** von der oberen rechten Ecke bis eine dynamische Gerätegruppe erstellen basierend auf den Filterkriterien.
- Klicken Sie auf das Befehlsmenü ⋮ und wählen Sie dann PDF oder CSV, um die Geräteliste in eine Datei zu exportieren.

Finden Sie Geräte mit AI Search Assistant

Mit dem AI Search Assistant können Sie nach Geräten suchen, deren Fragen in natürlicher, alltäglicher Sprache verfasst sind. So können Sie im Vergleich zur Erstellung einer Standard-Suchanfrage mit denselben Kriterien schnell komplexe Abfragen erstellen.

Wenn Sie beispielsweise „Welche Geräte haben HTTP-Verkehr mit TLS v1.0?“ eingeben , die folgende AI Search Assistant-Abfrage wird angezeigt:

```
(Detection Activity where  Device Role = As Participant and  Type =
 Deprecated SSL/TLS Versions )
```

Hier sind einige Dinge, die Sie bei der Suche nach Geräten mit AI Search Assistant beachten sollten:

- Eingabeaufforderungen sind demselben zugeordnet Filterkriterien für Gerät die Sie beim Erstellen einer Standardsuche angeben. Das ExtraHop-System ist möglicherweise nicht in der Lage, eine Abfrage zu verarbeiten, die Anfragen nach Geräteinformationen enthält, die außerhalb der Kriterien liegen.
- Die Eingabeaufforderungen können absolute und relative Zeitbereiche enthalten, z. B. „Welches meiner Geräte war diese Woche an blockierten Datenübertragungen beteiligt?“. Das aktuelle Jahr wird verwendet, wenn ein Jahr nicht im Datum enthalten ist.
- Die Eingabeaufforderungen sollten so klar und präzise wie möglich sein. Wir empfehlen Ihnen, einige Variationen zu schreiben, um Ihre Ergebnisse zu maximieren.
- Das ExtraHop-System kann Benutzeranweisungen zur Produktverbesserung speichern. Wir empfehlen, dass Sie in Ihren Eingabeaufforderungen keine urheberrechtlich geschützten oder vertraulichen Daten angeben.
- Sie können die Abfragefilterkriterien bearbeiten, um die Suchergebnisse zu verfeinern.

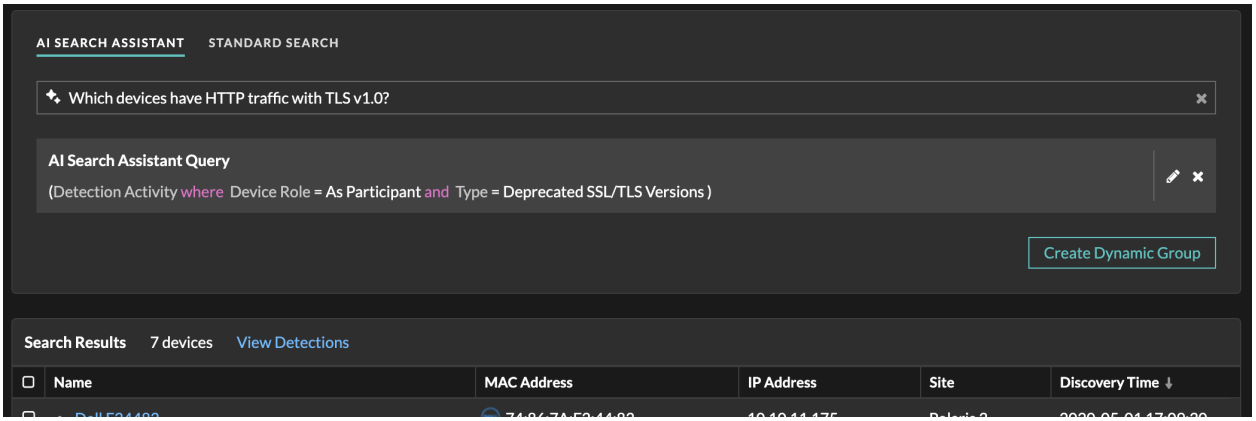
Bevor Sie beginnen

- Ihr ExtraHop-System muss verbunden mit ExtraHop Cloud Services.
- Der AI Search Assistant muss von Ihrem ExtraHop-Administrator aktiviert werden.

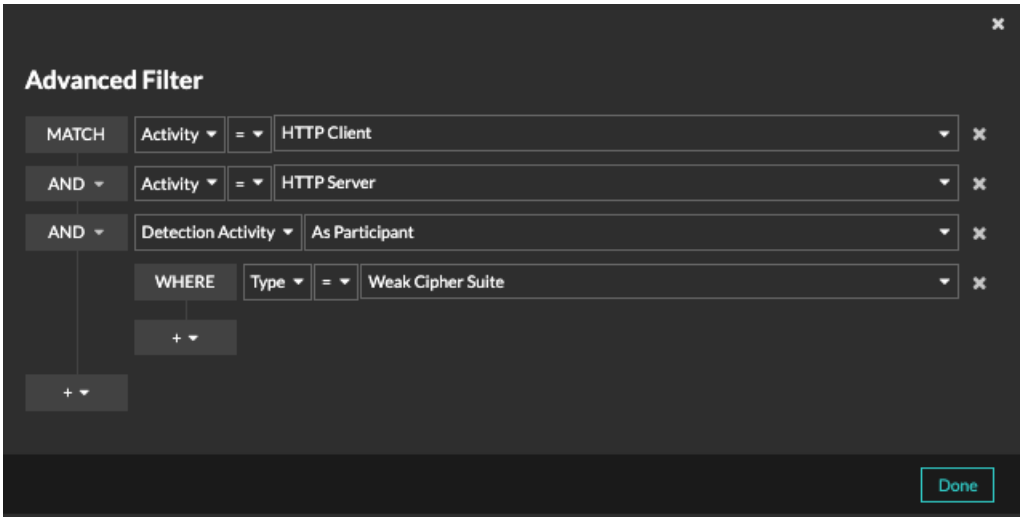
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Vermögenswerte**.
3. Schreiben Sie eine Aufforderung in das Feld AI Search Assistant und drücken Sie die EINGABETASTE.

   Hinweis: Klicken Sie auf das Suchaufforderungsfeld, um eine aktuelle Abfrage oder eine vorgeschlagene Suche auszuwählen.

   Die Abfrageausgabe des AI Search Assistant und die Ergebnisliste werden angezeigt.



4. Optional: Klicken Sie im Abschnitt AI Search Assistant Query auf das Bearbeitungssymbol um das Fenster Erweiterter Filter zu öffnen und Ihre Abfragefilterkriterien zu verfeinern.



a) Klicken Sie auf das Symbol „Filter hinzufügen“ + und wähle **Filter hinzufügen** oder **Filtergruppe hinzufügen** um weitere Kriterien auf der obersten oder sekundären Ebene des Filters anzugeben.

Eine neue Filtergruppe fügt dem Ergebnis des ursprünglichen Filters Kriterien hinzu. Wenn Sie beispielsweise nach HTTP-Clients und -Servern suchen, die an Erkennungen einer Schwache Verschlüsselung Suite beteiligt waren , können Sie eine Filtergruppe hinzufügen, um Erkennungen mit einer Risikoscore unter 30 auszuschließen.

b) Klicken Sie **Erledigt**.

Nächste Schritte

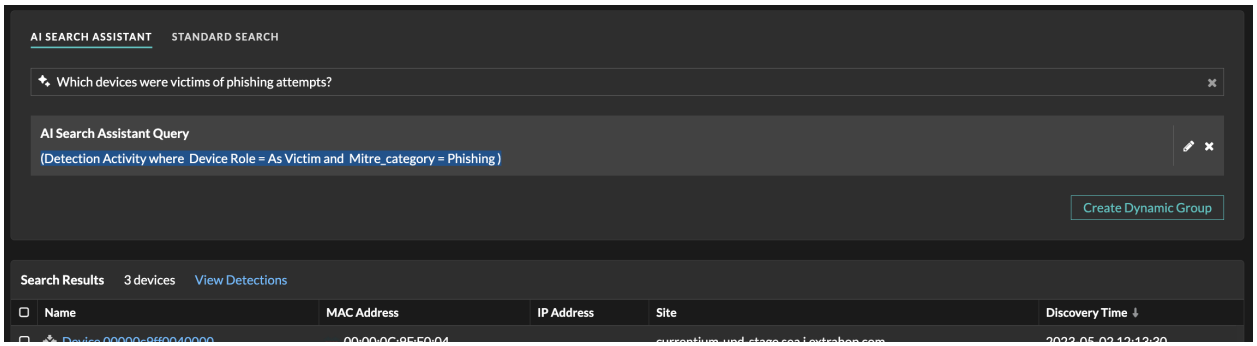
- Klicken Sie **Erkennungen anzeigen** um zur Seite „Entdeckungen“ zu navigieren; der Gerätefilter wird auf die Zusammenfassung der Erkennungen angewendet. Klicken Sie **Erweiterter Gerätefilter** um Filterkriterien anzuzeigen und zu bearbeiten.
- Klicken Sie auf einen Gerätenamen, um Geräteeigenschaften und Messwerte auf der Seite „ Geräteübersicht“.
- Klicken Sie auf das Befehlsmenü ⋮ und wählen Sie dann PDF oder CSV, um die Geräteliste in eine Datei zu exportieren.

Finden Sie Geräte mit Suchvorschlägen

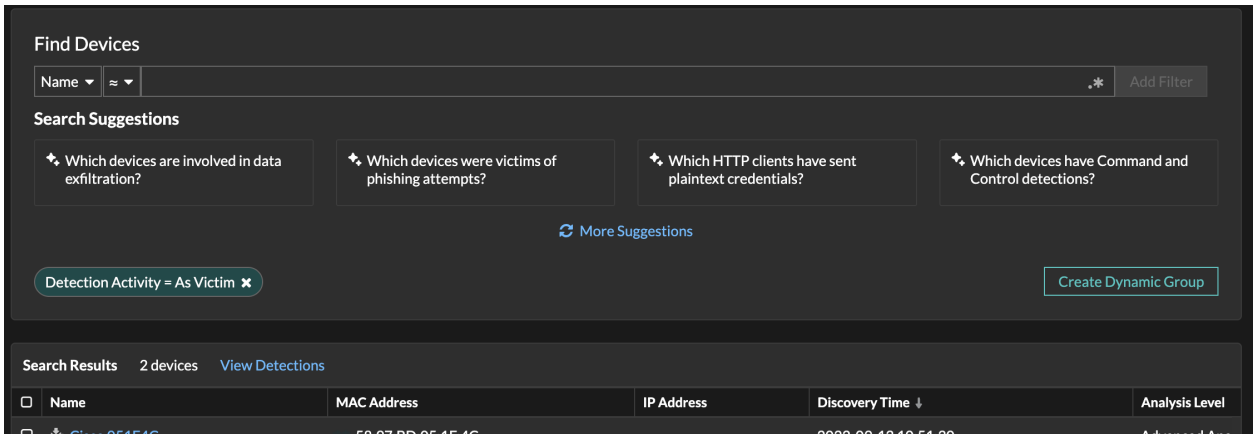
Das ExtraHop-System bietet mehrere Suchvorschläge mit vorgefertigten Filtern, mit denen Sie häufig verwendete Gerätesuchen effizienter durchführen können. Nachdem Sie eine vorgeschlagene Suche ausgewählt haben, können Sie die Filterkriterien bearbeiten, um Ihre Ergebnisse zu verfeinern.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Vermögenswerte**.
3. Klicken Sie auf eine vorgeschlagene Suchaufforderung.

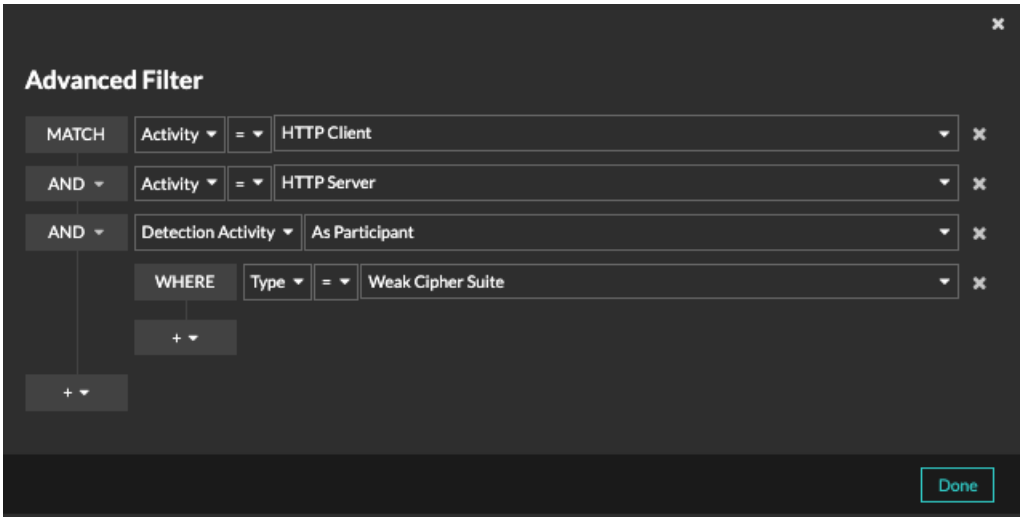
   Wenn AI Search Assistant aktiviert ist, werden Filterkriterien im Abfragefeld AI Search Assistant angezeigt.



   Andernfalls zeigt die Seite den Standardfilter an.



4. Optional: Klicken Sie im Abfragefeld des AI Search Assistant auf das Bearbeitungssymbol oder klicken Sie auf den Standardfilter , um das Fenster Erweiterter Filter zu öffnen und Ihre Abfrage zu verfeinern.



a) Klicken Sie auf das Symbol „Filter hinzufügen“ + und wähle **Filter hinzufügen** oder **Filtergruppe hinzufügen** um weitere Kriterien auf der obersten oder sekundären Ebene des Filters anzugeben.

   Eine neue Filtergruppe fügt dem Ergebnis des ursprünglichen Filters Kriterien hinzu. Wenn Sie beispielsweise nach HTTP-Clients und -Servern suchen, die an Erkennungen einer Schwache Verschlüsselung Suite beteiligt waren , können Sie eine Filtergruppe hinzufügen, um Erkennungen auszuschließen, deren Risikoscore unter 30 liegt.

b) Klicken Sie **Erledigt**.

Nächste Schritte

- Klicken Sie **Erkennungen anzeigen** um zur Seite „Entdeckungen“ zu navigieren; der Gerätefilter wird auf die Zusammenfassung der Erkennungen angewendet. Klicken Sie **Erweiterter Gerätefilter** um Filterkriterien anzuzeigen und zu bearbeiten.
- Klicken Sie **Dynamische Gruppe erstellen** von der oberen rechten Ecke bis eine dynamische Gerätegruppe erstellen basierend auf den Filterkriterien.
- Klicken Sie auf einen Gerätenamen, um Geräteeigenschaften und Messwerte auf der Seite „ Geräteübersicht“.
- Klicken Sie auf das Befehlsmenü ⋮ und wählen Sie dann PDF oder CSV, um die Geräteliste in eine Datei zu exportieren.

Geräte anhand der Erkennungsaktivität finden

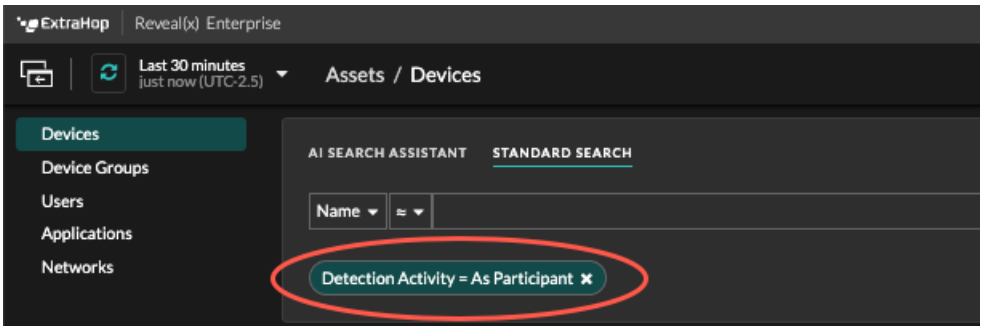
Sie können anhand der zugehörigen Erkennungen nach Geräten suchen, indem Sie Ihrem Suchfilter die Option Kriterien für Erkennungsaktivitäten hinzufügen und Ihre Suche dann mit Kriterien wie Erkennungskategorien, Risikobewertungen und MITRE-Techniken weiter verfeinern.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Vermögenswerte** und klicken Sie dann auf **Aktive Geräte** Diagramm.
3. Optional: Klicken Sie **Standard-Suche** wenn die Registerkarte angezeigt wird.
4. Klicken Sie im Dreifeld-Filter auf **Name** und wähle **Erkennungsaktivität**.
5. Klicken Sie **Wählen Sie einen Artikel aus...** und wählen Sie eine der folgenden Optionen:

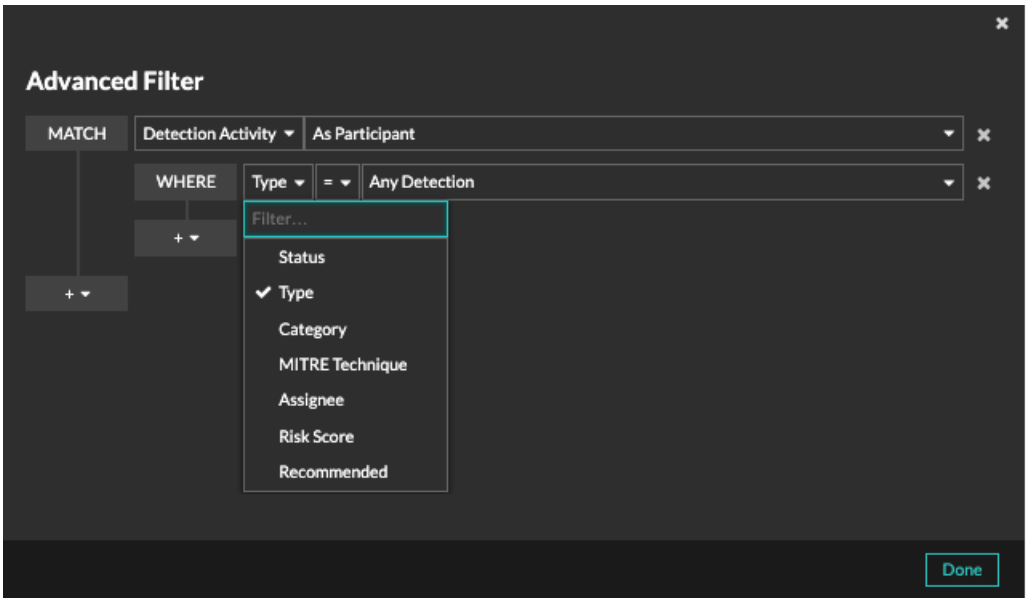
Option	Description
Als Teilnehmer	Filtert Geräte, die an einer Erkennung teilgenommen haben.

Option	Description
Als Täter	Filtert Geräte, die nur an einer Erkennung als Täter beteiligt waren.
Als Opfer	Filtert Geräte, die nur als Opfer an einer Erkennung teilgenommen haben.

6. Klicken Sie **Filter hinzufügen**.
7. Optional: Um zusätzliche Kriterien für die Erkennungsaktivität anzugeben, klicken Sie auf den Filter, den Sie gerade hinzugefügt haben.



Der erweiterte Filter wird geöffnet und zeigt die von Ihnen hinzugefügten MATCH-Kriterien an. Ein WHERE-Operator wird automatisch auf der sekundären Ebene des Filters für Erkennungsaktivitätskriterien hinzugefügt.



8. Klicken Sie **Typ** und wählen Sie eines der folgenden Kriterien für Erkennungsaktivitäten aus:

Option	Description
Status	Filtert Erkennungen nach Status, z. B. ob die Erkennung bestätigt oder geschlossen wurde
Typ	Filtert Erkennungen nach Typ, z. B. Datenexfiltration oder abgelaufene TLS-Serverzertifikate.

Option	Description
Kategorie	Filtert Erkennungen nach Kategorien, z. B. Angriff, Betrieb, Absicherung und Eindringen.
MITRE-Technik	Filtert Erkennungen nach der MITRE-Technik-ID. Das MITRE-Framework ist eine weithin anerkannte Wissensdatenbank für Angriffe.
Abtretungsempfänger	Filtert Erkennungen nach dem zugewiesenen Benutzer.
Risiko-Score	Filtert Erkennungen nach Risikoscore.
Empfehlenswert	Filtert Erkennungen, die für die Triage empfohlen werden, auch bekannt als Smart Triage. (nur NDR-Modul)

siehe Erkennungen filtern für weitere Informationen zu den Kriterien für Erkennungsaktivitäten.

9. Optional: Klicken Sie auf das Symbol „Filter hinzufügen“  und wähle **Filter hinzufügen** oder **Filtergruppe hinzufügen** um weitere Kriterien auf der obersten oder sekundären Ebene des Filters anzugeben.

   Eine neue Filtergruppe fügt dem Ergebnis des ursprünglichen Filters Kriterien hinzu. Wenn Sie beispielsweise nach Geräten suchen, die in der Kategorie „Datenexfiltration“ als Straftäter gehandelt haben, können Sie eine Filtergruppe hinzufügen, um Erkennungen mit dem Status „ Geschlossen“ aus diesen Ergebnissen auszuschließen.
10. Klicken Sie **Speichern**.

Nächste Schritte

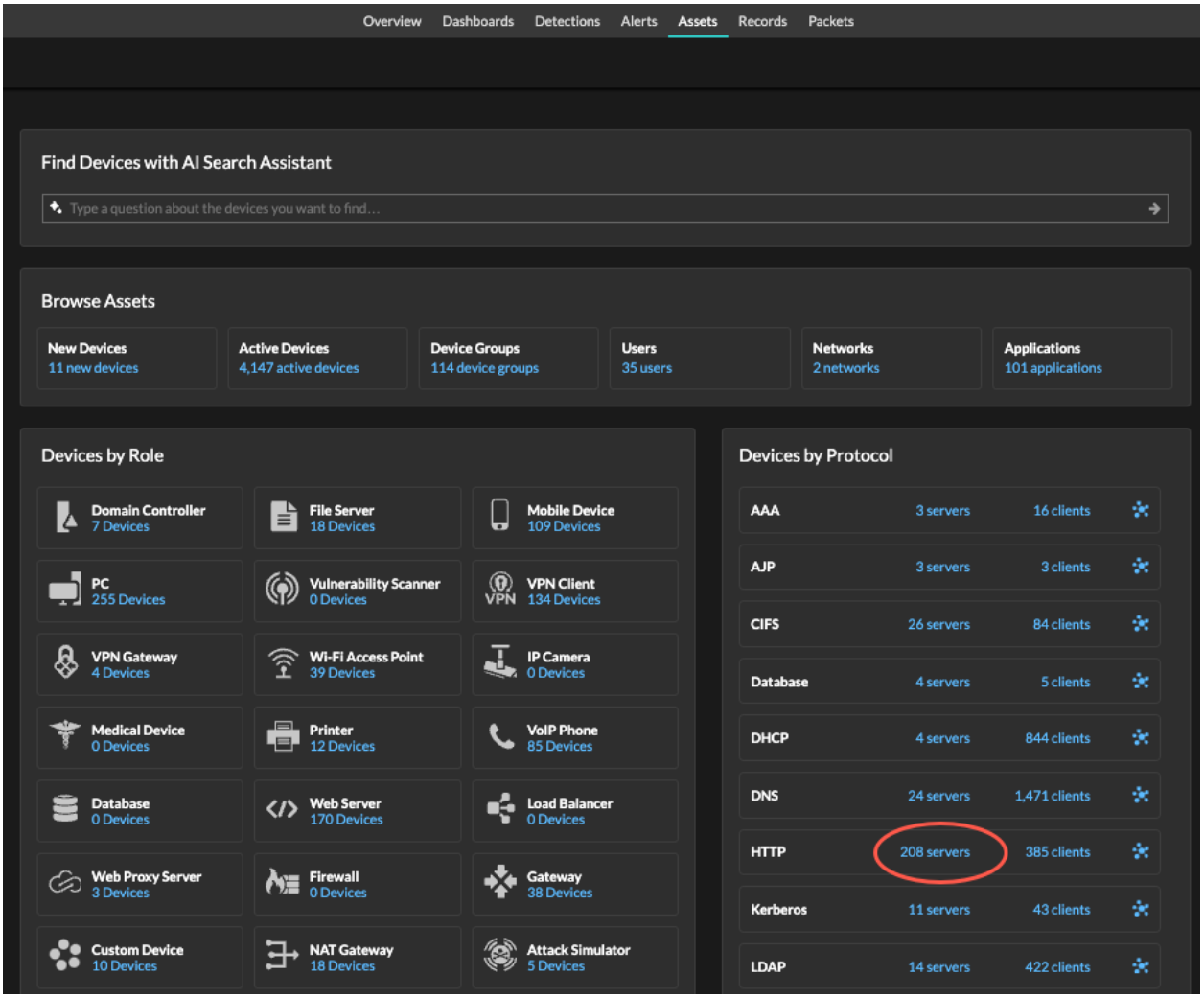
- Klicken Sie auf einen Gerätenamen, um Geräteeigenschaften und Messwerte auf der Seite „ Geräteübersicht“.
- Klicken Sie auf das Befehlsmenü ⋮ und wählen Sie dann PDF oder CSV, um die Geräteliste in eine Datei zu exportieren.

Geräte anhand der Protokollaktivität finden

Auf der Seite Geräte werden alle Protokolle angezeigt, die während des ausgewählten Zeitintervalls aktiv auf dem ExtraHop-System kommunizieren. Sie können schnell ein Gerät finden, das mit einem Protokoll verknüpft ist, oder ein stillgelegtes Gerät erkennen, das immer noch aktiv über ein Protokoll kommuniziert.

Im folgenden Beispiel zeigen wir Ihnen, wie Sie innerhalb der Gruppe der HTTP-Server nach einem Webserver suchen.

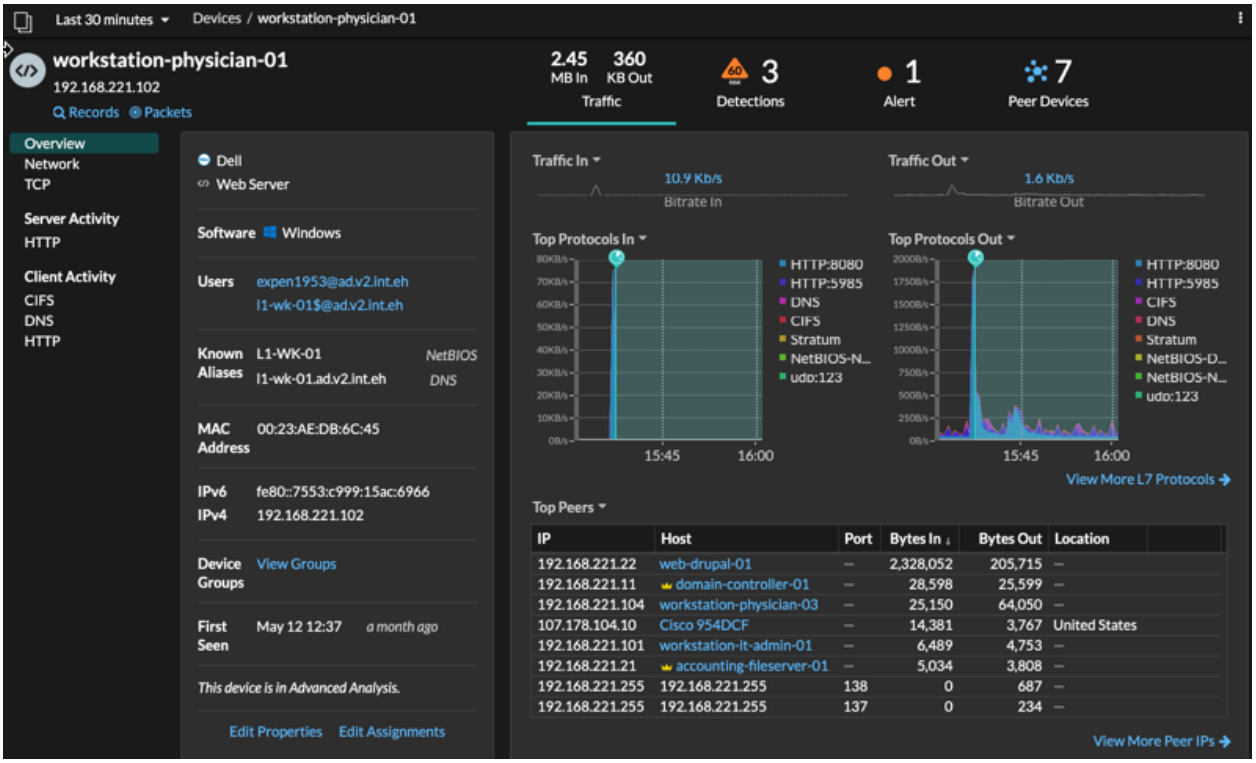
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Vermögenswerte**.
3. Klicken Sie im Diagramm Geräte nach Protokollaktivität auf die Anzahl der HTTP-Server, wie in der folgenden Abbildung dargestellt.



Hinweis: Wenn Sie das gewünschte Protokoll nicht sehen, hat das ExtraHop-System diese Art von Protokollverkehr über die Leitung während des angegebenen Zeitintervalls möglicherweise nicht beobachtet, oder für das Protokoll ist möglicherweise eine Modullizenz erforderlich. Weitere Informationen finden Sie in der Ich sehe nicht den Protokollverkehr, den ich erwartet hatte? Abschnitt in den Häufig gestellten Fragen zur Lizenz.

Auf der Seite werden Verkehrs- und Protokollmetriken angezeigt, die der Gruppe von HTTP-Servern zugeordnet sind.

4. Klicken Sie oben auf der Seite auf **Mitglieder der Gruppe**.
   Auf der Seite wird eine Tabelle mit allen Geräten angezeigt, die während des ausgewählten Zeitintervalls HTTP-Antworten über die Leitung gesendet haben.
5. Klicken Sie in der Tabelle auf einen Gerätenamen.
   Auf der Seite werden Verkehrs- und Protokollmetriken angezeigt, die mit diesem Gerät verknüpft sind, ähnlich der folgenden Abbildung.



Finden Sie Geräte, auf die ein bestimmter Benutzer zugegriffen hat

Auf der Seite Benutzer können Sie aktive Benutzer und die Geräte sehen, mit denen sie sich während des angegebenen Zeitintervalls am ExtraHop-System angemeldet haben.

Hinweis: Du kannst auch Suche nach Benutzern aus dem globalen Suchfeld oben auf der Seite.

Dieses Verfahren zeigt Ihnen, wie Sie eine Suche von der Benutzerseite aus durchführen.

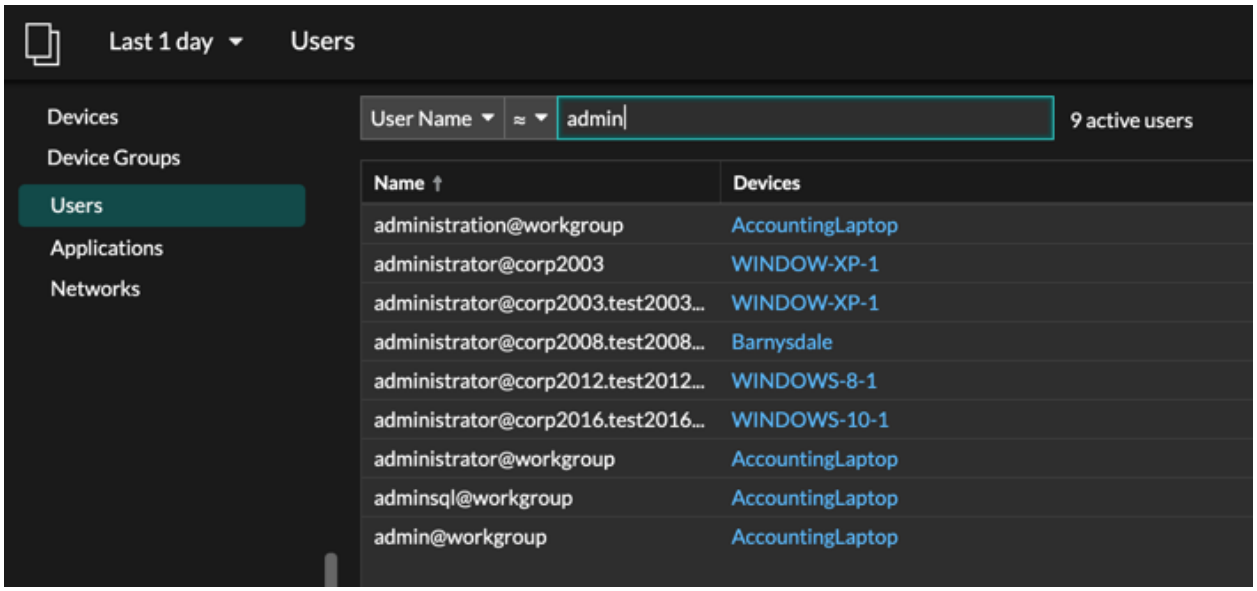
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Vermögenswerte** und klicken Sie dann auf **Nutzer** Diagramm.
3. Wählen Sie in der Suchleiste eine der folgenden Kategorien aus der Dropdownliste aus:

Option	Description
Nutzername	Suchen Sie nach dem Benutzernamen, um zu erfahren, auf welche Geräte der Benutzer zugegriffen hat. Der Benutzername wird aus dem Authentifizierungsprotokoll wie LDAP oder Active Directory extrahiert.
Protokoll	Suchen Sie nach Protokollen, um zu erfahren, welche Benutzer auf Geräte zugegriffen haben, die über dieses Protokoll kommunizieren.
Gerätename	Suchen Sie nach dem Gerätenamen, um zu erfahren, welche Benutzer auf das Gerät zugegriffen haben.

4. Wählen Sie einen der folgenden Operatoren aus der Dropdownliste aus:

Option	Description
=	Suchen Sie nach einem Namen oder Gerät, der genau mit dem Textfeld übereinstimmt.
≈	Suchen Sie nach Namen oder Geräten, die nicht genau mit dem Textfeld übereinstimmen.
≈ (Standard)	Suchen Sie nach einem Namen oder Gerät, das den Wert des Textfeldes enthält.
≈/	Suchen Sie nach einem Namen oder Gerät, das den Wert des Textfeldes ausschließt.

5. Geben Sie in das Textfeld den Namen des Benutzers oder Gerät Sie zuordnen oder ausschließen möchten.
Auf der Seite „Benutzer“ wird eine Ergebnisliste angezeigt, die der folgenden Abbildung ähnelt:



6. Klicken Sie auf den Namen eines Gerät, um das zu öffnen Seite „ Geräteübersicht“ und zeigen Sie alle Benutzer an, die während des angegebenen Zeitintervalls auf das Gerät zugegriffen haben.

Finden Sie Peer-Geräte

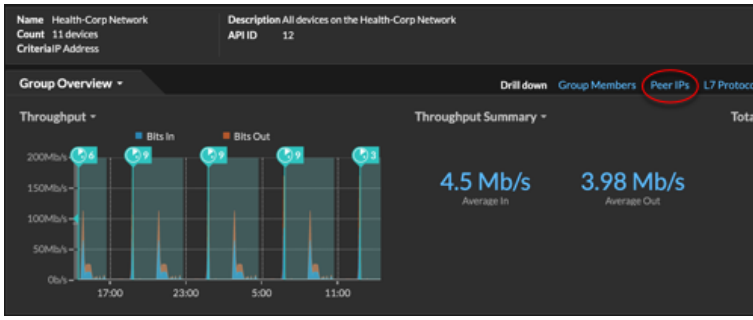
Wenn Sie wissen möchten, welche Geräte aktiv miteinander kommunizieren, können Sie auf einer Gerät- oder Gerätegruppen-Protokollseite einen Drilldown nach Peer-IPs durchführen.

Wenn du nach unten bohren Anhand der Peer-IP-Adresse können Sie eine Liste von Peer-Geräten untersuchen, Leistungs- oder Durchsatzmetriken anzeigen, die Peer-Geräten zugeordnet sind , und dann auf den Namen eines Peer-Geräts klicken, um weitere Protokollmetriken anzuzeigen.

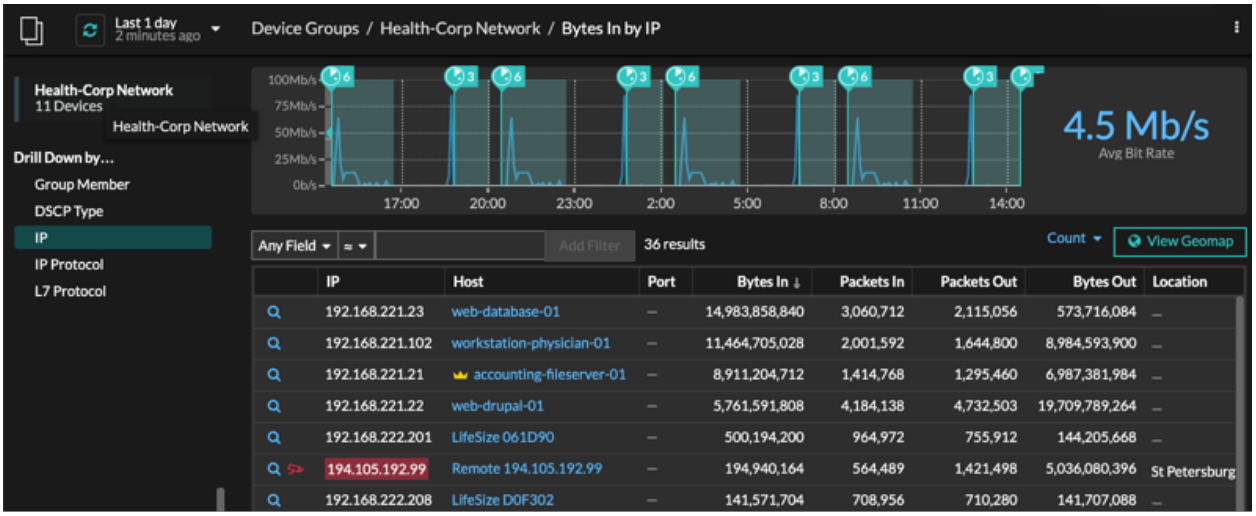
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Vermögenswerte** und wählen Sie dann **Gerät** oder **Gerätegruppe** im linken Bereich.
3. Suche nach einem Gerät oder Gerätegruppe, und klicken Sie dann in der Ergebnisliste auf den Namen.
4. Klicken Sie auf der Übersichtsseite für das ausgewählte Gerät oder die Gerätegruppe auf einen der folgenden Links:

Option	Description
Für Geräte	klicken **Weitere Peer-IPs anzeigen**, befindet sich am unteren Rand des Top-Peer-Diagramms.

Für Gerätegruppen	klicken **Peer-IPs**, befindet sich im Abschnitt Details in der oberen rechten Ecke der Seite.



Eine Liste von Peer-Geräten wird angezeigt, die nach IP-Adresse aufgeschlüsselt sind. Sie können Netzwerk-Byte- und Paketinformationen für jedes Peer-Gerät untersuchen, wie in der folgenden Abbildung dargestellt.



Einen Gerätenamen ändern

Das ExtraHop-System benennt Geräte automatisch, indem es den Verkehr mit den Benennungsprotokollen (DNS, DHCP, NETBIOS, CDP) passiv überwacht. Wenn für ein Gerät kein Benennungsprotokollverkehr beobachtet wird, zeigt der Gerätename entweder die IP-Adresse oder die MAC-Adresse an. In beiden Fällen können Sie den automatischen Gerätenamen in einen benutzerdefinierten Namen ändern. Der benutzerdefinierte Name wird im gesamten ExtraHop-System angezeigt.

Hier sind einige wichtige Überlegungen zum Ändern eines Gerätenamens:

- Benutzerdefinierte Namen werden nicht zwischen den verbundenen ExtraHop-Systemen synchronisiert. Beispielsweise ist ein auf einem Sensor erstellter benutzerdefinierter Name von einem verbundenen Gerät nicht verfügbar Konsole.
- Das ExtraHop-System führt keine DNS-Suchen nach Gerätenamen durch. Das ExtraHop-System leitet den DNS-Namen für ein Gerät ab, indem es den DNS-Verkehr über Kabeldaten beobachtet. Weitere Informationen finden Sie unter Erkennung von Geräten.
- Wenn ein Gerät mehrere Namen hat, Die Reihenfolge der Anzeigepriorität ist in den Administrationseinstellungen festgelegt.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Vermögenswerte** und klicken Sie dann auf **Aktive Geräte** Diagramm.
3. Filtern Sie die Geräteliste, um das gewünschte Gerät zu finden, und klicken Sie dann auf den Gerätenamen.
   Die Seite Geräteübersicht wird angezeigt, auf der der Datenverkehr und die Protokollaktivitäten für das ausgewählte Gerät angezeigt werden.
4. klicken **Eigenschaften bearbeiten**.
5. klicken **Benutzerdefinierten Namen anzeigen**.
6. Geben Sie einen benutzerdefinierten Namen in das Feld ein.
7. klicken **Speichern**.

Eine Geräterolle ändern

Das ExtraHop-System erkennt und klassifiziert automatisch Geräte in Ihrem Netzwerk anhand der Protokollaktivität oder des Gerätemodells und weist jedem Gerät eine Rolle zu, z. B. einem Gateway, einem Dateiserver, einer Datenbank oder einem Load Balancer. Sie können die einem Gerät zugewiesene Rolle jederzeit ändern.

Im Folgenden finden Sie einige wichtige Überlegungen zum Ändern einer Geräterolle:

- Nachdem Sie das geändert haben Geräterolle, das Gerät könnte entfernt oder hinzugefügt werden dynamische Gerätegruppen die eine Gerät als Kriterien beinhalten.
- Änderungen der Geräterolle werden nicht zwischen den verbundenen ExtraHop-Systemen synchronisiert. Wenn Sie beispielsweise eine Geräterolle auf einem ändern Sensor, die Rolle wird von einer verbundenen nicht geändert Konsole.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Vermögenswerte** und klicken Sie dann auf **Aktive Geräte** Diagramm.
3. Filtern Sie die Geräteliste, um das gewünschte Gerät zu finden, und klicken Sie dann auf den Gerätenamen.
   Die Seite Geräteübersicht wird angezeigt, auf der der Datenverkehr und die Protokollaktivitäten für das ausgewählte Gerät angezeigt werden.
4. klicken **Eigenschaften bearbeiten** .
5. In der Rolle des Geräts Abschnitt, klicken Sie auf die Dropdownliste, und klicken Sie dann auf eine der folgenden Rollen:

Rolle	Beschreibung
Automatisch	Weisen Sie dem Gerät die Rolle zu, die das ExtraHop-System für das Gerät identifiziert hat, was in Klammern steht.
Angriffssimulator	Einem Gerät zuweisen, auf dem eine Sicherheitsverletzung- und Angriffssimulationssoftware (BAS) ausgeführt wird, um Angriffe in einem Netzwerk zu simulieren.
Datenbank	Einem Gerät zuweisen, das eine Datenbankinstanz hostet.
DHCP-Server	Einem Gerät zuweisen, dessen Hauptfunktion die Verarbeitung der DHCP-Serveraktivität ist.
DNS-Server	Einem Gerät zuweisen, dessen Hauptfunktion die Verarbeitung der DNS-Serveraktivität ist.
Domänencontroller	Einem Gerät zuweisen, das als Domänencontroller für Kerberos-, SMB- und MSRPC-Serveraktivitäten fungiert.
Dateiserver	Einem Gerät zuweisen, das auf Lese- und Schreibanforderungen für Dateien über NFS - und SMB-Protokolle reagiert.
Brandmauer	Einem Gerät zuweisen, das den eingehenden und ausgehenden Netzwerkverkehr überwacht und den Verkehr gemäß den Sicherheitsregeln blockiert.

Rolle	Beschreibung
Tor	Einem Gerät zuweisen, das als Router oder Gateway fungiert.
IP-Kamera	Einem Gerät zuweisen, das Bild- und Videodaten über das Netzwerk sendet, z. B. Sicherheitskameras.
Load Balancer	Einem Gerät zuweisen, das als Reverse-Proxy für die Verteilung des Datenverkehrs auf mehrere Server fungiert.
Medizinisches Gerät	Weisen Sie es einem Gerät zu, das speziell für medizinische Bedürfnisse und medizinische Umgebungen entwickelt wurde.
Mobiles Gerät	Einem Gerät zuweisen, auf dem ein mobiles Betriebssystem wie iOS oder Android installiert ist.
NAT-Gateway	Einem Gerät zuweisen, das als Network Address Translation (NAT) -Gateway fungiert. Ein NAT-Gateway ist in der Regel mit vier oder mehr Betriebssystem-Fingerabdruckfamilien oder mit vier oder mehr Hardware- oder Herstellermarken und -modellen verknüpft. Nachdem einem Gerät diese Rolle zugewiesen wurde, werden die Geräteeigenschaften für Software, Hardwaremarke und -modell sowie authentifizierte Benutzer für das Gerät nicht mehr angezeigt.
PC	Einem Gerät zuweisen, z. B. einem Laptop, einem Desktop, einer Windows-VM oder einem macOS-Gerät.
Drucker	Einem Gerät zuweisen, mit dem Benutzer Text und Grafiken von anderen angeschlossenen Geräten drucken können.
VoIP-Telefon	Einem Gerät zuweisen, das Voice over IP (VoIP) -Telefonanrufe verwaltet.
VPN-Gateway	Einem Gerät zuweisen, das zwei oder mehr VPN-Geräte oder Netzwerke miteinander verbindet, um Remote-Verbindungen zu überbrücken.
Schwachstellen-Scanner	Einem Gerät zuweisen, auf dem Schwachstellen-Scanner-Programme ausgeführt werden.
Web-Proxyserver	Einem Gerät zuweisen, das HTTP-Anfragen zwischen einem Gerät und einem anderen Server verarbeitet.
Webserver	Einem Gerät zuweisen, das Webressourcen hostet und auf HTTP-Anfragen reagiert.
Wi-Fi-Zugangspunkt	Einem Gerät zuweisen, das ein drahtloses lokales Netzwerk erstellt und ein drahtloses Netzwerksignal auf einen bestimmten Bereich projiziert.

Rolle	Beschreibung
Andere	Einem Gerät zuweisen, wenn die Geräteaktivität keine einzelne Rolle eindeutig identifiziert.

6. klicken **Speichern**.

Ein Gerätemodell ändern

Das ExtraHop-System beobachtet den Netzwerkverkehr auf Geräten, um automatisch Marke und Modell zu ermitteln . Sie können das Gerätemodell jedoch manuell ändern.

Hier sind einige wichtige Überlegungen zum Ändern eines Gerätemodells:

- Geräte werden anhand von Kriterien, die auf Gerätemodellen basieren, automatisch zu dynamischen Gerätegruppen hinzugefügt und daraus entfernt.
- Sie können ein Gerätemodell von ändern Sensoren und Konsolen. Wenn das Gerät auf einem aktualisiert wird Konsole, die Änderung wird mit Connected synchronisiert Sensoren. Die Änderung wird jedoch nicht von einzelnen Personen synchronisiert Sensoren zu den verbundenen Konsole.

Bevor Sie beginnen
Du musst haben volle Schreibrechte oder höher.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Vermögenswerte** und klicken Sie dann auf **Aktive Geräte** Diagramm.
3. Filtern Sie die Geräteliste, um das gewünschte Gerät zu finden, und klicken Sie dann auf den Gerätenamen.
   Das Geräte im Überblick Eine Seite wird angezeigt, auf der die Verkehrs- und Protokollaktivitäten für das ausgewählte Gerät angezeigt werden.
4. Klicken Sie **Eigenschaften bearbeiten**.
5. In der Modell des Geräts Abschnitt, wählen Sie eine der folgenden Optionen:

Option	Description
Automatisch	• Wählen Sie diese Option, damit das ExtraHop-System automatisch die Marke und das Modell des Gerät ermitteln kann, die in Klammern angezeigt werden.
Benutzerdefiniert	1. Wählen Sie diese Option, um die Marke und das Modell des Gerät manuell anzugeben. 2. Klicken Sie **Geben Sie eine Gerätemarke an...** und geben Sie den Namen der gewünschten Marke ein. In der Dropdownliste werden passende Marken angezeigt. 3. Wählen Sie eine Marke aus der Dropdownliste aus, oder geben Sie einen Namen für die benutzerdefinierte Marke ein. 4. Klicken Sie **Geben Sie ein Gerätemodell an...** und geben Sie den Namen des gewünschten Modells ein. Wenn Sie eine bestehende Marke ausgewählt haben, werden in der Dropdownliste passende Modelle für diese Marke angezeigt.

Option	Description
	5. Wählen Sie ein Modell aus der Dropdownliste aus, oder geben Sie einen benutzerdefinierten Modellnamen ein.

6. Klicken Sie **Speichern**.

Manuelles Identifizieren eines Gerät als hoher Wert

Das ExtraHop-System identifiziert Geräte, die Authentifizierung oder wichtige Dienste bereitstellen, automatisch als hoher Wert, aber Sie können ein Gerät auch manuell als hoher Wert oder nicht identifizieren.

Im Folgenden finden Sie einige wichtige Überlegungen zur Identifizierung eines Gerät als hoher Wert:

- Die Risikowerte für Erkennungen auf hoher Wert Geräten werden erhöht.
- Geräte werden automatisch dynamischen Gerätegruppen hinzugefügt und aus ihnen entfernt, wobei die Kriterien auf einem hoher Wert basieren.
- Sie können hoher Wert Geräte manuell identifizieren von Sensoren und Konsolen. Wenn das Gerät auf einem aktualisiert wird Konsole, die Änderung wird mit Connected synchronisiert Sensoren. Die Änderung wird jedoch nicht von einzelnen Personen synchronisiert Sensoren zu den verbundenen Konsole.

Bevor Sie beginnen
Das musst du haben volle Schreibrechte oder höher.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie im oberen Menü auf **Vermögenswerte** und klicken Sie dann auf **Aktive Geräte** Diagramm.
3. Filtern Sie die Geräteliste, um das gewünschte Gerät zu finden, und klicken Sie dann auf den Gerätenamen.
   Die Seite Geräteübersicht wird angezeigt, auf der der Datenverkehr und die Protokollaktivitäten für das ausgewählte Gerät angezeigt werden.
4. Klicken Sie **Eigenschaften bearbeiten**.
5. Wählen Sie im Abschnitt Hoher Wert eine der folgenden Optionen aus:
   - Wählen **Automatisch** damit das ExtraHop-System automatisch ermitteln kann, ob es sich bei dem Gerät um hoher Wert handelt, der in Klammern steht.
   - Wählen **Ja** um das Gerät manuell als hoher Wert zu identifizieren.
   - Wählen **Nein** um manuell festzustellen, dass das Gerät keinen hoher Wert.
6. Klicken Sie **Speichern**.

Ein Geräte-Tag erstellen

Tags sind benutzerdefinierte Labels, die Sie an ein Gerät anhängen können. Mithilfe von Tags können Geräte im ExtraHop-System unterschieden werden, die ein gemeinsames Attribut oder eine gemeinsame Eigenschaft aufweisen. Sie können dann nach Geräten suchen oder dynamische Geräte erstellen Gerätegruppen basierend auf dem Geräte-Tag.

Hinweis Sie können ein Geräte-Tag nicht umbenennen, nachdem es erstellt wurde.

Hinweis Du kannst auch Automatisieren Sie diese Aufgabe über die REST-API.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.

2. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Schlagworte**.
3. klicken **Erstellen**.
4. In der **Name** Feld, geben Sie einen eindeutigen Namen für das Tag ein.
5. Optional: Gehen Sie wie folgt vor, um das neue Tag sofort zu einem Gerät hinzuzufügen:
   a) klicken **Wählen Sie ein Gerät**.
   b) Geben Sie einen Gerätenamen, eine IP-Adresse, eine MAC-Adresse oder einen Hostnamen ein.
   c) Wählen Sie das Gerät aus den Suchergebnissen aus.
   Der Gerätename wird im Fenster angezeigt und weist darauf hin, dass das neue Tag zu diesem Gerät hinzugefügt wird.
6. klicken **Speichern**.
   Das neue Tag erscheint im Schlagworte verwalten Fenster.
7. klicken **Erledigt** um das Fenster zu schließen.

Hinweis: Sie können ein Tag auch von einer Geräteübersichtsseite aus hinzufügen. Finde ein Gerät und klicken Sie dann auf den Gerätenamen. Aus dem Seite „ Geräteübersicht“, klicken **Eigenschaften bearbeiten**, und klicken Sie dann auf **Schlagworte**.

Nächste Schritte

- Suchen Sie nach einem Gerät anhand eines Tags
- Erstellen Sie eine dynamische Gerätegruppe nach Tag

Eine Gerätegruppe erstellen

Sie können Gerätegruppen erstellen, die Metriken für alle angegebenen Geräte in einer Gruppe sammeln. Bei Gerätegruppen können Sie weiterhin Messwerte für jedes einzelne Gerät oder Gruppenmitglied anzeigen. Gerätegruppen können auch als Metrikquelle festgelegt werden.

Nutzer mit eingeschränkte Schreibrechte kann sowohl dynamische als auch statische Gerätegruppen erstellen und bearbeiten.

- Erstellen Sie eine dynamische Gerätegruppe um automatisch alle Geräte, die den angegebenen Kriterien entsprechen, zur Gruppe hinzuzufügen.
- Erstellen Sie eine statische Gerätegruppe um jedes Gerät manuell hinzuzufügen.

Im Folgenden finden Sie einige Überlegungen zur Leistung beim Erstellen einer Gerätegruppe:

- Die Verarbeitung einer großen Anzahl von Gerätegruppen mit einer großen Anzahl von Geräten nimmt mehr Zeit in Anspruch.
- Statische Gruppen werden schneller verarbeitet als dynamische Gruppen und werden für eine bestimmte Gruppe von Geräten empfohlen.
- Dynamische Gruppen mit komplexen Kriterien können höhere Leistungseinbußen haben.

Erstellen Sie eine dynamische Gerätegruppe

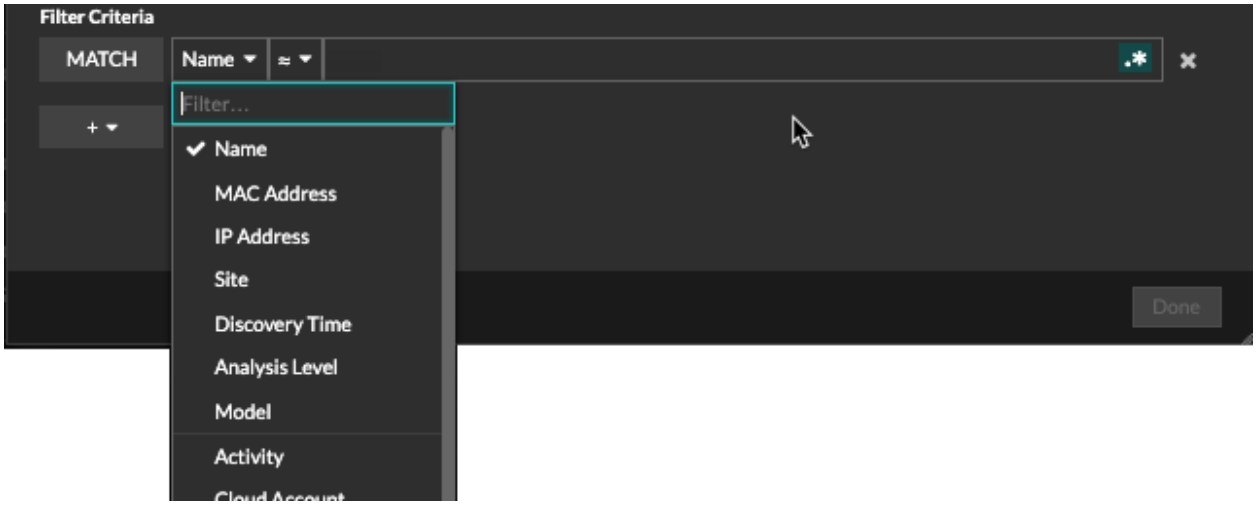
Sie können dynamische Gerätegruppen mit komplexen Filtern erstellen, mit denen Sie mehrere Kriterien angeben und verschachtelte Kriteriengruppen erstellen können.

Hinweis: Auf der Seite Geräte können Sie schnell eine dynamische Gerätegruppe aus einer gefilterten Geräteliste erstellen. klicken **Dynamische Gruppe erstellen** aus der oberen rechten Ecke.

Sie können auch eine dynamische Gerätegruppe aus einer integrierten Gerätegruppe erstellen. Klicken Sie auf der Seite Assets auf eine Rolle oder ein Protokoll, aktualisieren Sie die Filterkriterien und klicken Sie dann auf Speichern Symbol in der oberen rechten Ecke.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie im oberen Menü auf **Vermögenswerte** und klicken Sie dann auf **Gerätegruppen** Diagramm.

3. klicken **Gerätegruppe erstellen**.
4. In der **Name der Gruppe** Feld, geben Sie einen beschreibenden Namen ein, um die Gruppe zu identifizieren
5. Optional: Aus dem **Redakteure** Wählen Sie in der Dropdownliste Benutzer mit eingeschränkten Schreibrechten aus, die diese Gerätegruppe bearbeiten können. Dieses globale Privileg muss in den Administrationseinstellungen aktiviert werden.
   - In der Liste werden nur begrenzte Schreibbenutzer mit aktiven Konten angezeigt.
   - Nur ein Benutzer mit Bearbeitungsberechtigungen für eine Gerätegruppe kann weitere Benutzer mit eingeschränktem Schreibzugriff hinzufügen.
6. Optional: In der **Beschreibung** Feld, fügen Sie Informationen zu dieser Gerätegruppe hinzu.
7. In der Art der Gruppe Abschnitt, klicken Sie **Dynamisch**.
8. In der Filterkriterien Abschnitt, **Name** und wählen Sie eine der folgenden Kategorien aus der Dropdownliste aus:
9. klicken **Name** und wählen Sie eine der folgenden Kategorien aus der Dropdownliste aus:



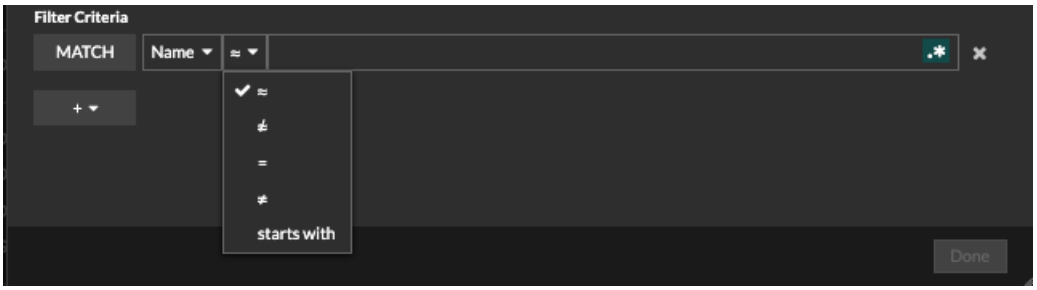
Option	Description
Name	Filtert Geräte nach dem erkannten Gerätenamen. Ein ermittelter Gerätename kann beispielsweise die IP-Adresse oder den Hostnamen enthalten.
MAC-Adresse	Filtert Geräte nach der MAC-Adresse des Gerät.
IP Adresse	Filtert Geräte nach IP-Adresse in den Blockformaten IPv4, IPv6 oder CIDR.
Standort	Filtert Geräte, die einer verbundenen Standort zugeordnet sind. Nur für die Konsole.
Zeit für Entdeckungsreisen	Filtert Geräte, die vom ExtraHop-System innerhalb des angegebenen Zeitintervalls automatisch erkannt werden. Weitere Informationen finden Sie unter Erstellen Sie eine Gerätegruppe basierend auf der Erkennungszeit.
Analyseebene	Filtert Geräte nach Analyseebene, die bestimmt, welche Daten und Metriken für ein Gerät erfasst werden.

Option	Description
	Sie können keine dynamische Gerätegruppe für Geräte erstellen, die nach Analyseebene gefiltert sind.
Modell	Filtert Geräte nach Marke, Familie oder Modellname. Die Marke steht für den Hersteller des Gerät. Eine Familie steht für eine Gruppierung, z. B. eine Produktlinie. Die folgenden Tipps können Ihnen helfen, das gewünschte Gerätemodell zu finden: • Sie können aus einer Liste von Marken auswählen, die in Ihrem ExtraHop-System gefunden wurden, und dann auf den Filter klicken, um die Ergebnisse zu verfeinern. • Sie können Hovertips neben Marken und Produktfamilien anzeigen, um zu sehen, wie viele Geräte und passende Modelle gefunden wurden. • Sie können eine Marke oder eine Familie auswählen, um alle Geräte in dieser Gruppe zu finden, unabhängig vom Modell.
Aktivität	Filtert Geräte nach Protokollaktivität, die dem Gerät zugeordnet ist. Wenn Sie beispielsweise HTTP-Server auswählen, werden Geräte mit HTTP-Server-Metriken und jedes andere Gerät zurückgegeben, dessen Geräterolle auf HTTP-Server festgelegt ist. Filtert auch Geräte, die eine externe Verbindung akzeptiert oder initiiert haben, sodass Sie feststellen können, ob Geräte verdächtige Aktivitäten ausführen.
Cloud-Konto	Filtert Geräte nach dem Cloud-Dienstkonto, das dem Gerät zugeordnet ist.
Cloud-Instanz-ID	Filtert Geräte nach der Cloud-Instanz-ID, die dem Gerät zugeordnet ist.
Cloud-Instanztyp	Filtert Geräte nach dem Cloud-Instanztyp, der dem Gerät zugeordnet ist.
SHA-256-Datei-Hash	Filtert Geräte, auf denen Dateien beobachtet wurden, die mit dem SHA-256-Hashing-Algorithmus gehasht wurden. Sie können eine Tabelle mit Hash-Dateien auf der Seite „Dateien“.
Hoher Wert	Filtert Geräte, die als hoher Wert eingestuft werden, weil sie Authentifizierungsdienste bereitstellen, wichtige Dienste in Ihrem Netzwerk unterstützen oder die vom Benutzer als hochwertig eingestuft wurden.
Derzeit aktiv	Filtert Geräte nach Aktivitäten, die in den letzten 30 Minuten auf einem Gerät beobachtet wurden.

Option	Description
Netzwerk-Lokalitätstyp	Filtert Geräte nach allen internen oder externen Netzwerkstandorten.
Name der Netzwerklokalität	Filtert Geräte nach dem Namen der Netzwerklokalität.
Rolle	Filtert Geräte nach der zugewiesenen Geräterolle wie Gateway, Firewall, Load Balancer und DNS-Server.
Software	Filtert Geräte nach der auf dem Gerät erkannten Betriebssystemsoftware.
Art der Software	Filtert Geräte nach der Art der auf dem Gerät beobachteten Software, z. B. Angriffssimulator, Fernzugriff oder Datenbankserver.
Subnetz	Filtert Geräte nach dem Subnetz, das dem Gerät zugeordnet ist.
Schlagwort	Filtert Geräte nach benutzerdefinierten Geräte-Tags.
Verkäufer	Filtert Geräte nach dem Namen des Geräteherstellers, der durch die OUI-Suche (Organizationally Unique Identifier) ermittelt wurde.
Virtuelle private Cloud	Filtert Geräte nach der VPC, die dem Gerät zugeordnet ist.
VLAN	Filtert Geräte nach dem Geräte-VLAN-Tag. VLAN-Informationen werden aus VLAN-Tags extrahiert, wenn der Datenverkehrsspiegelungsprozess sie auf dem Spiegelport beibehält. Nur verfügbar, wenn `devices_accross_vlans` Einstellung ist gesetzt auf `False` in der laufenden Konfigurationsdatei.
CDP-Name	Filtert Geräte nach dem CDP-Namen, der dem Gerät zugewiesen ist.
Name der Cloud-Instanz	Filtert Geräte nach dem Cloud-Instanznamen, der dem Gerät zugewiesen ist.
Benutzerdefinierter Name	Filtert Geräte nach dem benutzerdefinierten Namen, der dem Gerät zugewiesen wurde.
DHCP-Name	Filtert Geräte nach dem DHCP-Namen, der dem Gerät zugewiesen ist.
DNS-Name	Filtert Geräte nach einem beliebigen DNS-Namen, der dem Gerät zugewiesen ist.
NetBIOS-Name	Filtert Geräte nach dem NetBIOS-Namen, der dem Gerät zugewiesen ist.
Erkennungsaktivität	Filtert Geräte mit Erkennungsaktivität wo das Gerät ein Teilnehmer war. Aktiviert zusätzliche Kriterien wie Kategorie, Risikoscore und MITRE-Technik.

Option	Description
	Hinweis: Sie können keine Gerätegruppe erstellen, die diese Kriterienoption enthält.

10. Wählen Sie einen der folgenden Operatoren aus der Dropdownliste aus. Die verfügbaren Operatoren basieren auf der ausgewählten Kategorie:

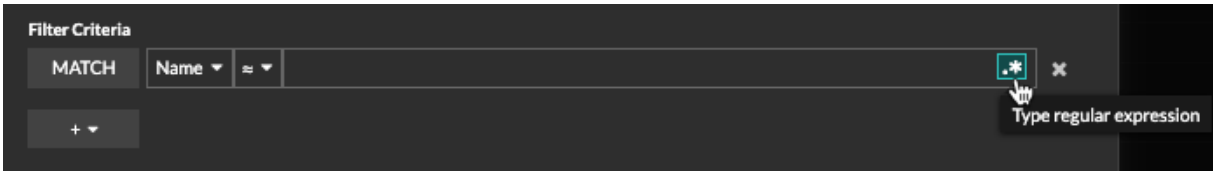


Option	Description
=	Filtert Geräte, die exakt dem Suchfeld für die ausgewählte Kategorie entsprechen.
≈	Filtert Geräte, die nicht genau dem Suchfeld entsprechen.
≈	Filtert Geräte, die den Wert des Suchfelds für die ausgewählte Kategorie enthalten.
≈/	Filtert Geräte, die den Wert des Suchfelds für die ausgewählte Kategorie ausschließen.
beginnt mit	Filtert Geräte, die mit dem Wert des Suchfeldes für die ausgewählte Kategorie beginnen.
existiert	Filtert Geräte, die einen Wert für die ausgewählte Kategorie haben.
existiert nicht	Filtert Geräte, die keinen Wert für die ausgewählte Kategorie haben.
Spiel	Filtert Geräte, die den Wert des Suchfelds für die ausgewählte Kategorie enthalten.
und	Filtert Geräte, die den in zwei oder mehr Suchfeldern angegebenen Bedingungen entsprechen.
oder	Filtert Geräte, die mindestens eine in zwei oder mehr Suchfeldern angegebene Bedingung erfüllen.
nicht	Filtert Geräte, die die in einem Suchfeld angegebenen Bedingungen nicht erfüllen.

11. Geben Sie im Suchfeld die Zeichenfolge ein, die abgeglichen werden soll, oder wählen Sie einen Wert aus der Dropdownliste aus. Der Eingabetyp wird durch die gewählte Kategorie bestimmt.

    Wenn Sie beispielsweise Geräte anhand des Namens suchen möchten, geben Sie die Zeichenfolge, die abgeglichen werden soll, in das Suchfeld Feld. Wenn Sie Geräte anhand der Rolle suchen möchten, wählen Sie diese aus der Dropdownliste der Rollen aus.

    Hinweis: Abhängig von der ausgewählten Kategorie können Sie im Textfeld auf das Regex-Symbol klicken, um den Abgleich per regulärem Ausdruck zu aktivieren.



12. Optional: Klicken Sie auf das Symbol „Filter hinzufügen“ + und wähle **Filter hinzufügen** oder **Filtergruppe hinzufügen** um weitere Kriterien auf der obersten oder sekundären Ebene des Filters anzugeben.

    Wenn Sie beispielsweise nach Gerätenamen filtern, die mit „Konto“ beginnen, können Sie eine neue Gruppe von Kriterien hinzufügen, die nach einer bestimmten Rolle oder einem bestimmten Tag innerhalb der Gruppe von Geräten filtern, die mit „Konto“ beginnen.
13. klicken **Speichern**.

Sie können die Kriterien ändern, indem Sie auf der Seite Gerätegruppen auf die Gruppe klicken, die Sie ändern möchten, und klicken Sie dann auf **Eigenschaften**.

Erstellen Sie eine statische Gerätegruppe

Hinweis: Auf der Seite Geräte können Sie das Kontrollkästchen neben einem oder mehreren Geräten auswählen und auf **Zur Gruppe hinzufügen** um schnell eine statische Gerätegruppe zu erstellen oder Geräte zu einer vorhandenen Gruppe hinzuzufügen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie im oberen Menü auf **Vermögenswerte** und klicken Sie dann auf **Gerätegruppen** Diagramm.
3. klicken **Gerätegruppe erstellen**.
4. In der **Name der Gruppe** Feld, geben Sie einen Namen für die neue Gruppe ein.
5. Optional: Aus dem **Redakteure** Wählen Sie in der Dropdownliste Benutzer mit eingeschränkten Schreibrechten aus, die diese Gerätegruppe bearbeiten können. Dieses globale Privileg muss in den Administrationseinstellungen aktiviert werden.
   - In der Liste werden nur begrenzte Schreibbenutzer mit aktiven Konten angezeigt.
   - Nur ein Benutzer mit Bearbeitungsberechtigungen für eine Gerätegruppe kann weitere Benutzer mit eingeschränktem Schreibzugriff hinzufügen.
6. Optional: In der **Beschreibung** Feld, fügen Sie Informationen zu dieser Gerätegruppe hinzu.
7. In der Art der Gruppe Abschnitt, auswählen **Statisch**.
8. Klicken Sie **Speichern**.
   Ihre Gerätegruppe ist jetzt erstellt.
9. Füge deiner Gruppe ein bestimmtes Gerät hinzu.
   a) Klicken Sie auf die gewünschte statische Gerätegruppe und klicken Sie auf **Geräte** aus dem linken Bereich.
   b) Klicken Sie oben in der Gerätetabelle auf das Feld Gerät suchen..., geben Sie den Namen des gewünschten Gerät ein, und wählen Sie dann das Gerät aus der Liste aus.
   c) Klicken Sie **Zur Gruppe hinzufügen**.
10. Fügen Sie Geräte mit bestimmten Kriterien zu Ihrer Gruppe hinzu.
    a) Klicken Sie **Geräte** im linken Bereich.
    b) Finde ein Gerät und aktivieren Sie dann das Kontrollkästchen neben den Geräten, die Sie zu Ihrer Gruppe hinzufügen möchten.
    c) Klicken Sie oben in der Gerätetabelle auf **Zur Gruppe hinzufügen**.
    d) Wählen Sie im Dialogfeld Zur Gruppe hinzufügen **Zu einer bestehenden Gruppe hinzufügen**.
    e) Wählen Sie eine Gerätegruppe aus dem Gruppe Dropdownliste.
    f) Klicken Sie **Zur Gruppe hinzufügen**.

Nächste Schritte
Geräte aus einer Gruppe entfernen, indem Sie das Kontrollkästchen neben dem Gerätenamen markieren und auf **Aus Gruppe entfernen** in der oberen rechten Ecke.

Benutzerdefiniertes Gerät erstellen

Erfassen Sie Metriken für ein Verkehrssegment über mehrere IP-Adressen und Ports, indem Sie ein benutzerdefiniertes Gerät erstellen. Benutzerdefinierte Geräte sind nützlich, um den Verkehr außerhalb Ihrer lokalen Broadcast-Domain zu überwachen, z. B. in Filialen, Geschäften oder Kliniken.

Hier sind einige wichtige Überlegungen zu kundenspezifischen Geräten:

- Benutzerdefinierte Geräte werden erst im ExtraHop-System angezeigt, nachdem Traffic beobachtet wurde, der Ihren angegebenen Kriterien entspricht.
- Vermeiden Sie es, mehrere benutzerdefinierte Geräte für dieselben IP-Adressen oder Ports zu erstellen. Benutzerdefinierte Geräte, die mit sich überschneidenden Kriterien konfiguriert sind, können die Systemleistung beeinträchtigen.
- Vermeiden Sie es, ein benutzerdefiniertes Gerät für eine Vielzahl von IP-Adressen oder Ports zu erstellen, da dies die Systemleistung beeinträchtigen könnte.
- Ein einzelnes benutzerdefiniertes Gerät zählt als ein Gerät auf Ihre lizenzierte Kapazität für Erweiterte Analyse und Standardanalyse.
- Du kannst auch Automatisieren Sie diese Aufgabe über die REST-API.

Bevor Sie beginnen
Du musst haben volle Schreibrechte oder höher.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Maßgeschneiderte Geräte**.
3. klicken **Erstellen**.
4. In der Name Feld, geben Sie einen eindeutigen Namen für das benutzerdefinierte Gerät ein.
5. In der Discovery-ID Feld, geben Sie einen eindeutigen Bezeichner ein.

   Wenn dieses Feld leer gelassen wird, wird aus dem benutzerdefinierten Gerätenamen eine Discovery-ID generiert. Die Discovery-ID darf keine Leerzeichen enthalten und kann nach dem Speichern des benutzerdefinierten Gerät nicht geändert werden.
6. Aus dem **Fühler** Wählen Sie in der Dropdownliste den Sensor aus, den Sie dem benutzerdefinierten Gerät zuordnen möchten. (Nur Konsolen.)
7. Wählen Sie den **Benutzerdefiniertes Gerät aktivieren** Checkbox, um das benutzerdefinierte Gerät zu aktivieren oder zu deaktivieren.
8. Optional: In der Beschreibung Feld, fügen Sie Informationen über das benutzerdefinierte Gerät hinzu.
9. klicken **Kriterien hinzufügen** um eine IP-Adresse, einen Portbereich oder einen VLAN-Bereich als Übereinstimmungskriterien für das benutzerdefinierte Gerät anzugeben.

   Sie können eine einzelne Option angeben, z. B. eine IP-Adresse, oder eine Kombination von Kriterienoptionen angeben. Sie müssen nicht jedes Feld ausfüllen.

   a) In der IP Adresse Feld, geben Sie eine IP-Adresse oder eine CIDR-Notation ein. Wenn Sie eine IP-Adresse angeben, können Sie auch die Richtung des Datenverkehrs und eine Peer-IP-Adresse angeben.

      - (Optional): Aus dem **Richtung des Verkehrs** Drop-down-Liste, wählen **Ausgehend von der IP-Adresse** oder **Eingehend von der IP-Adresse** als Übereinstimmungskriterium. Mit diesen Optionen können Sie ein benutzerdefiniertes Gerät erstellen, das nur Messwerte für den Datenverkehr erfasst, der an oder von dieser IP-Adresse gesendet wird. Die Standardauswahl ist Bidirektional.

- (Optional): In der Peer-IP-Adresse Feld, geben Sie eine IP-Adresse oder CIDR-Notation an, die mit der in der **IP Adresse** Feld. Mit dieser Option können Sie ein benutzerdefiniertes Gerät erstellen, das nur Messwerte für den Verkehr zwischen bestimmten Quelle- und Ziel-IP-Adressen erfasst.

  Hinweis: Wenn Sie eine Peer-IP-Adresse angeben, können Sie nicht auswählen **Bidirektional** für die Verkehrsrichtung.

b) In der Zielportbereich Felder, geben Sie eine minimale und eine maximale Zielportnummer ein. Wenn kein Bereich angegeben ist, gelten alle Ports als Übereinstimmungskriterien.

10. Optional: klicken **Erweiterte Optionen anzeigen** um einen Quellport oder einen VLAN-Bereich zu konfigurieren.
    a) In der Quell-Port-Bereich Felder, geben Sie eine minimale und eine maximale Quellportnummer ein. Wenn kein Bereich angegeben ist, gelten alle Ports als Übereinstimmungskriterien.
    b) In der VLAN-Bereich Felder, geben Sie eine minimale und eine maximale VLAN-ID ein.
11. Optional: klicken **Kriterien hinzufügen** um zusätzliche IP-Adressen, Portbereiche oder VLAN-Bereiche zu konfigurieren.
12. klicken **Speichern**.

Hinweis: klicken **Alle Änderungen speichern** um alle benutzerdefinierten Geräte zu speichern, die ungespeicherte Konfigurationsänderungen haben.

Nächste Schritte

- Remote-Sites für benutzerdefinierte Geräte konfigurieren
- Finde ein Gerät
- Ein benutzerdefiniertes Gerät zur Beobachtungsliste hinzufügen
- Hinzufügen eines Tags zu einem benutzerdefinierten Gerät
- Benutzerdefiniertes Gerät löschen oder deaktivieren

Benutzerdefiniertes Gerät löschen oder deaktivieren

Benutzerdefinierte Geräte werden manuell auf einem ExtraHop-System erstellt, um Messwerte für den über mehrere IP-Adressen und Ports beobachteten Datenverkehr zu sammeln. Wenn eine große Anzahl von benutzerdefinierten Geräten die Systemleistung beeinträchtigt, können Sie ein benutzerdefiniertes Gerät löschen oder deaktivieren.

Bevor Sie beginnen
Vollständige Rechte oder höher sind erforderlich für erstellen oder löschen Sie ein benutzerdefiniertes Gerät.

- Wenn Sie ein benutzerdefiniertes Gerät löschen oder deaktivieren, wird das Gerät inaktiv, was bedeutet, dass das System die Erfassung von Messwerten für dieses Gerät beendet.
- Wenn Sie ein benutzerdefiniertes Gerät löschen oder deaktivieren, wird das Gerät weiterhin als Asset angezeigt, bis alle für dieses Gerät gesammelten Messwerte lokal überschrieben werden Datenspeicher.
- Wenn Sie ein benutzerdefiniertes Gerät löschen, verbleibt die eindeutige Discovery-ID für das benutzerdefinierte Gerät immer im System und kann nicht auf ein neues benutzerdefiniertes Gerät angewendet werden.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Maßgeschneiderte Geräte**.
3. Optional: Suchen Sie im Filtertextfeld nach dem benutzerdefinierten Gerät.

   Das Filtertextfeld unterstützt den Abgleich von Teilzeichenfolgen nach benutzerdefiniertem Gerätenamen, Beschreibung, Status, Sensorund Discovery ID.

4. Wählen Sie in der Tabelle das gewünschte benutzerdefinierte Gerät aus, und führen Sie dann einen der folgenden Schritte aus:
   - Löschen Sie in den Konfigurationsoptionen den **Benutzerdefiniertes Gerät aktiviert** Checkbox. Das ausgewählte Gerät wird inaktiv und aus der vollständigen Anzahl von Analysegeräten entfernt. Sie können das benutzerdefinierte Gerät jederzeit wieder aktivieren, und Sie können weiterhin auf benutzerdefinierte Gerätemetriken aus früheren Zeitintervallen zugreifen, bis sie im lokalen überschrieben werden Datenspeicher.
   - Klicken Sie oben auf der Seite auf **Gerät löschen**, und klicken Sie dann **Benutzerdefiniertes Gerät löschen** aus dem Bestätigungsfenster. Das ausgewählte benutzerdefinierte Gerät wurde dauerhaft aus dem ExtraHop-System entfernt und kann nicht wiederhergestellt werden.

Remote-Sites für benutzerdefinierte Geräte konfigurieren

Benutzerdefinierte Geräte sind nützlich, um den Verkehr außerhalb Ihrer lokalen Broadcast-Domain zu überwachen, z. B. in Filialen, Geschäften oder Kliniken. Sie können Metriken zu benutzerdefinierten Geräten an entfernten Standort sammeln, um auf einfache Weise zu erfahren, wie Dienste an entfernten Standorten genutzt werden, und um einen Überblick über den Verkehr zwischen entfernten Standorten und einem Rechenzentrum zu erhalten.

Erstellen Sie beispielsweise ein Dashboard und fügen Sie ein benutzerdefiniertes Gerät als Metrikquelle hinzu, um Metriken an entfernten Standort wie eingehenden und ausgehenden Durchsatz, Timeouts für erneute Übertragungen, Roundtrip-Zeiten und Nullfenster anzuzeigen. Sehen Sie die Referenz zu Protokollmetriken für eine vollständige Liste der Metriken und Beschreibungen von Remote-Standorten.

Im Folgenden finden Sie einige wichtige Überlegungen zu Remotestandorten für benutzerdefinierte Geräte:

- Die Konfiguration von Remote-Standorten gilt für alle aktivierten benutzerdefinierten Geräte. Sie können Remote-Sites nicht für ein einzelnes benutzerdefiniertes Gerät konfigurieren.
- Metriken für Remote-Standorte werden nur dann im Metrikkatalog und im Metric Explorer angezeigt, wenn die Erfassung von Metriken an Remote-Standorten aktiviert ist.

Bevor Sie beginnen
Du musst volle Schreibrechte oder höher.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Maßgeschneiderte Geräte**.
3. klicken **Remote-Sites konfigurieren**.
4. Wählen oder löschen Sie die **Erfassen Sie Metriken für Remote-Standorte** Checkbox.
5. klicken **Speichern**.

Geben Sie eine Netzwerklokalität an

Mithilfe von Netzwerklokalisierungen können Sie den Datenverkehr von IP-Adressen und CIDR-Blöcken als intern oder extern in Ihrem Netzwerk klassifizieren. Sie können auch einen Namen für jeden Standort angeben, z. B. „DMZ“ oder „Gastnetzwerk“, und in Geräten und Datensätzen nach diesem Namen filtern.

Im Folgenden finden Sie einige wichtige Überlegungen zu diesen Einstellungen:

- Die Benennung von Netzwerkstandorten wirkt sich auf Erkennungen und Auslöser sowie auf verwandte Funktionen wie Benachrichtigungen, Übersichtsseiten und den Security Operations Report aus.
- Wenn Ihre ExtraHop-Bereitstellung eine Konsole umfasst, empfehlen wir Ihnen Transfermanagement aller an die Konsole angeschlossenen Sensoren.
- Für ExtraHop RevealX 360 werden diese Einstellungen auf allen angeschlossenen Sensoren synchronisiert. Sie sollten diese Einstellungen nicht für einzelne Sensoren konfigurieren.

- Bei ExtraHop RevealX Enterprise werden diese Einstellungen für alle Sensoren synchronisiert, wenn Sie die Verwaltung auf eine verbundene Konsole übertragen. Andernfalls müssen die Netzwerkstandorteinstellungen auf allen Sensoren und Konsolen konfiguriert werden.
- Sie müssen vollständig schreiben können Privilegien um diese Einstellungen zu ändern.

Video: Sehen Sie sich die entsprechende Schulung an: Netzwerkstandorte konfigurieren

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Netzwerk-Lokalitäten**.
3. Klicken Sie **Erstellen**.
4. Geben Sie im Feld Network Locality Name einen eindeutigen Namen ein.
5. Optional: In der Beschreibung Feld, geben Sie Informationen über den Netzwerkstandort ein.
6. Wählen Sie im Abschnitt Network Locality Type die Option Intern oder Extern aus, je nachdem, welche Klassifizierung Sie auf die IP-Adressen und CIDR-Blöcke anwenden möchten.
7. Geben Sie in das Feld IP-Adressen und CIDR-Blöcke die IP-Adressen und CIDR-Blöcke ein, die Sie der Lokalität hinzufügen möchten. Sie müssen einen eindeutigen Bereich von Adressen oder Blöcken eingeben.
8. Klicken Sie **Speichern**.

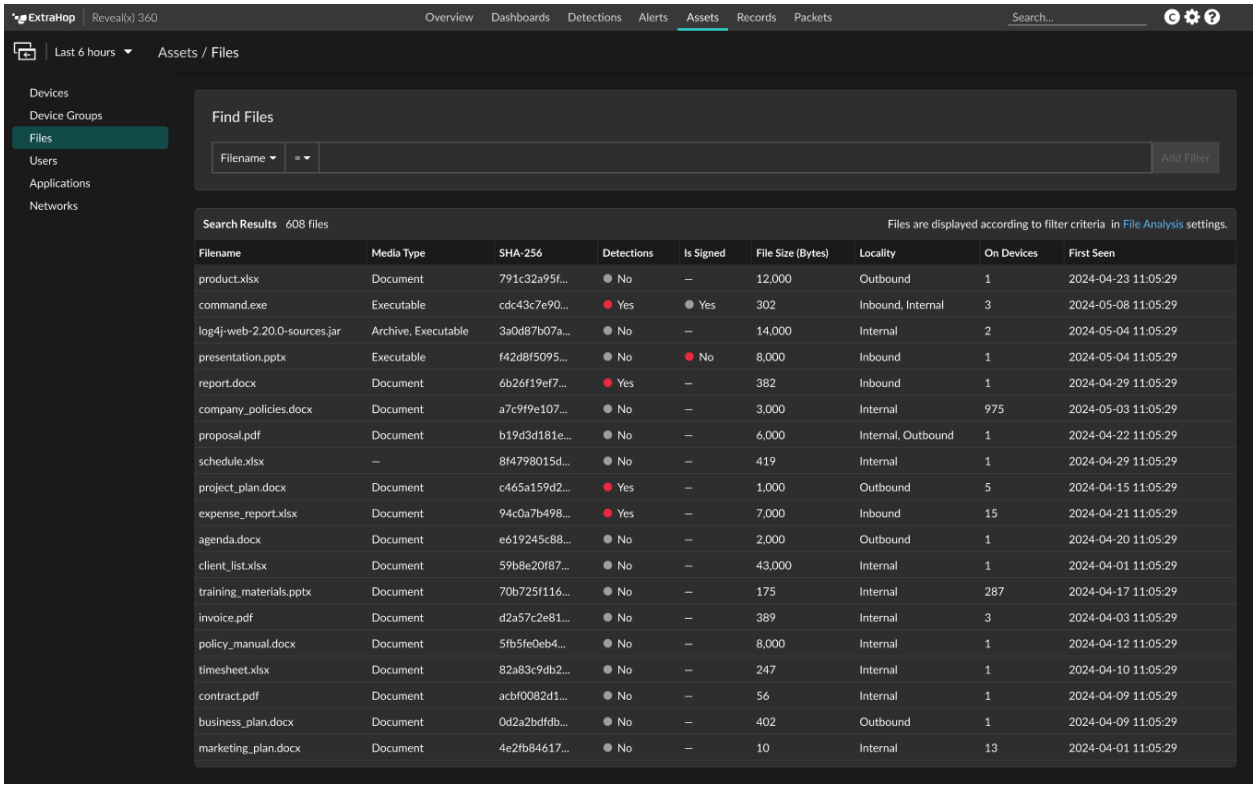
Nächste Schritte

- Auf der Seite „Assets“ Geräte finden nach Netzwerklokalität.
- Drilldown zu einer Metrik nach Client, Server oder IP-Adresse und wähle Intern oder Extern als Netzwerklokalität im Dreifeld-Filter aus.
- Filtern Sie Datensätze, indem Sie einen der folgenden Filter angeben:
  - Name der Netzwerklokalität
  - Lokalitätsname des Client-Netzwerks
  - Lokalitätsname des Servernetzwerks
  - Lokalitätsname des Absendernetzwerks
  - Lokalitätsname des Empfängernetzwerks

Dateien

Metadaten aus Hash-Dateien sind ein wertvolles Tool zur Identifizierung von Malware und Risiken in Ihrem Netzwerk. Beispielsweise sind Dateien, die von mehreren Geräten heruntergeladen wurden, Dateien mit einer Erweiterung, die nicht dem Medientyp entspricht, unsignierte Dateien oder große ausgehende oder eingehende Dateiübertragungen Beobachtungen, die es wert sind, untersucht zu werden. Auf der Seite „Dateien“ wird eine Tabelle mit Hash-Dateien und zugehörigen Dateidetails angezeigt, die Sie filtern und durchsuchen können. Um die Seite „Dateien“ anzuzeigen, klicken Sie auf **Vermögenswerte** aus dem oberen Navigationsmenü und klicken Sie dann auf **Dateien** Diagramm.

Dateien werden mit dem SHA-256-Hashing-Algorithmus gehasht und in der Tabelle „Dateien“ gemäß den Filterkriterien angezeigt, die in der Einstellungen für die Dateianalyse. Sie können Filter hinzufügen in Dateien finden Abschnitt, um die Ergebnisse in der Tabelle Dateien zu verfeinern.

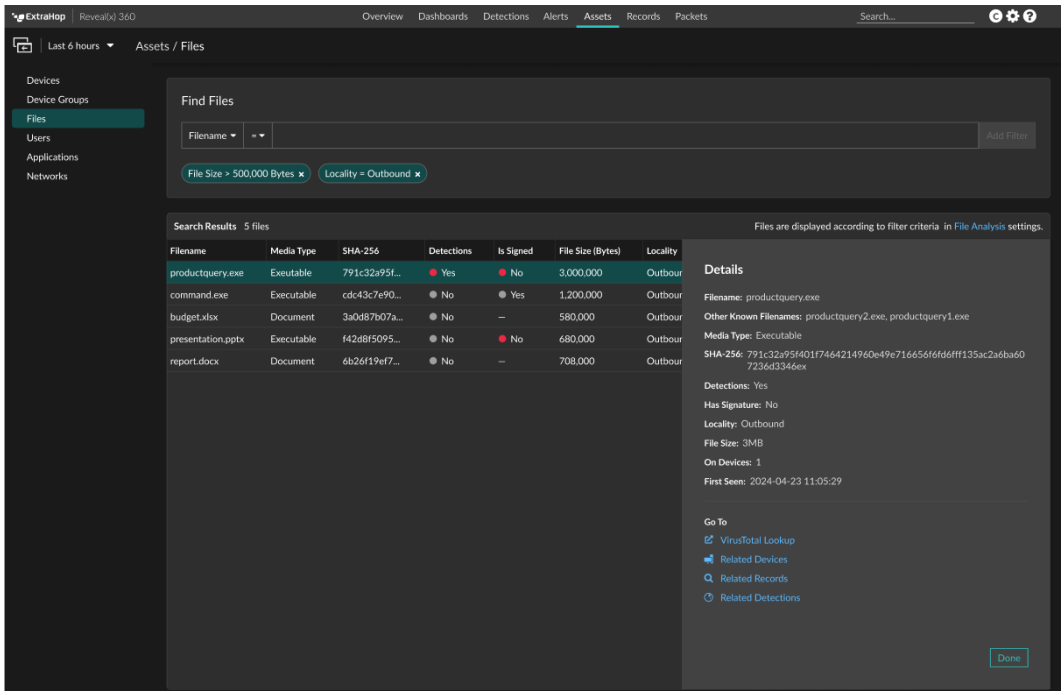


In der Tabelle Dateien werden die folgenden Details für jede Datei angezeigt.

Detail der Datei	Beschreibung
Dateiname	Der Name der Hash-Datei. Andere Dateinamen, die von demselben SHA-256-Hashing-Algorithmus zurückgegeben werden, werden im Detailbereich angezeigt.
Art des Mediums	Der Medientyp der Hash-Datei. Unterstützte Dateitypen sind Dokument, Archiv und Ausführbar. Das ExtraHop-System bestimmt den Datei-Medientyp, indem es Muster im Header und in den Anfangsbytes der Dateinutzlast analysiert.

Detail der Datei	Beschreibung
SHA-256	Der SHA-256-Datei-Hashing-Algorithmus wurde auf die Datei angewendet. Tipp: Du kannst findet Geräte, die bestimmten Hash-Dateien zugeordnet sind indem Sie den SHA-256-Filter zu einer Gerätesuche hinzufügen.
Erkennungen	Gibt an, ob die Hash-Datei an einer Erkennung beteiligt war, die einem Indikator in einer Bedrohungssammlung entsprach, z. B. einer Übertragung bösartige Datei. (Nur auf einer Konsole verfügbar, die an einen Sensor des Intrusion Detection System (IDS) angeschlossen ist, für Benutzer mit NDR-Modulzugriff)
Ist signiert	Gibt an, ob eine Signatur in der Hash-Datei beobachtet wurde, überprüft aber nicht, ob die Signatur gültig ist.
Größe der Datei	Die Größe der Hash-Datei in Byte.
Lokalität	Die Lokalität oder Flussrichtung der Hash-Datei. Unterstützte Orte sind Inbound, Outbound und Internal.
Auf Geräten	Die Anzahl der Geräte, auf denen die Hash-Datei beobachtet wurde.
Zuerst gesehen	Der Zeitstempel, zu dem die Hash-Datei zum ersten Mal beobachtet wurde.

Klicken Sie auf eine Datei in der Tabelle, um den Detailbereich zu öffnen und mehrere Links anzuzeigen, mit denen Sie den SHA-256-Datei-Hash untersuchen können.



- Klicken Sie **VirusTotal-Suche** um zur VirusTotal-Site zu navigieren und den Datei-Hash auf bösartige Inhalte zu überprüfen.
- Klicken Sie **Verwandte Geräte** um Geräte nach dem Datei-Hash zu filtern und Ergebnisse auf der Geräte Seite.
- Klicken Sie **Verwandte Datensätze** um Datensätze nach dem Datei-Hash zu filtern und Ergebnisse auf der Aufzeichnungen Seite.
- Klicken Sie **Verwandte Erkennungen** um Erkennungen nach dem Datei-Hash zu filtern und die Ergebnisse auf der Erkennungen Seite. (Nur auf einer Konsole verfügbar, die an einen IDS-Sensor (Intrusion Detection System) angeschlossen ist, für Benutzer mit Zugriff auf das NDR-Modul.)

Dateianalyse konfigurieren

Mithilfe der Dateianalyse können Sie Dateien angeben, die mit dem SHA-256-Hashing-Algorithmus gehasht werden sollen. Datei-Hashes, die einer Bedrohungssammlung entsprechen, generieren eine Erkennung, und Datei-Hashdaten können in Datensätzen abgefragt werden.

ExtraHop empfiehlt, dass Sie diese Einstellungen über eine ExtraHop-Konsole verwalten. Dies ist die Standardkonfiguration in RevealX 360. Bei RevealX Enterprise verwalten Sensoren diese Einstellungen standardmäßig. Wenn Sie die Einstellungen lieber auf einer Konsole statt auf einem Sensor verwalten möchten, können Sie die Verwaltung auf eine Konsole übertragen.

Voraussetzungen

- Sie benötigen System- und Zugriffsadministration oder Systemadministration (nur RevealX 360) Benutzerrechte.

Konfigurieren Sie eine Größenbeschränkung für Dateifilter

Sie können eine Größenbeschränkung angeben, die global für alle Dateifilter gilt. Jede Datei, die dieses Limit überschreitet, wird nicht gehasht.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Datei-Analyse**.
3. In der Größenbeschränkung (MB) Feld, geben Sie eine Dateigröße in MB an.

   Der Bereich reicht von 1 bis 1.000.000 MB. Der Standardwert ist 10 MB.
4. Klicken Sie **Speichern**.

Erstellen Sie einen Dateifilter

Sie können benutzerdefinierte Dateifilter erstellen, die bestimmen, welche Dateien auf dem ExtraHop-System gehasht werden. Der ExtraHop Default-Filter wird automatisch aktiviert und so konfiguriert, dass er ausführbare Mediendateien und Dateien hasht, die auf allen Protokollen, Lokalisationen und Dateierweiterungen beobachtet werden, die von der Dateianalyse unterstützt werden. Sie können den Standardfilter deaktivieren, aber Sie können die Filterkonfiguration nicht ändern.

Hinweis: Das Aktivieren einer großen Anzahl benutzerdefinierter Dateifilter kann sich auf die Systemleistung auswirken.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Datei-Analyse**.
3. In der Dateifilter Abschnitt, klicken **Filter hinzufügen**.
4. In der Name Feld, geben Sie einen eindeutigen Namen für den Filter ein.
5. Aus dem **Protokoll** Wählen Sie in der Dropdownliste eine der folgenden Protokolloptionen aus:
   - Beliebiges Protokoll (Standard)

- HTTP
- SMP
- FTP

Auswahl **Irgendein Protokoll** hasht nur Dateien, die auf HTTP-, SMB- oder FTP-Protokollen beobachtet wurden.

6. Aus dem **Lokalität** Wählen Sie in der Dropdownliste eine der folgenden Optionen für die Flussrichtung aus:
   - Beliebiger Ort (Standard)
   - Eingehend
   - Intern
   - Ausgehend
7. In der Format der Datei Abschnitt, wählen Sie den Typ der zu filternden Dateien aus:
   - Um nach Medientyp zu filtern, klicken Sie auf **Art des Mediums**, und wählen Sie dann eine der folgenden Medienoptionen aus:
     - Archiv
     - Dokument
     - Ausführbar
   - Um nach Dateierweiterung zu filtern, klicken Sie auf **Dateierweiterung**, und geben Sie dann eine oder mehrere Dateierweiterungen ein, getrennt durch ein Komma. Sie können Erweiterungen in einem der folgenden Formate eingeben: `txt` oder `.txt`.
8. Wählen Sie im Abschnitt Optionen die **Dateifilter aktivieren** Kontrollkästchen, um den Filter zu aktivieren und mit dem Hashing von Dateien zu beginnen, die den Kriterien entsprechen.
9. Optional: Wenn der Dateifilter aktiviert ist, können Sie den **Hash-Dateien in der Tabelle „Dateien“ anzeigen** Kontrollkästchen zur Anzeige von Hash-Dateien und zugehörigen Metadaten in der Die Tabelle „Dateien“ ist auf der Seite „Assets“ verfügbar.
10. Klicken Sie **Speichern**.

Übertragungsverwaltung von Dateianalyseeinstellungen

Für RevealX 360 verwalten ExtraHop-Konsolen standardmäßig die Dateianalyseeinstellungen. Für RevealX Enterprise verwalten ExtraHop-Sensoren diese Einstellungen.

Sie können sich an einer Konsole anmelden und die Verwaltung der Dateianalyseeinstellungen auf einen Sensor übertragen, oder Sie können sich bei einem Sensor anmelden und die Verwaltung an eine Konsole übertragen.

Hinweis: Durch die Übertragung der Verwaltung für diese Einstellungen wird auch die Verwaltung für alle übertragen. geteilte Einstellungen.

1. Melden Sie sich bei der Konsole oder dem Sensor an, der derzeit die Dateianalyseeinstellungen verwaltet, über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Datei-Analyse**.
3. Übertragung der Verwaltung der Dateianalyse auf ein anderes System.

Option	Description
Übertragung vom Sensor zur Konsole	1. klicken **Verwaltung von Transfers**. 2. Aus dem **Konsole verwalten** Wählen Sie in der Dropdownliste einen Konsolennamen aus.
Transfer von der Konsole zum Sensor	1. klicken ***N* von *N* angeschlossene Sensoren**. Im Fenster Verwaltungseinstellungen werden eine Liste der Sensoren angezeigt, für die die Konsole gemeinsame

Option	Description
	Einstellungen verwaltet, und eine Liste der Sensoren, die ihre eigenen Einstellungen verwalten. 2. Klicken Sie auf den Namen des Sensor, dessen Einstellungen Sie selbst verwalten möchten. 3. Loggen Sie sich in den Sensor ein. 4. klicken **Verwaltung von Transfers**. 5. Aus dem **Konsole verwalten** Dropdownliste, wählen **Sensorgerät — Selbst**.

Prioritäten der Analyse

Das ExtraHop-System analysiert den Verkehr und sammelt Daten von allen erkannten Geräten auf einem einzigen Sensor. Jedes erkannte Gerät erhält eine Analyseebene, die bestimmt, welche Daten und Metriken für ein Gerät erfasst werden. Analyseprioritäten bestimmen, welche Analysestufe ein Gerät erhält.

Wichtig: Analyseprioritäten können sein zentral verwaltet von einer Konsole aus.

Video: Sehen Sie sich die entsprechende Schulung an: Analyse-Prioritäten

Geräte und Gruppen priorisieren

Das ExtraHop-System kann Hunderttausende von Geräten analysieren und automatisch bestimmen, welche Analysestufe jedes Gerät erhält. Sie können jedoch steuern, welche Geräte für Advanced und Standard Analysis priorisiert werden.

Die meisten Geräte können zu einer Beobachtungsliste hinzugefügt werden, um Erweiterte Analyse sicherzustellen, oder Sie können Gerätegruppen zu einer geordneten Liste hinzufügen, um sie für Advanced Analysis und Standard Analysis zu priorisieren.

Hier sind einige wichtige Überlegungen zur Priorisierung von Geräten anhand der Beobachtungsliste:

- Geräte bleiben auf der Beobachtungsliste, auch wenn sie inaktiv sind, aber es werden keine Messwerte für inaktive Geräte erfasst.
- Die Anzahl der Geräte auf der Beobachtungsliste darf Ihre Erweiterte Analyse Analysis-Kapazität nicht überschreiten.
- Geräte können der Beobachtungsliste nur von einer Geräteeigenschaftenseite oder der Gerätelistenseite aus hinzugefügt werden. Sie können der Beobachtungsliste keine Geräte von der Seite Analyseprioritäten aus hinzufügen.
- Wenn Sie mehrere Geräte zur Beobachtungsliste hinzufügen möchten, empfehlen wir Ihnen eine Gerätegruppe erstellen und dann priorisieren Sie diese Gruppe für Advanced Analysis .
- Geräte, die L2 Parent Analysis oder Flow Analysis empfangen, können nicht zur Beobachtungsliste hinzugefügt werden.

Hier sind einige wichtige Überlegungen zur Priorisierung von Gerätegruppen:

- Ordnen Gerät Gerätegruppen von der höchsten zur niedrigsten Priorität in der Liste an.
- Klicken und ziehen Sie Gruppen, um ihre Reihenfolge in der Liste zu ändern.
- Stellen Sie sicher, dass jedes Gerät in der Gruppe aktiv ist. Gruppen, die eine große Anzahl von Geräten enthalten, beanspruchen Kapazität und inaktive Geräte generieren keine Messwerte.
- Sie können nicht mehr als 200 Gerätegruppen für jede Ebene priorisieren.

Standardmäßig füllt das ExtraHop-System die Stufen Advanced und Standard Analysis automatisch bis zur maximalen Kapazität aus. Hier sind einige wichtige Überlegungen zu den Kapazitätsniveaus und der automatischen Fülloption:

- Geräte, die in der Beobachtungsliste oder über eine priorisierte Gruppe priorisiert wurden, füllen zuerst die höheren Analysestufen und dann die Geräte, die am frühesten entdeckt wurden.
- Geräte werden für die erweiterte Analyse priorisiert, wenn das Gerät mit bestimmten Erkennungen verknüpft ist, wenn das Gerät eine externe Verbindung akzeptiert oder initiiert hat oder wenn auf dem Gerät gängige Angriffstools ausgeführt werden.
- Geräteeigenschaften wie Rolle, Hardware und Software, Protokollaktivität, Erkennungsverlauf und hoher Wert können ebenfalls die Analysestufen bestimmen.
- Die Option Automatisch ausfüllen ist standardmäßig aktiviert. Wenn diese Option deaktiviert ist, werden alle Geräte entfernt, die sich nicht in priorisierten Gruppen oder in der Beobachtungsliste befinden, und das ExtraHop-System legt die Priorität für jedes Gerät fest.

- Ihr ExtraHop-Abonnement und Ihre Lizenz bestimmen die maximale Kapazität.

Sehen Sie die Häufig gestellte Fragen zu Analyseprioritäten um mehr über Kapazitäten auf Analyseebene zu erfahren.

Analysestufen vergleichen

Analyseebene	Funktionen	So erhalten Sie dieses Level
Entdeckungsmodus	• Erkennungen • Beobachtete Protokolle • IP-Adressen • Authentifizierte Benutzer • Software • Marke und Modell der Hardware	Geräte erhalten automatisch den Entdeckungsmodus, wenn sie sich nicht in Standard, Advanced oder L2 Parent Analysis befinden.
Standardanalyse	• L2-L3-Metriken • Karten mit Aktivitäten • Erkennungen • Beobachtete Protokolle • IP-Adressen • Authentifizierte Benutzer • Software • Marke und Modell der Hardware	Gerätegruppen für die Standardanalyse priorisieren.
Erweiterte Analyse	• L2-L7-Metriken • Benutzerdefinierte Metriken • Karten mit Aktivitäten • Erkennungen • Beobachtete Protokolle • IP-Adressen • Authentifizierte Benutzer • Software • Marke und Modell der Hardware	Gerätegruppen für Erweiterte Analyse priorisieren oder einzelne Geräte zur Beobachtungsliste hinzufügen.
L2-Elternanalyse (Gilt nur, wenn L3-Entdeckung ist aktiviert)	• L2-L3-Metriken • Karten mit Aktivitäten	L2-Elterngeräte erhalten automatisch L2 Parent Analysis, mit Ausnahme von Gateways und Routern.
Strömungsanalyse	• L2-L3-Metriken • Karten mit Aktivitäten • Beobachtete Protokolle • IP-Adresse • Eigenschaften der Cloud-Instanz • Eingeschränkte Erkennungsarten	Geräte erhalten automatisch eine Durchflussanalyse, wenn sie auf einem Flusssensor entdeckt werden.

Transfermanagement der Analyseprioritäten

Jeder Paketsensor kann seine eigenen Analyseprioritäten verwalten, die bestimmen, welche Geräte empfangen Erweiterte Analyse oder Standardanalyse. Wenn Ihr Sensor an eine Konsole angeschlossen ist, können Sie die Prioritätsverwaltung auf diese Konsole übertragen, um eine zentrale Ansicht dieser Einstellungen zu erhalten.

Hier sind einige wichtige Überlegungen zur Übertragung der Verwaltung:

- Sie müssen über volle Schreibrechte verfügen, um Analyseprioritäten bearbeiten zu können.
- Nach der Übertragung des Managements auf einen Konsole, alle weiteren Änderungen, die Sie an einzelnen Sensoren vornehmen, sind inaktiv. Sehen Sie, welche andere Einstellungen werden ebenfalls übertragen.
- Die Einstellungen für Analyseprioritäten sind für Durchflusssensoren nicht verfügbar. Die Verwaltung kann nicht übertragen werden.

Die folgenden Schritte zeigen Ihnen, wie Sie das Prioritätsmanagement an einen übertragen Konsole:

1. Loggen Sie sich in das ExtraHop-System ein.

   Wiederholen Sie diese Schritte für jeden Sensor in Ihrer Umgebung.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Prioritäten der Analyse**.
3. Klicken Sie oben auf der Seite auf das Konsole Dropdownliste und wählen Sie die Konsole aus, auf die Sie die Verwaltung übertragen möchten.
4. Klicken Sie **Übertragung**.

Hinweis: Um Analyseunterbrechungen zu vermeiden, können Sie einen Entwurf der Einstellungen für die Analyseprioritäten für jeden Sensor speichern, bevor Sie die Verwaltung an eine Konsole übertragen.

Priorisieren Sie Gruppen für Erweiterte Analyse

Sie können Gerätegruppen für Erweiterte Analyse auf der Grundlage ihrer Bedeutung für Ihr Netzwerk angeben. Die Gruppen werden in einer geordneten Liste geordnet.

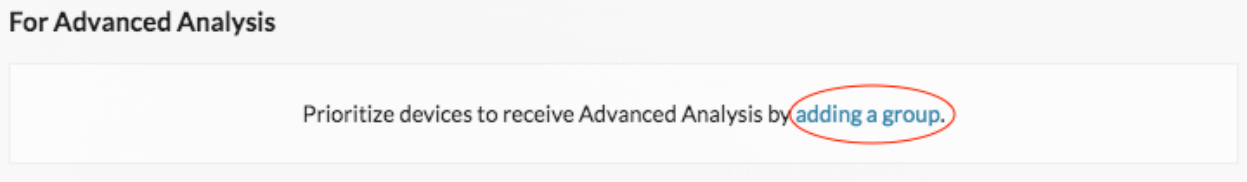
Hier sind einige wichtige Überlegungen zu Erweiterte Analyse:

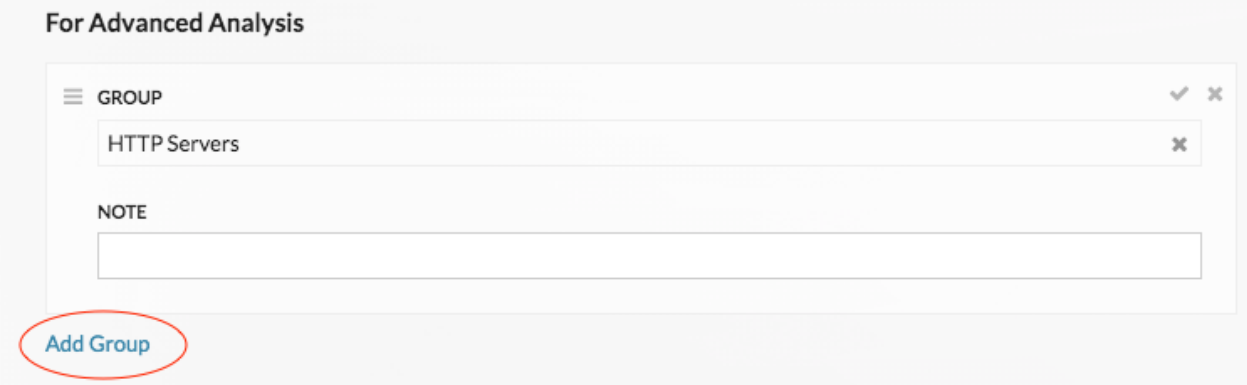
- Geräte auf dem Beobachtungsliste sind garantiert Erweiterte Analyse und haben Vorrang vor Gerätegruppen.
- Geräte innerhalb einer Gerätegruppe, die inaktiv sind, wirken sich nicht auf die Kapazität von Erweiterte Analyse aus.
- Benutzerdefinierte Metriken sind nur für Geräte in Erweiterte Analyse verfügbar. Wenn Sie benutzerdefinierte Messwerte für ein bestimmtes Gerät sehen möchten, priorisieren Sie eine Gruppe, die das Gerät enthält, oder fügen Sie das Gerät zur Beobachtungsliste hinzu.
- Sie benötigen volle Schreibberechtigungen, um Analyseprioritäten bearbeiten zu können.
- Sie können nicht mehr als 200 Gerätegruppen für Erweiterte Analyse priorisieren.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.

   (Diese Schritte müssen auf der Konsole oder Sensor, das ist Verwaltung dieser gemeinsamen Einstellungen.)
2. Gehen Sie zu den Einstellungen für Standardprioritäten.
   - Klicken Sie auf einer Konsole auf das Symbol Systemeinstellungen und dann klicken **Prioritäten der Analyse**. Dann klicken Sie **Prioritäten bearbeiten** neben dem Sensor, den Sie ändern möchten.
   - Klicken Sie auf einem Sensor auf das Symbol Systemeinstellungen und dann klicken **Prioritäten der Analyse**.

3. Priorisieren Sie Gruppen, indem Sie die folgenden Schritte ausführen:
   a) In der Für Erweiterte Analyse Abschnitt, klicken **eine Gruppe hinzufügen** um die erste Gruppe hinzuzufügen oder **Gruppe hinzufügen** um weitere Gruppen hinzuzufügen.





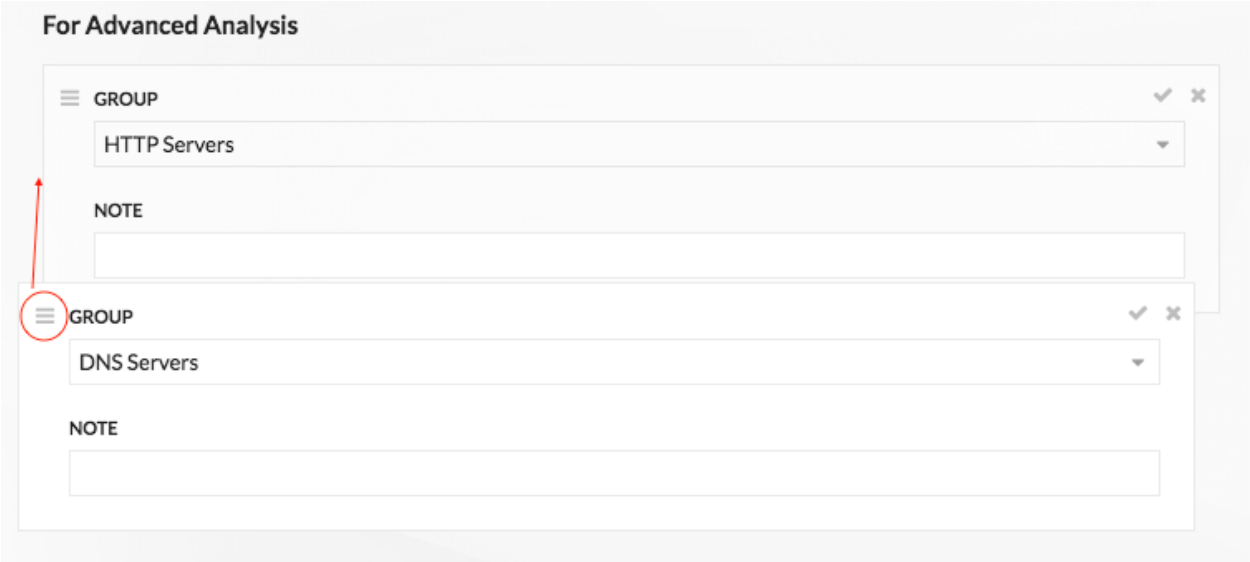
   b) In der **Gruppe** Dropdownliste, geben Sie den Namen einer Gerätegruppe ein und klicken Sie dann in den Suchergebnissen auf den Gruppennamen. Geben Sie beispielsweise `HTTP-Server` und wählen Sie **HTTP-Server** Gerätegruppe.
   c) Optional: In der **Hinweis** Feld, geben Sie Informationen über die Gruppe ein.
4. In der Automatisch füllen Abschnitt, vergewissern Sie sich **Auf** ist ausgewählt.

   Hinweis: Wenn Ihr System Leistungsprobleme hat, klicken Sie auf **Aus**. Nur Geräte, die sich in priorisierten Gruppen oder auf der Beobachtungsliste befinden, erhalten die erweiterte Analyse.
5. Klicken Sie oben auf der Seite auf **Speichern**.

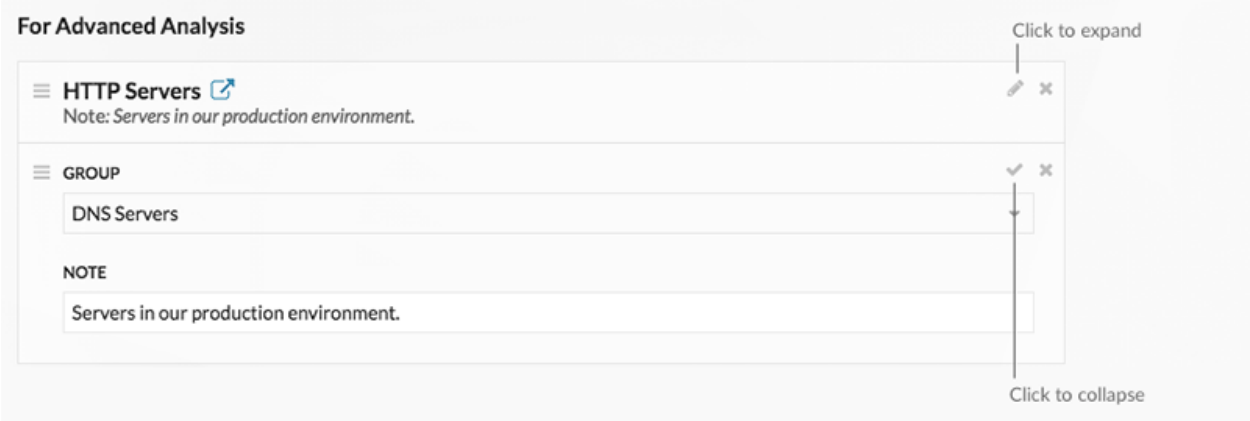
Nächste Schritte

Im Folgenden finden Sie einige zusätzliche Möglichkeiten, Gruppen, die Advanced Analysis erhalten, zu verwalten und zu verfeinern:

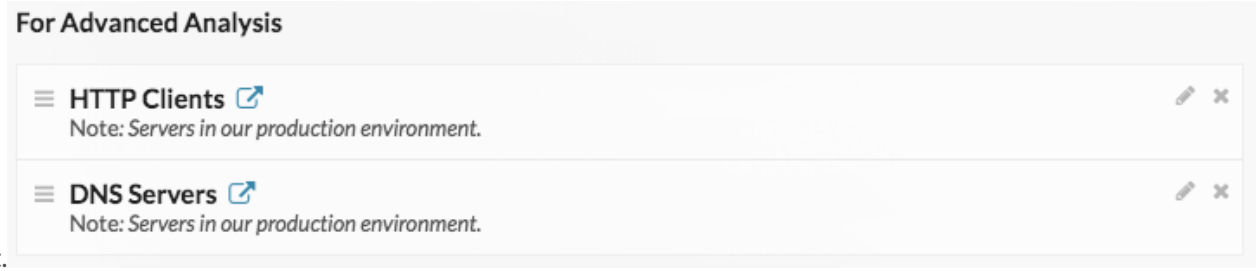
- Wenn Sie mehrere Gruppen hinzufügen, werden die Gruppen von oben nach unten priorisiert. Klicken Sie auf das Symbol oben links neben Gruppe, und ziehen Sie die Gruppe dann an eine andere Position in der sortierten Liste.



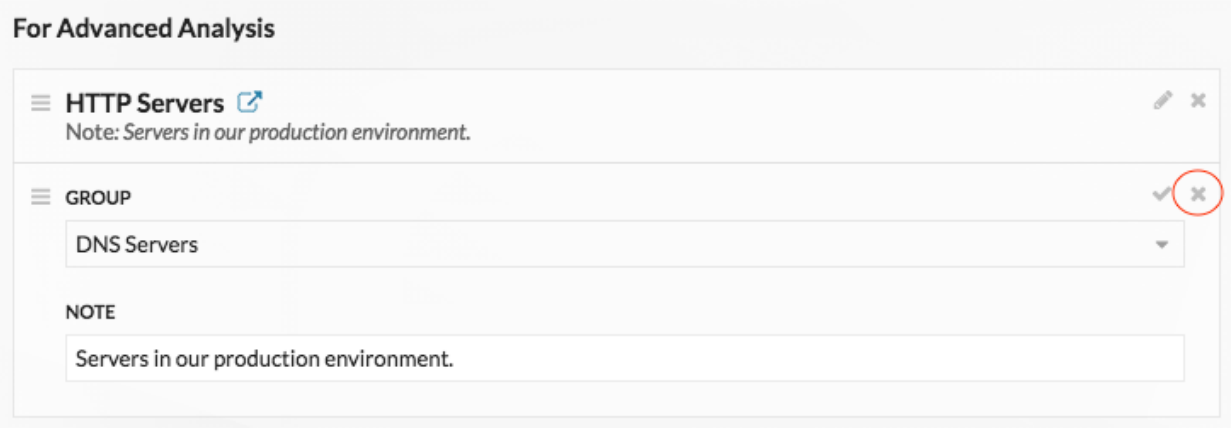
- Klicken Sie auf den Scheck Symbol, um die Gruppe zu reduzieren. Klicke auf den Stift Symbol, um die Gruppe erneut zu erweitern, wie in der folgenden Abbildung dargestellt.



- Klicken Sie auf Gehe zu Symbol neben einem Gruppennamen, um zur Gerätegruppenseite zu navigieren. Auf der Gerätegruppenseite wird angezeigt, welche Geräte und wie viele Geräte sich in der Gruppe befinden. Das Symbol ist nur verfügbar, wenn die Gruppe ausgeblendet ist.



- Klicken Sie auf das X-Symbol, um eine Gruppe aus der Liste zu entfernen, wie in der folgenden Abbildung



dargestellt.

Priorisieren Sie Gruppen für die Standardanalyse

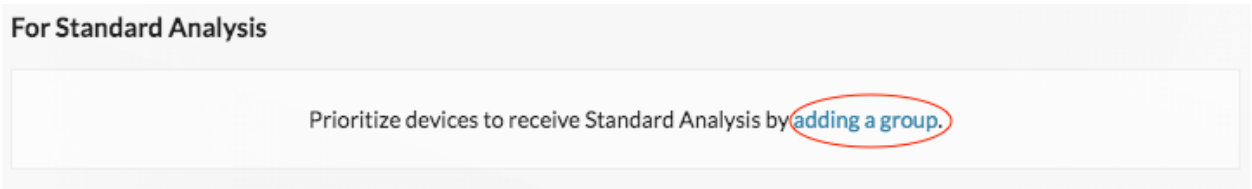
Sie können Gerätegruppen für die Standardanalyse auf der Grundlage ihrer Bedeutung für Ihr Netzwerk angeben. Die Gruppen werden in einer geordneten Liste geordnet.

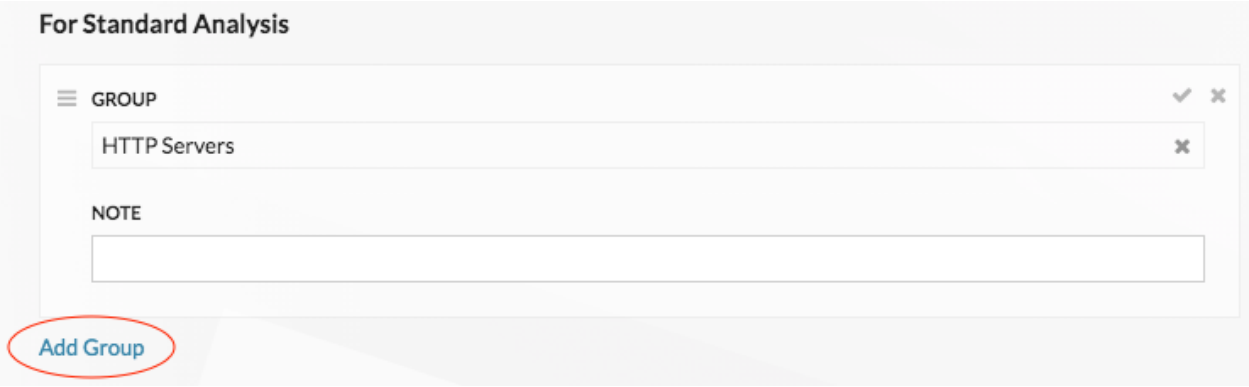
Hier sind einige wichtige Überlegungen zu Standardanalyse:

- Geräte, die für den Bereich Standardanalyse priorisiert wurden, erhalten die erweiterte Analyse, wenn genügend Kapazität vorhanden ist.
- Sie benötigen volle Schreibberechtigungen, um Analyseprioritäten bearbeiten zu können.
- Sie können nicht mehr als 200 Gerätegruppen für die Standardanalyse priorisieren.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.

   (Diese Schritte müssen auf der Konsole oder Sensor, das ist Verwaltung dieser gemeinsamen Einstellungen.)
2. Gehen Sie zu den Einstellungen für Standardprioritäten.
   - Klicken Sie auf einer Konsole auf das Symbol Systemeinstellungen und dann klicken **Prioritäten der Analyse**. Dann klicken Sie **Prioritäten bearbeiten** neben dem Sensor, den Sie ändern möchten.
   - Klicken Sie auf einem Sensor auf das Symbol Systemeinstellungen und dann klicken **Prioritäten der Analyse**.
3. Priorisieren Sie Gruppen, indem Sie die folgenden Schritte ausführen:
   a) In der Für Standardanalysen Abschnitt, klicken **eine Gruppe hinzufügen** um die erste Gruppe hinzuzufügen oder **Gruppe hinzufügen** um weitere Gruppen hinzuzufügen.





b) In der **Gruppe** Dropdownliste, geben Sie den Namen einer Gerätegruppe ein und klicken Sie dann in den Suchergebnissen auf den Gruppennamen. Geben Sie beispielsweise `HTTP-Server` und wählen Sie **HTTP-Server** Gerätegruppe.

c) Optional: In der **Hinweis** Feld, geben Sie Informationen über die Gruppe ein.

4. In der Automatisch füllen Abschnitt, vergewissern Sie sich **Auf** ist ausgewählt.

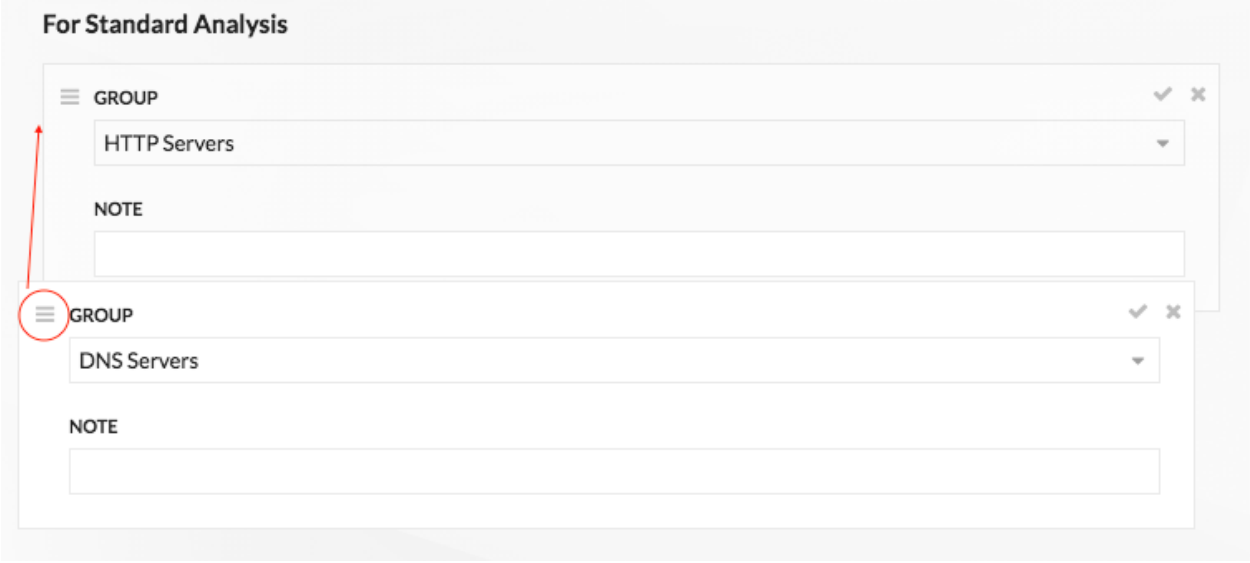
   Hinweis: Wenn Ihr System Leistungsprobleme hat, klicken Sie auf **Aus**. Nur Geräte, die sich in priorisierten Gruppen befinden, erhalten die Standardanalyse.

5. Klicken Sie oben auf der Seite auf **Speichern**.

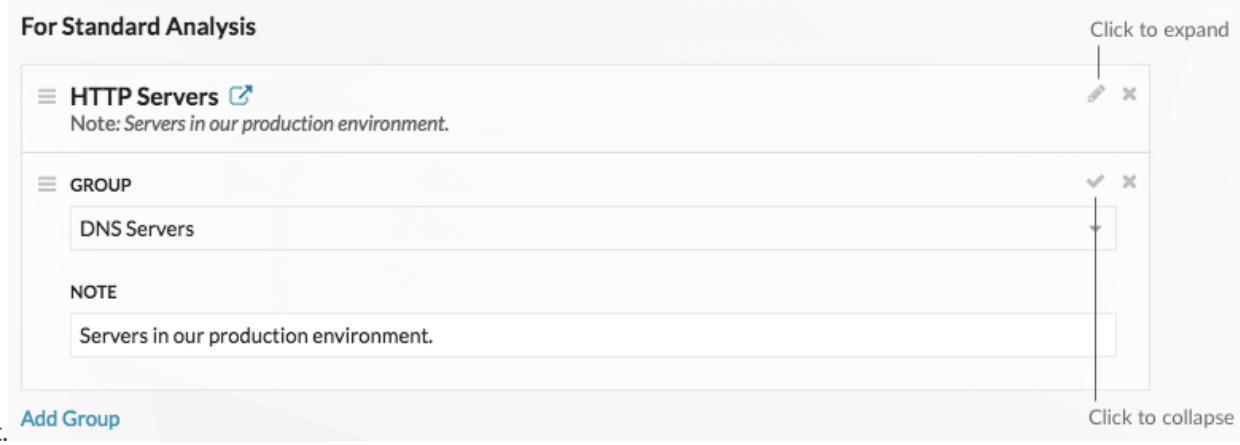
Nächste Schritte

Im Folgenden finden Sie einige zusätzliche Möglichkeiten, Gruppen, die Standardanalysen erhalten, zu verwalten und zu verfeinern:

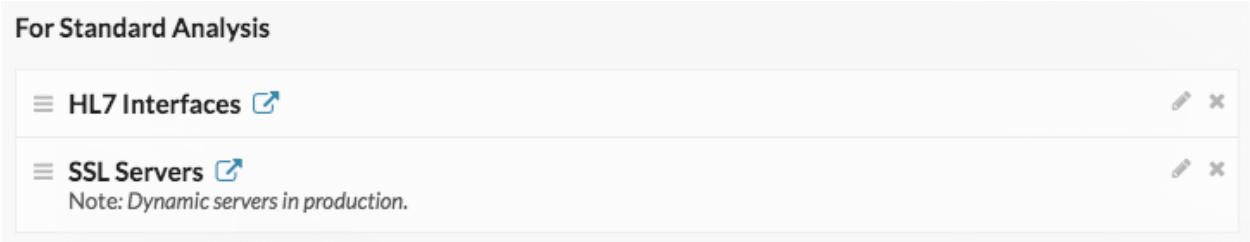
- Wenn Sie mehrere Gruppen hinzufügen, werden die Gruppen von oben nach unten priorisiert. Klicken Sie auf das Symbol oben links neben Gruppe, und ziehen Sie die Gruppe dann an eine andere Position in der sortierten Liste.



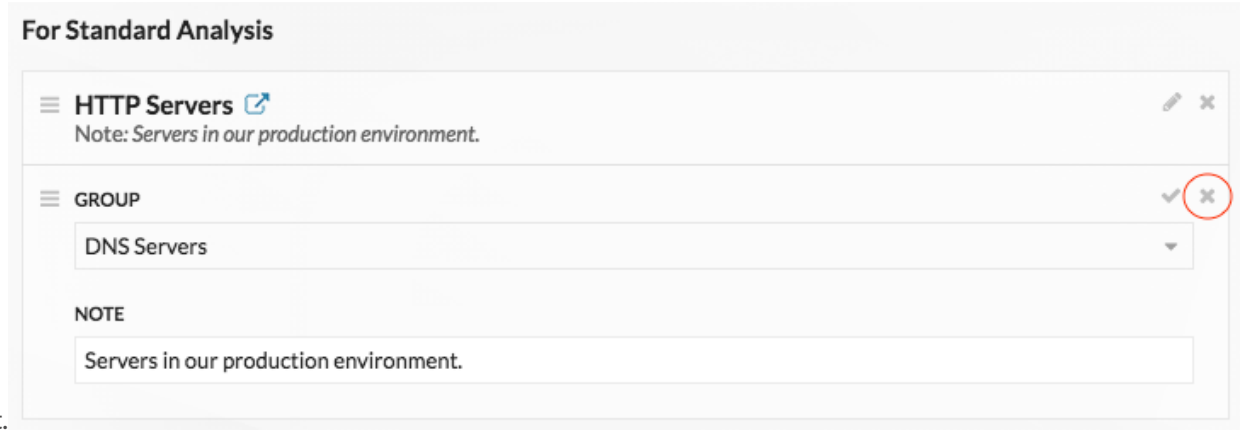
- Klicken Sie auf den Scheck Symbol, um die Gruppe zu reduzieren. Klicke auf den Stift Symbol, um die Gruppe erneut zu erweitern, wie in der folgenden Abbildung dargestellt.



- Klicken Sie auf Gehe zu Symbol neben einem Gruppennamen, um zur Gerätegruppenseite zu navigieren. Auf der Gerätegruppenseite wird angezeigt, welche Geräte und wie viele Geräte sich in der Gruppe befinden. Das Symbol ist nur verfügbar, wenn die Gruppe ausgeblendet ist.



- Klicken Sie auf das X-Symbol, um eine Gruppe aus der Liste zu entfernen, wie in der folgenden Abbildung dargestellt.

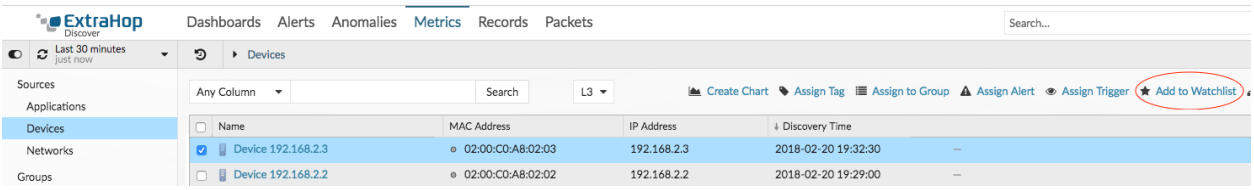


Gerät zur Beobachtungsliste hinzufügen

Fügen Sie Geräte zur Watchlist hinzu, um eine erweiterte Analyse zu gewährleisten. Sie können der Watchlist ein benutzerdefiniertes Gerät hinzufügen, aber Sie können der Watchlist kein übergeordnetes L2-Gerät hinzufügen, es sei denn, das Gerät ist ein Gateway oder Router, und Sie können in Flow Analysis kein Gerät hinzufügen. Geräte bleiben auf der Beobachtungsliste, egal ob sie inaktiv oder aktiv sind, aber ein Gerät muss aktiv sein, damit das ExtraHop-System Erweiterte Analyse Analysis-Metriken erfassen kann.

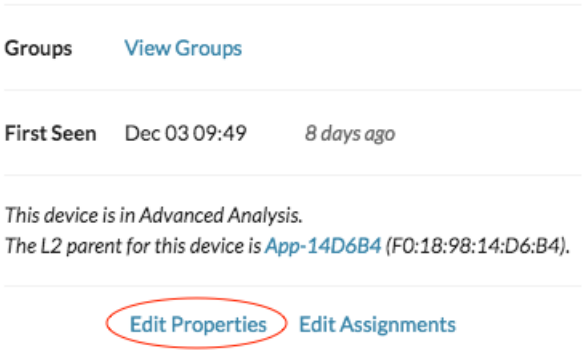
Hinweis: Anstatt mehrere Geräte zur Beobachtungsliste hinzuzufügen, eine Gerätegruppe erstellen und dann priorisieren Sie diese Gruppe für die erweiterte Analyse. Oder fügen Sie mehrere Geräte auf der Gerätelistenseite zur Beobachtungsliste hinzu. Klicken Sie auf das Kontrollkästchen

neben einem oder mehreren Geräten und dann auf das Symbol Zur Watchlist hinzufügen. ★ in der oberen rechten Ecke.



Erfahre mehr über Prioritäten der Analyse.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Vermögenswerte** und klicken Sie dann auf **Aktive Geräte** Diagramm.
3. Suchen Sie nach dem gewünschten Gerät und klicken Sie dann auf den Gerätenamen. Die Seite „ Geräteübersicht“ wird angezeigt, auf der die mit dem Gerät verbundenen Verkehrs- und Protokollmetriken angezeigt werden.
4. Klicken Sie **Eigenschaften bearbeiten**.



5. Klicken Sie **Dieses Gerät zur Beobachtungsliste hinzufügen**.
6. Klicken Sie **Erledigt**.

Ihr Gerät ist jetzt auf der Beobachtungsliste. Besuchen Sie die Watchlist-Seite, um ein Gerät von der Beobachtungsliste entfernen .

Ein Gerät von der Beobachtungsliste entfernen

Sie können Geräte, die auf der Beobachtungsliste stehen, von der Seite Analyseprioritäten entfernen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.

   (Diese Schritte müssen auf der Konsole oder Sensor, das ist Verwaltung dieser gemeinsamen Einstellungen .)
2. Gehen Sie zu den Einstellungen für Standardprioritäten.
   - Klicken Sie auf einer Konsole auf das Symbol Systemeinstellungen und dann klicken **Prioritäten der Analyse**. Dann klicken Sie **Prioritäten bearbeiten** neben dem Sensor, den Sie ändern möchten.
   - Klicken Sie auf einem Sensor auf das Symbol Systemeinstellungen und dann klicken **Prioritäten der Analyse**.
3. Oben auf der Seite in der Beobachtungsliste für Erweiterte Analyse Abschnitt, klicken **Sehen Sie sich die Watchlist an**. Die Beobachtungsliste Die Seite erscheint und zeigt alle Geräte auf der Beobachtungsliste an.
4. Gehen Sie wie folgt vor, um Geräte aus der Beobachtungsliste zu entfernen:

a) Markieren Sie das Kästchen neben dem Gerätenamen.
b) klicken **Geräte entfernen**.

5. klicken **Speichern**.

Hinweis: Es ist möglich, Geräte anhand ihrer eindeutigen MAC-Adressen zu einer Blockliste hinzuzufügen, indem die laufende Konfigurationsdatei auf dem ExtraHop-System geändert wird. Wenden Sie sich an Ihren ExtraHop-Administrator, um Geräte zu einer Blockliste hinzuzufügen.

Karten der Aktivitäten

Eine Aktivitätsdiagramm ist eine dynamische visuelle Darstellung der L4-L7-Protokollaktivität zwischen Geräten in Ihrem Netzwerk. Sie können ein 2D- oder 3D-Layout der Geräteverbindungen in Echtzeit sehen , um mehr über den Verkehrsfluss und die Beziehungen zwischen Geräten zu erfahren.

Aktivitätskarten können dir bei den folgenden Anwendungsfällen helfen:

Schließen Sie eine Rechenzentrum- oder Cloud-Migration ab

Im Rahmen Ihrer Migrationsstrategie müssen Sie festlegen, welche Dienste wann ausgeschaltet werden können. Mithilfe einer Aktivitätsdiagramm können Sie erkennen, welche Geräte noch verbunden sind, sodass Sie unerwartete Serviceunterbrechungen während des Migrationsprozesses verhindern können. Weitere Informationen finden Sie in der Planen und überwachen Sie Ihre Migration mit Activity Maps Komplettlösung.

Identifizieren Sie die Ursache für eine langsame Anwendung

Anwendungen hängen oft von mehreren Dienstebenen innerhalb eines Netzwerk ab. Mithilfe einer Aktivitätsübersicht können Sie die Lieferkette des Datenverkehrs zu Ihrem langsamen Anwendungsserver identifizieren. Klicken Sie auf ein Gerät, um verwandte Messwerte zu untersuchen, die mehr Aufschluss über die Ursache der Verlangsamung geben können.

Verfolgen Sie verdächtige Geräte oder unerwartete Verbindungen

Während eines Sicherheitsereignisses kann Ihnen eine Aktivitätsdiagramm dabei helfen, betroffene Geräte zu identifizieren, indem sie den Ost-West-Verkehr in Echtzeit verfolgt, der mit einem verdächtigen Gerät verbunden ist. Im Rahmen einer täglichen Sicherheitsüberwachungsstrategie können Sie eine Aktivitätsdiagramm erstellen, um zu bestätigen, dass Geräte keine unerwarteten Verbindungen zu anderen Geräten herstellen.

Hier sind einige wichtige Überlegungen zu Aktivitätskarten:

- Du kannst Aktivitätskarten erstellen für Geräte in den Bereichen Advanced, Standard, L2 Parent Analysis und Flow Analysis. Sie können keine Aktivitätsdiagramm für Geräte im Entdeckungsmodus erstellen. Weitere Informationen finden Sie unter Prioritäten der Analyse.
- Wenn Sie eine Aktivitätsdiagramm für ein Gerät oder eine Gerätegruppe erstellen, die während des ausgewählten Zeitintervalls keine Protokollaktivität aufweist, wird die Karte ohne Daten angezeigt. Ändern Sie das Zeitintervall oder Ihre Ursprungsauswahl und versuchen Sie es erneut.
- Sie können eine Aktivitätsdiagramm aus einem erstellen Konsole um die Geräteverbindungen aller Ihrer Sensoren anzuzeigen.
- Du kannst eine Aktivitätsdiagramm speichern und teilen , gewährt anderen Systembenutzern oder Gruppen Lese- oder Bearbeitungszugriff. Du kannst auch eine gespeicherte Aktivitätsdiagramm laden um die Karteneigenschaften zu ändern.

Weitere Informationen zu Aktivitätskarten finden Sie in der Häufig gestellte Fragen zu Aktivitätskarten.

Navigiere durch Aktivitätskarten

Nach eine Aktivitätskarte erstellen, können Sie mit der Untersuchung von Daten beginnen. In den folgenden Abschnitten finden Sie Informationen zur Interaktion mit einer Aktivitätsdiagramm und Informationen zu den Daten, die Sie sich gerade ansehen.

Grundriss

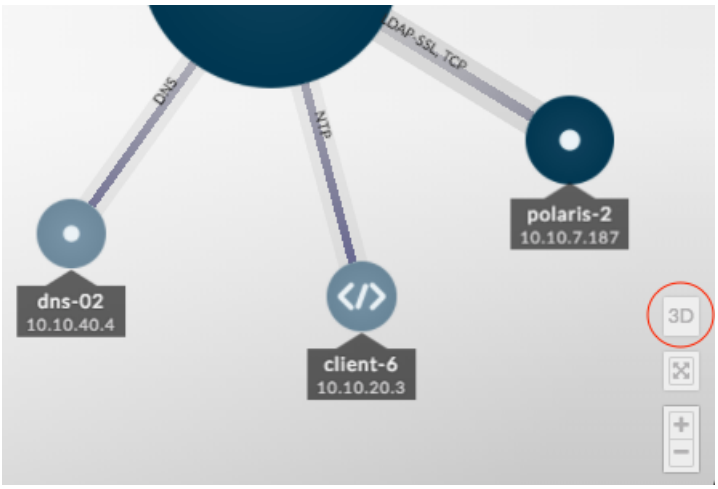
Geräte werden durch Kreise und Verbindungen durch Linien dargestellt.

Die Platzierung der Geräte ist für die Anzeige von Informationen optimiert. Das Layout kann sich ändern, wenn Daten zur Geräteaktivität in Echtzeit aktualisiert werden. Beispielsweise wird das Layout aktualisiert , wenn neue Verbindungen beobachtet werden oder Geräte inaktiv werden.

Hinweis: Wenn das Zeitintervall in der oberen linken Ecke der Seite auf Letzte 30 Minuten, Letzte 6 Stunden oder Letzter Tag eingestellt ist, werden die Aktivitätsdiagramm Map-Daten kontinuierlich jede Minute mit Echtzeitdaten aktualisiert. Legen Sie ein benutzerdefiniertes Zeitintervall mit einer bestimmten Start- und Endzeit fest, um Layoutaktualisierungen in Echtzeit zu stoppen.

2D- oder 3D-Layout

Standardmäßig werden Aktivitätskarten in einem 2D-Layout angezeigt, aber Sie können auf 3D klicken, um die Anzeige in ein rotierendes 3D-Modell zu ändern. Möglicherweise möchten Sie 3D-Karten auf einem großen Bildschirm in einem Netzwerk- oder Sicherheitszentrum präsentieren.

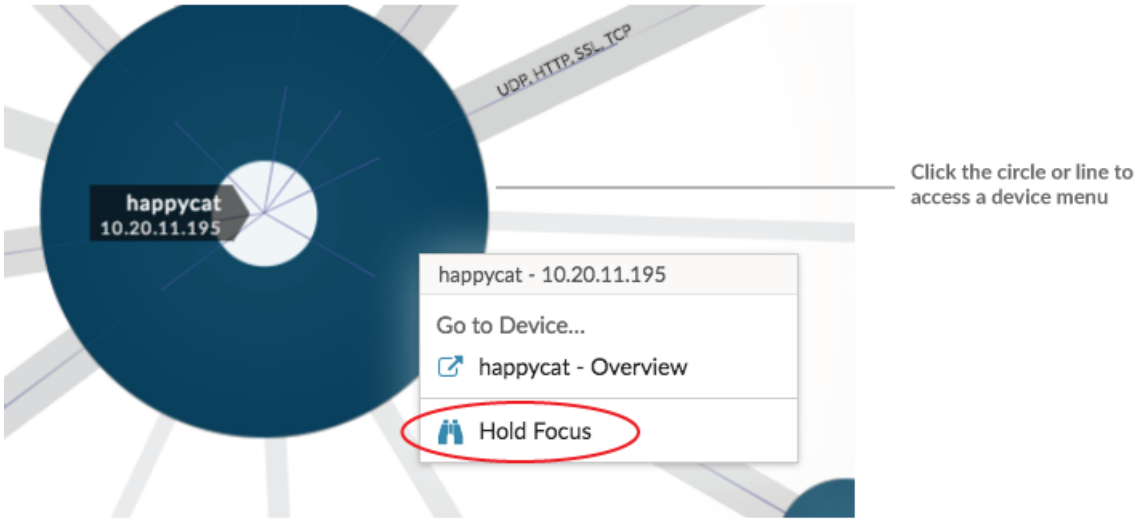


Neu positionieren, drehen und zoomen

Zoomen Sie mit den Steuerelementen in der unteren rechten Ecke der Seite in eine Karte hinein und heraus oder zoomen Sie mit dem Mausrad. Klicken und ziehen Sie mit der Maus, um eine 2D-Karte neu zu positionieren oder eine 3D-Karte zu drehen.

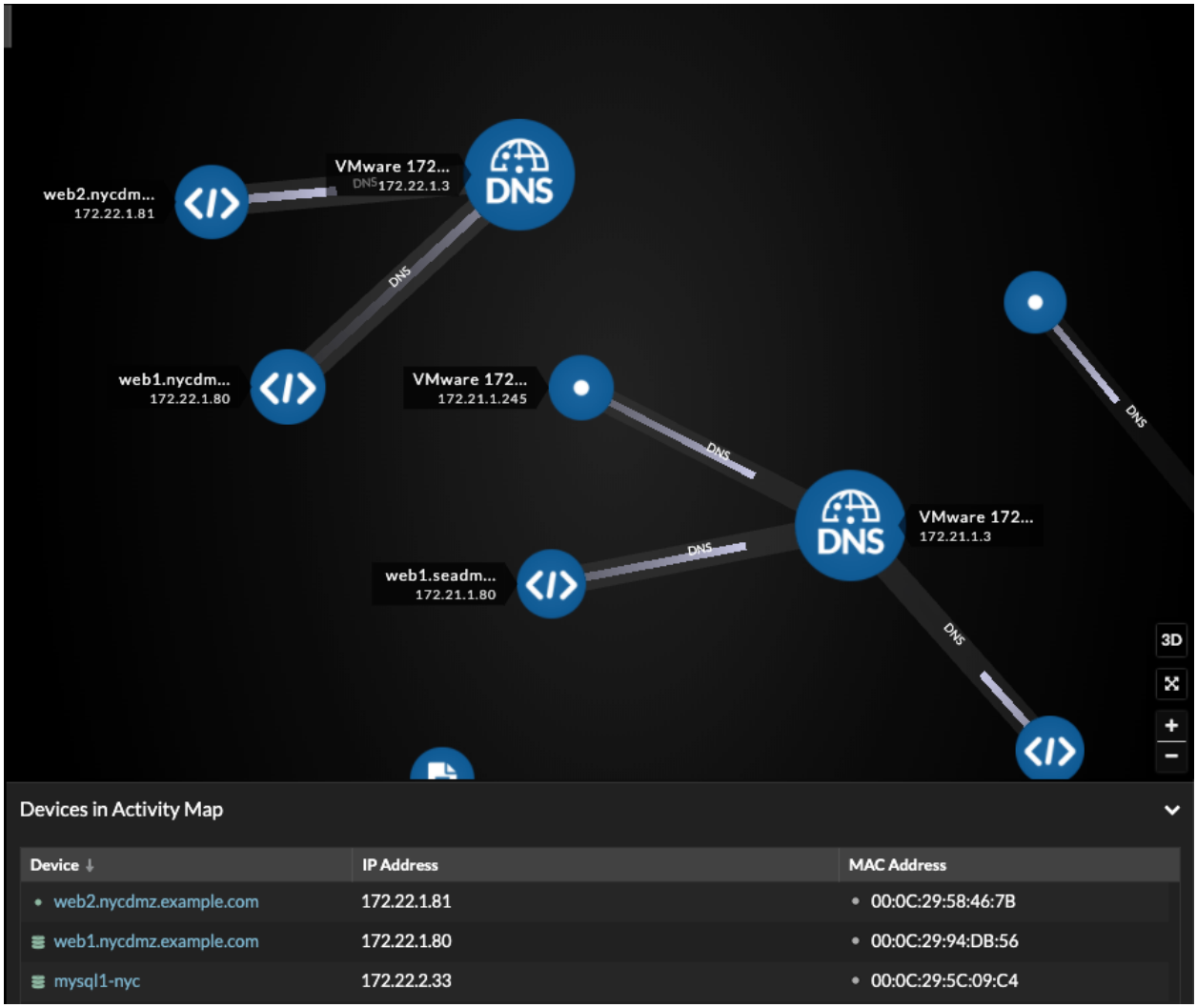
Fokus behalten

Klicken Sie auf ein beliebiges Gerät und wählen Sie **Fokus halten**. Sie können dann je nach Layout neu positionieren oder drehen und die Karte vergrößern oder verkleinern, während Sie sich auf das ausgewählte Gerät und seine unmittelbaren Gegenspieler konzentrieren.



Geräteliste anzeigen

klicken **Geräte in der Activity Map** unten auf der Seite, um eine Liste aller Geräte mit ihren Namen, IP-Adressen und MAC-Adressen anzuzeigen. Klicken Sie auf einen Gerätenamen, um zur Geräteseite zu navigieren.

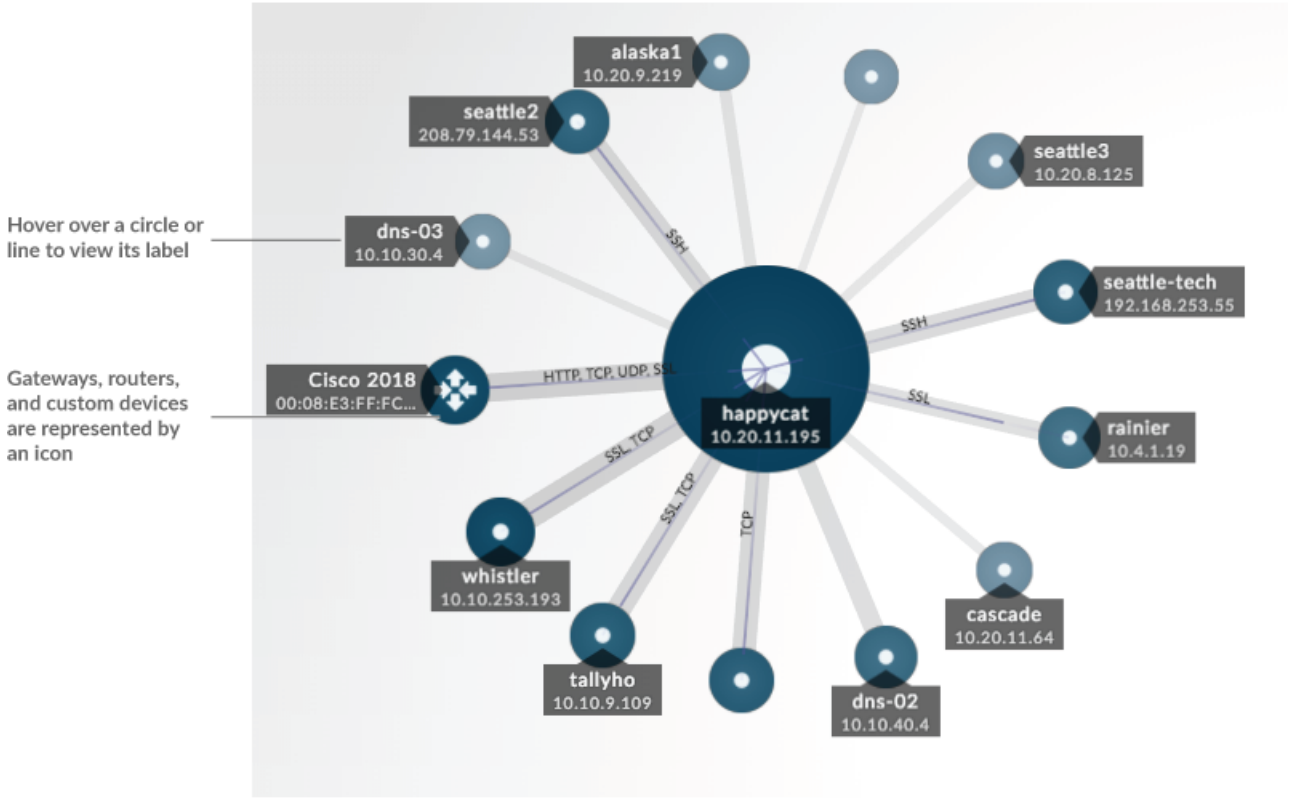


Beschriftungen und Icons

Kreisbeschriftungen enthalten Details wie den Hostnamen, die IP-Adresse oder die MAC-Adresse des Gerät.

Linienbeschriftungen enthalten Protokollnamen, die mit der Geräteverbindung und der Richtung des Datenverkehrs zwischen den Geräten verknüpft sind, was als animierte Impulse angezeigt wird. Spezifisch Geräterollen werden durch ein Symbol dargestellt.

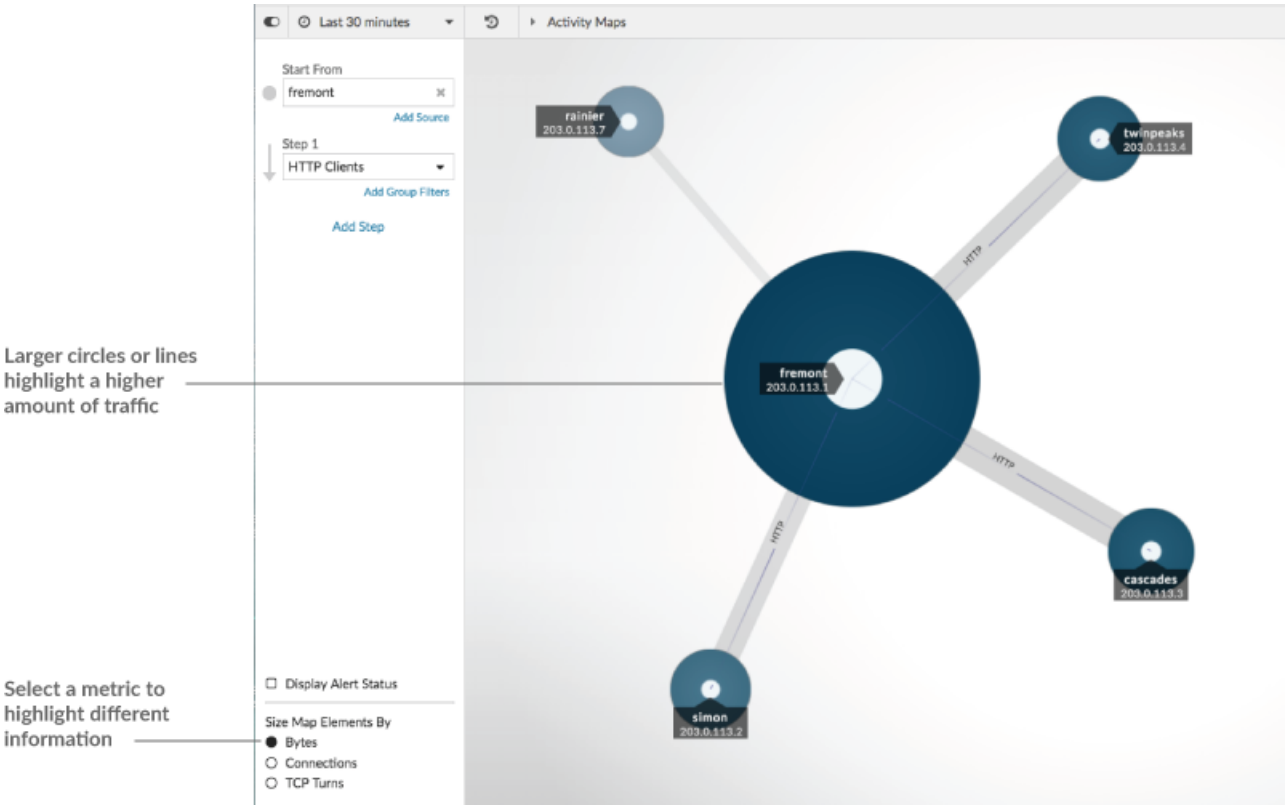
Um die Anzeige von Informationen zu optimieren, wird nicht jedes Etikett angezeigt. Bewegen Sie den Mauszeiger über einen Kreis oder eine Linie, um deren Bezeichnung anzuzeigen, wie in der folgenden Abbildung dargestellt.



Hinweis: Geräterollen werden einem Gerät automatisch zugewiesen, basierend auf der Art des Datenverkehrs, den das ExtraHop-System für dieses Gerät beobachtet. Weitere Informationen finden Sie unter Eine Geräterolle ändern.

Kreis- und Liniengröße

Die Größe der Objekte in der Karte entspricht einem Metrikwert, der dazu beiträgt, Bereiche mit erhöhter Aktivität hervorzuheben, z. B. die Anzahl der Byte oder das Verkehrsaufkommen, die mit einer Geräteverbindung verbunden sind.



Unten im linken Bereich können Sie eine andere Metrik für Kartenelemente auswählen:

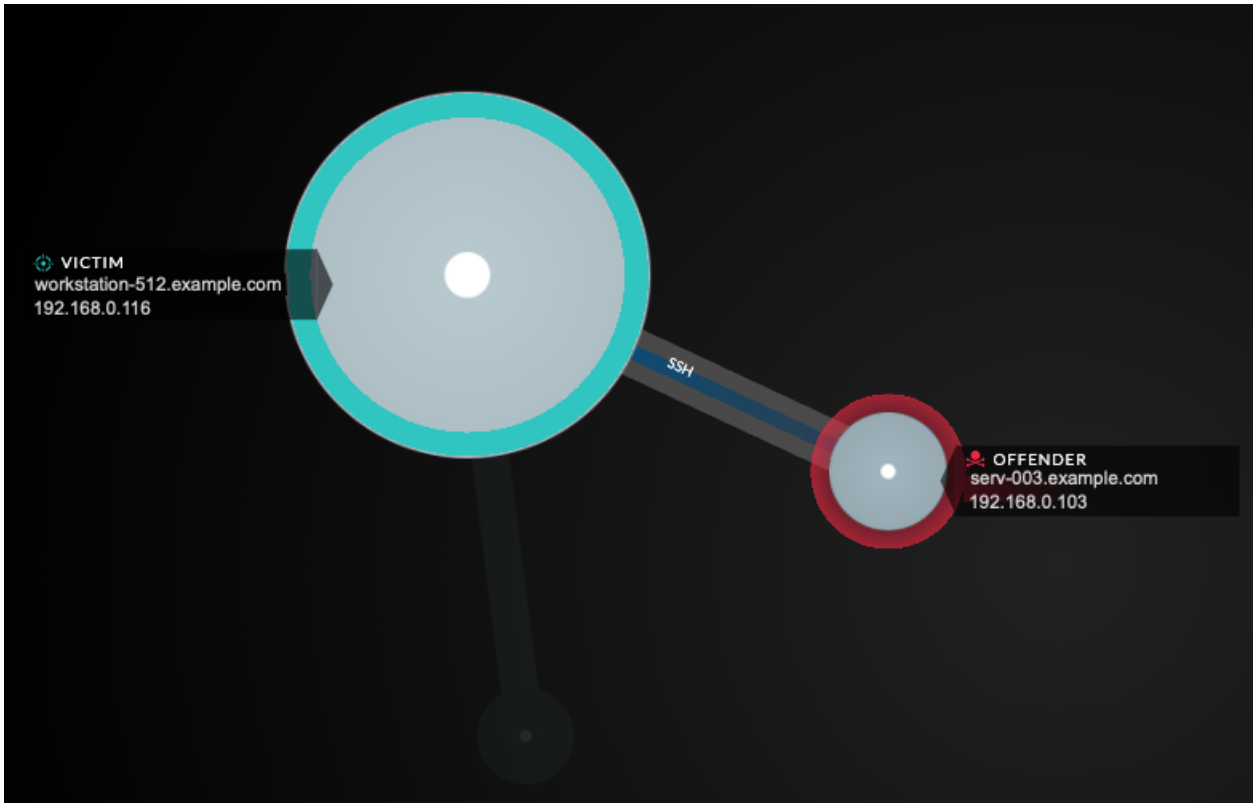
- **Byte:** Sehen Sie sich alle Geräte an, die während des Zeitintervalls Daten senden oder empfangen.
- **Verbindungen:** Es werden nur die Geräte angezeigt, die während des Zeitintervalls mindestens einmal eine neue Verbindung hergestellt haben.
- **TCP-Kurven:** Es werden nur die Geräte angezeigt, die während des Zeitintervalls mindestens einmal zwischen Senden und Empfangen von Daten gewechselt haben.

Farbe

Blau und Grau sind Standardfarben für Kreise und Linien. Diese Standardfarben sind für die Anzeige von Informationen in einer Karte optimiert. Sie können Ihrer Karte jedoch unterschiedliche Farben zuweisen, um den Schweregrad einer Alarm hervorzuheben oder anzuzeigen, wann eine Geräteverbindung hergestellt wurde.

Erkennungen

Erkennungen Die einem Gerät auf der Karte zugewiesenen Geräte erscheinen um den Kreis herum als animierte Impulse, sogenannte Erkennungsmarkierungen. Die Farbe des Pulses ist rot, wenn das Gerät der Täter ist, und blaugrün, wenn das Gerät Opfer der Erkennung ist. Der Teilnehmerstatus erscheint auch auf dem Geräteetikett.



Hinweis: Erkennungen durch maschinelles Lernen erfordern eine Verbindung zu ExtraHop Cloud Services.

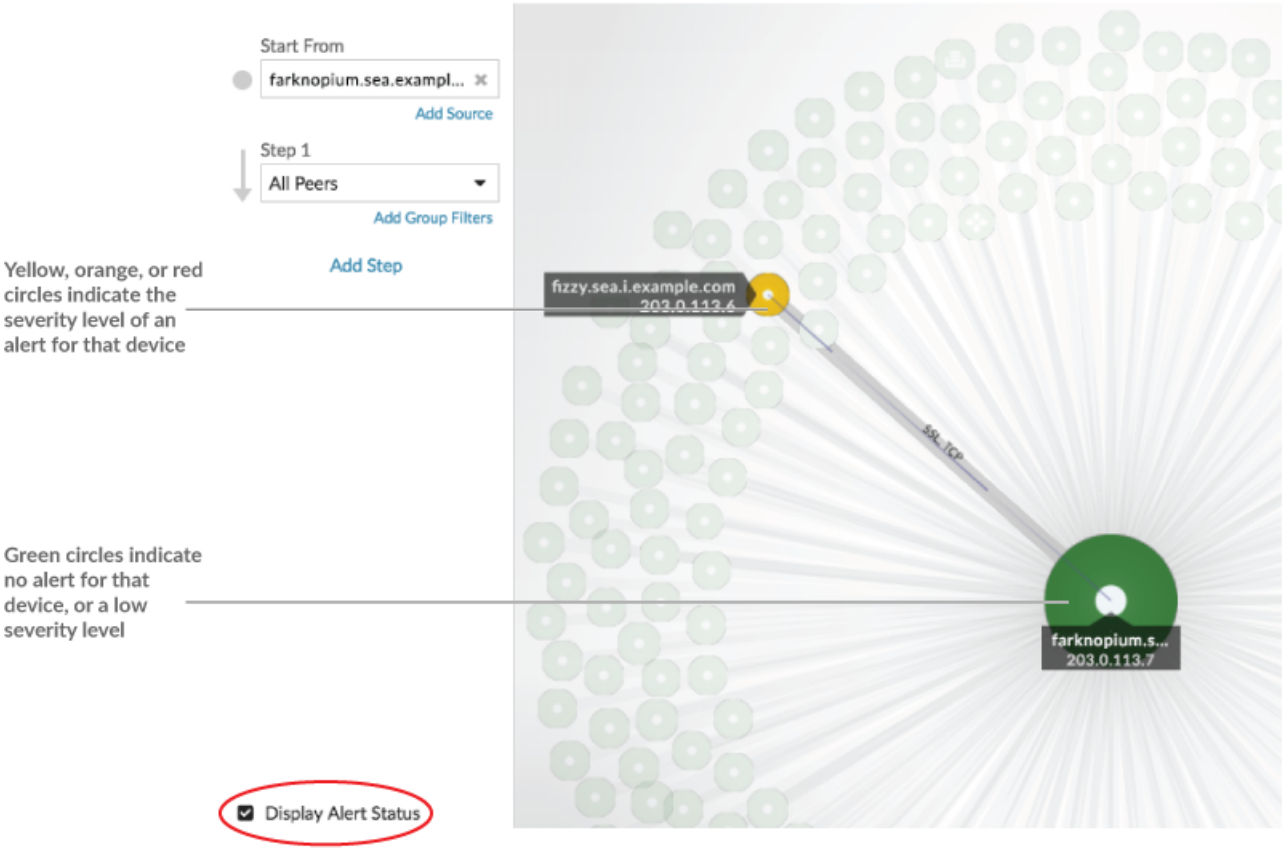
Klicken Sie auf einen Kreis mit einer Erkennungsmarkierung, um zugehörige Erkennungen anzuzeigen und zu ihnen zu navigieren, oder Seite „ Geräteübersicht“.

Wenn Erkennungsmarkierungen nicht wie erwartet auf Ihren Aktivitätskarten angezeigt werden, sind Erkennungsmarkierungen möglicherweise deaktiviert. Du kannst Erkennungsmarkierungen aktivieren oder deaktivieren von der **Nutzer** Speisekarte.

Alarmstatus (NPM-Modulzugriff erforderlich)

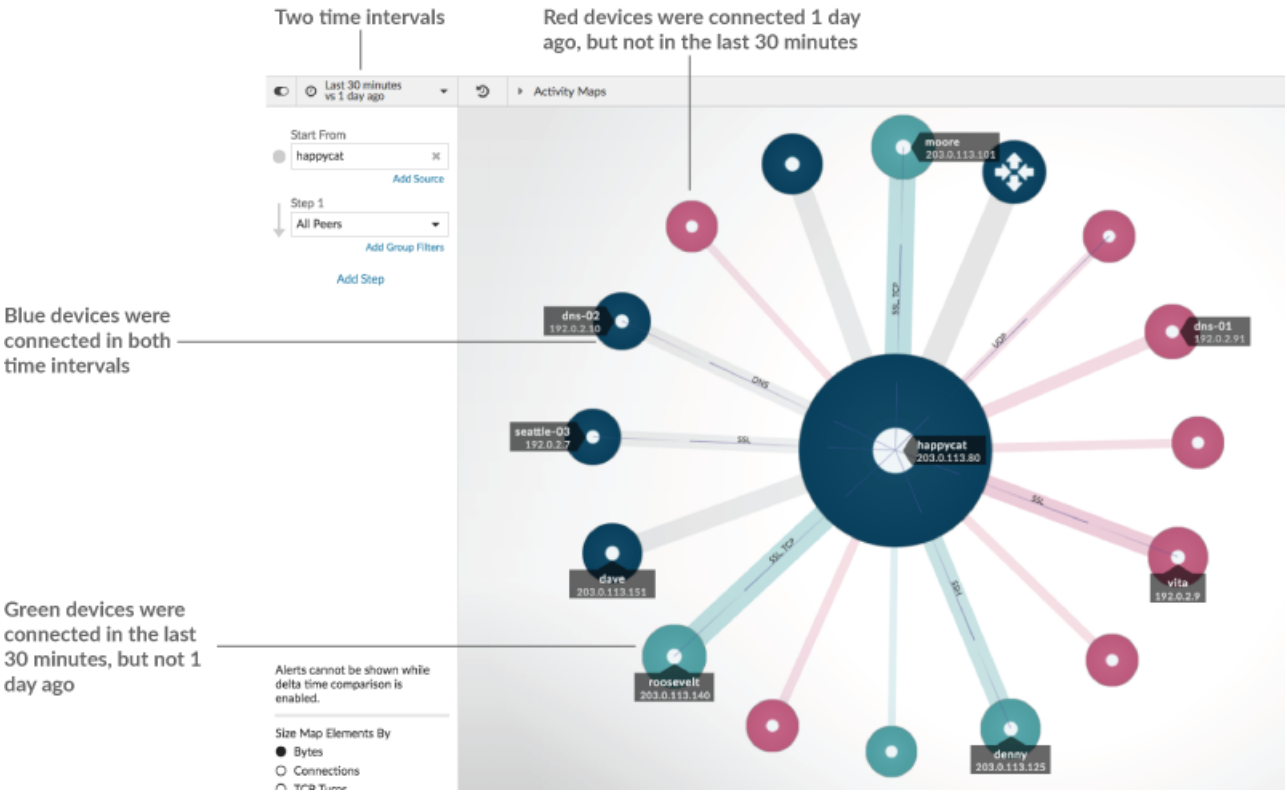
Um den Schweregrad einer Alarm für ein Gerät in Ihrer Karte anzuzeigen, wählen Sie **Warnstatus anzeigen** in der unteren linken Ecke oder auf der Seite, wie in der folgenden Abbildung dargestellt. Die Kreisfarbe entspricht dann dem schwerwiegendsten Status für alle Alarme, die einem Gerät während des Zeitintervalls zugewiesen wurden. Wenn einem Gerät keine Alarm zugewiesen ist oder die Warnstufe informativ ist, ist die Standardfarbe des Kreises grün.

Um die Alarm zu untersuchen, klicken Sie auf den Kreis und wählen Sie dann den Gerätenamen in der Gehe zu Gerät... Abschnitt. Scrollen Sie auf der Protokollseite des Geräts nach unten zu die Seite „Benachrichtigungen“ anzeigen.



Vergleich von Zeitintervallen

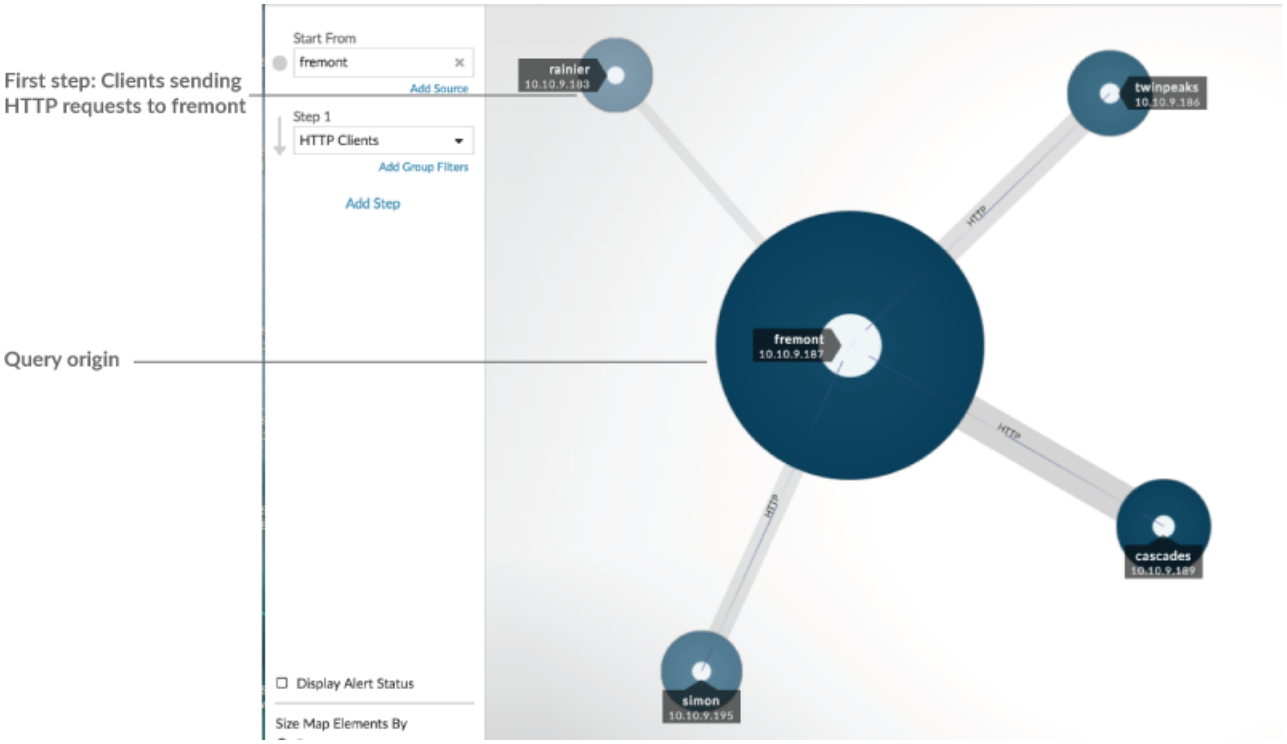
Wenn du Vergleiche zwei Zeitintervalle, um Metrik Deltas zu finden, anhand verschiedener Farben in der Karte können Sie feststellen, wann Geräteverbindungen hergestellt wurden oder wann sich die Protokollaktivität für ein Gerät geändert hat. Zum Beispiel nach dem Erstellen eines Vergleichs zwischen **Gestern** und der **Letzte 30 Minuten**, neue Geräteverbindungen oder Aktivitäten, die nur im neueren Zeitintervall auftreten, werden grün angezeigt. Frühere Geräteverbindungen oder Aktivitäten, die nur im früheren Zeitintervall aufgetreten sind, sind rot. Geräteverbindungen, die sich zwischen den Zeitintervallen nicht geändert haben, sind blau. In der folgenden Abbildung werden neue Verbindungen, die in den letzten dreißig Minuten hergestellt wurden, durch grüne Kreise und Linien dargestellt.



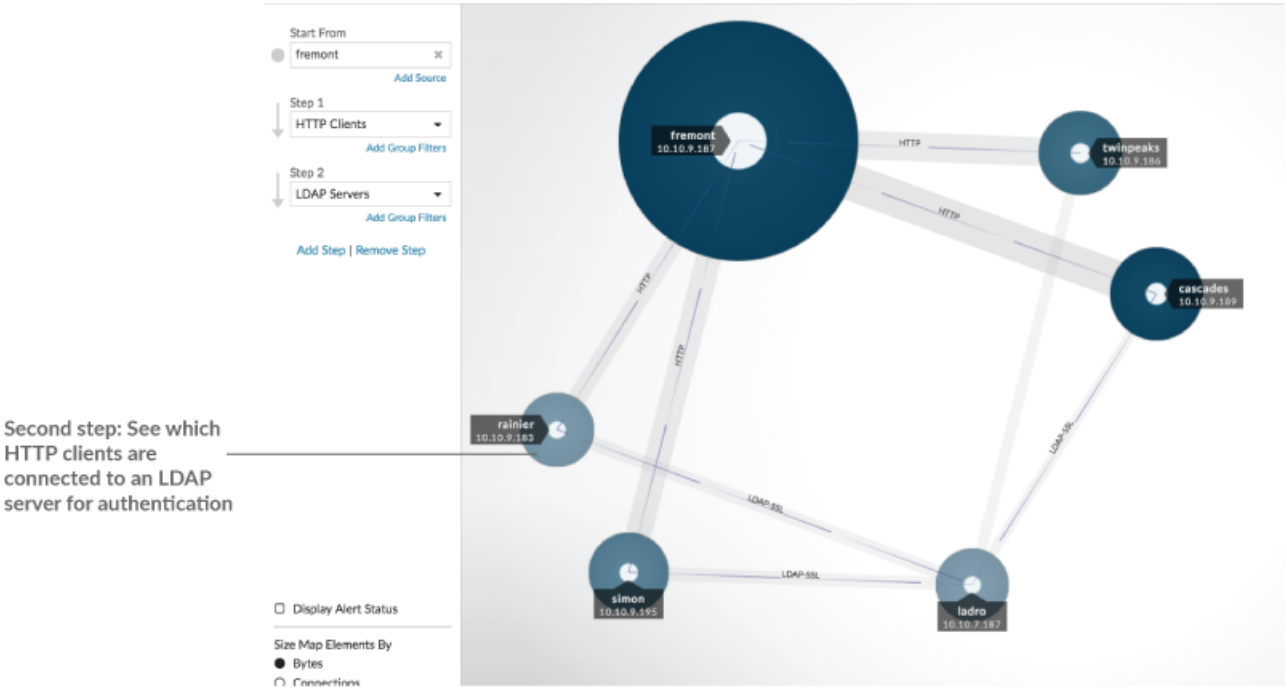
Hinweis: Wenn alle Geräte eine einzige Farbe haben, z. B. grün, bedeutet dies, dass die Abfrage im früheren Zeitintervall keine Ergebnisse erbracht hat. Beispielsweise hatte das Ursprungsgerät im früheren Zeitintervall keine Protokollaktivität.

Schritte und Filter zu einer Map hinzufügen

Ein Schritt ist eine Ebene von Verbindungen zwischen Geräten. Die Geräte in jedem Schritt haben eine Beziehung zu den Geräten im vorherigen Schritt. Diese Beziehungen werden durch ihre Protokollaktivität definiert.



Fügen Sie einer Aktivitätsdiagramm einen neuen Schritt hinzu, um Ihrer Karte eine weitere Informationsebene hinzuzufügen. Klicken Sie auf die Dropdownliste für einen bestimmten Schritt und wählen Sie dann eine Protokollaktivität aus.



Sie können Geräte auch in einem Schritt nach ihrer Gruppenmitgliedschaft filtern. Wenn Sie beispielsweise HTTP-Server auswählen, aber nur Ihre Testserver in der Map sehen möchten, können Sie HTTP-Server nach einer Gerätegruppe filtern, z. B. Meine Testserver.

Weitere Informationen zum Hinzufügen von Schritten und Filtern zu einer Map finden Sie unter Erstellen Sie eine Aktivitätsdiagramm.

Aktivitätskarten verwalten

Die folgenden Optionen zur Verwaltung deiner Aktivitätsdiagramm sind im Befehlsmenü in der oberen rechten Ecke verfügbar:

- Speichern und teilen Sie eine Aktivitätsdiagramm
- Eine gespeicherte Aktivitätsdiagramm laden und verwalten
- Aktivitätsdiagramm als PDF-, PNG- oder SVG-Datei exportieren

Bewährte Methoden für die Untersuchung von Aktivitätsdiagramm Map-Daten

Wenn Sie auf Ihrer Karte ein Gerät finden, das es wert ist, untersucht zu werden, haben Sie mehrere Möglichkeiten, weitere Informationen über dieses Gerät zu sammeln.

Suchen Sie nach kürzlich verbundenen Geräten

Klicken Sie auf das Zeitintervall in der oberen linken Ecke der Seite und klicken Sie auf **Vergleiche**. Sie können sehen, wie sich die Geräteverbindungen zwischen zwei verschiedenen Zeitintervallen geändert haben.

Weitere Informationen finden Sie unter Vergleich von Zeitintervallen.

Navigieren Sie zu den Protokollseiten, um verwandte Metrikaktivitäten zu finden

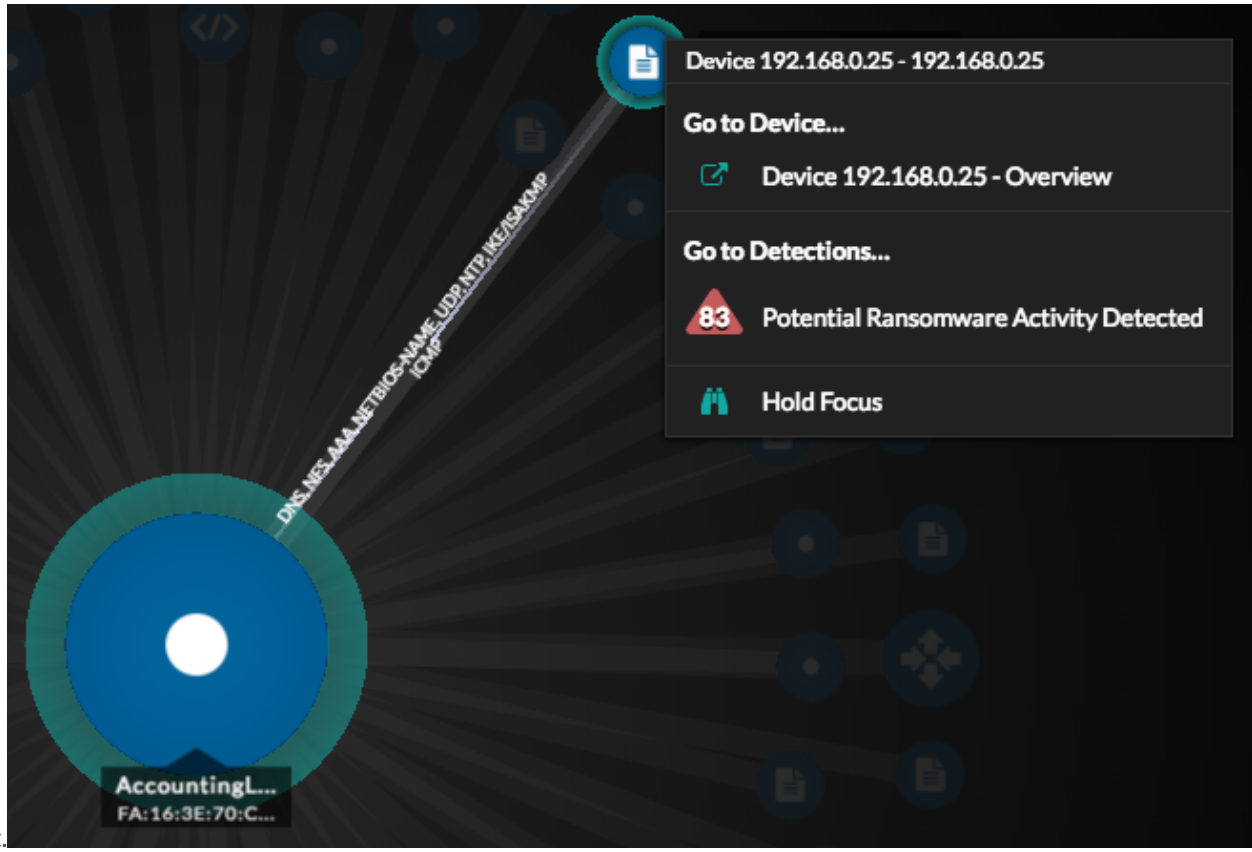
Klicken Sie auf einen Kreis oder eine Linie, um ein Dropdownmenü aufzurufen, wie in der folgenden Abbildung dargestellt.

Wählen Sie den Gerätenamen aus dem Menü aus, um die Seite Geräteübersicht aufzurufen. Klicken Sie im linken Bereich auf einen Protokollnamen, um die Protokollseite aufzurufen, die eine Zusammenfassung wichtiger Protokollmetriken enthält, die beobachtet wurden und mit dem Gerät verknüpft wurden. Auf einer Protokollseite finden Sie verwandte Metriken wie Fehler, Anfragen, Antworten und Serververarbeitungszeit. Sie können eine Metrik auch von einer Protokollseite aus aufschlüsseln, um Metrikdetails wie Server-IP-Adresse, Client-IP-Adresse, Statuscodes, Methoden und URIs anzuzeigen.

Navigieren Sie zu den auf dem Gerät identifizierten Erkennungen

Geräte auf einer Aktivitätsdiagramm, denen Erkennungen zugeordnet sind, werden als animierte Impulse rund um das kreisförmige Etikett angezeigt. Klicken Sie auf einen Kreis mit dieser

Erkennungsmarkierung, um ein Dropdownmenü aufzurufen, wie in der folgenden Abbildung dargestellt.



Wählen Sie einen Erkennungsnamen aus dem Menü aus, um zur Detailseite für diese Erkennung zu gelangen. Die Detailseite enthält Informationen über die Art der Erkennung und ihre Bedeutung sowie über den Zeitpunkt der Erkennung und die Dauer des Problems. Weitere Informationen finden Sie unter Seite mit Erkennungsdetails.

Suchen Sie nach Transaktionsdatensätzen, die mit einer Verbindung verknüpft sind (erfordert einen konfigurierten Recordstore)

Klicken Sie auf einen Kreis oder eine Linie, um das Drop-down-Menü aufzurufen. klicken **Aufzeichnungen**. Eine Datensatzabfrageseite wird geöffnet und zeigt alle Datensätze von jedem verbundenen Gerät an, einschließlich aller Datensatztypen, die den Geräteverbindungsprotokollen zugeordnet sind.

Erstellen Sie eine Aktivitätsdiagramm

Eine Aktivitätsdiagramm ist eine interaktive 2D- oder 3D-Anzeige von Geräteverbindungen in Echtzeit, die auf der Protokollaktivität zwischen Geräten basiert. Mithilfe von Aktivitätskarten können Sie Verkehrsflüsse visualisieren und anhand eines interessanten Datenpunkts auf einer Karte die Fehlerbehebung einleiten.

Sie können eine Aktivitätsdiagramm für ein aktives einzelnes Gerät oder eine Gerätegruppe erstellen. Nachdem Sie eine Basiskarte generiert haben, können Sie Geräte und Verbindungen in Ihrer Karte filtern.

Hinweis Sie können Aktivitätskarten für Geräte in Advanced, Standard, L2 Parent Analysis und Flow Analysis erstellen. Sie können keine Aktivitätsdiagramm für Geräte im Entdeckungsmodus erstellen. Weitere Informationen finden Sie unter Prioritäten der Analyse.

Erstellen Sie eine grundlegende Aktivitätsdiagramm

Eine grundlegende Aktivitätsdiagramm zeigt Ihnen einen einzelnen Schritt oder eine Ebene von Geräteverbindungen zwischen Originalgeräten und Peer-Geräten in Ihrem Netzwerk.

Hinweis: Sie können Aktivitätskarten für Geräte in Advanced, Standard, L2 Parent Analysis und Flow Analysis erstellen. Sie können keine Aktivitätsdiagramm für Geräte im Entdeckungsmodus erstellen. Weitere Informationen finden Sie unter Prioritäten der Analyse.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Vermögenswerte**.
3. Führen Sie je nach Herkunftsart der Aktivitätskarte einen der folgenden Schritte aus:

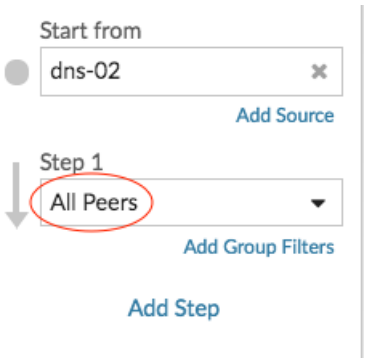
Option	Description
Für ein Gerät	klicken **Geräte** im linken Bereich und klicken Sie dann auf einen einzelnen Gerätenamen.
Für eine Gerätegruppe	klicken **Gerätegruppen** im linken Bereich und klicken Sie dann auf einen Gerätegruppennamen.
Für eine Gerätegruppe nach Protokollaktivität	klicken **Aktivität** im linken Bereich und klicken Sie dann auf die Gruppe von Clients, Servern oder Geräten für das gewünschte Protokoll.

4. Klicken Sie auf einen der folgenden Links, um die Aktivitätsdiagramm zu erstellen:

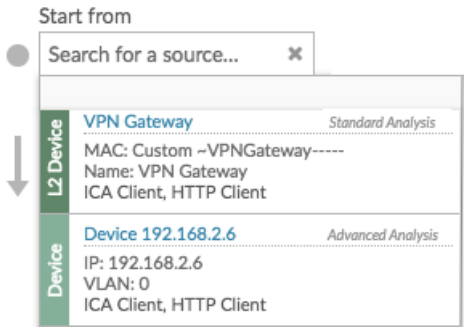
Option	Description
Für ein Gerät	klicken **Peer-Geräte**, befindet sich oben auf der Seite.
Für eine Gerätegruppe	klicken **Karte der Aktivitäten**, befindet sich in der Nähe der oberen rechten Ecke der Seite.

Hinweis: Wenn das Gerät oder die Gerätegruppe während des angegebenen Zeitintervalls keine Protokollaktivität aufweist, wird die Aktivitätsdiagramm ohne Daten angezeigt. Ändern Sie das Zeitintervall oder Ihre Herkunftsauswahl und versuchen Sie es erneut.

5. Filtern Sie in der Aktivitätsdiagramm Verbindungen nach Protokollaktivität, indem Sie die folgenden Schritte ausführen:
   a) Klicken Sie auf die Drop-down-Liste in der Schritt 1 Abschnitt des linken Bereichs, wie in der folgenden Abbildung dargestellt.

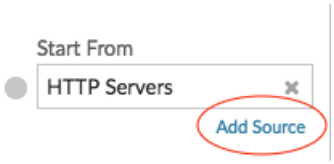


   b) Suchen Sie oben in der Dropdownliste nach einer Protokollaktivität und Rolle und wählen Sie sie aus. Sie können mehr als eine Auswahl treffen.
   c) Klicken Sie auf eine beliebige Stelle außerhalb der Dropdownliste.
6. Optional: Ändern Sie das primäre Ursprungsgerät, indem Sie die folgenden Schritte ausführen:
   a) In der Beginne von Klicken Sie im linken Bereich auf den Gerät- oder Gruppennamen. Eine Dropdownliste wird angezeigt.



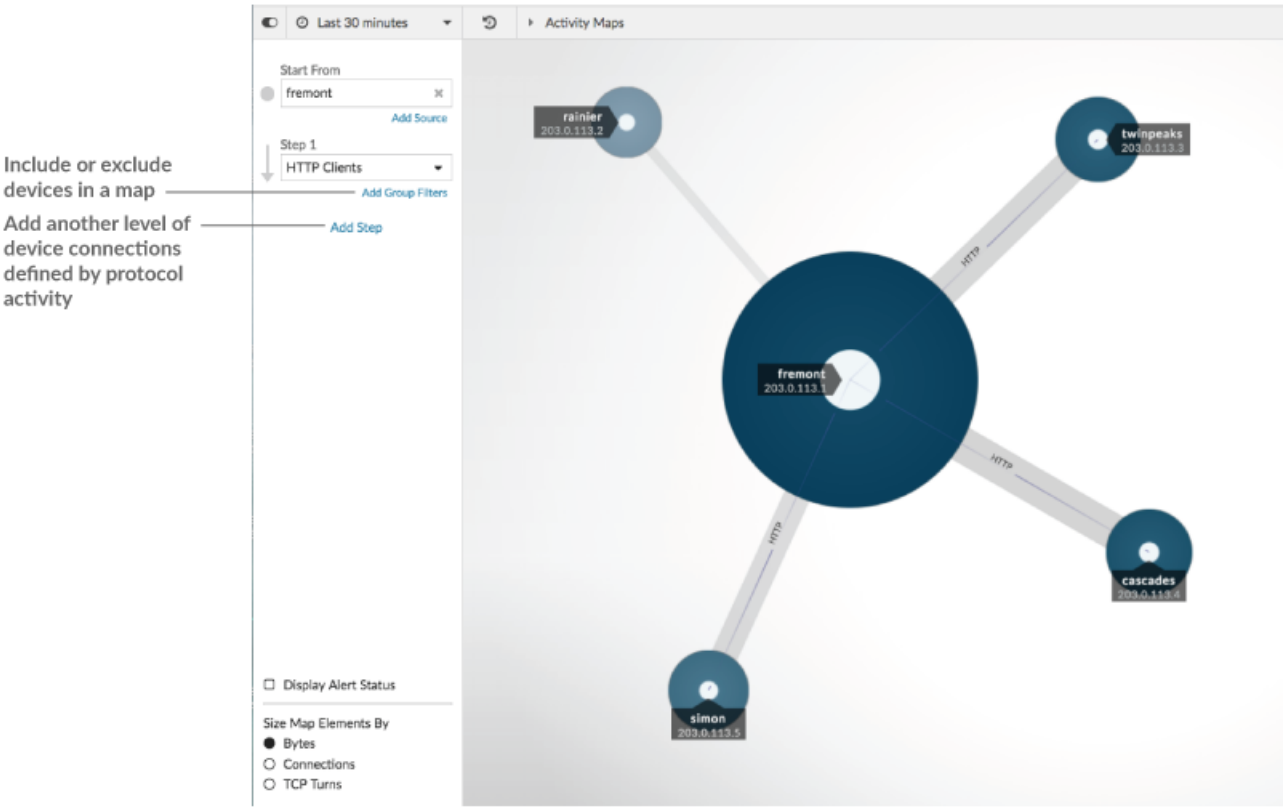
b) Suchen Sie nach einem anderen Gerät oder einer anderen Gruppe und wählen Sie sie aus, um den Kartenursprung für die angezeigte Karte dynamisch zu aktualisieren.

7. Optional: Erstellen Sie eine Ad-hoc-Gruppe von Quellen, um schnell den Datenverkehr zu untersuchen, der von mehreren Geräten in derselben Map stammt. klicken **Quelle hinzufügen**.



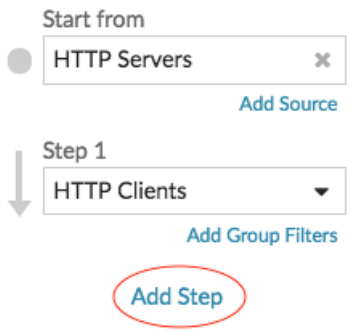
Fügen Sie Verbindungen hinzu und filtern Sie Geräte zu Ihrer Karte

Um den Pfad des Datenverkehrs von den Ursprungsgeräten zu den nachgeschalteten Geräten besser zu verstehen, können Sie Ihrer Karte weitere Schritte hinzufügen. Sie können auch Filter erstellen, um Geräte in die Karte ein- oder auszuschließen. Die folgende Abbildung zeigt Ihnen, wie Sie Schritte hinzufügen und Filter erstellen.

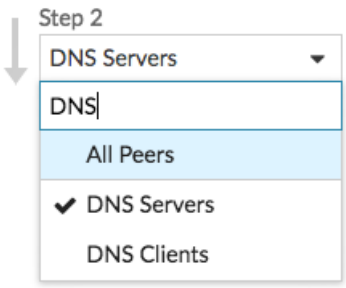


Fügen Sie eine weitere Ebene von Geräteverbindungen hinzu
Ein Schritt definiert eine Verbindungsebene zwischen Geräten in einer Map. Die Geräte in jedem Schritt haben eine Beziehung zu den Geräten im vorherigen Schritt. Diese Beziehungen werden durch ihre Protokollaktivität definiert. Sie können bis zu 5 Schritte hinzufügen, um zu sehen, wie der Datenverkehr von einem Gerät zum anderen fließt.

1. klicken **Schritt hinzufügen**, wie in der folgenden Abbildung dargestellt. **Alle Kollegen** ist standardmäßig ausgewählt.



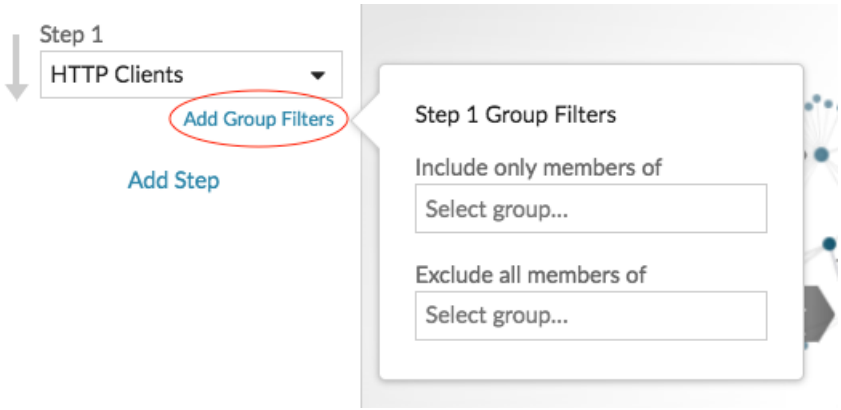
2. Suchen Sie oben in der Dropdownliste nach einer Protokollaktivität und Rolle und wählen Sie sie aus. Sie können mehr als eine Auswahl treffen.



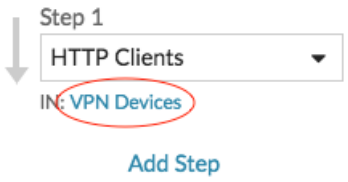
3. Klicken Sie auf eine beliebige Stelle außerhalb der Dropdownliste.

Geräte einbeziehen oder ausschließen
Sie können Geräte innerhalb eines Schritts nach ihren Filtern Gerätegruppe Mitgliedschaft.

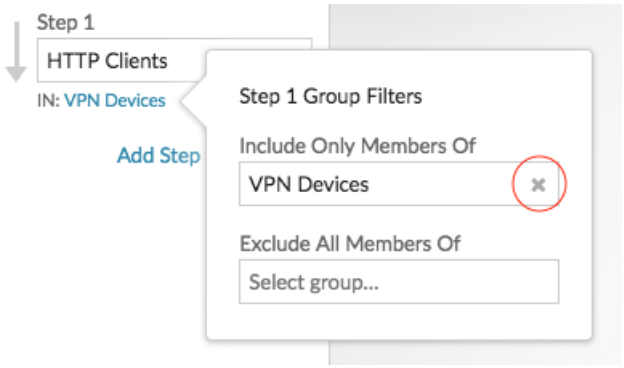
1. klicken **Gruppenfilter hinzufügen**.



2. Klicken Sie auf eine Dropdownliste, um nach einer Gerätegruppe zu suchen und diese auszuwählen.
3. Klicken Sie auf eine beliebige Stelle außerhalb des Filtermenüs, um Ihre Filter anzuwenden.
4. Gehen Sie wie folgt vor, um einen Filter zu entfernen oder zu ändern:
   a) Klicken Sie auf den Namen der Gerätegruppe.



   b) Ändern Sie den Filter, indem Sie auf die Drop-down-Liste klicken und dann eine andere Gerätegruppe auswählen.
   c) Entfernen Sie den Filter, indem Sie auf **x** Symbol, wie in der folgenden Abbildung dargestellt.



d) Klicken Sie auf eine beliebige Stelle außerhalb des Filtermenüs, um Ihre Filteraktualisierungen anzuwenden.

Nächste Schritte

- Speichern und teilen Sie eine Aktivitätsdiagramm

Speichern und teilen Sie eine Aktivitätsdiagramm

Sie können eine Aktivitätsdiagramm speichern und mit anderen teilen. Standardmäßig sind alle Aktivitätskarten, die Sie erstellen, privat, was bedeutet, dass keine ExtraHop-Benutzer Ihre Map ansehen oder bearbeiten können. Sie können Ihre Map jedoch beim Speichern teilen, indem Sie anderen ExtraHop-Benutzern und -Gruppen Ansichts- oder Bearbeitungszugriff gewähren.

Hier sind einige wichtige Überlegungen zum Teilen von Activity Maps:

- Wie ein Benutzer mit einer Activity Aktivitätsdiagramm interagiert und welche Informationen er im ExtraHop-System einsehen kann, hängt von den Benutzerrechten ab, die ihm vom ExtraHop-Administrator zugewiesen werden. Weitere Informationen finden Sie in der Benutzerrechte Abschnitt im ExtraHop-Administratorhandbuch.
- Wenn Sie einem Benutzer Bearbeitungszugriff gewähren, kann dieser Benutzer die Activity Map ändern und mit anderen teilen. Andere Benutzer können die Aktivitätsdiagramm jedoch nicht löschen. Nur der Kartenbesitzer kann eine Aktivitätsdiagramm löschen.
- Gruppeninformationen werden aus LDAP (wie OpenLDAP oder Active Directory) in das ExtraHop-System importiert. Benutzerinformationen sind verfügbar, nachdem sich ein ExtraHop-Benutzer bei seinem Konto angemeldet hat.
- Wenn Sie einen Benutzer löschen, haben Sie die Möglichkeit, seine Aktivitätskarten auf einen anderen Benutzer zu übertragen.

Die folgenden Schritte zeigen dir, wie du eine Aktivitätsdiagramm speichern und teilen kannst:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Erstellen Sie eine Aktivitätsdiagramm.
3. Klicken Sie auf das Speichern-Symbol in der oberen rechten Ecke der Seite.
4. Geben Sie einen Namen für Ihre Map ein. Der Name muss eindeutig sein.
5. Optional: Geben Sie eine Beschreibung ein.
6. Optional: Ändern Sie den Permalink-Shortcode in einen benutzerfreundlichen Namen.

   Sie können beispielsweise eine Map so konfigurieren, dass Warnstatus angezeigt werden, und „/alerts“ an den Shortcode anhängen, um Benutzern mitzuteilen, dass die gespeicherte Map standardmäßig Warnmeldungen anzeigt.

   Hinweis: Der Shortcode darf keine Leerzeichen enthalten und der Shortcode muss eindeutig sein .

7. Teile deine Aktivitätsdiagramm, indem du die folgenden Schritte ausführst:
   a) Geben Sie einen Benutzernamen oder eine Gruppe ein.
   b) Treffen Sie eine der folgenden Optionen:

Art des Zugriffs	Auswahl
ExtraHop-Benutzer können Folgendes ansehen	Wählen **Kann ansehen** und dann klicken **Hinzufügen**.
ExtraHop-Benutzer können sie sowohl ansehen als auch bearbeiten	klicken **Kann ansehen** und dann klicken **Kann bearbeiten**. klicken **Hinzufügen**.

8. klicken **Speichern**.

Hinweis: Sie können die Eigenschaften einer gespeicherten Map auch ändern, indem Sie auf das Befehlsmenü ⋮ und dann klicken **Eigenschaften der Karte**. Um Freigabeberechtigungen schnell zu ändern, klicken Sie auf das Befehlsmenü ⋮ und dann klicken **Teilen**.

Nächste Schritte

- Wenn Sie Ihre Karte geteilt haben, kopieren Sie die gesamte Karten-URL aus Ihrem Browser und senden Sie die URL dann an die Benutzer mit Zugriff auf Ihre Karte.
- Eine gespeicherte Aktivitätsdiagramm laden und verwalten.
- Zugriff auf eine Aktivitätsdiagramm entfernen oder ändern

Zugriff auf eine Aktivitätsdiagramm entfernen oder ändern

Sie können den Zugriff auf eine Aktivitätsdiagramm, die Sie Benutzern und Gruppen gewährt haben, entfernen oder ändern. Sie müssen zuerst eine Aktivitätsdiagramm erstellen, um auf Optionen zum Ändern von gespeicherten Activity Maps zugreifen zu können.

1. Erstellen Sie eine Aktivitätsdiagramm, und klicken Sie dann auf das Symbol Öffnen 🗁 in der oberen rechten Ecke der Seite.
2. Klicken Sie auf den Namen der Aktivitätsdiagramm.
3. Führen Sie im Abschnitt Teilen einen der folgenden Schritte aus:
   - Um Benutzern oder Gruppen den Zugriff zu entziehen, klicken Sie auf das rote Löschen **x** Symbol neben dem Benutzer- oder Gruppennamen.
   - Um den Zugriff für einen vorhandenen Benutzer oder eine bestehende Gruppe zu ändern, klicken Sie auf **Kann ansehen** oder **Kann bearbeiten**, und treffen Sie eine andere Auswahl.
   - Um einen neuen Benutzer oder eine neue Gruppe hinzuzufügen, suchen Sie nach dem Benutzernamen und klicken Sie darauf. klicken **Kann ansehen** oder **Kann bearbeiten**, und klicken Sie dann **Hinzufügen**.
4. klicken **Speichern**.

Eine gespeicherte Aktivitätsdiagramm laden und verwalten

Sie können gespeicherte Aktivitätskarten anzeigen, aktualisieren oder löschen. Zunächst müssen Sie eine neue Map erstellen, um auf eine Liste mit gespeicherten und geteilten Maps zugreifen zu können.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Erstellen Sie eine Aktivitätsdiagramm, und klicken Sie dann auf das Symbol Öffnen 🗁 in der oberen rechten Ecke der Seite.
3. Wählen Sie eine der folgenden Optionen für die Aktivitätsdiagramm:

- Um eine Karte zu laden, klicken Sie auf den Namen der Karte. Wenn Sie die Map ändern und dann erneut speichern möchten, nehmen Sie Ihre Änderungen vor und klicken Sie dann auf **Speichern** Ikone.

  Hinweis: Sie können die Eigenschaften einer gespeicherten Map auch ändern, indem Sie auf das Befehlsmenü klicken. ⋮ und dann klicken **Eigenschaften der Karte**.
- Um eine Map zu löschen, klicken Sie **Löschen** neben dem Kartennamen.

Hinweis: Benutzer müssen über Rechte zum Anzeigen oder Interagieren mit Activity Maps verfügen. siehe Benutzerrechte im ExtraHop-Administratorhandbuch.

Erkennungen

Das ExtraHop-System wendet Techniken des maschinellen Lernens und eine regelbasierte Überwachung Ihrer wire data an, um ungewöhnliche Verhaltensweisen und potenzielle Risiken für die Sicherheit und Leistung Ihres Netzwerk zu identifizieren.

Bevor Sie beginnen
Benutzern muss Folgendes gewährt werden Privilegien um Erkennungen anzuzeigen.

Wenn anomales Verhalten erkannt wird, generiert das ExtraHop-System eine Erkennung und zeigt die verfügbaren Daten und Optionen an. Steuerelemente auf der Seite „Erkennungen“ führen zu folgenden Oberflächenerkennungen : für die Triage empfohlen und helfe dir filtern und sortieren Ihre Ansichten, sodass Sie sich schnell auf Erkennungen im Zusammenhang mit kritischen Systemen konzentrieren können.

Mit dem NPM-Modulzugriff können Erkennungen Ihnen auf folgende Weise bei der Wartung Ihres Netzwerk helfen:

- Erfassen Sie hochwertige, verwertbare Daten, um die Ursachen von Netzwerkproblemen zu ermitteln.
- Finden Sie unbekannte Probleme mit Leistung oder Infrastruktur.

Mit dem Zugriff auf das NDR-Modul können Erkennungen Ihnen helfen, Ihr Netzwerk auf folgende Weise zu schützen:

- Identifizieren Sie bösartiges Verhalten, das mit verschiedenen Angriffskategorien oder MITRE-Techniken in Verbindung steht.
- Sehen Sie sich verwandte Erkennungen an oder erstellen Sie Ihre eigenen Untersuchung um Erkennungen zu gruppieren und potenzielle Angriffskampagnen zu verfolgen.
- Kennzeichnen Sie verdächtige IP-Adressen, Hostnamen und URIs, die anhand von Bedrohungsinformationen identifiziert wurden.
- Heben Sie bewährte Methoden zur Erhöhung der Sicherheit hervor.

Erfahre mehr über Optimierung von Erkennungen.

Wichtig: Obwohl Erkennungen Sie über Sicherheitsrisiken und Leistungsprobleme informieren können, ersetzen Erkennungen nicht die Entscheidungsfindung oder das Fachwissen über Ihr Netzwerk. Immer überprüfen Sicherheit und Performance Erkennungen, um die Ursache für ungewöhnliches Verhalten zu ermitteln und zu ermitteln, wann Maßnahmen ergriffen werden müssen.

Video: Sehen Sie sich die entsprechenden Schulungen an:

- Sicherheitserkennungen
- Leistungserkennungen

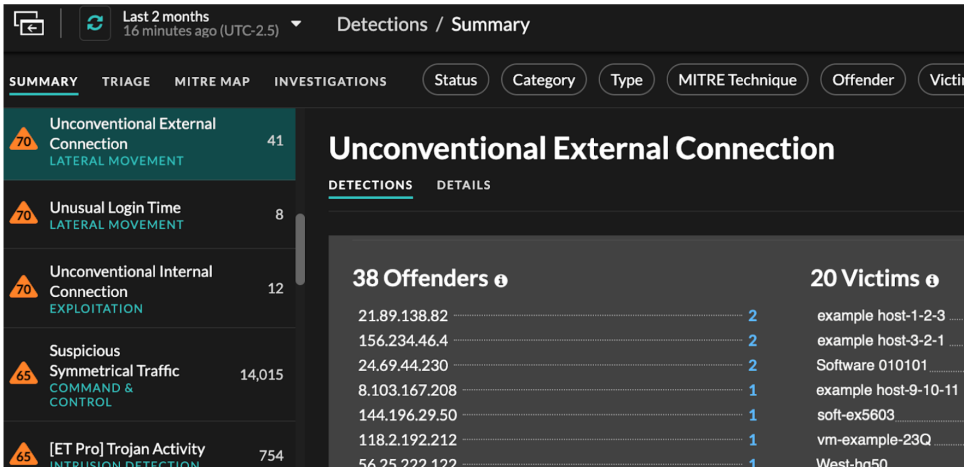
Erkennungen anzeigen

In der oberen linken Ecke der Erkennungsseite gibt es vier Optionen zum Anzeigen von Erkennungen: Zusammenfassung, Triage, MITRE Map und Untersuchungen. Diese Optionen bieten jeweils eine einzigartige Ansicht Ihrer Erkennungsliste.

Zusammenfassung

Standardmäßig werden Erkennungen auf der Seite Erkennungen in der Übersichtsansicht angezeigt, in der Informationen zu Erkennungen zusammengefasst werden, um Aktivitätsmuster in Ihrer Umgebung hervorzuheben. Sie können Ihre Erkennungsliste in der Übersichtsansicht sortieren und gruppieren, um sich auf häufig auftretende Erkennungstypen und die aktivsten Teilnehmer zu konzentrieren.

Hinweis Standardmäßig ist der **Offen** Der Statusfilter wird angewendet auf den Erkennungen Seite. Klicken Sie auf **Offen** filtern, um auf andere zuzugreifen Optionen filtern.



Sortierung von Erkennungen in der Übersichtsansicht

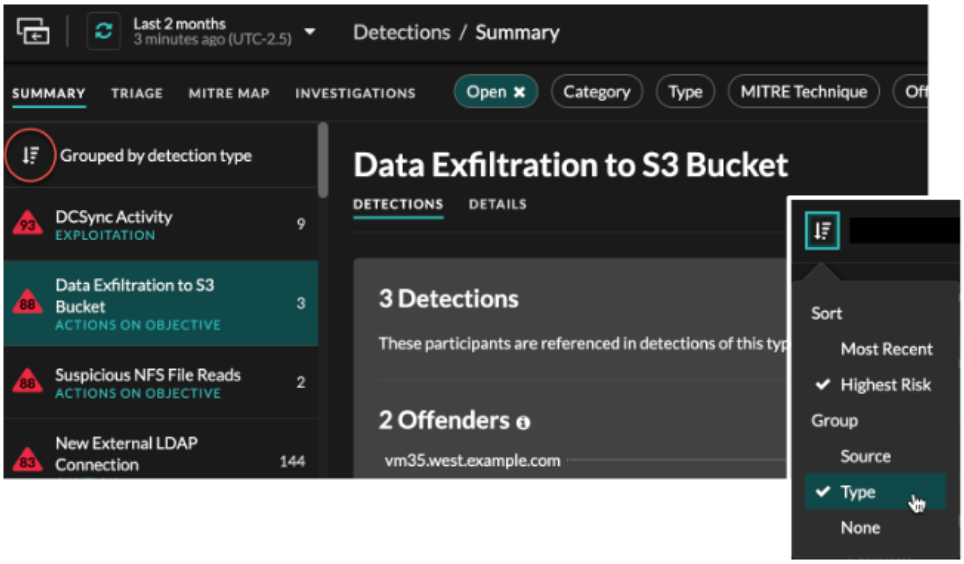
Sie können Erkennungen entweder nach der höchsten Risikoscore oder nach dem jüngsten Ereignis sortieren.

Wenn sie nach Risikobewertung sortiert sind, sind dies Erkennungen für die Triage empfohlen erscheinen zuerst, gefolgt von Entdeckungen mit der höchsten Risikoscore.

Wenn sortiert nach **Aktuellste**, Erkennungen mit der letzten Endzeit werden zuerst angezeigt. Wenn noch zwei Erkennungen andauern, wird die Erkennung mit dem letzten Aktualisierungszeitpunkt zuerst angezeigt. Klicken Sie auf das Sortiersymbol über der Erkennungsliste, um eine Option auszuwählen.

Gruppierung von Erkennungen in der Übersichtsansicht

Sie können Erkennungen nach Erkennungstyp (z. B. Spike in SSH-Sitzungen) oder nach Erkennungsquelle (z. B. IP-Adresse des Täters) gruppieren, oder Sie können festlegen, dass Ihre Erkennungsliste überhaupt nicht gruppiert wird.



Nach Typ gruppieren

Beim Gruppieren der Zusammenfassungsansicht nach **Typ**, können Sie Wertelisten anzeigen, die mit Erkennungen verknüpft sind, die während des ausgewählten Zeitintervalls aufgetreten sind, z. B. Teilnehmer, Erkennungseigenschaften oder Netzwerklokalitäten.

Sie können auf Teilnehmerwerte klicken, um mehr über dieses Gerät oder diese IP-Adresse zu erfahren. Klicken Sie auf einen beliebigen Wert, um nur Erkennungen anzuzeigen, die mit diesem Wert verknüpft sind, oder alle zugehörigen Erkennungen verfolgen.

Teilnehmer

Führt alle Täter und Opfer der ausgewählten Erkennungsart auf. Die Täter- und Opferlisten sind nach der Anzahl der Erkennungen geordnet , bei denen der Teilnehmer auftaucht.

Immobilienwerte

Listet die Eigenschaftswerte auf, die dem Erkennungstyp zugeordnet sind. Die Liste der Eigenschaftswerte ist nach der Anzahl der Erkennungen sortiert, in denen der Eigenschaftswert vorkommt.

Lokalitäten im Netzwerk

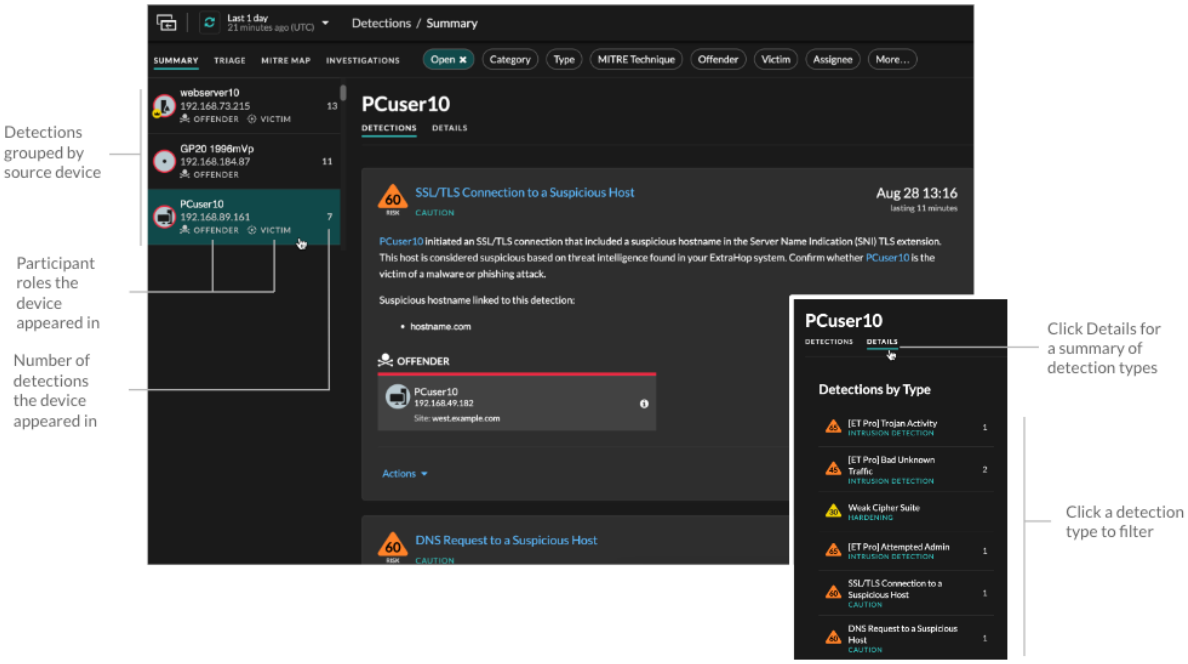
Führt die Netzwerklokalitäten auf, die Erkennungen des ausgewählten Typs enthalten. Die Liste der Netzwerkortschaften ist nach der Anzahl der Entdeckungen in der Netzwerklokalität sortiert.

Am unteren Rand des Übersichtsfensters befinden sich Links, mit denen Sie alle Erkennungen verfolgen in der Zusammenfassung enthalten. Du kannst eine Optimierungsregel erstellen um alle in der Zusammenfassung enthaltenen Erkennungen auszublenden oder versteckte Entdeckungen dieses Erkennungstyps anzuzeigen.

Sie können über den Übersichtsbereich hinaus scrollen, um einzelne Erkennungskarten anzuzeigen. Erkennungen, die für die Triage empfohlen erscheinen zuerst.

Nach Quelle gruppieren

Wenn Sie die Übersichtsansicht nach Quelle gruppieren, können Sie Teilnehmer anzeigen, die die Quelle einer Erkennung sind, wobei die Anzahl der Erkennungen neben dem Namen des Teilnehmers angezeigt wird. Klicken Sie auf eine Quelle, um die Erkennungen anzuzeigen, bei denen das Gerät entweder als Täter oder als Opfer aufgetreten ist. klicken **Einzelheiten** unter dem Gerätenamen, um eine Liste der Erkennungstypen anzuzeigen, in denen das Gerät aufgetreten ist, und klicken Sie dann auf einen Erkennungstyp, um nach diesem Erkennungstyp zu filtern.



Nach Keiner gruppieren

Bei der Gruppierung nach **Keine** Auf der Seite Erkennungen können Sie ein Zeitdiagramm mit der Gesamtzahl der Entdeckungen anzeigen, die innerhalb des ausgewählten Zeitintervalls identifiziert wurden. Jeder horizontale Balken im Diagramm stellt die Dauer einer einzelnen Erkennung dar und ist entsprechend der Risikoscore farblich gekennzeichnet.

- Klicken und ziehen Sie, um einen Bereich im Diagramm hervorzuheben, um einen bestimmten Zeitraum zu vergrößern. Erkennungen werden für das neue Zeitintervall aufgelistet.
- Bewegen Sie den Mauszeiger über einen Balken, um die Bewertung des Erkennungsrisikos anzuzeigen.
- Klicken Sie auf eine Leiste, um direkt zur Seite mit den Erkennungsdetails zu gelangen.

Unter der Zeitleiste wird in einem Flussdiagramm die Anzahl der Erkennungen angezeigt, die jeder Angriffskategorie zugeordnet sind. Kategorien werden zu einer Angriffskette zusammengefasst, die den Verlauf der Schritte beschreibt, die ein Angreifer unternimmt, um letztendlich sein Ziel zu erreichen, z. B. sensible Daten zu stehlen. Klicken Sie auf eine Angriffskategorie, um nur Erkennungen in dieser Kategorie anzuzeigen.

Triage

(nur NDR-Modul) In der Triage-Ansicht werden Erkennungen angezeigt, die ExtraHop für die Triage empfiehlt, basierend auf einer kontextuellen Analyse von Faktoren in Ihrer Umgebung, auch bekannt als Smart Triage.

Erkennungskarten, die für die Triage empfohlen werden, sind mit einem gelben Etikett gekennzeichnet und listen die Faktoren auf, die zu der Empfehlung geführt haben.

Beinhaltet einen hochwertigen Asset

Das Asset bietet Authentifizierung oder wichtige Dienste, oder ein Asset, das manuell als hoher Wert identifiziert.

Beinhaltet einen Top-Täter

Das Gerät oder die IP-Adresse hat an zahlreichen Erkennungen und einer Vielzahl von Erkennungstypen teilgenommen.

Beinhaltet einen seltenen Erkennungstyp

Der Erkennungstyp ist in letzter Zeit nicht in Ihrer Umgebung aufgetreten. Ungewöhnliche Erkennungstypen können auf einzigartiges, bösartiges Verhalten hinweisen.

Beinhaltet einen verdächtigen Hostnamen oder eine verdächtige IP-Adresse

Der Hostname oder die IP-Adresse lautet in einer Bedrohungssammlung referenziert das ist auf Ihrem System aktiviert.

Beinhaltet eine empfohlene Untersuchung

Die Erkennung ist Teil einer potenziellen Angriffskette in einem empfohlene Untersuchung.

Erkennungen, die für die Triage empfohlen werden, werden in der Zusammenfassungsansicht priorisiert und erscheinen unabhängig von der Sortierung ganz oben in Ihrer Erkennungsliste.

Du kannst Erkennungen filtern um nur Erkennungen anzuzeigen, die für die Triage empfohlen werden, und „Empfohlen für Triage“ als Kriterium für eine Benachrichtigungsregel.

Im Folgenden finden Sie einige Überlegungen zu Empfehlungen für die Triage:

- Empfehlungen, die auf hoher Wert Ressourcen basieren, sind auf maximal fünf Erkennungen desselben Erkennungstyps über einen Zeitraum von zwei Wochen begrenzt.
- Zwei Wochen an Sensordaten sind erforderlich, bevor Empfehlungen auf der Grundlage von Faktoren ausgesprochen werden, bei denen es sich um die häufigsten Straftäter oder um seltene Erkennungsfaktoren handelt.
- Empfehlungen auf der Grundlage von Bedrohungsinformationen sind auf zwei Erkennungen desselben Erkennungstyps für denselben Bedrohungsindikator über einen Zeitraum von dreißig Tagen beschränkt.

MITRE karte

Klicken Sie auf das **MITRE Karte** anzeigen, wenn Sie Ihre Erkennungen nach Angriffstechnik anzeigen möchten.

Jede Kachel in der Matrix steht für eine Angriffstechnik aus der MITRE ATT&CK® Matrix for Enterprise. Wenn eine Kachel hervorgehoben ist, erfolgte die mit dieser Technik verbundene Erkennung während des ausgewählten Zeitintervalls. Klicken Sie auf eine beliebige Kachel, um Erkennungen zu sehen, die dieser Technik entsprechen.

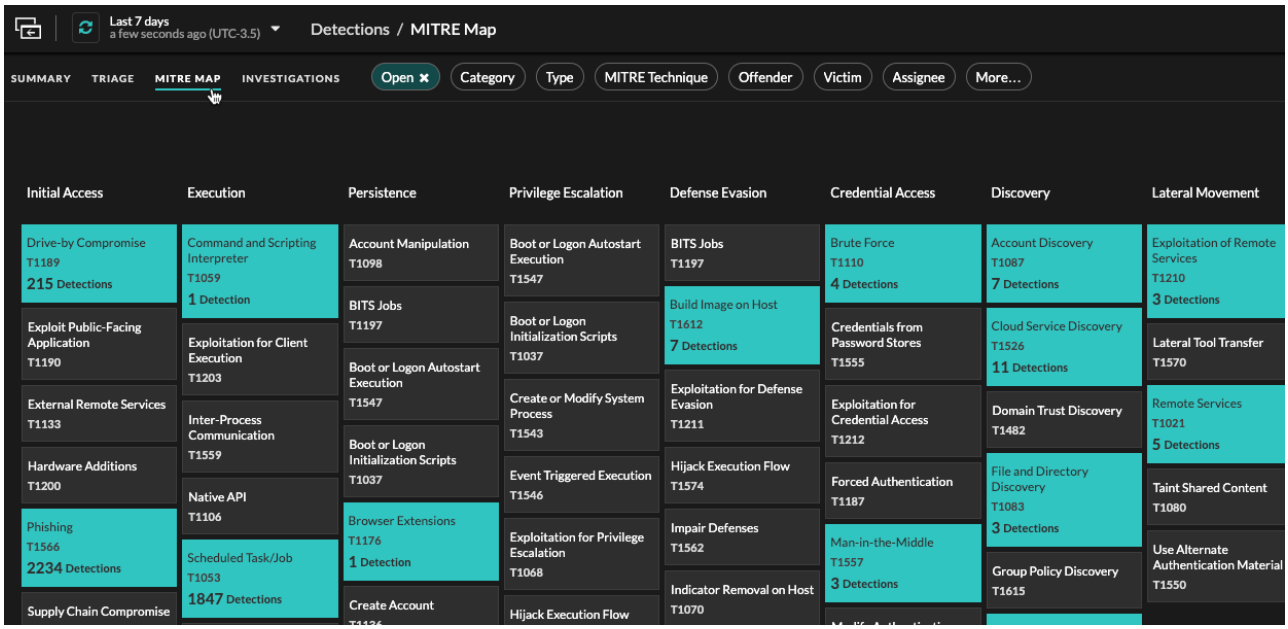


Tabelle „Untersuchungen“

In der Ansicht Untersuchungen werden alle vom Benutzer erstellten und empfohlenen Untersuchungen angezeigt, die während des ausgewählten Zeitintervalls erstellt wurden.

Klicken Sie auf einen Ermittlungsnamen, um die Untersuchung zu öffnen. Erfahre mehr über Ermittlungen.

Erkennungen filtern

Sie können die Seite „Entdeckungen“ filtern, um nur die Erkennungen anzuzeigen, die Ihren angegebenen Kriterien entsprechen. Beispielsweise könnten Sie nur an Exfiltrationserkennungen interessiert sein, die über HTTP erfolgen , oder an Erkennungen, die Teilnehmern zugeordnet sind, bei denen es sich um wichtige Server handelt.

Status

Sie können Erkennungen mit einem bestimmten Erkennungsstatus filtern, z. B. Bestätigt, In Bearbeitung oder Geschlossen. Standardmäßig ist der **Öffnen** Der Statusfilter wird angewendet auf Erkennungen Seite. Klicken Sie auf **Öffnen** Filter, um auf andere Filteroptionen zuzugreifen.

Sie können das auswählen **Versteckt** Status, um nur Erkennungen anzuzeigen, die derzeit versteckt von Tuning-Regeln.

Kategorie

Sie können nach Angriffs- oder Leistungserkennungen filtern oder eine spezifischere Kategorie auswählen, um Ihre Ansicht der Seite „Entdeckungen“ weiter zu verfeinern. Wenn Sie auf den Kategoriefilter klicken, werden die meisten Kategorien unter dem **Alle Angriffskategorien** und **Alle Leistungskategorien** Die Optionen sind nach der Anzahl der Funde in der Kategorie sortiert. Härteerkennungen werden immer am Ende der Liste angezeigt.

Zu den Erkennungen von Angriffen gehören die folgenden Kategorien, die den Phasen der Angriffskette entsprechen.

Befehl und Steuerung

Ein externer Server, der eine Verbindung zu einem kompromittierten Gerät in Ihrem Netzwerk hergestellt und aufrechterhalten hat. C&C-Server können Malware, Befehle und Payloads senden, um den Angriff zu unterstützen. Diese Erkennungen identifizieren, wenn ein internes Gerät mit einem Remotesystem kommuniziert, das anscheinend als C&C-Server fungiert.

Aufklärung

Ein Angreifer sucht nach hochwertigen Zielen und Schwächen, die er ausnutzen kann. Diese Erkennungen identifizieren Scans und Aufzählungstechniken.

Hinweis Bei Erkennungen kann ein bekannter Schwachstellenscanner wie Nessus und Qualys identifiziert werden. Klicken Sie auf den Gerätenamen, um zu bestätigen, ob dem Gerät bereits eine Vulnerability Scanner-Rolle im ExtraHop-System zugewiesen ist. Informationen zum Ausblenden von Erkennungen im Zusammenhang mit diesen Geräten finden Sie unter Erkennungen abstimmen.

Ausbeutung

Ein Angreifer nutzt eine bekannte Schwachstelle in Ihrem Netzwerk aus, um Ihre Ressourcen aktiv auszunutzen. Diese Erkennungen identifizieren ungewöhnliche und verdächtige Verhaltensweisen im Zusammenhang mit Ausnutzungstechniken.

Seitliche Bewegung

Ein Angreifer hat Ihr Netzwerk infiltriert und bewegt sich auf der Suche nach höherwertigen Zielen von Gerät zu Gerät. Diese Erkennungen identifizieren ungewöhnliches Geräteverhalten im Zusammenhang mit Datenübertragungen und Verbindungen im Ost-West-Korridor.

Zielgerichtete Maßnahmen

Der Angreifer ist kurz davor, sein Ziel zu erreichen, das vom Diebstahl sensibler Daten bis hin zur Verschlüsselung von Dateien bis hin zum Lösegeld reichen kann. Diese Erkennungen identifizieren, wenn ein Angreifer kurz davor ist, ein Kampagnenziel zu erreichen.

Vorsicht

Heben Sie Aktivitäten hervor, die keine unmittelbare Gefahr für den Betrieb darstellen, aber angegangen werden sollten, um eine gesunde Sicherheitslage aufrechtzuerhalten. Diese Erkennungen identifizieren auch Aktivitäten verdächtiger Teilnehmer, die mit Bedrohungsinformationen in Verbindung stehen.

Aufführung Erkennungen umfassen die folgenden Kategorien.

Authentifizierung und Zugriffskontrolle

Markieren Sie erfolglose Versuche von Benutzern, Clients und Servern, sich anzumelden oder auf Ressourcen zuzugreifen. Diese Erkennungen identifizieren potenzielle WLAN-Probleme im Zusammenhang mit Authentifizierung-, Autorisierungs- und Auditprotokollen (AAA), übermäßige LDAP-Fehler oder decken Geräte mit eingeschränkten Ressourcen auf.

Datenbank

Heben Sie Zugriffsprobleme für Anwendungen oder Benutzer auf der Grundlage der Analyse von Datenbankprotokollen hervor. Diese Erkennungen identifizieren Datenbankprobleme, z. B. Datenbankserver, die eine übermäßige Anzahl von Antwortfehlern senden , die zu langsamen oder fehlgeschlagenen Transaktionen führen können.

Desktop- und Anwendungsvirtualisierung

Heben Sie lange Ladezeiten oder Sitzungen mit schlechter Qualität für Endbenutzer hervor. Diese Erkennungen identifizieren Anwendungsprobleme, z. B. eine übermäßige Anzahl von Zero Windows, was darauf hindeutet, dass ein Citrix-Server überlastet ist.

Netzwerk-Infrastruktur

Heben Sie ungewöhnliche Ereignisse über die TCP-, DNS- und DHCP-Protokolle hervor. Diese Erkennungen können auf DHCP-Probleme hinweisen, die verhindern, dass Clients eine IP-Adresse vom Server abrufen, oder zeigen, dass Dienste Hostnamen aufgrund übermäßiger DNS-Antwortfehler nicht auflösen konnten.

Verschlechterung des Dienstes

Heben Sie Serviceprobleme oder Leistungseinbußen im Zusammenhang mit Voice over IP (VoIP), Dateiübertragungs- und E-Mail-Kommunikationsprotokollen hervor. Diese Erkennungen zeigen möglicherweise Dienstverschlechterungen an, bei denen VoIP-Anrufe fehlgeschlagen sind, und geben den entsprechenden SIP-Statuscode an, oder zeigen, dass nicht autorisierte Anrufer versucht haben, mehrere Anrufanfragen zu stellen.

Aufbewahrung

Heben Sie Probleme mit dem Benutzerzugriff auf bestimmte Dateien und Freigaben hervor, die bei der Auswertung des Netzwerkdateisystemverkehrs festgestellt wurden. Diese Erkennungen könnten darauf hinweisen, dass Benutzer aufgrund von SMB-Problemen am Zugriff auf Dateien auf Windows-Servern gehindert wurden oder dass NAS-Server (Netzwerk Attached Storage) aufgrund von NFS-Fehlern nicht erreicht werden konnten.

Web-Applikation

Heben Sie eine schlechte Webserverleistung oder Probleme hervor, die bei der Verkehrsanalyse über das HTTP-Protokoll beobachtet wurden. Diese Erkennungen zeigen möglicherweise, dass interne Serverprobleme zu einer übermäßigen Anzahl von Fehlern auf der Ebene 500 führen, sodass Benutzer nicht auf die Anwendungen und Dienste zugreifen können, die sie benötigen.

Aushärten Erkennungen identifizieren Sicherheitsrisiken und Möglichkeiten zur Verbesserung Ihrer Sicherheitslage.

Aushärten

Heben Sie bewährte Methoden zur Erhöhung der Sicherheit hervor, die durchgesetzt werden sollten, um das Risiko einer Ausnutzung zu minimieren. Diese Erkennungen identifizieren Möglichkeiten zur Verbesserung der Sicherheitslage Ihres Netzwerk, z. B. zur Verhinderung der Offenlegung von Anmeldeinformationen und zum Entfernen abgelaufener TLS-Zertifikate von Servern. Nachdem Sie auf eine Härteerkennung geklickt haben, können Sie zusätzliche Filter anwenden, um bestimmte Erkennungen innerhalb dieses Härteerkennungstyps anzuzeigen. Erfahre mehr über Filtern und Abstimmung von Härteerkennungen.

System zur Erkennung von Eindringlingen (Intrusion Detection System) Erkennungen identifizieren Sicherheitsrisiken und bösartiges Verhalten.

Erkennung von Eindringlingen

Heben Sie den Netzwerkverkehr hervor, der bekannten Signaturen unsicherer Praktiken, Exploit-Versuche und Indikatoren für Sicherheitslücken im Zusammenhang mit Malware und Command-and-Control-Aktivitäten entspricht.

Wichtig: Während IDS-Erkennungen Links zu Paketen für alle Protokolltypen beinhalten, sind Links zu Datensätzen nur für L7-Protokolle verfügbar.

Typ

Filtern Sie Ihre Erkennungsliste nach einem bestimmten Erkennungstyp, z. B. nach Datenexfiltration oder abgelaufenen SSL-Serverzertifikaten. Sie können auch eine CVE-Identifikationsnummer in diesen Filter eingeben, um nur Erkennungen für eine bestimmte öffentliche Sicherheitslücke anzuzeigen.

MITRE-Technik

Markieren Sie Erkennungen, die bestimmten MITRE-Technik-IDs entsprechen. Das MITRE-Framework ist eine weithin anerkannte Wissensdatenbank für Angriffe.

Täter und Opfer

Die mit einer Erkennung verbundenen Endpunkte von Täter und Opfer werden als Teilnehmer bezeichnet. Sie können Ihre Erkennungsliste so filtern, dass nur Erkennungen für einen bestimmten Teilnehmer angezeigt werden, z. B. für einen Täter, der eine unbekannte Remote-IP-Adresse hat, oder ein Opfer, das ein wichtiger Server ist. Gateway- oder Load Balancer-Geräte, die Externer Endpunkt Endpunktteilnehmern zugeordnet sind, können ebenfalls in diesen Filtern angegeben werden.

Abtretungsempfänger

Filtert Erkennungen nach dem Benutzer, der der Erkennung zugewiesen ist.

Mehr Filter

Sie können Ihre Erkennungen auch nach den folgenden Kriterien filtern:

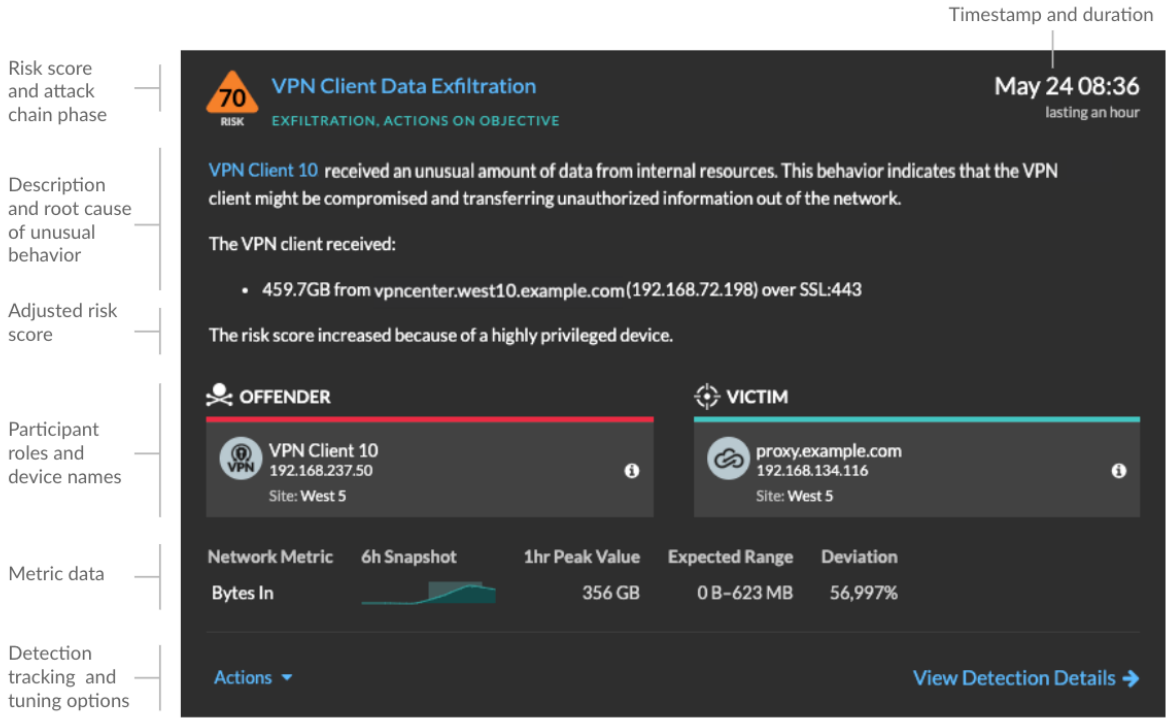
- Für Triage empfohlen
- Geräterollen
- Quelle
- Site (nur Konsole)
- Ticket-ID-Filter (Ticketverfolgung durch Dritte nur)
- Mindestrisikobewertung

Durch Erkennungen navigieren

Nachdem Sie ausgewählt haben, wie Ihre Erkennungsliste angezeigt, gruppiert und gefiltert werden soll, klicken Sie auf eine beliebige Erkennungskarte, um zur Erkennungsdetailseite zu gelangen.

Erkennungskarten

Jede Erkennungskarte identifiziert die Ursache der Entdeckung, die Erkennungskategorie, den Zeitpunkt der Erkennung sowie die Teilnehmer des Opfers und des Täters. Sicherheitserkennungen beinhalten eine Risikoscore.



Risikobewertung

Misst die Wahrscheinlichkeit, Komplexität und geschäftliche Auswirkungen einer Sicherheitserkennung. Diese Bewertung liefert eine Schätzung, die auf Faktoren wie Häufigkeit und Verfügbarkeit bestimmter Angriffsvektoren im Vergleich zu den erforderlichen Fähigkeiten eines potenziellen Hackers und den Folgen eines erfolgreichen Angriffs basiert. Das Symbol ist nach Schweregrad als rot (80-99), orange (31-79) oder gelb (1-30) farblich gekennzeichnet.

Teilnehmer

Identifiziert jeden an der Erkennung beteiligten Teilnehmer (Täter und Opfer) anhand des Hostnamens oder der IP-Adresse. Klicken Sie auf einen Teilnehmer, um grundlegende Details anzuzeigen und auf Links zuzugreifen. Interne Endpunkte zeigen einen Link zur Seite Geräteübersicht an; externe Endpunkte zeigen die Geolokalisierung der IP-Adresse an. Endpunkt-Suchlinks wie ARIN Whois und ein Link zur IP-Adressdetailseite. Wenn ein Teilnehmer ein anderes Gerät wie einen Load Balancer oder ein Gateway passiert hat, werden sowohl der Teilnehmer als auch das Gerät auf der Teilnehmerkarte angezeigt, aber nur der Ausgangsendpunkt wird als Teilnehmer betrachtet.

Hinweis Eine TLS-Entschlüsselung ist erforderlich, um die Ausgangsendpunkte anzuzeigen, wenn HTTPS aktiviert ist. Erfahre mehr über TLS-Entschlüsselung.

Bei der Gruppierung nach **Typ**, wird unter dem Erkennungstyp ein Übersichtsfeld angezeigt, das die Erkennungen nach Tätern und Opfern aufschlüsselt und Ihnen ermöglicht, schnell Teilnehmerfilter anwenden.

Bei der Gruppierung nach **Quelle**, die internen Geräterollensymbole sind rot hervorgehoben, wenn das Gerät bei einer Erkennung ein Täter war, und blaugrün, wenn das Gerät ein Opfer war. Du kannst klicken **Einzelheiten** unter dem Quellennamen, um eine Zusammenfassung der Entdeckungen anzuzeigen, an denen diese Quelle Teilnehmer war. Diese Gerätedetails werden neben der Erkennungskarte auf Breitbildschirmen (1900 Pixel oder mehr) angezeigt.

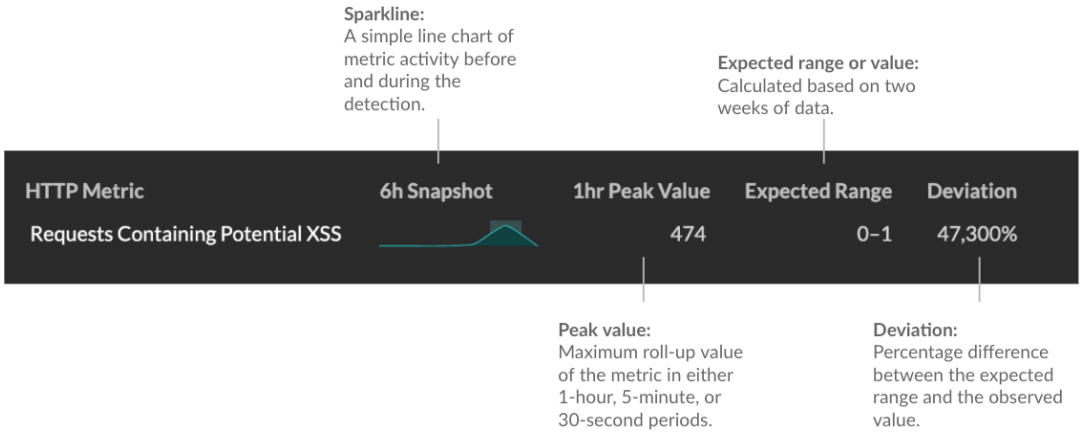
Dauer

Gibt an, wie lange das ungewöhnliche Verhalten erkannt wurde, oder zeigt FORTLAUFEND an, wenn das Verhalten gerade auftritt.

Bei Erkennungen, die auf bewährte Methoden zur Erhöhung der Sicherheit hinweisen, werden zwei Daten angezeigt: das erste und das Datum, an dem der Verstoß zuletzt identifiziert wurde.

Metrische Daten

Identifiziert zusätzliche Metrikdaten, wenn das ungewöhnliche Verhalten mit einer bestimmten Metrik oder einem bestimmten Schlüssel verknüpft ist. Wenn Metrikdaten für die Erkennung nicht verfügbar sind, wird die Art der anomalen Protokollaktivität angezeigt.



Erkennungsmanagement

Du kannst Spur oder stimmen die Erkennung aus der Dropdownliste Aktionen, oder klicken Sie auf **Erkennungsdetails anzeigen** um zur Seite mit den Erkennungsdetails zu navigieren.

Seite mit Erkennungsdetails

Die meisten Daten, die Sie benötigen, um eine Erkennung zu verstehen und zu validieren, werden auf der Erkennungsdetailseite angezeigt: Tabellen mit relevanten Metrikdaten, Aufzeichnungstransaktionen und Links zu Rohpaketen.

Auf die Informationen der Erkennungskarte folgen alle verfügbaren Abschnitte für die Erkennung. Diese Abschnitte variieren je nach Art der Erkennung.

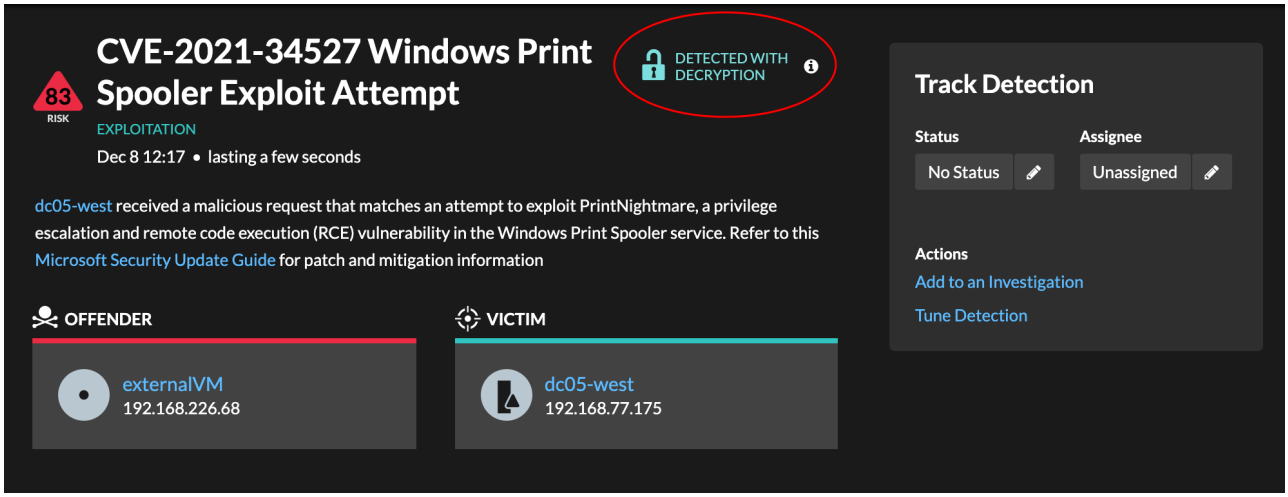
Spurerkennung

Du kannst Spur oder stimmen die Erkennung, oder klicken Sie auf **Zu einer Untersuchung hinzufügen** um die Erkennung in eine neue oder bestehende aufzunehmen Untersuchung.

Wenn Sie eine konfiguriert haben CrowdStrike-Integration auf Ihrem ExtraHop-System können Sie die Eindämmung von CrowdStrike-Geräten einleiten das sind Teilnehmer an der Erkennung. (Nur RevealX 360.)

Entschlüsselungsabzeichen

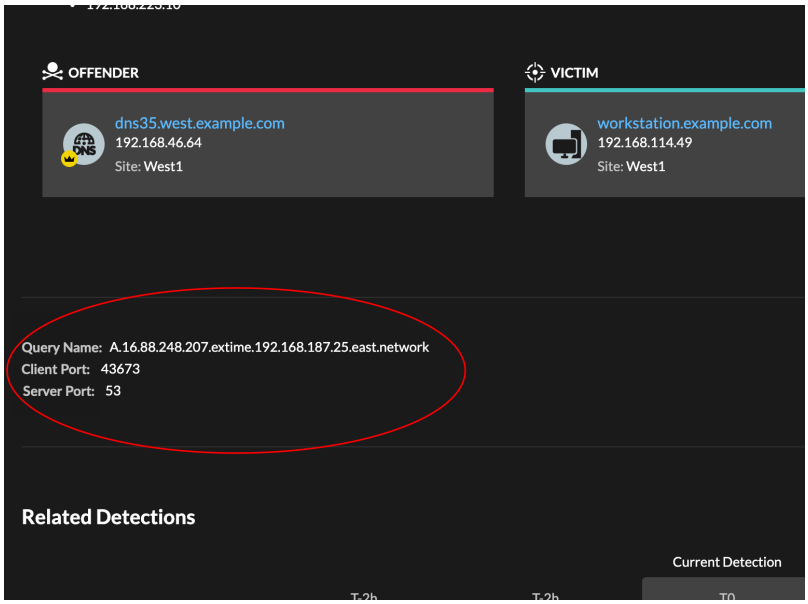
Wenn das ExtraHop-System verdächtiges Verhalten oder einen potenziellen Angriff in entschlüsselten Verkehrsaufzeichnungen feststellt, wird auf der Erkennungsdetailseite rechts neben dem Erkennungsnamen ein Entschlüsselungskennzeichen angezeigt.



Erfahre mehr über TLS-Entschlüsselung und Entschlüsseln des Datenverkehrs mit einem Windows-Domänencontroller.

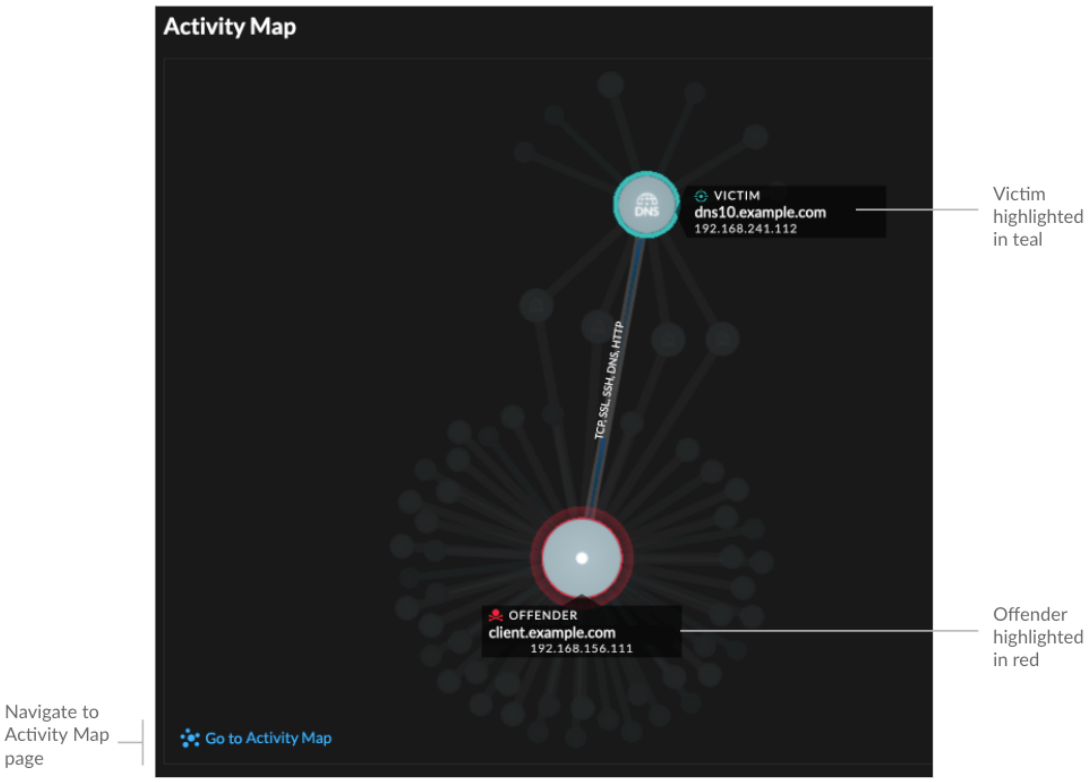
Erkennungseigenschaften

Stellt eine Liste der Eigenschaften bereit, die für die Erkennung relevant sind. Zu den Erkennungseigenschaften können beispielsweise eine Abfrage, eine URI oder ein Hacking-Tool gehören, das für die Erkennung von zentraler Bedeutung ist.



Karte der Aktivitäten

Bietet eine Aktivitätsdiagramm das hebt die Teilnehmer hervor, die an der Erkennung beteiligt waren. Auf der Aktivitätsdiagramm wird der Ost-West-Verkehr des mit der Erkennung verknüpften Protokoll angezeigt, sodass Sie den Umfang der bösartige Aktivität besser einschätzen können. Klicken Sie auf das Opfer oder den Täter, um ein Drop-down-Menü mit Links zur Geräteübersichtsseite und anderen Erkennungen aufzurufen, an denen das Gerät Teilnehmer ist.



Erkennungsdaten und Links

Stellt zusätzliche Daten im Zusammenhang mit der zu untersuchenden Entdeckung bereit. Die Datentypen können verwandte Metriken, Links zu enthalten Datensatz Transaktionsabfragen und ein Link zu einer allgemeinen Pakete abfrage. Die Verfügbarkeit von Metriken, Datensätzen und Paketen variiert je nach Erkennung. IDS-Erkennungen umfassen beispielsweise Links zu Paketen für alle Protokolltypen, aber Links zu Datensätzen sind nur für L7-Protokolle verfügbar.

Metrikdaten und Datensatztransaktionen werden in Tabellen angezeigt. Klicken Sie in einer Metriktabelle auf das Symbol um zugehörige Datensatztransaktionen anzuzeigen. Klicken Sie in einer Datensatztabelle auf das Symbol um die zugehörige Paketabfrage für eine Transaktion anzuzeigen.

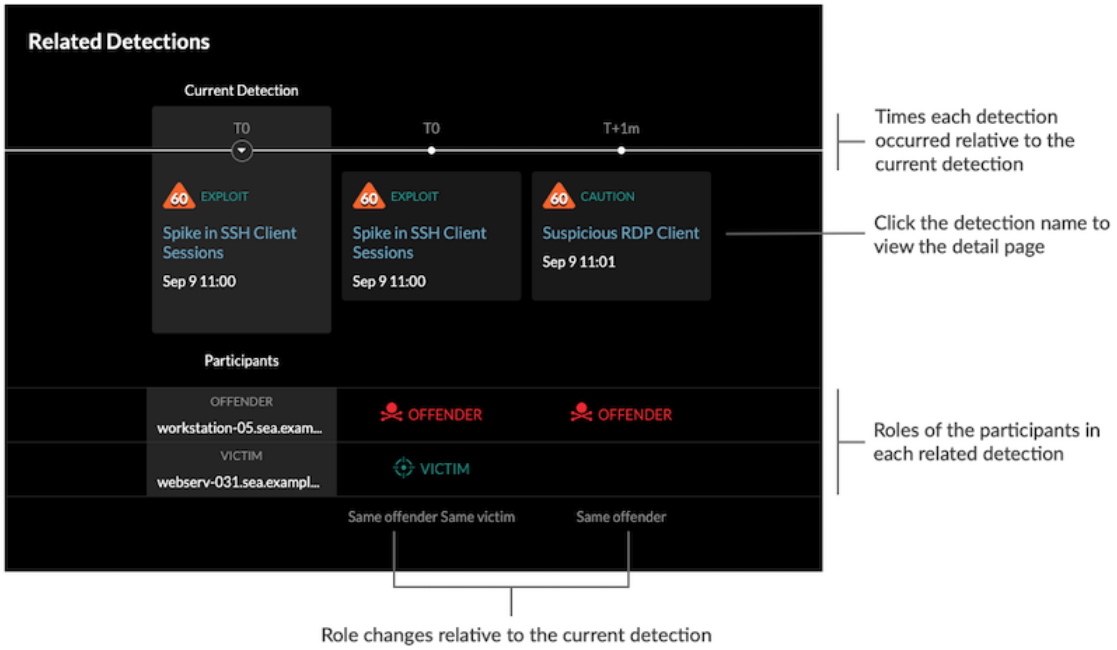
Hinweis: EIN Recordstore muss für die Anzeige von Transaktionen und fortlaufenden Transaktionen konfiguriert sein PCAP muss für das Herunterladen von Paketen konfiguriert sein.

Verhalten vergleichen

Stellt ein Diagramm bereit, in dem die Aktivität des Täters neben den Aktivitäten ähnlicher Geräte im Zeitraum angezeigt wird, in dem die Erkennung stattgefunden hat. Das Diagramm wird für Erkennungen im Zusammenhang mit unkonventionellen Aktivitäten eines Gerät angezeigt. Unerwartetes Verhalten wird hervorgehoben, indem es neben dem Verhalten von Geräten im Netzwerk mit ähnlichen Eigenschaften angezeigt wird.

Verwandte Erkennungen

Bietet eine Zeitleiste der Erkennungen im Zusammenhang mit der aktuellen Erkennung, anhand derer Sie eine größere Angriffskampagne identifizieren können. Zu den zugehörigen Erkennungen gehören die Rolle des Teilnehmer, die Dauer, der Zeitstempel und alle Rollenänderungen, wenn der Täter bei einer Erkennung zum Opfer einer anderen Erkennung wird. Klicken Sie in der Zeitleiste auf eine zugehörige Erkennung, um die Detailseite für diese Erkennung anzuzeigen.

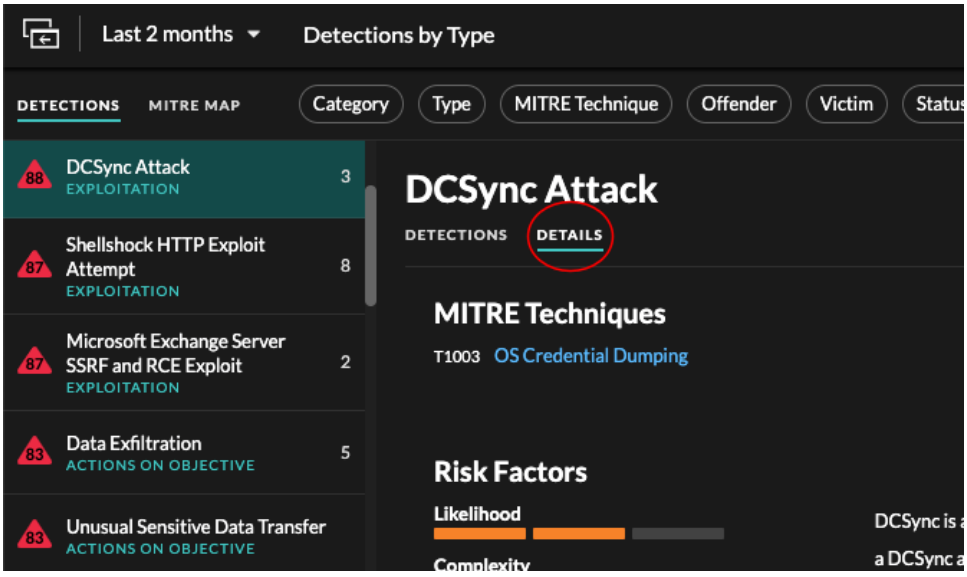


Verwandte Erkennungen, die in einem enthalten sind empfohlene Untersuchung sind mit goldenen Links gekennzeichnet und können angeklickt werden, um zur Ermittlungsseite zu gelangen.

Einzelheiten zur Erkennung

Enthält eine ausführliche Beschreibung der Erkennung, z. B. zugehörige MITRE-Techniken, Risikofaktoren, Angriffshintergründe und -diagramme, Abhilfemaßnahmen und Referenzlinks zu Sicherheitsorganisationen wie MITRE.

Diese Details werden neben der Erkennungskarte auf Breitbildschirmen angezeigt, oder Sie können auf sie zugreifen, indem Sie auf **Einzelheiten** unter dem Erkennungstitel, wenn die Erkennungsseite nach gruppiert wird **Typen**.



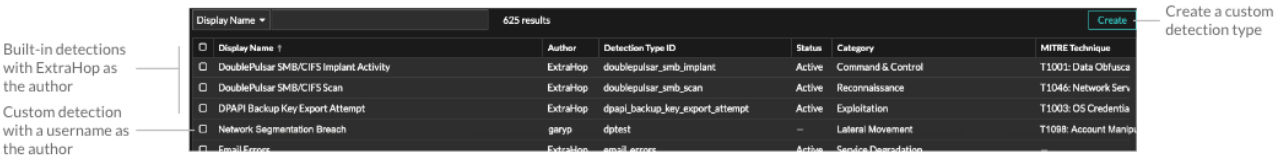
Für einige Erkennungstypen ist ein So funktioniert dieser Detektor Dieser Abschnitt enthält Antworten auf häufig gestellte Fragen dazu, warum eine Erkennung in Ihrem ExtraHop-System erscheint.

Hinweis: Du kannst Erkennung von Aktien Detailseiten mit anderen ExtraHop-Benutzern.

Erkennungskatalog

Der Erkennungskatalog enthält eine vollständige Liste aller Erkennungstypen im ExtraHop-System, einschließlich Erkennungstypen, die derzeit inaktiv sind oder überprüft werden. Sie können benutzerdefinierte Erkennungstypen auch auf der Seite Erkennungskatalog verwalten.

Sie können auf die Seite Erkennungskatalog zugreifen, indem Sie auf das Symbol Systemeinstellungen klicken. .



Zusätzlich zum Anzeigenamen und Autor können Sie die Liste der Erkennungstypen nach ID, Status, Kategorie, MITRE-Techniken, die dem Erkennungstyp zugeordnet sind, und Erkennungstypen filtern, die Daten aus dem Fluss unterstützen Sensoren.

Klicken Sie auf eine von ExtraHop verfasste Erkennung, um die Einstellungen für den Erkennungstyp Bereich, in dem der Name des Erkennungstyps, die ID, der Autor, der aktuelle Status des Erkennungstyps, das Datum, an dem der Erkennungstyp erstmals für die Produktion freigegeben wurde (sofern verfügbar), und die zugehörigen Kategorien angezeigt werden. Um mehr über die Erkennung zu erfahren, klicken Sie auf **Details zum Entdeckungstyp**.

Status des Entdeckungstyps

Dieser Status gibt an, ob eine Erkennung in Ihrer Umgebung verfügbar ist.

Aktiv

Aktive Erkennungstypen sind für alle Sensoren verfügbar und können in Ihrer Umgebung zu Erkennungen führen.

Inaktiv

Inaktive Erkennungstypen wurden von allen Sensoren entfernt und erzeugen keine Erkennungen mehr. Wenn ein Erkennungstyp inaktiv wird, werden bestehende Erkennungen dieses Typs weiter anzeigen.

Im Rückblick

In Review werden die Erkennungstypen auf einer begrenzten Anzahl von ExtraHop-Systemen evaluiert, bevor sie für alle Sensoren verfügbar sind. Diese Erkennungstypen werden einer gründlichen Prüfung auf Effizienz und Genauigkeit unterzogen, bevor sie einer zunehmenden Anzahl von Sensoren zur Verfügung gestellt werden. Der Überprüfungszeitraum kann bis zu mehreren Wochen dauern. Nach Abschluss der Überprüfung wird der Status des Entdeckungstyps auf Aktiv aktualisiert.

Im Folgenden finden Sie einige wichtige Überlegungen dazu, ob Erkennungen eines bestimmten Typs in Ihrer Umgebung sichtbar sind:

- Wenn aktive Erkennungen nicht wie erwartet angezeigt werden, erfordert der Erkennungstyp möglicherweise Entschlüsselung oder unterstützt möglicherweise keine Durchflusssensoren (nur RevealX 360).
- RevealX Enterprise-Systeme müssen verbunden sein mit Cloud-Dienste um regelmäßige Updates für den Erkennungskatalog zu erhalten. Ohne eine Verbindung zu Cloud Services Updates sind verzögert bis die Firmware aktualisiert ist.

Benutzerdefinierte Erkennungen

Sie können benutzerdefinierte Erkennungen auf der Seite Erkennungskatalog anzeigen und verwalten.

- Um einen benutzerdefinierten Erkennungstyp zu erstellen, klicken Sie auf **Erstellen** in der oberen rechten Ecke der Seite. Die Erkennungstyp-ID für den neuen Erkennungstyp muss mit der ID übereinstimmen, die im benutzerdefinierten Erkennungsauslöser enthalten ist. Erfahre mehr über Erstellen einer benutzerdefinierten Erkennung.
- Um eine benutzerdefinierte Erkennung zu bearbeiten, klicken Sie auf die Erkennung und bearbeiten Sie den Anzeigenamen, den Autor, die Erkennungskategorien und die zugehörigen MITRE-Techniken in der Erkennungstyp bearbeiten Panel. Sie können keine Erkennungen bearbeiten, bei denen ExtraHop als Autor aufgeführt ist.
- Um eine benutzerdefinierte Erkennung zu löschen, klicken Sie auf die Erkennung und dann auf **Löschen** aus dem Einstellungen für den Erkennungstyp Panel.
- Bei benutzerdefinierten Erkennungen wird unter Status immer ein Bindestrich (-) angezeigt.

Ermittlungen

(nur NDR-Modul) Mithilfe von Untersuchungen können Sie mehrere Funde in einer einzigen Zeitleiste und Karte hinzufügen und anzeigen. Anhand einer Zusammenfassung verbundener Erkennungen können Sie feststellen, ob verdächtiges Verhalten eine gültige Bedrohung darstellt und ob die Bedrohung von einem einzelnen Angriff oder Teil einer größeren Angriffskampagne stammt.

Sie können Untersuchungen von einer Entdeckungsdetailseite aus erstellen und zu ihnen hinzufügen oder von **Aktionen** Menü auf jeder Erkennungskarte. Ihr ExtraHop-System erstellt außerdem empfohlene Untersuchungen durch Smart Investigations, bei denen es sich um Untersuchungen handelt, die automatisch als Reaktion auf potenziell bösartige Aktivität erstellt werden.

Jede Ermittlungsseite enthält die folgenden Tools:

Zeitplan der Untersuchung

Die Untersuchungszeitleiste wird auf der linken Seite der Seite angezeigt und listet die hinzugefügten Funde auf, beginnend mit der neuesten Erkennung. Neue Funde, die der Untersuchung hinzugefügt werden, werden in der Zeitleiste entsprechend der Uhrzeit und dem Datum der Erkennung angezeigt. Erkennungsteilnehmer werden unter dem Erkennungstitel angezeigt, und Informationen zur Erkennungsverfolgung, wie Beauftragter und Status, werden neben den Teilnehmern angezeigt.

Angriffskategorien

Die Kategorien der hinzugefügten Funde werden oben auf der Ermittlungsseite angezeigt.

Die Kette der Angriffskategorien zeigt die Anzahl der Funde in jeder Kategorie an, nicht die Reihenfolge, in der die Erkennungen aufgetreten sind. Einen genauen Überblick darüber, wie die Erkennungen im Laufe der Zeit aufgetreten sind, finden Sie im Zeitplan der Untersuchung.

Untersuchungen anzeigen

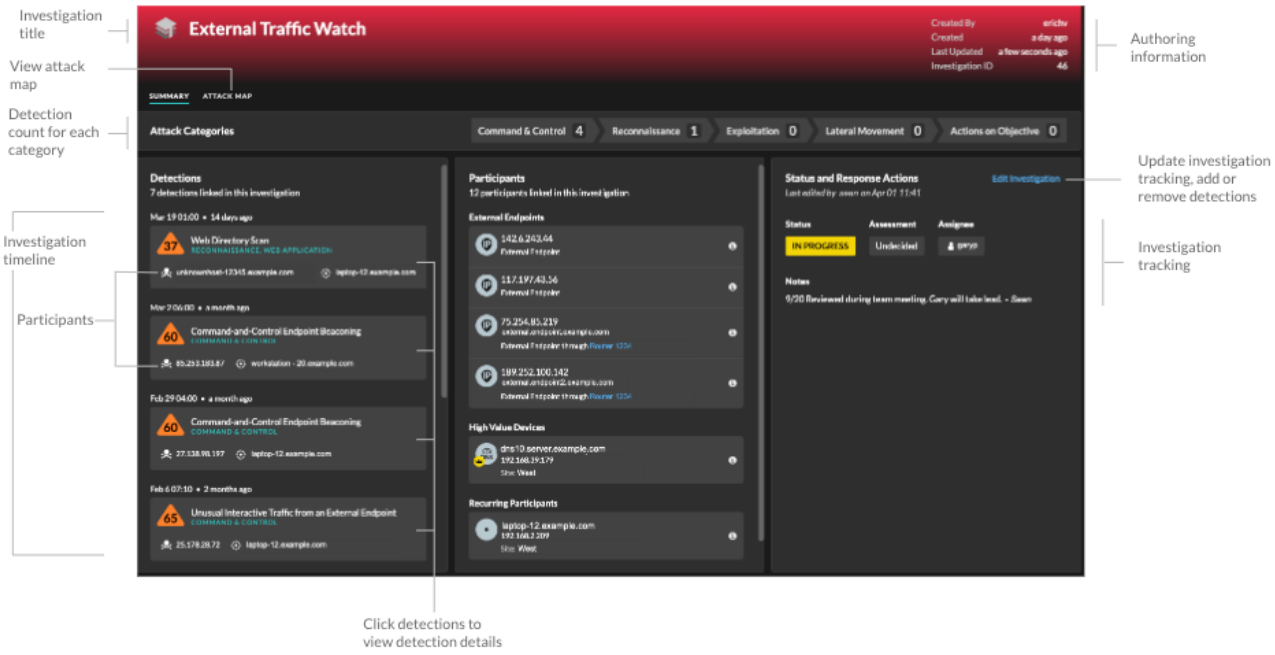
Oben auf der Ermittlungsseite gibt es zwei Optionen, um die Untersuchung anzuzeigen: Zusammenfassung und Angriffskarte. Beide Optionen bieten einen einzigartigen Überblick über Ihre Untersuchung.

Zusammenfassung

Standardmäßig beginnen Ermittlungen in **Zusammenfassung** Ansicht, die den Zeitplan für die Erkennung, eine aggregierte Teilnehmerliste und ein Panel zur Verfolgung des Status und der Reaktionsmaßnahmen für die Untersuchung enthält.

Sie können in der Untersuchungszeitleiste auf eine Erkennung klicken, um sie anzuzeigen Erkennungsdetails, klicken Sie dann auf das X-Symbol, um die Erkennungsdetails zu schließen und zur Zusammenfassung der Untersuchung zurückzukehren. Sie können auch auf Gehe zu klicken Symbol in der oberen rechten Ecke, um die Seite mit den Erkennungsdetails in einem neuen Tab anzuzeigen.

Im Panel „ Teilnehmer“ werden die Teilnehmer an der Untersuchung nach externen Endpunkten, hoher Wert Geräten und wiederkehrenden Teilnehmern gruppiert. Dabei handelt es sich um Teilnehmer, die bei mehreren Funden in der Untersuchung vorkommen. Klicken Sie auf einen Teilnehmer, um Details anzuzeigen und auf Links zuzugreifen.

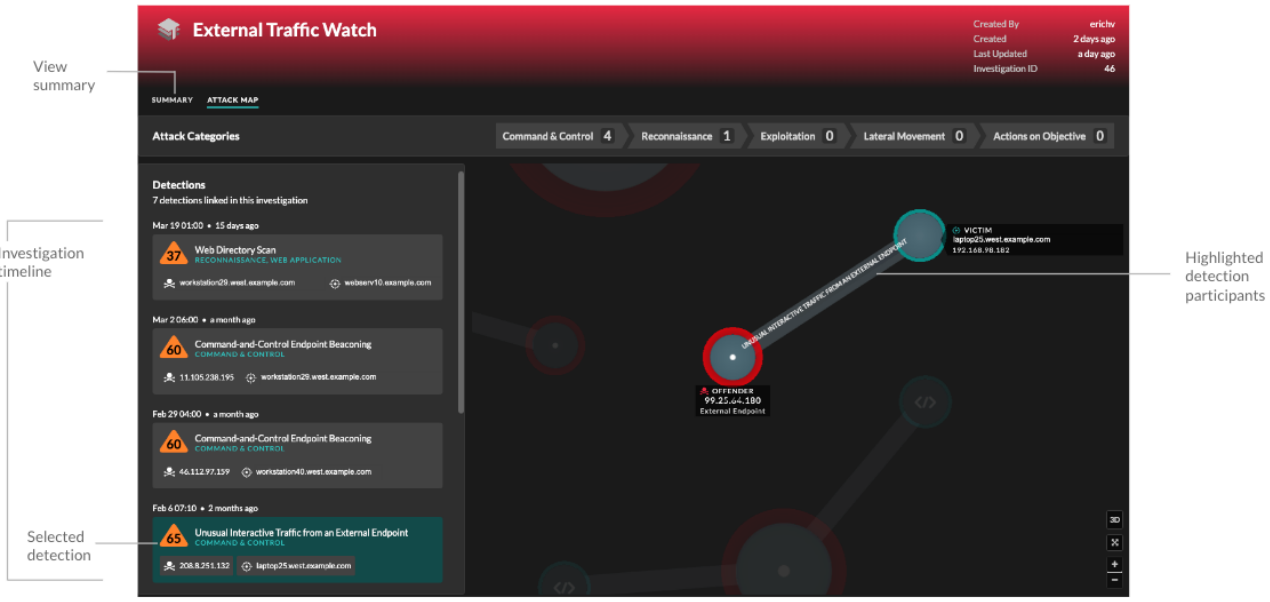


In der Status - und Reaktionsmaßnahmen Panel, klicken **Untersuchung bearbeiten** um den Namen der Untersuchung zu ändern, den Status oder die endgültige Bewertung der Untersuchung festzulegen, einen Beauftragten anzugeben oder Anmerkungen hinzuzufügen .

Sie können fortfahren Verfolgen Sie einzelne Erkennungen nachdem Sie sie zu einer Untersuchung hinzugefügt haben.

Angriffskarte

In **Angriffskarte** Ansicht, der Täter und das Opfer von jeder Erkennung in der Untersuchung werden auf einer interaktiven Karte neben dem Zeitplan der Untersuchung angezeigt.



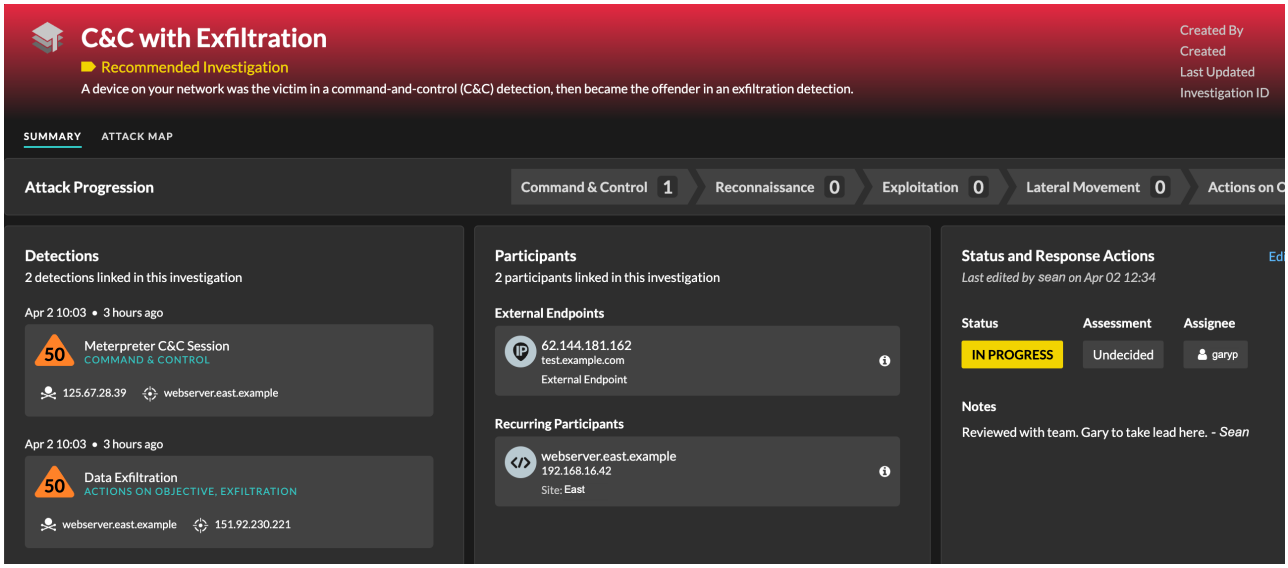
Die Teilnehmer sind durch Linien verbunden, die mit dem Erkennungstyp beschriftet sind, und die Geräterollen werden durch ein Symbol dargestellt.

- Klicken Sie in der Zeitleiste der Untersuchung auf eine Erkennung, um die Teilnehmer hervorzuheben. Kreise werden rot hervorgehoben, wenn das Gerät bei mindestens einer Erkennung im Rahmen der Untersuchung als Täter aufgetreten ist, und blaugrün hervorgehoben, wenn es sich bei dem Gerät um ein Opfer handelt. Die Markierungen werden aktualisiert , wenn Sie auf eine andere Erkennung klicken, damit Sie leichter erkennen können, wann ein Teilnehmer vom Opfer zum Täter wird.
- Klicken Sie auf einen Kreis, um Details wie den Hostnamen, die IP-Adresse oder die MAC-Adresse des Gerät anzuzeigen oder um zu den zugehörigen Erkennungen oder dem Seite „Geräteübersicht“.
- Zeigen Sie mit der Maus auf einen Kreis oder eine Linie, um das Etikett anzuzeigen.

Empfohlene Untersuchungen

Der ExtraHop Machine Learning Service überwacht die Netzwerkaktivität auf Kombinationen von Angriffstechniken, die auf bösartiges Verhalten hinweisen könnten. Wenn eine Kombination identifiziert wird, erstellt das ExtraHop-System eine empfohlene Untersuchung, sodass Ihre Sicherheitsteams die Situation beurteilen und schnell reagieren können, wenn bösartiges Verhalten bestätigt wird.

Wenn beispielsweise ein Gerät Opfer einer Erkennung in der Kategorie Command-and-Control wird, bei einer Exfiltrationserkennung aber zum Täter wird, empfiehlt das ExtraHop-System eine C&C mit Exfiltrationsuntersuchung.



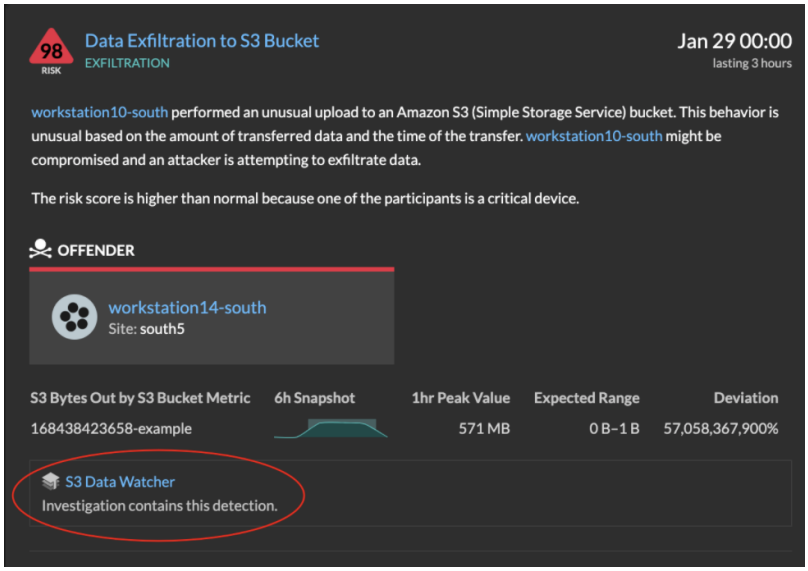
Sie können mit empfohlenen Untersuchungen auf die gleiche Weise interagieren wie von Benutzern erstellte Untersuchungen, z. B. indem Sie Erkennungen hinzufügen oder entfernen, einen Beauftragten angeben und einen Status und eine Bewertung festlegen.

Empfohlene Untersuchungen finden Sie in der Tabelle der Untersuchungen. Sie können die sortieren Erstellt von Spalte, um Untersuchungen zu finden, die von ExtraHop erstellt wurden.

Durch Ermittlungen navigieren

Nachdem eine Erkennung zu einer Untersuchung hinzugefügt wurde, wird unten auf der Erkennungskarte und auf der Seite mit den Erkennungsdetails ein Link zu der Untersuchung angezeigt.

Klicken Sie auf den Namen, um die Untersuchung zu öffnen, und klicken Sie dann auf der Ermittlungsseite auf den Namen der Entdeckung, um zur Erkennungsdetailseite zurückzukehren.



Erfahren Sie, wie eine Untersuchung erstellen.

Auffinden von Funden im ExtraHop-System

Die Seite „Erkennungen“ bietet zwar schnellen Zugriff auf alle Funde, aber im gesamten ExtraHop-System gibt es Indikatoren und Links zu Erkennungen.

Hinweis: Erkennungen bleiben im System entsprechend Ihrer System-Lookback-Kapazität für 1-Stunden-Metriken mit einer Mindestspeicherzeit von fünf Wochen. Erkennungen verbleiben im System ohne unterstützende Metriken, wenn Ihre System-Lookback-Kapazität weniger als fünf Wochen beträgt.

- Klicken Sie auf einer Seite mit der Geräteübersicht auf Erkennungen, um eine Liste der zugehörigen Erkennungen anzuzeigen. Klicken Sie auf den Link für eine einzelne Erkennung, um die Seite mit den Erkennungsdetails anzuzeigen.
- Klicken Sie auf einer Seite mit der Gerätegruppen-Übersicht auf den Link Erkennungen, um zur Seite „ Erkennungen“ zu gelangen. Die Erkennungsliste wird nach Teilnehmern gefiltert, die Mitglieder der Gerätegruppe sind.
- Klicken Sie auf einer Aktivitätsdiagramm auf ein Gerät, das animierte Impulse rund um die Kreisbeschriftung anzeigt, um eine Liste der zugehörigen Funde anzeigen. Klicken Sie auf den Link für eine einzelne Erkennung, um die Erkennungsdetails anzuzeigen.
- Bewegen Sie den Mauszeiger in einem Diagramm auf einem Dashboard oder einer Protokollseite über Erkennungsmarker um den Titel der zugehörigen Erkennung anzuzeigen, oder klicken Sie auf die Markierung, um die Erkennungsdetails anzuzeigen.

Erkennungen optimieren

Hier sind einige bewährte Methoden, die Sie implementieren sollten, um Ihre Erkennungen zu verbessern: Fügen Sie Details zu Ihrem Netzwerk hinzu, aktivieren Sie das ExtraHop-System, potenziell verdächtigen Traffic zu erkennen, und filtern Sie Ihre Seitenaufrufe nach Ihren Prioritäten.

Die meisten dieser Einstellungen bieten Kontext zu Ihrem Netzwerk, den Sie bereitstellen können, um sowohl maschinelles Lernen als auch regelbasierte Erkennungen zu verbessern. Diese Einstellungen werden manchmal übersehen und können die Qualität Ihrer Erkennungen beeinträchtigen.

Entschlüsselung konfigurieren

Verschlüsselter HTTP-Verkehr ist ein häufiger Angriffsvektor, auch weil Angreifer wissen, dass der Verkehr in der Regel versteckt ist. Und wenn Ihr Netzwerk über Active Directory verfügt, sind eine Reihe von Erkennungen im verschlüsselten Datenverkehr in der gesamten Domain versteckt.

Wir empfehlen dringend, die Entschlüsselung für zu aktivieren TLS und Active Directory.

Tuning-Parameter konfigurieren

Diese Einstellung verbessert die Genauigkeit regelbasierter Erkennungen. Du das ExtraHop-System mit Details versorgen über Ihre Netzwerkumgebung, um den Kontext zu den beobachteten Geräten bereitzustellen.

Beispielsweise wird eine regelbasierte Erkennung generiert, wenn ein internes Gerät mit externen Datenbanken kommuniziert. Wenn Datenverkehr zu einer externen Datenbank erwartet wird oder die Datenbank Teil einer legitimen Cloud-basierten Speicher- oder Produktionsinfrastruktur ist, können Sie einen Optimierungsparameter festlegen, um den Datenverkehr zur genehmigten externen Datenbank zu ignorieren.

Netzwerkstandorte konfigurieren

Mit dieser Einstellung können Sie intern oder extern klassifizieren Endpunkte, denen Sie vertrauen, z. B. ein CIDR-Block von IP-Adressen, mit denen Ihre Geräte regelmäßig eine Verbindung herstellen. Erkennungen und Systemmetriken durch maschinelles Lernen basieren auf Gerät- und Verkehrsklassifizierungen.

Wenn Ihre Geräte beispielsweise regelmäßig eine Verbindung zu einer unbekannten, aber vertrauenswürdigen Domain herstellen, die als externe IP-Adresse eingestuft ist, werden Erkennungen für diese Domain unterdrückt.

Tuning-Regeln erstellen

Mit diesen Einstellungen können Sie Erkennungen ausblenden nachdem das System sie generiert hat. Wenn Sie eine Erkennung sehen, die keinen Mehrwert bietet, können Sie das Rauschen aus Ihrer Gesamtansicht reduzieren.

Wenn beispielsweise eine Erkennung anhand eines Täters, eines Opfers oder anderer Kriterien generiert wird, die für Ihr Netzwerk kein Problem darstellen, können Sie alle früheren und zukünftigen Erkennungen mit diesen Kriterien ausblenden.

Teilen Sie externe Klartext-Daten

Mit dieser Option kann der Machine Learning Service Erfassen Sie IP-Adressen, Hostnamen und Domains die mit verdächtigen Aktivitäten in Verbindung stehen.

Wenn Sie diese Option aktivieren, erweitern Sie einen kollektiven Datensatz potenzieller Bedrohungen, der Ihnen und Ihrem Beitrag zur Sicherheitsgemeinschaft helfen kann.

Erkennungen verfolgen

Mit dieser Option können Sie Weisen Sie einem Benutzer eine Erkennung zu, fügen Sie Notizen hinzu und aktualisieren Sie den Status von bestätigt bis geschlossen. Anschließend können Sie die Seite „Erkennungen“ filtern, um gelöste Probleme aus der Ansicht zu entfernen oder die Erkennungen zu überprüfen.

Eine Erkennung teilen

Sie können die URL von einer Erkennungsdetailseite an andere Benutzer des ExtraHop-Systems senden.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Erkennungen**.
3. Suchen Sie die Erkennung, die Sie teilen möchten, und klicken Sie dann auf den Erkennungstitel.
4. Kopieren Sie oben im Browser die gesamte URL.

Hinweis: Teilen Sie eine PDF-Datei der Erkennungsdetailseite, indem Sie auf das PDF-Symbol in der oberen rechten Ecke der Seite klicken.

Nächste Schritte

- Erstellen Sie eine Regel für Erkennungsbenachrichtigungen um E-Mail-Benachrichtigungen über eine Erkennung zu erhalten.

Bestätigen Sie Erkennungen

Bestätigungen bieten eine visuelle Möglichkeit, um zu erkennen, dass eine Erkennung erkannt wurde. Sie können eine Erkennung bestätigen, um die Teammitglieder darüber zu informieren, dass Sie ein Ticket untersuchen oder dass das Problem geprüft wurde und für die weitere Bearbeitung priorisiert werden sollte. Sie können Ihre Ansicht der Erkennungen auch so filtern, dass nur unbestätigte Erkennungen angezeigt werden.

Bevor Sie beginnen
Benutzer müssen über eingeschränkte Schreibzugriffe oder höher verfügen Privilegien um eine Erkennung zu bestätigen oder eine Bestätigung zu löschen.

Im Folgenden finden Sie wichtige Überlegungen zur Bestätigung von Erkennungen:

- Eine Bestätigung verbirgt die Erkennung nicht.

- Nachdem eine Erkennung bestätigt wurde, werden ein Zeitstempel und der Benutzername der Person angezeigt , die die Erkennung bestätigt hat.
- Eine Bestätigung kann von jedem Benutzer gelöscht werden, auch wenn er nicht der Benutzer ist, der die Erkennung ursprünglich bestätigt hat.

Gehen Sie wie folgt vor, um eine Erkennung zu bestätigen:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Erkennungen**.
3. klicken **Bestätigen** aus der unteren linken Ecke der Erkennungskarte.

   Die Erkennung zeigt den Benutzernamen und den Zeitstempel an. klicken **Zurücksetzen** um eine Bestätigung zu löschen.

Eine Untersuchung erstellen

Erstellen Sie eine Untersuchung, um mehrere Funde in einer einzigen Zeitleiste und Karte anzuzeigen.

Sie können auf die Liste der erstellten Untersuchungen von der **Ermittlungen** Symbol in der oberen rechten Ecke der Erkennungsseite.

Bevor Sie beginnen

- Benutzern muss der Zugriff auf das NDR-Modul gewährt werden und sie müssen nur über eingeschränkte Schreibberechtigungen verfügen Privilegien oder höher, um die Aufgaben in diesem Handbuch abzuschließen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Erkennungen**.
3. Klicken Sie **Aktionen** aus der unteren linken Ecke der Erkennungskarte.
4. Klicken Sie **Zu einer Untersuchung hinzufügen...**.
5. Wählen **Erkennung zu einer neuen Untersuchung hinzufügen**.
6. Klicken Sie **Weiter**.
7. Geben Sie einen Namen ein und fügen Sie Anmerkungen zur neuen Untersuchung hinzu.
8. Klicken Sie **Erstellen**.

Nachdem der Name der Untersuchung unten auf der Erkennungskarte angezeigt wird, können Sie auf den Namen der Untersuchung klicken, um die Zeitleiste und die Karte anzuzeigen.

- Um der Untersuchung eine Erkennung hinzuzufügen, klicken Sie auf **Aktionen**, und klicken Sie dann auf **Zu einer Untersuchung hinzufügen...**.
- Um eine Erkennung aus einer Untersuchung zu löschen, klicken Sie in der Untersuchungszeitleiste auf das Löschsymbol (X) neben der Erkennung.

Erstellen Sie eine Regel für Erkennungsbenachrichtigungen

Erstellen Sie eine Benachrichtigungsregel, wenn Sie eine Benachrichtigung über Entdeckungen erhalten möchten , die bestimmten Kriterien entsprechen.

Video: Sehen Sie sich die entsprechende Schulung an: Erkennungsbenachrichtigungen konfigurieren

Wenn eine Erkennung generiert wird, die Ihren Kriterien entspricht, wird eine Benachrichtigung mit Informationen von Erkennungskarte.

Sie können das System so konfigurieren, dass es eine E-Mail an eine Empfängerliste sendet oder einen bestimmten Webhook aufruft. RevealX 360-Benutzer können eine Benachrichtigungsregel erstellen, die einen Webhook aufruft, um Erkennungsdaten an einen zu exportieren konfigurierte Integration.

Hinweis: (Nur RevealX 360) Wenn Sie eine Benachrichtigungsregel erstellen, um Erkennungsdaten in eine SIEM-Integration zu exportieren, erstellen Sie die Benachrichtigung direkt aus dem Integrationen Seite in den Verwaltungseinstellungen , um Felder für Benachrichtigungsregeln vorab auszufüllen.

Bevor Sie beginnen

- Benutzern muss der Zugriff auf das NDR- oder NPM-Modul gewährt werden und sie müssen über vollständige Schreibberechtigungen verfügen Privilegien oder höher, um die Aufgaben in diesem Handbuch abzuschließen.
- RevealX Enterprise benötigt eine Verbindung zu ExtraHop Cloud Services um Benachrichtigungen per E-Mail zu senden, kann aber eine Benachrichtigung über einen Webhook ohne Verbindung senden.
- E-Mail-Benachrichtigungen werden über ExtraHop Cloud Services gesendet und können identifizierbare Informationen wie IP-Adressen, Benutzernamen, Hostnamen, Domainnamen, Gerätenamen oder Dateinamen enthalten. RevealX Enterprise-Benutzer, deren behördliche Anforderungen externe Verbindungen verbieten, können Benachrichtigungen mit Webhook-Aufrufen so konfigurieren, dass Benachrichtigungen ohne externe Verbindung gesendet werden.
- E-Mail-Benachrichtigungen werden von no-reply@notify.extrahop.com gesendet. Stellen Sie sicher, dass Sie diese Adresse zu Ihrer Liste der zulässigen Absender hinzufügen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Regeln für Benachrichtigungen**.
3. Klicken Sie **Erstellen**.
4. Klicken Sie auf eine der folgenden Optionen:
   - Wählen Sie für NDR-Module **Sicherheitserkennung**.
   - Wählen Sie für NPM-Module **Leistungserkennung**.
5. In der Name Feld, geben Sie einen eindeutigen Namen für die Benachrichtigungsregel ein.
6. In der Beschreibung Feld, fügen Sie Informationen zur Benachrichtigungsregel hinzu.
7. In der Kriterien Abschnitt, klicken Sie **Kriterien hinzufügen** um Kriterien anzugeben, nach denen eine Benachrichtigung generiert wird.
   - **Für Triage empfohlen**
   - **Mindestrisikobewertung**
   - **Typ**
   - **Kategorie**
   - **MITRE-Technik** (nur NDR)
   - **Täter**
   - **Opfer**
   - **Rolle des Geräts**
   - **Teilnehmer**
   - **Standort**

   Die Kriterienoptionen entsprechen den Filteroptionen auf der Seite „Erkennungen“.
8. In der Ziel Wählen Sie im Abschnitt aus den folgenden Optionen aus, wie die Benachrichtigung gesendet werden soll:

Option	Description
E-Mail senden	Senden Sie E-Mail-Benachrichtigungen an eine Verteilerliste.

Option	Description
Benutzerdefinierter Webhook	Senden Sie eine JSON-Nutzlast an eine Webhook-URL.
Integration	Exportieren Sie Erkennungsdaten in eine konfigurierte Integration. Für Integrationen empfehlen wir, dass ExtraHop-Administratoren Regeln für Erkennungsbenachrichtigungen aus dem Integrationen Seite.

9. Wenn Sie E-Mail senden als Ziel ausgewählt haben, führen Sie die folgenden Schritte aus:
   a) Geben Sie einzelne E-Mail-Adressen an, getrennt durch ein Komma.
   b) Klicken Sie **Speichern**.
10. Wenn Sie Benutzerdefinierter Webhook als Ziel ausgewählt haben, führen Sie die folgenden Schritte aus:
    a) In der Nutzlast-URL Feld, geben Sie die URL des Webhooks ein.
    b) Klicken Sie **Erweiterte Verbindungsoptionen anzeigen** um Folgendes zu konfigurieren:
       - In der Benutzerdefinierte Header Abschnitt, klicken **Header hinzufügen** um benutzerdefinierte Schlüssel:Wert-Paare anzugeben.

         Benutzerdefinierte Header werden dem Header der Webhook-HTTP-POST-Anforderung hinzugefügt.
       - Wählen Sie einen Authentifizierungstyp aus.
         - Keine Authentifizierung
         - Standardauthentifizierung

           Geben Sie den Benutzernamen und das Passwort für die Zielanwendung ein.
         - Inhaber-Token

           Geben Sie das Zugriffstoken für die Zielanwendung ein.
       - Konfigurieren Sie die Verbindungsmethode.
         - Wählen Sie diese Option, um den Webhook über einen konfigurierten globalen Proxy zu leiten. (Nur RevealX Enterprise.)
         - Wählen Sie, um die Serverzertifikatsüberprüfung zu überspringen.
    c) Unter Verhalten bei Benachrichtigungen, wählen Sie aus, wann das ExtraHop-System Benachrichtigungen bei einer Erkennung sendet.
       - **Für jedes Erkennungsupdate senden**

         Erhalten Sie jedes Mal eine Benachrichtigung, wenn die Erkennung aktualisiert wird.

         Diese Auswahl wird empfohlen, wenn Sie Erkennungsdaten in ein SIEM exportieren und einen umfassenden Überblick über die Erkennungsaktivitäten wünschen.
       - **Einmal pro Erkennung senden**

         Erhalten Sie eine einzige Benachrichtigung, wenn eine Erkennung erstellt wird.

         Diese Auswahl ist optimal, um eine Gruppe zu benachrichtigen, wenn eine Erkennung auftritt, ohne die Gruppe mit nachfolgenden Aktualisierungen zu überfordern.
    d) Unter Payload-Optionen, wählen Sie aus, ob Sie das senden möchten Standard-Nutzlast oder geben Sie eine benutzerdefinierte JSON-Nutzlast ein.

       Wenn Sie unter Benachrichtigungsverhalten ausgewählt haben, dass Benachrichtigungen einmal pro Erkennung gesendet werden sollen, müssen Sie eine benutzerdefinierte Nutzlast senden.
       - **Standard-Nutzlast**

Füllen Sie die Webhook-Nutzlast mit einem Kernsatz von Erkennungsfeldern.

In der Dropdownliste „Payload-Felder hinzufügen “ können Sie auf zusätzliche Felder klicken, die Sie in die Payload aufnehmen möchten.

- **Benutzerdefinierte Nutzlast**

  Füllen Sie die Webhook-Nutzlast mit benutzerdefiniertem JSON auf.

  Sie können die vorgeschlagene benutzerdefinierte Nutzlast in der **Nutzlast bearbeiten** Fenster.

e) Klicken Sie **Speichern**.

f) Klicken Sie **Verbindung testen**.

Eine Nachricht mit dem Titel Testbenachrichtigung wird an die Payload-URL gesendet, um die Verbindung zu bestätigen.

Hinweis Bestätigen Sie nach dem Testen der Verbindung, dass Sie die Benachrichtigung in der Zielanwendung erhalten haben. RevealX Enterprise zeigt eine Fehlermeldung an, wenn die Testbenachrichtigung nicht erfolgreich war.

11. In der Optionen Abschnitt, der **Benachrichtigungsregel aktivieren** Das Kontrollkästchen ist standardmäßig aktiviert. Deaktivieren Sie das Kontrollkästchen, um die Benachrichtigungsregel zu deaktivieren.

Wenn eine Erkennung den Kriterien entspricht, wird eine Benachrichtigung gesendet.

Referenz zur Webhook-Benachrichtigung

Dieses Handbuch enthält Informationen zum Schreiben benutzerdefinierter Payloads für Sicherheits- oder Leistungserkennungsbenachrichtigungen mit benutzerdefinierten Webhook- oder Integrationszielen. Das Handbuch enthält einen Überblick über die Payload (JSON) -Schnittstelle, die Standardnutzlast für Webhook-Ziele, eine Liste von Payload-Feldern, die Sie der Standard-Payload hinzufügen können, und Beispiele für die JSON-Struktur für gängige Webhook-Ziele wie Slack, Microsoft Teams und Google Chat.

Hier sind einige Überlegungen zu Webhook-Benachrichtigungen:

- RevealX 360 kann keine Webhook-Aufrufe an Endpunkte in Ihrem internen Netzwerk senden. Webhook-Ziele müssen für externen Verkehr geöffnet sein.
- RevealX Enterprise muss eine direkte Verbindung zu Webhook-Endpunkten herstellen, um Benachrichtigungen zu senden.
- Webhook-Ziele müssen über ein Zertifikat verfügen, das von einer Zertifizierungsstelle (CA) des Mozilla CA Certificate Program signiert wurde. siehe https://wiki.mozilla.org/CA/Included_Certificates für Zertifikate von vertrauenswürdigen öffentlichen CAs.

Weitere Informationen zu Benachrichtigungsregeln finden Sie unter Erstellen Sie eine Regel für Erkennungsbenachrichtigungen.

Nutzlast JSON

ExtraHop-Webhooks sind in JSON formatiert und werden unterstützt von Jinja2-Template-Engine. Wenn Sie eine Regel für Benachrichtigungen zur Sicherheits- oder Leistungserkennung erstellen und einen benutzerdefinierten Webhook oder eine benutzerdefinierte Integration als Ziel auswählen, haben Sie die Möglichkeit, eine Standardnutzlast auszuwählen oder Ihre eigene benutzerdefinierte Nutzlast zu schreiben.

Standard-Nutzlast

Die Standard-Payload-Option ist verfügbar, wenn Sie als Benachrichtigungsverhalten für den Webhook auswählen, dass für jedes Erkennungsupdate eine Benachrichtigung gesendet wird. Die Standardnutzlast enthält den folgenden Basissatz an Informationen zu einer Erkennung.

```
{
    "title": "{{ title }}",
    "type": "{{ type }}",
    "src": {
```

```
        "type": "{{ src.type }}",
        "hostname": "{{ src.hostname }}",
        "ipaddr": "{{ src.ipaddr }}",
        "role": "{{ src.role }}",
        "endpoint": "{{ src.endpoint }}",
        "device": {
            "oid": {{ src.device.oid }},
            "name": "{{ src.device.name }}",
            "ipaddrs": {{ src.device.ipaddrs | safe }},
            "macaddr": "{{ src.device.macaddr }}"
        }
    },
    "dst": {
        "type": "{{ dst.type }}",
        "hostname": "{{ dst.hostname }}",
        "ipaddr": "{{ dst.ipaddr }}",
        "role": "{{ dst.role }}",
        "endpoint": "{{ dst.endpoint }}",
        "device": {
            "oid": {{ dst.device.oid }},
            "name": "{{ dst.device.name }}",
            "ipaddrs": {{ dst.device.ipaddrs | safe }},
            "macaddr": "{{ dst.device.macaddr }}"
        }
    },
    "additional_participants": {{ additional_participants | safe }},
    "properties": {{ properties }},
    "description": "{{ description }}",
    "categories_ids": {{ categories_ids | safe }},
    "mitre_techniques": {{ mitre_techniques | safe }},
    "recommended": "{{ recommended }}",
    "recommended_factors": {{ recommended_factors | safe }},
    "url": "{{ url }}",
    "risk_score": {{ risk_score }},
    "time": {{ time }},
    "id": {{ detection_id or id }}
}
```

Sie können die Standardnutzlast ändern, indem Sie Felder aus der Dropdownliste Payload-Felder hinzufügen auswählen. Um benutzerdefinierte Änderungen vorzunehmen, können Sie Ihre Payload-Option in ändern **Benutzerdefinierte Nutzlast**, bearbeiten Sie dann die vorgeschlagene Nutzlast in der **Nutzlast bearbeiten** Fenster.

Benutzerdefinierte Nutzlast
Wählen Sie die benutzerdefinierte Payload-Option, um das vorgeschlagene JSON für einen Benachrichtigungsregel-Webhook zu bearbeiten.

Wenn Sie auswählen, dass für jedes Erkennungsupdate eine Benachrichtigung gesendet werden soll unter Verhalten bei Benachrichtigungen, die vorgeschlagene benutzerdefinierte Nutzlast enthält den folgenden JSON-Code:

```
{
    "title": "{{ title }}",
    "type": "{{ type }}",
    "src": {
        "type": "{{ src.type }}",
        "hostname": "{{ src.hostname }}",
        "ipaddr": "{{ src.ipaddr }}",
        "role": "{{ src.role }}",
        "endpoint": "{{ src.endpoint }}",
        "device": {
            "oid": {{ src.device.oid }},
            "name": "{{ src.device.name }}",
```

```
            "ipaddrs": {{ src.device.ipaddrs | safe }},
            "macaddr": "{{ src.device.macaddr }}"
        }
    },
    "dst": {
        "type": "{{ dst.type }}",
        "hostname": "{{ dst.hostname }}",
        "ipaddr": "{{ dst.ipaddr }}",
        "role": "{{ dst.role }}",
        "endpoint": "{{ dst.endpoint }}",
        "device": {
            "oid": {{ dst.device.oid }},
            "name": "{{ dst.device.name }}",
            "ipaddrs": {{ dst.device.ipaddrs | safe }},
            "macaddr": "{{ dst.device.macaddr }}"
        }
    },
    "additional_participants": {{ additional_participants | safe }},
    "properties": {{ properties }},
    "description": "{{ description }}",
    "categories_ids": {{ categories_ids | safe }},
    "mitre_techniques": {{ mitre_techniques | safe }},
    "recommended": "{{ recommended }}",
    "recommended_factors": {{ recommended_factors | safe }},
    "url": "{{ url }}",
    "risk_score": {{ risk_score }},
    "time": {{ time }},
    "id": {{ detection_id or id }}
}
```

Wenn Sie auswählen, dass pro Erkennungsupdate eine Benachrichtigung gesendet werden soll unter Verhalten bei Benachrichtigungen, die vorgeschlagene benutzerdefinierte Nutzlast enthält den folgenden JSON-Code:

```
{
    "title": "{{ title }}",
    "type": "{{ type }}",
    "url": "{{ url }}",
    "description": "{{ description }}",
    "api": {{ api | safe }},
    "categories_string": "{{ categories_string }}",
    "categories_array": {{ categories_array | safe }},
    "victims": {{ victims | safe }},
    "offenders": {{ offenders | safe }},
    "description_format": "{{ description_format }}",
    "victim_primary": {{ victim_primary | safe }},
    "offender_primary": {{ offender_primary | safe }}
}
```

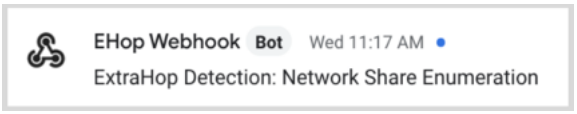
Hinweis: Bevor Sie sich die Zeit nehmen, eine lange benutzerdefinierte Nutzlast einzugeben, empfehlen wir Ihnen, Ihre Verbindung zur Webhook-URL zu testen. Auf diese Weise können Sie sicher sein, dass Probleme nicht auf einen Verbindungsfehler zurückzuführen sind.

Syntaxvalidierung
Der Webhook-Editor bietet JSON- und Jinja2-Syntaxvalidierung. Wenn Sie eine Zeile eingeben , die eine falsche JSON- oder Jinja2-Syntax enthält, wird unter dem Payload-Feld ein Fehler mit dem Fehler angezeigt.
Variablen
Erkennungsvariablen werden der Nutzlast hinzugefügt, indem der Variablenname zwischen doppelten Gruppen geschweifter Klammern ({{und}}) eingefügt wird.

Das Beispiel in der Payload enthält beispielsweise eine Variable für den Erkennungstitel:

```
"text": "ExtraHop Detection: {{title}}"
```

Wenn eine Erkennung einer Benachrichtigungsregel mit der Variablen entspricht, wird die Variable durch den Erkennungstitel ersetzt. Wenn die Benachrichtigungsregel beispielsweise mit der Erkennung für Network Share Enumeration übereinstimmt, wird die Variable durch den Titel in der Benachrichtigung ersetzt, ähnlich der folgenden Abbildung:



Sehen Sie eine Liste von Erkennungsvariablen.

Filter
: Filter ermöglichen es Ihnen, eine Variable zu ändern.

JSON übergeben

Wenn die Variable einen Wert zurückgibt, der in JSON formatiert ist, wird der Wert automatisch maskiert und in eine Zeichenfolge übersetzt. Wenn Sie gültiges JSON an Ihr Webhook-Ziel übergeben möchten, müssen Sie Folgendes angeben: `safe` filtern:

```
{{<variable> | safe }}
```

Im folgenden Beispiel gibt die Variable Erkennungsdaten über Teilnehmer im JSON-Format direkt an das Webhook-Ziel zurück:

```
{{api.participants | safe }}
```

IF-Kontoauszüge
: Eine IF-Anweisung kann überprüfen, ob ein Wert für die Variable verfügbar ist. Wenn die Variable leer ist, können Sie eine alternative Variable angeben.

```
 {% if {{<variable>}} %}
```

Im folgenden Beispiel prüft die IF-Anweisung, ob ein Wert für die Opfervariable verfügbar ist:

```
{% if victims %}
```

Im folgenden Beispiel prüft die IF-Anweisung, ob ein Täternname verfügbar ist. Wenn es keinen Wert für den Namen des Täters gibt, wird stattdessen der Wert für die Variable IP-Adresse des Täters zurückgegeben.

```
{% if offender.name %}{{offender.name}}{%else%}{{offender.ipaddr}}
{% endif %}
```

FÜR Schleifen
: Eine FOR-Schleife kann es der Benachrichtigung ermöglichen, ein Array von Objekten anzuzeigen.

```
{% for <array-object-variable> in <array-variable> %}
```

Im folgenden Beispiel wird eine Liste mit Täternamen aus dem Täter-Array in der Benachrichtigung angezeigt. Eine IF-Anweisung sucht nach weiteren Elementen im Array (`{% if not loop.last %}`) und

fügt einen Zeilenumbruch hinzu, bevor der nächste Wert gedruckt wird (\n). Wenn ein Tätername leer ist, gibt der Standardfilter „Unbekannter Name“ für den Wert zurück.

```
{% for offender in offenders %}
  {{offender.name | default ("Unknown Name")}}
  {% if not loop.last %}\n
  {% endif %}
{% endfor %}
```

Verfügbare Erkennungsvariablen

Die folgenden Variablen sind für Webhook-Benachrichtigungen über Erkennungen verfügbar.

titel: *Schnur*

Der Titel der Erkennung.

Beschreibung: *Schnur*

Eine Beschreibung der Erkennung.

typ: *Schnur*

Die Art der Erkennung.

ID: *Zahl*

Die eindeutige Kennung für die Erkennung.

url: *Schnur*

Die URL für die Erkennung im ExtraHop-System.

Risikobewertung: *Zahl*

Die Risikoscore der Erkennung.

Standort: *Schnur*

Der Standort, an dem die Erkennung stattgefunden hat.

Startzeit_Text: *Schnur*

Die Uhrzeit, zu der die Erkennung gestartet wurde.

Endzeittext: *Schnur*

Die Uhrzeit, zu der die Erkennung beendet wurde.

kategorien_array: *Reihe von Zeichenketten*

Eine Reihe von Kategorien, zu denen die Erkennung gehört.

kategorien_string: *Schnur*

Eine Zeichenfolge, die die Kategorien auflistet, zu denen die Erkennung gehört.

mitre_tactics: *Reihe von Zeichenketten*

Eine Reihe von MITRE-Taktik-IDs, die mit der Erkennung verknüpft sind.

mitre_tactics_string: *Schnur*

Eine Zeichenfolge, die die mit der Erkennung verknüpften MITRE-Taktik-IDs auflistet.

mitre_techniques: *Reihe von Zeichenketten*

Eine Reihe von MITRE-Technik-IDs, die mit der Erkennung verknüpft sind.

mitre_techniques_string: *Schnur*

Eine Zeichenfolge, die die MITRE-Technik-IDs auflistet, die mit der Erkennung verknüpft sind.

primärer Täter: *Objekt*

(Veraltet) Ein Objekt, das den Haupttäter identifiziert und die folgenden Eigenschaften enthält:

extern: *Boolesch*

Der Wert ist `true` wenn die IP-Adresse des primären Täters außerhalb Ihres Netzwerk liegt.

ipaddr: *Schnur*

Die IP-Adresse des Haupttäters.

Name: ***Schnur***

Der Name des Haupttäters.

Straftäter: ***Reihe von Objekten***

Eine Reihe von Täterobjekten, die mit der Erkennung verknüpft sind. Jedes Objekt enthält die folgenden Eigenschaften:

extern: ***Boolesch***

Der Wert ist `true` wenn die IP-Adresse des Täters außerhalb Ihres Netzwerk liegt.

ipaddr: ***Schnur***

Die IP-Adresse des Täters. Gilt für Feststellungen mit mehreren Tätern.

Name: ***Schnur***

Der Name des Täters. Gilt für Feststellungen mit mehreren Tätern.

primäres Opfer: ***Objekt***

(Veraltet) Ein Objekt, das das primäre Opfer identifiziert und die folgenden Eigenschaften enthält:

extern: ***Boolesch***

Der Wert ist `true` wenn die IP-Adresse des primären Opfers außerhalb Ihres Netzwerk liegt.

ipaddr: ***Schnur***

Die IP-Adresse des primären Opfers.

Name: ***Schnur***

Der Name des Hauptopfers.

Opfer: ***Reihe von Objekten***

Eine Reihe von Opferobjekten, die mit der Erkennung verknüpft sind. Jedes Objekt enthält die folgenden Eigenschaften:

extern: ***Boolesch***

Der Wert ist `true` wenn die IP-Adresse des Opfers außerhalb Ihres Netzwerk liegt.

ipaddr: ***Schnur***

Die IP-Adresse des Opfers. Gilt für Erkennungen mit mehreren Opfern.

Name: ***Schnur***

Der Name des Opfers. Gilt für Erkennungen mit mehreren Opfern.

api: ***Objekt***

Ein Objekt, das alle Felder enthält, die von `GET /detections/{id}operation`. Weitere Informationen finden Sie in der Einführung in die ExtraHop REST API.

Webhook-Beispiele

Die folgenden Abschnitte enthalten JSON-Vorlagen für gängige Webhook-Ziele.

Slack

Nachdem du eine Slack-App erstellt und eingehende Webhooks für die App aktiviert hast, kannst du einen eingehenden Webhook erstellen. Wenn du einen eingehenden Webhook erstellst, generiert Slack die URL, die du in das Feld Payload-URL in deiner Benachrichtigungsregel eingibst.

Das folgende Beispiel zeigt die JSON-Nutzlast für einen Slack-Webhook:

```
{
    "blocks": [
        {
            "type": "header",
            "text": {
                "type": "plain_text",
                "text": "Detection: {{ title }}"
            }
        },
```

```
        {
            "type": "section",
            "text": {
                "type": "mrkdwn",
                "text": "• *Risk Score:* {{ risk_score }}\n • *Category:*
 {{ categories_string }}\n • *Site:* {{ site }}\n • *Primary Offender:*
 {{ offender_primary.name}} ({{ offender_primary.ipaddr}})\n • *Primary
 Victim:* {{ victim_primary.name }} ({{ victim_primary.ipaddr }})\n"
            }
        },
        {
            "type": "section",
            "text": {
                "type": "plain_text",
                "text": "Detection ID: {{ id }}"
            },
            "text": {
                "type": "mrkdwn",
                "text": "<{{ url }}|View Detection Details>"
            }
        }
    ]
}
```

Microsoft-Teams

Du kannst einem Teams-Kanal einen eingehenden Webhook als Connector hinzufügen. Nachdem Sie einen eingehenden Webhook konfiguriert haben, generiert Teams die URL, die Sie in das Feld Payload-URL in Ihrer Benachrichtigungsregel eingeben müssen.

Das folgende Beispiel zeigt die JSON-Nutzlast für einen Microsoft Teams-Webhook:

```
{
   "type":"message",
   "attachments":[
      {
         "contentType":"application/vnd.microsoft.card.adaptive",
         "contentUrl":null,
         "content":{
            "$schema":"https://adaptivecards.io/schemas/adaptive-card.json",
            "type":"AdaptiveCard",
            "body":[
               {
                  "type":"ColumnSet",
                  "columns":[
                     {
                        "type": "Column",
                        "width":"16px",
                        "items":[
                           {
                              "type":"Image",
                              "horizontalAlignment":"center",
                              "url":"https://assets.extrahop.com/
favicon.ico",
                              "altText":"ExtraHop Logo"
                           }
                        ]
                     },
                     {
                        "type": "Column",
                        "width":"stretch",
                        "items":[
                           {
```

```
                                "type":"TextBlock",
                                "text":"ExtraHop RevealX",
                                "weight": "bolder"
                            }
                        ]
                    }
                ]
            },
            {
                "type":"TextBlock",
                "text":"**{{ title }}**"
            },
            {
                "type":"TextBlock",
                "spacing":"small",
                "isSubtle":true,
                "wrap":true,
                "text":"{{ description }}"
            },
            {
                "type":"FactSet",
                "facts":[
                    {
                        "title":"Risk Score:",
                        "value":"{{ risk_score }}"
                    },
                    {
                        "title":"Category:",
                        "value":"{{ categories_string }}"
                    },
                    {
                        "title":"Site:",
                        "value":"{{ site }}"
                    },
                    {
                        "title":"Primary Offender:",
                        "value":"{{ offender_primary.name }}
 ({{ offender_primary.ipaddr }})"
                    },
                    {
                        "title":"Primary Victim:",
                        "value":"{{ victim_primary.name }}
 ({{ victim_primary.ipaddr }})"
                    }
                ]
            },
            {
                "type":"ActionSet",
                "actions":[
                    {
                        "type":"Action.OpenUrl",
                        "title":"View Detection Details",
                        "url":"{{ url }}"
                    }
                ]
            }
        ]
    }
  ]
}
```

Google Chat

In einem Google-Chatroom können Sie auf das Drop-down-Menü neben dem Raumnamen klicken und Webhooks verwalten auswählen. Nachdem Sie einen Webhook hinzugefügt und ihm einen Namen gegeben haben, generiert Google Chat die URL, die Sie in das Feld Payload-URL in Ihrer Benachrichtigungsregel eingeben müssen.

Das folgende Beispiel zeigt die JSON-Nutzlast für einen Google Chat-Webhook:

```
{
    "cards": [
        {
            "header": {
                "title": "{{title}}"
            },
            "sections": [
                {
                    "widgets": [
                        {
                            "keyValue": {
                                "topLabel": "Risk score",
                                "content": "{{risk_score}}"
                            }
                        },
                        {
                            "keyValue": {
                                "topLabel": "Categories",
                                "content": "{{categories_string}}"
                            }
                        }
                        {% if offenders %}
                       ,{
                            "keyValue": {
                                "topLabel": "Offenders",
                                "contentMultiline": "true",
                                "content": "{% for offender in offenders %}
{% if offender.name %}{{offender.name}}{% else %}{{offender.ipaddr}}{% endif
 %}{% if not loop.last %}\n{% endif %}{% endfor %}"
                            }
                        }
                        {% endif %}
                        {% if victims %}
                       ,{
                            "keyValue": {
                                "topLabel": "Victims",
                                "contentMultiline": "true",
                                "content": "{% for victim in victims %}{%
 if victim.name %}{{victim.name}}{% else %}{{victim.ipaddr}}{% endif %}{% if
 not loop.last %}\n{% endif %}{% endfor %}"
                            }
                        }
                        {% endif %}
                    ]
                },
                {
                    "widgets": [
                        {
                            "buttons": [
                                {
                                    "textButton": {
                                        "text": "VIEW DETECTION DETAILS",
                                        "onClick": {
                                            "openLink": {
```

```
                                                "url": "{{url}}"
                                            }
                                        }
                                    }
                                }
                            ]
                        }
                    ]
                }
            ]
        }
    ]
}
```

Eine Benachrichtigungsregel für den Erkennungskatalog erstellen

Erstellen Sie eine Benachrichtigungsregel, wenn Sie eine Benachrichtigung erhalten möchten, wenn neue Erkennungen auf Ihrem ExtraHop-System aktiv werden.

Wenn ein Erkennungstypstatus im Erkennungskatalog auf Aktiv gesetzt ist, wird eine Benachrichtigung mit Informationen über die Erkennung, einschließlich Erkennungstyp und Erkennungsstatus, gesendet. Die Benachrichtigung enthält auch die Daten, an denen die Erkennung veröffentlicht wurde, und die letzte Aktualisierung, sofern diese Daten verfügbar sind.

Bevor Sie beginnen

- Benutzern muss der Zugriff auf das NDR- oder NPM-Modul gewährt werden und sie müssen Vollzugriff haben Privilegien oder höher, um die Aufgaben in diesem Handbuch abzuschließen.
- Das ExtraHop-System muss verbunden mit ExtraHop Cloud Services um Benachrichtigungen per E-Mail zu senden.
- E-Mail-Benachrichtigungen werden von no-reply@notify.extrahop.com gesendet. Stellen Sie sicher, dass Sie diese Adresse zu Ihrer Liste der zulässigen Absender hinzufügen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Regeln für Benachrichtigungen**.
3. Klicken Sie **Erstellen**.
4. Klicken Sie auf eine der folgenden Optionen:
   - Wählen Sie für NDR-Module Security Detection Catalog aus.
   - Wählen Sie für NPM-Module die Option Performance Detection Catalog aus.
5. Geben Sie im Feld Name einen eindeutigen Namen für die Benachrichtigungsregel ein.
6. Fügen Sie im Feld Beschreibung Informationen zur Benachrichtigungsregel hinzu.
7. Geben Sie einzelne E-Mail-Adressen an, getrennt durch ein Komma.
8. In der Optionen Abschnitt, der **Benachrichtigungsregel aktivieren** Das Kontrollkästchen ist standardmäßig aktiviert. Deaktivieren Sie das Kontrollkästchen, um die Benachrichtigungsregel zu deaktivieren.
9. Klicken Sie **Speichern**.

Eine Erkennung verfolgen

Mit der Erkennungsverfolgung können Sie Benutzer zuweisen, einen Status festlegen und Notizen zu einer Erkennungskarte hinzufügen.

Sie können Ihre Ansicht der Erkennungen auch nach einem bestimmten Status oder einem bestimmten Beauftragten filtern.

Video: Sehen Sie sich die entsprechende Schulung an: Erkennungsverfolgung

Bevor Sie beginnen
Benutzer müssen eingeschränkte Schreibmöglichkeiten haben Privilegien oder höher, um die Aufgaben in diesem Handbuch abzuschließen.

Sie können den Zuständigen in einen beliebigen Benutzer im System ändern, Notizen hinzufügen und den Status einer Erkennung auf einen der folgenden Werte setzen:

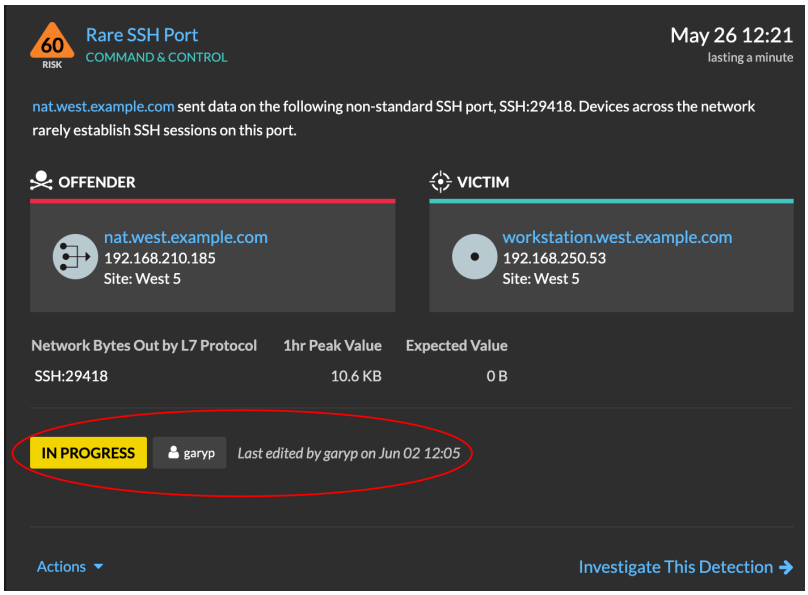
Öffnen
Die Erkennung wurde nicht überprüft.

Bestätigen
Die Erkennung wurde festgestellt und sollte bei der Nachverfolgung priorisiert werden.

Im Gange
Die Erkennung wurde einem Teammitglied zugewiesen und wird derzeit überprüft.

Geschlossen — Maßnahme ergriffen
Die Erkennung wurde überprüft und Maßnahmen ergriffen, um dem potenziellen Risiko zu begegnen.

Geschlossen — Keine Maßnahmen ergriffen
Die Erkennung wurde überprüft und erforderte keine Maßnahmen.



Im Folgenden finden Sie wichtige Überlegungen zu Tracking-Erkennungen:

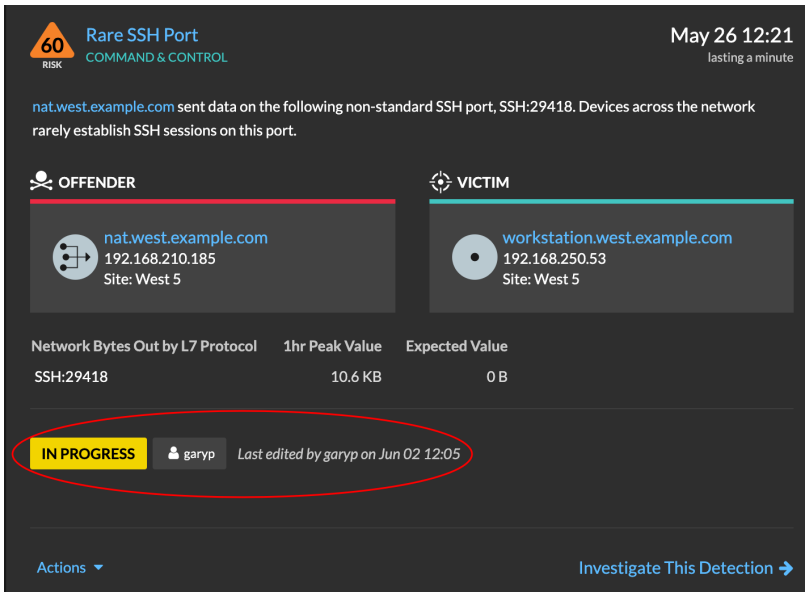
- Der Status Bestätigt oder Geschlossen verbirgt die Erkennung nicht.
- Der Erkennungsstatus kann von jedem berechtigten Benutzer aktualisiert werden.
- Sie können Erkennungsverfolgung mit ExtraHop und Systemen von Drittanbietern in der Verwaltung Einstellungen.

Gehen Sie wie folgt vor, um eine Erkennung zu verfolgen:

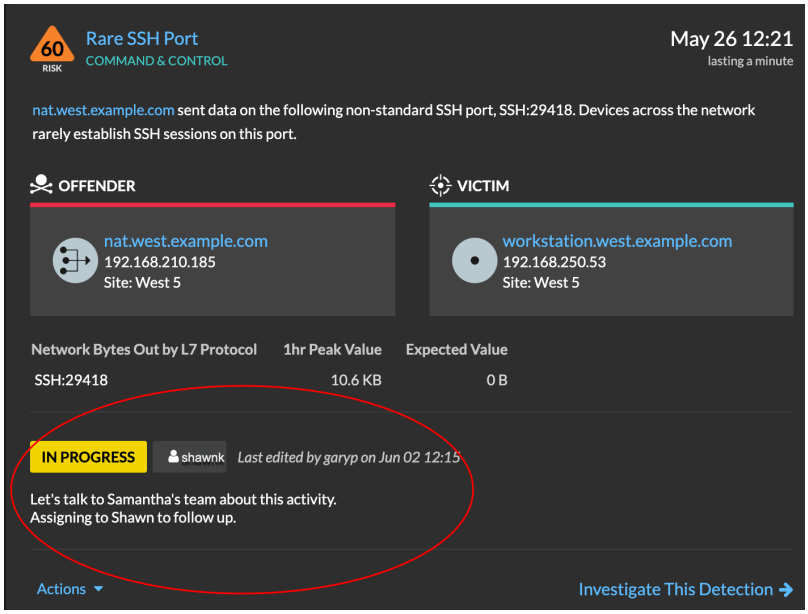
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Erkennungen**.
3. klicken **Aktionen** aus der unteren linken Ecke der Erkennungskarte.

4. Optional: Klicken Sie auf einen Erkennungsstatus, um ihn zur Erkennung hinzuzufügen.

Option	Description
Bestätigen	Die Erkennung wurde festgestellt und sollte bei der Nachverfolgung priorisiert werden.
Im Gange	Die Erkennung wurde einem Teammitglied zugewiesen und wird derzeit überprüft.
Geschlossen — Maßnahme ergriffen	Die Erkennung wurde überprüft und Maßnahmen ergriffen, um dem potenziellen Risiko zu begegnen.
Geschlossen — Keine Maßnahmen ergriffen	Die Erkennung wurde überprüft und erforderte keine Maßnahmen.



5. klicken **Spurerkennung...** um den Erkennungsstatus festzulegen, weisen Sie die Erkennung einem Benutzer zu und fügen Sie der Erkennungskarte Notizen hinzu.



Aus dem **Aktionen** Dropdown, wählen **Spurerkennung...** und dann **Öffnen** um den Status aus der Erkennung zu entfernen; der Beauftragte und die Notizen bleiben sichtbar.

Eine Erkennung von einer Erkennungskarte aus verfolgen

Sie können eine Erkennung verfolgen, indem Sie einen Beauftragten, einen Status und Notizen von einer Erkennungskarte hinzufügen.

Gehen Sie wie folgt vor, um eine Erkennung zu verfolgen:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Erkennungen**.
3. Klicken **Aktionen** aus der unteren linken Ecke der Erkennungskarte.
4. Optional: Klicken Sie auf einen Erkennungsstatus, um ihn zur Erkennung hinzuzufügen.
5. Klicken **Spurerkennung...** um den Erkennungsstatus festzulegen, weisen Sie die Erkennung einem Benutzer zu und fügen Sie der Erkennungskarte Notizen hinzu.

   Aus dem **Aktionen** Dropdown, wählen **Spurerkennung...** und dann **Offen** um den Status der Erkennung zu entfernen; der Beauftragte und die Notizen bleiben sichtbar.

Verfolgen Sie eine Gruppe von Erkennungen anhand einer Erkennungsübersicht

In einem Übersichtsfenster auf der Seite Erkennungen können Sie mehreren Erkennungen gleichzeitig einen Status, einen Beauftragten oder eine Notiz zuweisen.

Ein Übersichtsfenster wird angezeigt, wenn Erkennungen in der Übersichtsansicht auf der Seite Erkennungen nach Typ gruppiert sind.

Gehen Sie wie folgt vor, um eine Gruppe von Erkennungen anhand einer Erkennungsübersicht zu verfolgen:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Erkennungen**.

   Standardmäßig sollte sich die Seite in der Übersichtsansicht befinden, wobei die Erkennungen nach Typ gruppiert sind. Wenn dies nicht der Fall ist, klicken Sie auf Ansicht „Zusammenfassung“ und dann nach Typ gruppieren.
3. Klicken Sie in Ihrer Erkennungsliste auf einen Erkennungstyp.

4. Klicken Sie auf die Kriterien, nach denen Sie filtern möchten: Teilnehmer, Eigenschaften oder Netzwerkorte.
5. Klicken Sie in der unteren linken Ecke des Übersichtsfensters auf **Alle Erkennungen verfolgen**.

   Der Link enthält, wie viele Erkennungen Sie aktualisieren. Beispiel: Alle 14 Erkennungen verfolgen. Dieser Link wird nicht im Übersichtsfenster angezeigt, wenn der Filter Status Versteckt angewendet wird.
6. Optional: Wählen Sie den Status aus, den Sie auf alle ausgewählten Erkennungen anwenden möchten.
7. Optional: Wählen Sie den Verantwortlichen aus, den Sie auf alle ausgewählten Erkennungen anwenden möchten.
8. Optional: Wählen Sie aus, ob Sie den vorhandenen Notizen der ausgewählten Entdeckungen eine neue Notiz hinzufügen oder alle vorhandenen Notizen überschreiben möchten.

   Wenn Sie Ihre Notiz zu vorhandenen Notizen hinzufügen, wird die neue Notiz über den vorhandenen Notizen hinzugefügt.
9. klicken **Speichern**.

CrowdStrike-Geräte aus einer Erkennung eindämmen

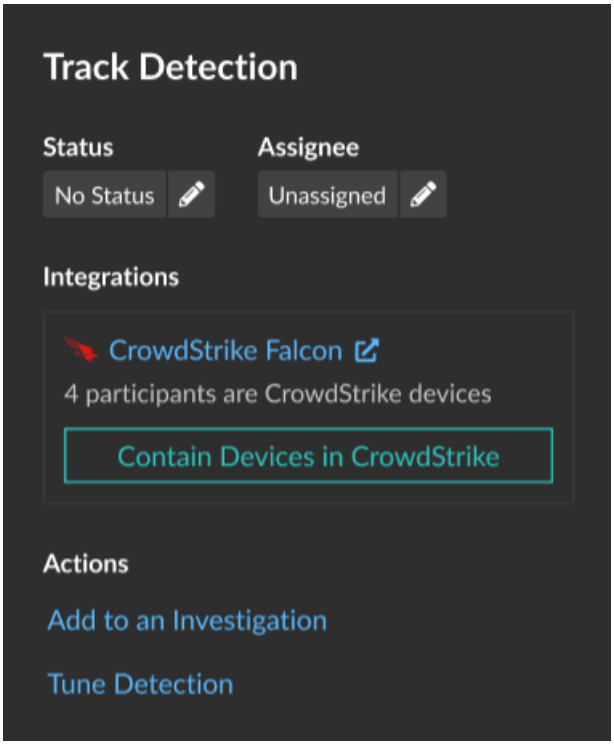
Sie können die Eindämmung von CrowdStrike-Geräten einleiten, die an einer Sicherheitserkennung Erkennung sind. Containment verhindert, dass Geräte Verbindungen zu anderen Geräten in Ihrem Netzwerk herstellen.

Nachdem Sie die Eindämmung anhand einer Erkennung eingeleitet haben, wird eine Anfrage an CrowdStrike Falcon gestellt, um die Geräte einzudämmen, und neben dem Teilnehmer wird der Status Eindämmung ausstehend angezeigt. Der Status wird erst dann auf Enthalten aktualisiert, wenn das ExtraHop-System eine Antwort von CrowdStrike erhalten hat.

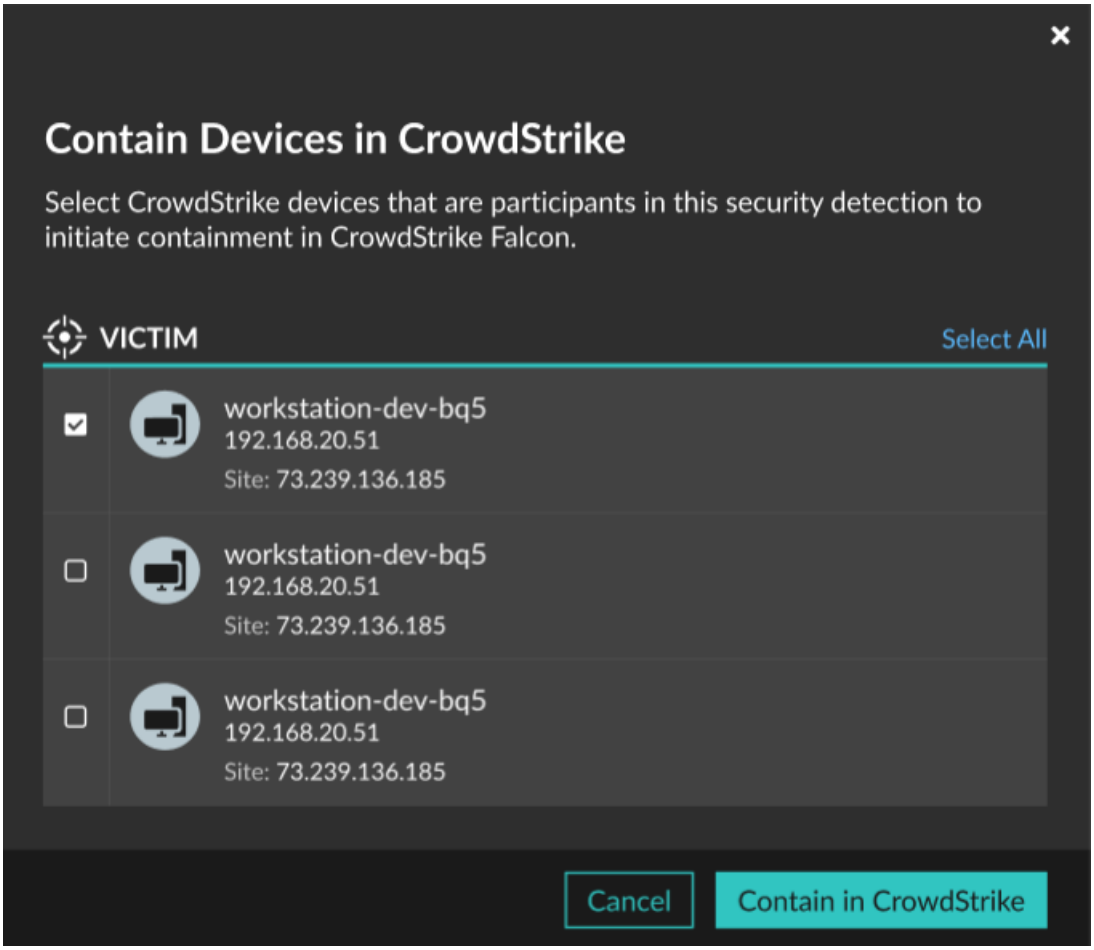
Bevor Sie beginnen

- Device Containment muss aktiviert sein für CrowdStrike-Integration.
- Benutzern muss Zugriff auf das NDR-Modul gewährt werden und sie müssen über eingeschränkte Schreibmöglichkeiten verfügen Privilegien oder höher, um die Aufgaben in diesem Handbuch zu erledigen.

1. <extrahop-hostname-or-IP-address>Melden Sie sich über https://beim ExtraHop-System an.
2. Klicken Sie oben auf der Seite auf **Erkennungen**.
3. Klicken Sie auf einen Erkennungstitel, um die Seite mit den Erkennungsdetails anzuzeigen. Die Anzahl der CrowdStrike-Geräte, die an der Erkennung beteiligt sind, wird im Abschnitt Integrationen unter Track Detection angezeigt.



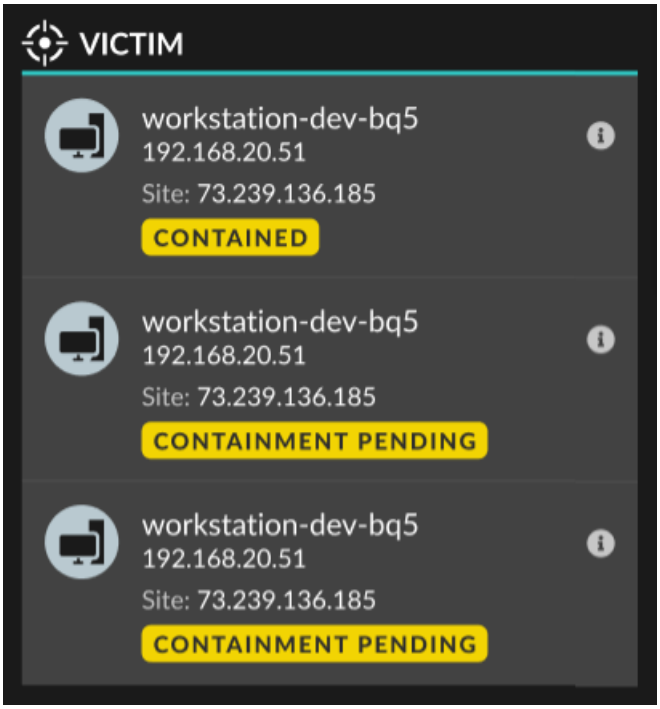
4. klicken **Geräte in CrowdStrike enthalten**.
Im Dialogfeld werden die CrowdStrike-Geräte angezeigt, die mit der Erkennung verknüpft sind.



5. Wählen Sie die Geräte aus, die Sie enthalten möchten, und klicken Sie auf **In CrowdStrike enthalten**. Eine Anfrage wird an CrowdStrike gesendet und neben jedem ausgewählten Teilnehmer wird der Status Containment Pending angezeigt.

Nächste Schritte

- Überprüfen Sie die Geräteeinhausung, indem Sie den Status anhand der Erkennungsdetails überprüfen. Der Containment-Status erscheint auch in der Eigenschaften Gerät.



- Versuchen Sie erneut, ein Gerät zu enthalten. Der Status „Eindämmung steht noch aus“ wird nicht mehr angezeigt, wenn eine Eindämmungsanfrage an CrowdStrike abgelehnt wird oder abläuft.
- Befreien Sie ein Gerät über die CrowdStrike Falcon-Konsole aus dem Container. Klicken Sie im Bereich Integrationen unter Track Detection auf **CrowdStrike Falcon** um die Konsole in einem neuen Tab zu öffnen. Der Containment-Status wird nicht mehr angezeigt, nachdem das ExtraHop-System eine Antwort von CrowdStrike erhalten hat.

Erstellen Sie eine benutzerdefinierte Erkennung

Mit benutzerdefinierten Erkennungen können Sie Kriterien angeben, anhand derer Erkennungen auf dem ExtraHop-System generiert werden. Maschinelles Lernen und regelbasierte Erkennungen erfassen ungewöhnliche Verhaltensweisen und häufige Bedrohungen. Durch die Erstellung einer benutzerdefinierten Erkennung können Sie jedoch die Geräte und Verhaltensweisen genauer untersuchen, die für Ihr Netzwerk von entscheidender Bedeutung sind.

Wenn Sie eine benutzerdefinierte Erkennung erstellen, müssen Sie einen Auslöser erstellen, der das Systemereignis und die Bedingungen identifiziert, auf die das System achten soll, und dann können Sie den Auslöser den spezifischen Geräten oder Gerätegruppen zuweisen, die Sie überwachen möchten. Wenn das Ereignis eintritt, wird eine Erkennung generiert.

In diesem Handbuch finden Sie die Schritte und ein Beispielskript, das eine benutzerdefinierte Erkennung generiert, wenn verdächtige Verbindungen zu bestimmten Websites über Windows PowerShell hergestellt werden.

Bevor Sie beginnen

- Sie müssen mit ExtraHop vertraut sein Trigger. Betrachten Sie insbesondere diese Best Practices beim Schreiben Ihres Skripts und beim Zuweisen von Triggern.
- Sie benötigen ein Benutzerkonto bei Privilegien erforderlich, um Trigger zu erstellen.
- Wenn du eine hast Konsole, erstelle einen Auslöser auf dem Konsole und der Auslöser läuft auf allen angeschlossenen Sensoren.

Einen Auslöser erstellen, um benutzerdefinierte Erkennungen zu generieren

Trigger generieren benutzerdefinierte Erkennungen, indem sie den `commitDetection` Funktion im Trigger-Skript.

Im folgenden Beispiel generiert der Auslöser eine benutzerdefinierte Erkennung, wenn ein PowerShell-Client eine Website aufruft, die als Staging-Site für exfiltrierte Daten bekannt ist.

Der Auslöser identifiziert PowerShell-Verbindungen, indem er nach JA3-Hashes des TLS-Clients sucht, die zu bekannten PowerShell-Clients gehören.

Wenn die TLS-Verbindung von einem PowerShell-Client zu einem verdächtigen Host hergestellt wird, generiert der Auslöser eine Erkennung. Die Erkennung umfasst die Version von PowerShell, die die Verbindung initiiert hat, die Server-IP-Adresse und die Client-IP-Adresse.

Hinweis: Für weitere Informationen über die `commitDetection` Funktion, siehe Trigger-API-Referenz.

1. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Trigger**.
2. Klicken Sie **Erstellen**.
3. Geben Sie die folgenden Trigger-Konfigurationseinstellungen an:

   Name

   Geben Sie einen Namen für Ihren Auslöser ein. Dieser Name identifiziert Ihren Auslöser, nicht die Erkennung.

   In unserem Beispiel geben wir den Namen ein: `Benutzerdefinierte Erkennung: PowerShell-Verbindung zur verdächtigen Site`.

   Beschreibung

   (Optional) Geben Sie die Beschreibung des Auslöser ein. Diese Beschreibung bezieht sich auf den Auslöser, nicht auf die Erkennung.

   In unserem Beispiel geben wir die Beschreibung ein: `Erzeugt jedes Mal eine Erkennung, wenn ein PowerShell-Client eine Verbindung zu pastebin, raw.githubusercontent.com oder Githack herstellt. PowerShell-Clients werden durch JA3-Hashes identifiziert.`

   Ereignisse

   Wählen Sie das Ereignis aus, bei dem der Auslöser ausgeführt wird.

   In unserem Beispiel wählen wir das Ereignis SSL_OPEN aus. Dieses Ereignis tritt ein, wenn zum ersten Mal eine TLS-Verbindung hergestellt wird.

   Zuweisungen

   Wählen Sie das Gerät oder die Gerätegruppe aus, die Sie überwachen möchten. Weisen Sie Ihren Auslöser zunächst einem einzelnen Gerät zum Testen zu. Nachdem Sie bestätigt haben, dass die benutzerdefinierte Erkennung ordnungsgemäß funktioniert, weisen Sie den Auslöser einer Gerätegruppe zu, die alle Geräte enthält, die Sie überwachen möchten.

   Da PowerShell ein Windows-Befehlszeilentool ist, wählen Sie einen Microsoft-Server aus, um den Auslöser zu testen. Nachdem Sie bestätigt haben, dass die benutzerdefinierte Erkennung ordnungsgemäß funktioniert, ändern Sie die Zuweisung zu einer Gerätegruppe, die alle Ihre wichtigen Microsoft-Server enthält. Weitere Informationen zum Erstellen von Gerätegruppen finden Sie unter Erstellen Sie eine Gerätegruppe.
4. Geben Sie im rechten Bereich den Code ein, der bestimmt, wann Ihre benutzerdefinierte Erkennung generiert wird.

   In unserem Beispiel identifiziert der folgende Triggercode, wenn ein Client eine Verbindung zu pastebin, githubusercontent oder githack initiiert:

```
if(SSL.host.match(/pastebin/i) || SSL.host.match(/
raw.githubusercontent.com/i) || SSL.host.match(/githack/i)) {
```

```
}
```

5. Geben Sie als Nächstes den Code ein, der Ihre benutzerdefinierte Erkennung festlegt. Das `commitDetection` Die Funktion muss im folgenden Format geschrieben werden:

```
commitDetection('<detection type ID>', {
       title: '<title>',
       description: '<detection description>',
       categories: ['<category>'],
       riskScore: <risk score>,
       participants: [{
           object:<offender participant>,
           role: 'offender'
           }, {
           object: <victim participant>,
           role: 'victim'
           }],
       identityKey: '<identity key>',
       identityTtl: '<time period>',
       });
```

Geben Sie Werte für jeden der folgenden Parameter in Ihrem Skript ein.

Wert	Beschreibung
Erkennungstyp-ID	Eine eindeutige Zeichenfolge, die Ihre benutzerdefinierte Erkennung identifiziert. Diese Zeichenfolge darf nur Buchstaben, Zahlen und Unterstriche enthalten.
Titel	Text, der oben auf der Erkennungskarte erscheint. Geben Sie einen aussagekräftigen Titel ein, der leicht zu scannen ist. Dieser Titel erscheint im Erkennungskatalog als Anzeigename für Ihren Erkennungstyp, gefolgt von `[benutzerdefiniert]`.
Beschreibung der Erkennung	Text, der unter dem Titel und der Kategorie auf einer Erkennungskarte erscheint. Geben Sie Informationen über das Ereignis ein, das die Erkennung generiert. Dieses Feld unterstützt Markdown. Wir empfehlen, Interpolationsvariablen einzubeziehen, um spezifische Informationen zu Ihrer Erkennung anzuzeigen. Zum Beispiel die Variablen `$(Flow.client.ipaddr)` und `$(Flow.server.ipaddr)` die IP-Adresse des Client- und Servergeräts im Fluss anzeigen und `$(Flow.l7proto)` zeigt das L7-Protokoll an. Einschließen `\n` am Ende jeder Textzeile, um sicherzustellen, dass die Beschreibung korrekt angezeigt wird.
Risikoscore	Eine Zahl, die die Wahrscheinlichkeit, Komplexität und geschäftliche Auswirkungen einer Sicherheitserkennung misst. Das Symbol

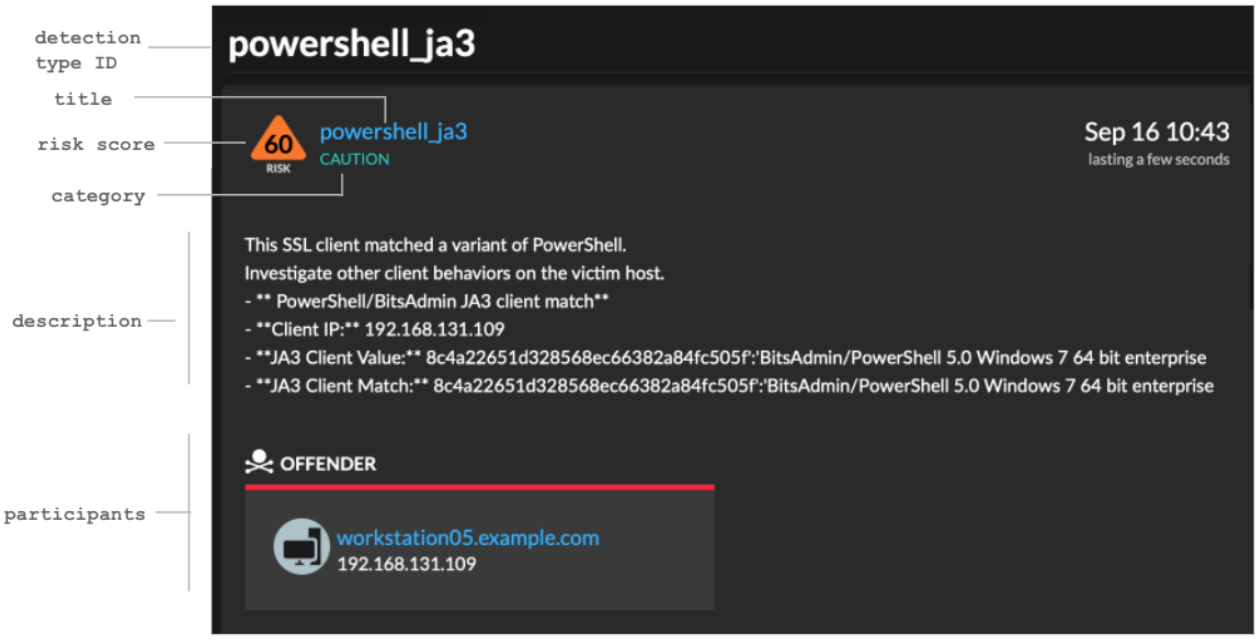
Wert	Beschreibung
	für die Risikobewertung wird oben auf der Erkennungskarte angezeigt und ist nach Schweregrad als rot (80-99), orange (31-79) oder gelb (1-30) farblich gekennzeichnet. Du kannst Entdeckungen nach Risiko sortieren.
Beteiligter des Täters Teilnehmer des Opfers	Eine Reihe von Objekten, die die Teilnehmer an der Erkennung identifiziert. Definieren Sie die Rolle des Teilnehmer als entweder `'offender'` oder `'victim'` und geben Sie einen Verweis auf ein Gerät, eine IP-Adresse oder ein Anwendungsobjekt für diese Rolle an. Beispielsweise identifiziert das folgende Array in einem Fluss den Server als Täter und den Client als Opfer: `participants: [ { role: 'offender', object: Flow.server.device}, { role: 'victim', object: Flow.client.device } ]` Weitere Informationen zu Gerät, IP-Adresse und Anwendungsobjekten finden Sie in der Trigger-API-Referenz.
Identitätsschlüssel	Eine Zeichenfolge, die die Identifizierung laufender Erkennungen ermöglicht. Wenn mehrere Erkennungen mit demselben Identitätsschlüssel und Erkennungstyp innerhalb des von der angegebenen Zeitspanne generiert werden `identityTtl` Parameter, die Erkennungen werden zu einer einzigen fortlaufenden Erkennung zusammengefasst. Erstellen Sie eine eindeutige Identitätsschlüsselfolge, indem Sie die Merkmale der Erkennung kombinieren. Beispielsweise wird der folgende Identitätsschlüssel erstellt, indem die Server-IP-Adresse und die Client-IP-Adresse kombiniert werden: `identityKey: [Flow.server.ipaddr, Flow.client.ipaddr].join('!!')`
Zeitraum	Der Zeitraum nach dem Generieren einer Erkennung, in dem doppelte Erkennungen zu einer fortlaufenden Erkennung zusammengefasst werden. Der Zeitraum wird zurückgesetzt und die Erkennung endet erst, wenn der Zeitraum abgelaufen ist.

Wert	Beschreibung
	Die folgenden Zeiträume sind gültig: • `hour` • `day` • `week` Der Standardzeitraum ist `hour`.

Das folgende Beispiel zeigt den abgeschlossenen Skriptabschnitt.

```
commitDetection('powershell_ja3', {
        title:
'PowerShell / BitsAdmin Suspicious Connection',
        description:
"This TLS client matched a variant of PowerShell." + "\n"+
"Investigate other client behaviors on the victim host." + "\n"+
"- ** PowerShell/BitsAdmin JA3 client match**" + "\n"+
"- **Client IP:** " + Flow.client.ipaddr + "\n"+
"- **JA3 Client Value:** " + ja3 + "\n"+
"- **JA3 Client Match:** " + suspect_ja3_hashes[ja3],
        riskScore: 60,
        participants: [{
            object:Flow.client.device,
            role: 'offender'
            }],
        identityKey: [
            Flow.server.ipaddr,
            Flow.client.ipaddr,
            hash
        ].join('!!'),
        identityTtl: 'hour',
});
```

Diese Werte werden auf der Erkennungskarte ähnlich der folgenden Abbildung angezeigt:



6. Klicken Sie **Speichern** und klicken Sie dann **Erledigt**.

   siehe Beispiel für einen benutzerdefinierten Erkennungsauslöser für ein vollständiges kommentiertes Skript.

Ihre benutzerdefinierte Erkennung wird dem Erkennungskatalog hinzugefügt, nachdem Ihr Auslöser zum ersten Mal ausgeführt wird. Erkennungskategorien und MITRE-Techniken hinzufügen zur Erkennung aus dem Erkennungskatalog.

Erstellen Sie einen benutzerdefinierten Erkennungstyp

Nachdem Sie einen Auslöser zur Generierung Ihrer benutzerdefinierten Erkennung erstellt haben, können Sie im Erkennungskatalog einen benutzerdefinierten Erkennungstyp erstellen, um weitere Informationen zu Ihrer Erkennung hinzuzufügen.

Sie können einen Anzeigenamen angeben und Erkennungskategorien hinzufügen, damit Sie Ihre Entdeckung auf der Seite Erkennungen leichter finden können. Sie können auch MITRE-Links hinzufügen, die es ermöglichen, dass Ihre benutzerdefinierte Erkennung in der Matrix auf der Seite Group by MITRE Technique angezeigt wird.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen ⚙ und dann klicken **Erkennungskatalog**.
3. Führen Sie auf der Seite Erkennungskatalog einen der folgenden Schritte aus:
   - Wenn Ihr Auslöser bereits ausgeführt wurde, fügt das System Ihre benutzerdefinierte Erkennung automatisch dem Katalog hinzu, wobei der im Auslöser angegebene Anzeigename vorangestellt ist `[benutzerdefiniert]`. Klicken Sie auf den Erkennungstyp, den Sie bearbeiten möchten.
   - Wenn Ihr Erkennungstyp noch nicht erstellt wurde, klicken Sie auf **Erstellen**.
4. Füllen Sie die folgenden Felder aus:

   Name anzeigen

   Geben Sie einen eindeutigen Namen für den Titel der Erkennung ein.

   Erkennungstyp-ID

   Geben Sie den Wert ein, den Sie für die Erkennungstyp-ID im Auslöser eingegeben haben. Wenn Sie beispielsweise Folgendes eingegeben haben: `commitDetection('network_segmentation_breach')`, die Erkennungstyp-ID lautet „network_segmentation_breach“. Sie können die Erkennungstyp-ID nicht bearbeiten, nachdem der Erkennungstyp gespeichert wurde.

   Autor

   Geben Sie den Autor der benutzerdefinierten Erkennung ein.

   MITRE Technik

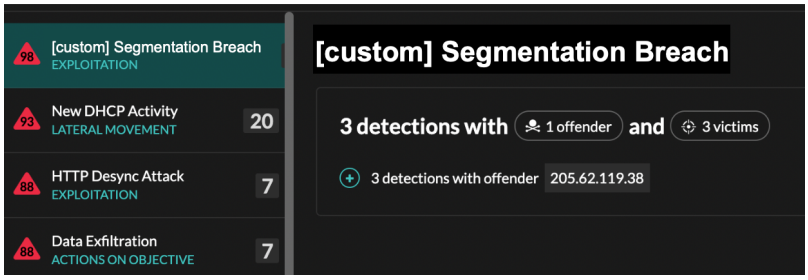
   Wählen Sie aus der Dropdownliste eine oder mehrere MITRE-Techniken aus, die Sie mit der Erkennung verknüpfen möchten.
5. klicken **Speichern**.

Benutzerdefinierte Erkennungen anzeigen

Sie können benutzerdefinierte Erkennungen auf der Erkennungen Seite mit anderen integrierten Erkennungen.

Gruppieren Sie die Erkennungsseite nach Typ. Alle Entdeckungen in der Erkennungsliste sind nach Erkennungstyp gruppiert.

Zum Beispiel, wenn Ihr Erkennungsanzeigename lautet `[custom]Segmentation Breach`, würde der Eintrag in der Erkennungsliste ähnlich der folgenden Abbildung erscheinen:



Wählen Sie links oben auf der Seite **MITRE Karte**. Die MITRE-Techniken, die mit der benutzerdefinierten Erkennung verknüpft wurden, sind in der Matrix hervorgehoben.

Die nächsten Schritte

Erstellen Sie eine Regel für Erkennungsbenachrichtigungen. Sie können das ExtraHop-System beispielsweise so konfigurieren, dass es Ihnen eine E-Mail sendet, wenn Ihre benutzerdefinierte Erkennung erfolgt.

Beispiel für einen benutzerdefinierten Erkennungsauslöser

Das folgende Skript ist das vollständige PowerShell/JA3-Beispiel, auf das in diesen Anweisungen verwiesen wird.

```
// If the server is internal, exit
if ( ! Flow.server.ipaddr.isExternal ) {
    return;
}
// If the TLS host name is not set, exit
if(SSL.host === null) { return; }

// Continue only if the TLS hostname belongs to one of the suspicious sites
if(SSL.host.match(/pastebin/i) || SSL.host.match(/raw.githubusercontent.com/
i) || SSL.host.match(/githack/i)) {

    // List of common PowerShell JA3 hashes
    let suspect_ja3_hashes = cache('suspect_ja3_hashes', () => ({
        '13cc575f247730d3eeb8ff01e76b245f':'PowerShell/BitsAdmin/PowerShell
 4.0 Windows Server 2012RT',
        '5e12c14bda47ac941fc4e8e80d0e536f':'PowerShell/BitsAdmin/PowerShell
 4.0 Windows Server 2012RT',
        '2c14bfb3f8a2067fbc88d8345e9f97f3':'PowerShell/BitsAdmin Windows
 Server 2012RT',
        '613e01474d42ebe48ef52dff6a20f079':'PowerShell/BitsAdmin Windows
 Server 2012RT',
        '05af1f5ca1b87cc9cc9b25185115607d':'BitsAdmin/PowerShell 5.0 Windows
 7 64 bit enterprise',
        '8c4a22651d328568ec66382a84fc505f':'BitsAdmin/PowerShell 5.0 Windows
 7 64 bit enterprise',
        '235a856727c14dba889ddee0a38dd2f2':'BitsAdmin/PowerShell 5.1 Server
 2016',
        '17b69de9188f4c205a00fe5ae9c1151f':'BitsAdmin/PowerShell 5.1 Server
 2016',
        'd0ec4b50a944b182fc10ff51f883ccf7':'PowerShell/BitsAdmin (Microsoft
 BITS/7.8) Server 2016',
        '294b2f1dc22c6e6c3231d2fe311d504b':'PowerShell/BitsAdmin (Microsoft
 BITS/7.8) Server 2016',
        '54328bd36c14bd82ddaa0c04b25ed9ad':'BitsAdmin/PowerShell 5.1 Windows
 10',
        'fc54e0d16d9764783542f0146a98b300':'BitsAdmin/PowerShell 5.1 Windows
 10',
```

```
        '2863b3a96f1b530bc4f5e52f66c79285':'BitsAdmin/PowerShell 6.0 Windows
 Server 2012RT',
        '40177d2da2d0f3a9014e7c83bdeee15a':'BitsAdmin/PowerShell 6.0 Windows
 Server 2012RT',
        '36f7277af969a6947a61ae0b815907a1':'PowerShell/BitsAdmin Windows 7
 32 bit enterprise',
    }));
    // Store the client JA3 hash in a variable
    const hash = SSL.ja3Hash;

    // Iterate through each PowerShell JA3 hash
    for ( let ja3 in suspect_ja3_hashes ) {

        // If the client JA3 hash is from PowerShell,
        // commit the detection
        if ( hash.includes(ja3) ) {

            commitDetection('PowerShell_JA3', {
                categories: ['sec.caution'],
                title: "PowerShell / BitsAdmin Suspicious Connection",
                // Specify the offender as the device object of the client
                participants: [
                    { role: 'offender', object: Flow.client.device }
                ],
                description:
                    "This TLS client matched a variant of PowerShell." +
 "\n"+
                    "Investigate other client behaviors on the victim host."
 + "\n"+
                    "- ** PowerShell/BitsAdmin JA3 client match**" + "\n"+
                    "- **Client IP:** " + Flow.client.ipaddr + "\n"+
                    "- **Server IP:** " + Flow.server.ipaddr + "\n"+
                    "- **JA3 Client Value:** " + ja3 + "\n"+
                    "- **JA3 Client Match:** " + suspect_ja3_hashes[ja3],
                // Create the identity key by combining the server IP
 address, client IP address, and PowerShell JA3 hash
                identityKey: [
                    Flow.server.ipaddr,
                    Flow.client.ipaddr,
                    hash
                ].join('!!'),
                riskScore: 60,
                identityTtl: 'hour'
            });
        }
    }
}
```

Laden Sie benutzerdefinierte IDS-Regeln hoch

Sie können einen benutzerdefinierten Satz von IDS-Regeln auf ExtraHop IDS-Sensoren hochladen. Das ExtraHop-System konvertiert die Regeln in Erkennungstypen, die Erkennungen generieren, die Sie anzeigen und untersuchen können.

Fügen Sie Regeln, die gemäß den Suricata-Richtlinien formatiert sind, zu einer oder mehreren .rules-Dateien hinzu und laden Sie sie in einer ZIP-Datei hoch. Beim Upload verarbeitet das ExtraHop-System jede Regel. Diese wird in einer Tabelle angezeigt, in der die Signatur-ID, der Name jeder Regel und einer der folgenden Regelstatus angezeigt werden.

- **Akzeptiert:** Das ExtraHop-System hat die Regel erfolgreich verarbeitet.

• **Abgelehnt:** Das ExtraHop-System konnte die Regel nicht verarbeiten. Die Regel enthält möglicherweise einen Formatierungsfehler oder die Regel enthält eine Aktion, ein Protokoll oder eine Option, die derzeit vom ExtraHop-System nicht unterstützt wird. Kontakt ExtraHop-Unterstützung um sich über zukünftige Unterstützung für die Regel zu erkundigen.

• **Upgrade erforderlich:** EIN Eine neuere Version der ExtraHop-Firmware ist erforderlich um die Regel zu unterstützen. Die erforderliche Systemversion wird angezeigt.

Im Folgenden finden Sie einige Überlegungen zu benutzerdefinierten IDS-Regeln:

- Benutzerdefinierte IDS-Regeln müssen als gültig formatiert sein .rules-Datei hochladen.
- Eine oder mehrere Suricata-.rules-Dateien müssen zu einer einzigen ZIP-Datei für den Upload hinzugefügt werden.
- Sie können nicht mehr als 10.000 benutzerdefinierte IDS-Regeln hochladen.
- Durch das Löschen einer Datei werden alle Regeln gelöscht, die mit der hochgeladenen Datei verknüpft sind. Dies kann mehrere Minuten dauern. Benutzern werden möglicherweise weiterhin Erkennungen angezeigt, die auf diesen Regeln basieren, bis der Löschvorgang abgeschlossen ist.
- Durch das Ersetzen einer Datei werden alle Regeln gelöscht, die mit der zuvor hochgeladenen Datei verknüpft sind, und dann werden die Regeln aus der neuen Datei verarbeitet.
- Integrierte IDS-Regeln werden nicht gelöscht oder ersetzt, wenn Sie Ihre benutzerdefinierten IDS-Regeln verwalten. Ihr ExtraHop-System ist mit den ExtraHop Cloud Services verbunden und die neuesten integrierten Regeln werden automatisch auf das System heruntergeladen, sobald aktualisierte Versionen verfügbar sind.

Hinweis: ExtraHop überprüft möglicherweise die hochgeladenen Regeln, um die Genauigkeit der Konvertierung zu überprüfen und um Produktverbesserungen im Hinblick auf die Konvertierung, Richtigkeit und Leistung der Suricata-Regeln anzuleiten.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Benutzerdefinierte IDS-Regeln**.
3. Klicken Sie **Datei hochladen**.
4. Klicken Sie **Wählen Sie eine Datei**, wählen Sie die gewünschte ZIP-Datei aus, und klicken Sie dann auf **Datei hochladen**.
   Der Upload-Vorgang kann mehrere Minuten dauern. Der Dateistatus und die Zeitstempel werden nach Abschluss der Verarbeitung aktualisiert.

Nächste Schritte
Klicken Sie **Erkennungen** von der oberen Navigationsmenüseite aus, um Erkennungen anzuzeigen, die anhand benutzerdefinierter IDS-Regeln generiert wurden. Diese Erkennungen deuten darauf hin, dass die Regel von einer benutzerdefinierten IDS-Datei bereitgestellt wurde und die Signatur-ID der Regel enthält.

Erkennungen abstimmen

Die Erkennungsoptimierung ermöglicht es Ihnen, Geräusche zu reduzieren und kritische Erkennungen zu erkennen, die sofortige Aufmerksamkeit erfordern.

Es gibt zwei Möglichkeiten, Erkennungen zu optimieren: Sie können Optimierungsparameter hinzufügen, die verhindern, dass Erkennungen überhaupt generiert werden, oder Sie können Optimierungsregeln erstellen, die vorhandene Erkennungen basierend auf Erkennungstyp, Teilnehmern oder Erkennungseigenschaften ausblenden.

Video: Sehen Sie sich die entsprechende Schulung an: Tuning-Regeln konfigurieren

Tuning-Parameter

Mithilfe von Optimierungsparametern können Sie bekannte und vertrauenswürdige Domänen, DNS-Server und HTTP CONNECT-Ziele angeben, die keine Erkennung generieren sollen. Sie können auch Tuning-Parameter aktivieren, die häufige und redundante Erkennungen von Gateway-Geräten und Tor-Knoten unterdrücken.

Die Tuning-Parameter werden über das verwaltet Tuning-Parameter Seite.

Tuning-Regeln

Mithilfe von Optimierungsregeln können Sie Kriterien angeben, die generierte Erkennungen verbergen, die jedoch von geringem Wert sind und keine Aufmerksamkeit erfordern.

Hinweis: Optimierungsregeln verbergen möglicherweise bestimmte Erkennungen nicht, wenn auf Ihren Paketsensoren nicht dieselbe Firmware-Version wie auf Ihrer Konsole ausgeführt wird.

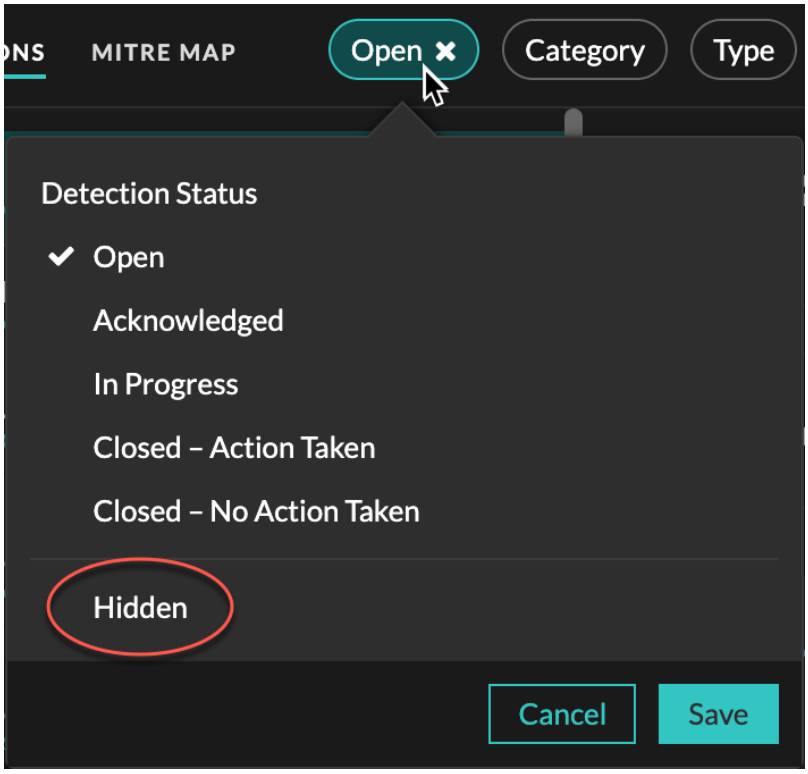
Tuning-Regeln verbergen alle vergangenen, aktuellen und zukünftigen Erkennungen und Teilnehmer, die den angegebenen Kriterien entsprechen und sich auf die folgenden Systembereiche auswirken:

- Versteckte Erkennungen führen nicht dazu, dass zugehörige Trigger und Warnungen ausgeführt werden, solange die Regel aktiviert ist.
- Versteckte Erkennungen werden in Diagrammen nicht als Erkennungsmarkierungen angezeigt.
- Versteckte Entdeckungen erscheinen nicht auf den Aktivitätskarten, aber versteckte Teilnehmer werden auf den Ermittlungskarten angezeigt.
- Versteckte Erkennungen erscheinen nicht in den Erkennungszahlen auf verwandten Seiten, z. B. auf der Seite „Geräteübersicht“ oder der Seite „Aktivität“.
- Versteckte Funde und Teilnehmer erscheinen nicht im Security Operations Report.
- Versteckte Erkennungen sind in E-Mail- und Webhook-Benachrichtigungen nicht enthalten.
- Versteckte Erkennungen werden nicht in ein integriertes SIEM oder SOAR exportiert.

Hinweis: Wenn Sie keine Erkennungsmarkierungen für Erkennungen sehen, bestätigen Sie dies Erkennungsmarker wurden nicht deaktiviert.

Versteckte Entdeckungen anzeigen
Wenn Sie auf der Seite Erkennungen den Status Versteckt anwenden, können Sie Erkennungen anzeigen, die derzeit durch eine Optimierungsregel ausgeblendet sind.

Der Filter Öffnen ist standardmäßig auf der Seite Erkennungen ausgewählt. Klicken Sie auf **Offen** filtern, um auf andere Filteroptionen zuzugreifen. Wenn der Filter Öffnen nicht angewendet wird, klicken Sie auf **Status** um die Filteroptionen anzuzeigen, und klicken Sie dann auf **Versteckt**. Die Zusammenfassung nur für versteckte Entdeckungen wird angezeigt.



Die Zusammenfassung identifiziert die Optimierungsregeln, die derzeit die ausgewählten Erkennungen, versteckten Teilnehmer, Erkennungseigenschaften und Netzwerklokalitäten verbergen.

Klicken Sie auf eine beliebige Optimierungsregel, einen Teilnehmer, eine Eigenschaft oder einen Wert für die Netzwerklokalität, um eine Zusammenfassung der versteckten Erkennungen anzuzeigen, die mit dem ausgewählten Wert verknüpft sind.

Teilnehmer

Listet sowohl Täter als auch Opfer auf, die derzeit versteckt sind. Die Täter- und Opferlisten sind nach der Anzahl der Entdeckungen geordnet, bei denen der Teilnehmer versteckt ist .

Immobilienwerte

Listet die Eigenschaftswerte auf, die dem Erkennungstyp für ausgeblendete Objekte zugeordnet sind. Die Liste der Eigenschaftswerte ist nach der Anzahl der Erkennungen sortiert, bei denen der Eigenschaftswert verborgen ist.

Betroffene Netzwerkstandorte

Führt die Netzwerklokalitäten auf, die versteckte Erkennungen des ausgewählten Typs enthalten. Die Liste der betroffenen Netzwerkorte ist nach der Anzahl der versteckten Entdeckungen in der Netzwerklokalität sortiert.

Indem Sie die Ergebnisse nach einer einzelnen Optimierungsregel, einem einzelnen Teilnehmer, einer Immobilie oder einem Ort filtern, können Sie die Anzahl der versteckten Erkennungen anzeigen, die mit dem angegebenen Wert verknüpft sind. Klicken Sie auf **Erkennungen anzeigen** Schaltfläche, um einzelne Erkennungskarten anzuzeigen.

Optimierte Best Practices

Es ist besser, einen einzelnen Parameter oder eine Regel zu erstellen, die umfassender ist, als mehrere überlappende Parameter und Regeln zu erstellen.

Im Folgenden finden Sie einige Empfehlungen zur Optimierung Ihrer Erkennungsoptimierung:

- Fügen Sie zunächst Optimierungsparameter hinzu, um Erkennungen zu vermeiden, an denen bekannte oder vertrauenswürdige Agenten beteiligt sind. Lesen Sie unbedingt die Tuning-Parameter und Netzwerk-Locations Seiten für bestehende Parameter, um Redundanz zu vermeiden.
- Legen Sie fest, ob Sie alle Erkennungen für einen bestimmten Teilnehmer, z. B. einen Schwachstellenscanner, ausblenden möchten, und wählen Sie **Alle Erkennungsarten**. Wenn Sie sich nach Geräterolle verstecken möchten, erweitern Sie den Bereich auf Gerätegruppe.
- Wenn ein **IP-Adresse oder CIDR-Block** ist in der Dropdownliste Täter oder Opfer ausgewählt. Fügen Sie der Liste im Feld IP-Adressen Einträge hinzu oder entfernen Sie sie, um den Geltungsbereich der Optimierungsregel zu erweitern oder zu reduzieren.
- Standardmäßig laufen Tuning-Regeln nach 8 Stunden ab. Sie können eine andere Ablaufzeit aus der Dropdownliste auswählen oder eine neue Ablaufzeit auswählen, nachdem Sie eine abgelaufene Regel aus dem Tuning-Regeln Seite.
- Das ExtraHop-System löscht automatisch Erkennungen, die seit Beginn der Erkennung 21 Tage im System waren, die nicht andauern und die ausgeblendet sind. Wenn eine neu erstellte oder bearbeitete Optimierungsregel eine Erkennung verbirgt , die diesen Kriterien entspricht, wird die betroffene Erkennung 48 Stunden lang nicht gelöscht.
- Wenn Sie beim Hinzufügen einer Tuning-Regel ein Gerät identifizieren, das nicht korrekt klassifiziert ist, können Sie die Geräterolle ändern.
- Bestimmte Erkennungen erfordern möglicherweise eine genaue Optimierungsregel, die auf einer bestimmten Eigenschaft der Erkennung basiert. Klicken Sie unter der Überschrift Eigenschaft auf das Kontrollkästchen neben einer Eigenschaft, um einen Wert oder regulären Ausdruck anzugeben und Kriterien für eine fokussierte Optimierungsregel hinzuzufügen.
- Wenden Sie das an **Versteckt** Statusfilter zum Erkennungen Seite, um Erkennungen anzuzeigen, die derzeit versteckt indem du Abstimmung optimierst.

Erfahren Sie, wie Unterdrücken Sie Erkennungen mit Tuning-Parametern und Ausblenden von Erkennungen mit Tuning-Regeln .

Unterdrücken Sie Erkennungen mit Tuning-Parametern

Stellen Sie Informationen über Ihre Netzwerkumgebung bereit, damit das ExtraHop-System verhindern kann, dass geringwertige oder redundante Erkennungen jemals generiert werden.

Sie können Kriterien aus dem Tuning-Parameter Seite oder direkt von einer Erkennungskarte. Darüber hinaus können Sie Netzwerk angeben, die IP-Adressbereiche als interne oder externe Adressbereiche Ihres Netzwerk klassifizieren.

Erfahre mehr über Abstimmung von Erkennungen.

Video: Sehen Sie sich die entsprechende Schulung an: Tuning-Parameter konfigurieren

Geben Sie Optimierungsparameter für Erkennungen und Metriken an

Geben Sie Optimierungsparameter an, um Metriken zu verbessern und zu verhindern, dass Erkennungen mit niedrigen Werten überhaupt generiert werden.

Wenn Ihre ExtraHop-Bereitstellung eine Konsole umfasst, empfehlen wir Ihnen Transfermanagement aller an die Konsole angeschlossenen Sensoren.

Hinweis: Die Felder auf dieser Seite können im Laufe der Zeit von ExtraHop hinzugefügt, gelöscht oder geändert werden.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Tuning-Parameter**.
3. Geben Sie Werte für einen der folgenden Parameter an, die auf der Seite verfügbar sind.

Option	Description
Gateway-Geräte	Standardmäßig werden Gateway-Geräte von regelbasierten Erkennungen ignoriert, da sie zu redundanten oder häufigen Erkennungen führen können. Wählen Sie diese Option, um potenzielle Probleme mit Gateway-Geräten wie Ihren Firewalls, Routern und NAT-Gateways zu identifizieren. Diese Einstellung wirkt sich nicht auf Erkennungen durch maschinelles Lernen aus.
Ausgehende Tor-Knoten	Standardmäßig werden ausgehende Verbindungen zu bekannten Tor-Knoten von regelbasierten Erkennungen ignoriert, da sie in Umgebungen mit minimalem Tor-Verkehr zu Erkennungen mit geringem Wert führen können. Wähle diese Option, um Erkennungen bei ausgehenden Verbindungen zu bekannten Tor-Knoten zu identifizieren, falls deine Umgebung erheblichen ausgehenden Tor-Verkehr beobachtet.
Eingehende Tor-Knoten	Standardmäßig werden eingehende Verbindungen von bekannten Tor-Knoten von regelbasierten Erkennungen ignoriert, da sie in Umgebungen mit minimalem Tor-Verkehr zu Erkennungen mit geringem Wert führen können. Wähle diese Option, um Erkennungen bei eingehenden Verbindungen von bekannten Tor-Knoten zu identifizieren, falls deine Umgebung erheblichen eingehenden Tor-Verkehr beobachtet.
Beschleunigte Beaconing-Erkennung	Standardmäßig erkennt das ExtraHop-System potenzielle Beaconing-Ereignisse über HTTP und TLS. Wählen Sie diese Option, um Beaconing-Ereignisse schneller als bei der Standarderkennung zu erkennen. Beachten Sie, dass die Aktivierung dieser Option die Erkennung von Beaconing-Ereignissen erhöhen kann, die nicht bösartig sind.
IDS-Erkennungen	Standardmäßig sind ExtraHop-Systeme mit verbundenen Sensoren des Intrusion Detection Systems (Intrusion Detection System) generiert nur Erkennungen für den Verkehr innerhalb Ihres Netzwerk. Wählen Sie diese Option, um IDS-Erkennungen für Datenverkehr zu generieren , der von einem Externer Endpunkt eingeht.

Option	Description
	Beachten Sie, dass die Aktivierung dieser Option die Anzahl der IDS-Erkennungen erheblich erhöhen kann.
Privilegierte Active Directory Directory-Konten	Geben Sie reguläre Ausdrücke (Regex) an, die privilegierten Active Directory-Konten in Ihrer Umgebung entsprechen. Die Parameterliste enthält eine Standardliste regulärer Ausdrücke für allgemeine privilegierte Konten , die Sie bearbeiten können. Das ExtraHop-System identifiziert privilegierte Konten und verfolgt die Kontoaktivitäten in Kerberos-Datensätzen und -Metriken.
Zulässige öffentliche DNS-Server	Geben Sie in Ihrer Umgebung zulässige öffentliche DNS-Server an, die regelbasierte Erkennungen ignorieren sollen. Geben Sie eine gültige IP-Adresse oder einen CIDR-Block an.
Zulässige HTTP CONNECT-Ziele	Geben Sie URIs an, auf die Ihre Umgebung über die HTTP CONNECT-Methode zugreifen kann. URIs müssen formatiert sein als *<hostname>:<Portnummer>* . Wildcards und Regex werden nicht unterstützt. Wenn Sie keinen Wert angeben, werden keine Erkennungen generiert, die auf diesem Parameter basieren.
Vertrauenswürdige Domänen	Fügen Sie legitime bekannte Domänen zur Liste der vertrauenswürdigen Domänen hinzu, um zukünftige Erkennungen zu unterdrücken, die auf bösartige Domänenaktivitäten für diese Domain abzielen. Geben Sie einen einzelnen Domänenname pro Feld ein. Wenn Sie einen Domänenname angeben, unterdrückt der Tuning-Parameter Erkennungen für alle Subdomänen. Wenn Sie beispielsweise example.com als vertrauenswürdige Domain hinzufügen, werden Erkennungen mit vendor.example.com als Täter ebenfalls unterdrückt. Wenn Sie eine Subdomain wie vendor.example.com hinzufügen, unterdrückt der Parameter nur Erkennungen, bei denen der Teilnehmer mit genau dieser Subdomain endet. In diesem Beispiel würde test.vendor.example.com unterdrückt werden, test.example.com jedoch nicht. Wildcards und Regex werden nicht unterstützt.

Option	Description
	Um mehr als einen vertrauenswürdigen Domänenname hinzuzufügen, klicken Sie auf **Domain hinzufügen**. Für Erkennungen, denen eine Domain zugeordnet ist, können Sie auch Fügen Sie eine vertrauenswürdige Domain direkt von einer Erkennungskarte hinzu.

4. Klicken Sie **Speichern**.

Nächste Schritte
Klicken Sie **Erkennungen** vom oberen Navigationsmenü zu Erkennungen anzeigen.

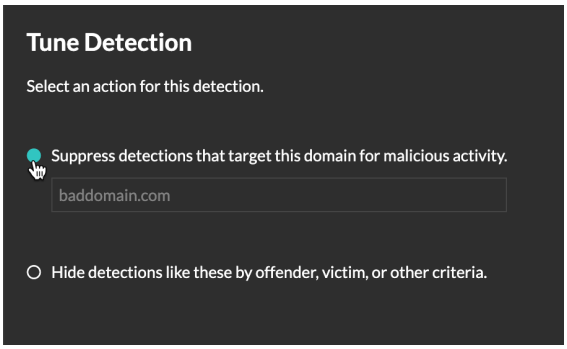
Hinzufügen eines Tuning-Parameters von einer Erkennungskarte

Wenn Sie auf eine Erkennung mit niedrigem Wert stoßen, können Sie direkt von einer Erkennungskarte aus Optimierungsparameter hinzufügen, um zu verhindern, dass ähnliche Erkennungen generiert werden.

Bevor Sie beginnen
Benutzer müssen Vollschreiben oder höher haben Privilegien um eine Erkennung zu optimieren.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Erkennungen**.
3. Klicken Sie **Aktionen** aus der unteren linken Ecke der Erkennungskarte.
4. Klicken Sie **Tune-Erkennung...**.

   Wenn der Erkennungstyp mit einem Tuning-Parameter verknüpft ist, wird die Option angezeigt, die Erkennung durch Hinzufügen eines Tuning-Parameters zu unterdrücken. Wenn der Erkennung kein Tuning-Parameter zugeordnet ist, können Sie die Erkennung mit einer Tuning-Regel ausblenden.



5. Klicken Sie auf **Erkennungen unterdrücken...** Option und klick **Speichern**.

   Die Bestätigung „Tuning-Parameter hinzugefügt“ wird angezeigt und der neue Parameter wird dem Tuning-Parameter Seite.

Erkennungen mit Optimierungsregeln ausblenden

Mithilfe von Optimierungsregeln können Sie Erkennungen ausblenden, die bestimmten Kriterien entsprechen.

Um redundante Regeln zu vermeiden, stellen Sie sicher, dass Sie zuerst Informationen über Ihre Netzwerkumgebung zum ExtraHop-System hinzufügen, indem Sie Angeben von Tuning-Parametern.

Erfahre mehr über Abstimmung von Erkennungen.

Eine Optimierungsregel erstellen

Erstellen Sie Optimierungsregeln, um Ihre Erkennungsliste zu optimieren, indem Sie Kriterien angeben, die vergangene, aktuelle und zukünftige Erkennungen verbergen, die von geringem Wert sind und keine Aufmerksamkeit erfordern.

Bevor Sie beginnen
Benutzer müssen über Vollschreibzugriff oder höher verfügen Privilegien um eine Optimierungsregel zu erstellen.

Erfahre mehr über Abstimmung von Best Practices.

Eine Optimierungsregel von einer Erkennungskarte hinzufügen
Wenn Sie auf eine Erkennung mit niedrigem Wert stoßen, können Sie direkt von einer Erkennungskarte aus eine Optimierungsregel erstellen, um ähnliche Erkennungen im ExtraHop-System auszublenden.

Bevor Sie beginnen
Benutzer müssen über Vollschreibzugriff oder höher verfügen Privilegien um eine Erkennung zu optimieren.

Erfahre mehr über Abstimmung von Best Practices.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Erkennungen**.
3. klicken **Aktionen** aus der unteren linken Ecke der Erkennungskarte.
4. klicken **Erkennung abstimmen...**.

   Wenn der Erkennungstyp mit einem Tuning-Parameter verknüpft ist, sehen Sie eine Option zum unterdrücke die Erkennung. Wenn Sie dennoch eine Optimierungsregel erstellen möchten, wählen Sie die Option Erkennungen wie diese ausblenden... und klicken Sie auf Speichern.
5. Spezifizieren Sie die Kriterien Abstimmung Optimierungsregeln und klicken **Erstellen**.

   Die Regel wird der Seite Tuning-Regeln hinzugefügt. Erfahre mehr über Verwaltung von Tuning-Regeln.

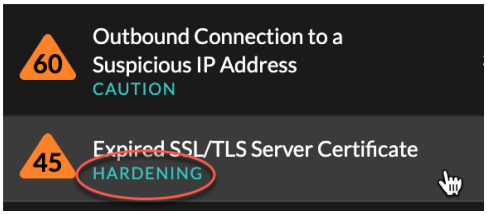
Eine Optimierungsregel aus einer Härtungserkennung hinzufügen
Klicken Sie auf eine Hardening-Erkennung, um eine Zusammenfassung aller Ressourcen, Erkennungseigenschaften und Netzwerkstandorte anzuzeigen, die mit diesem Erkennungstyp verknüpft sind. Sie können die Zusammenfassung filtern, indem Sie auf einen der zugehörigen Werte klicken, und dann eine Optimierungsregel erstellen, um Erkennungen auf der Grundlage der angezeigten Ergebnisse auszublenden.

Bevor Sie beginnen
Benutzer müssen über Vollschreibzugriff oder höher verfügen Privilegien um eine Erkennung zu optimieren.

Erfahre mehr über Filterung und Abstimmung von Härtungserkennungen.

Erfahre mehr über Abstimmung von Best Practices.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Erkennungen**.
3. Klicken Sie in der Erkennungsliste auf eine beliebige Hardening-Erkennung.



4. Filtern Sie die Ergebnisse auf der Seite mit der Zusammenfassung der Härtung.
   a) Klicken Sie auf ein betroffenes Asset, um nur Erkennungen anzuzeigen, bei denen dieses Asset an einer Erkennung Teilnehmer ist.
   b) Klicken Sie auf einen Eigenschaftswert, um nur Erkennungen anzuzeigen, die mit dem ausgewählten Erkennungseigenschaftswert verknüpft sind.
   c) Klicken Sie auf eine Netzwerklokalität, um nur Erkennungen anzuzeigen, bei denen sich der Teilnehmer in der ausgewählten Netzwerklokalität befindet.
5. klicken **Eine Optimierungsregel erstellen**.

   Kriterien für Optimierungsregeln werden automatisch so gefüllt, dass sie die gefilterten Ergebnisse auf der Übersichtsseite zur Härtung widerspiegeln.
6. klicken **Erstellen**.

   Die Regel wird der Seite „Tuning-Regeln“ hinzugefügt. Erfahre mehr über Verwaltung von Tuning-Regeln.

Eine Tuning-Regel von der Seite „Tuning-Regeln“ hinzufügen
Erstellen Sie Optimierungsregeln, um Erkennungen nach Erkennungstyp, Teilnehmer oder bestimmten Erkennungseigenschaften auszublenden.

Bevor Sie beginnen
Benutzer müssen Vollschreiben oder höher haben Privilegien um eine Erkennung zu optimieren.

Erfahre mehr über Abstimmung von Best Practices.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann auf **Tuning-Regeln**.
3. Klicken Sie **Erstellen**.
4. Spezifizieren Kriterien Abstimmung Optimierungsregeln und klicken Sie **Speichern**.

   Die Regel wird der Tabelle mit den Tuning-Regeln hinzugefügt.

Kriterien für Optimierungsregeln

Wählen Sie aus den folgenden Kriterien aus, um zu bestimmen, welche Erkennungen durch eine Optimierungsregel ausgeblendet werden.

Entdeckungstyp

Erstellen Sie eine Optimierungsregel, die für einen einzelnen Erkennungstyp gilt, oder legen Sie fest, dass die Regel je nach Systemmodul für alle Sicherheits- oder Leistungserkennungstypen gilt. Regeln, die alle Arten von Sicherheitserkennungen umfassen, sind in der Regel für Aktivitäten im Zusammenhang mit Schwachstellenscannern reserviert.

Teilnehmer

Erstellen Sie eine Optimierungsregel, die Erkennungen anhand bestimmter Täter- und Opferteilnehmer verbirgt.

Geben Sie die Teilnehmer an einer Optimierungsregel mit einer der folgenden Optionen an.

Jeder Täter oder Opfer

Sie können Any Offender oder Any Victim angeben, um alle Teilnehmer auszublenden. Diese Option ist effektiv, um Erkennungen während geplanter Tests oder beim Scannen von Schwachstelle auszublenden.

Gerätegruppe oder Gerät

Sie können ein erkanntes Gerät angeben oder Gerätegruppe um Teilnehmer zu verstecken. Sie können beispielsweise die integrierte Gerätegruppe für Vulnerability Scanner angeben, um Erkennungen auszublenden, an denen ein interner Scanner Teilnehmer ist.

Hinweis: Optimierungsregeln werden angewendet, wenn Erkennungen oder Optimierungsregeln erstellt oder aktualisiert werden. Optimierungsregeln werden nicht rückwirkend auf bestehende Erkennungen angewendet, wenn ein Teilnehmer zu einer dynamischen Gerätegruppe hinzugefügt oder daraus entfernt wird.

Externer Scan-Service

Sie können einen externen Scan-Service als Teilnehmer an einer Optimierungsregel angeben. Das ExtraHop-System verbirgt externe Scandienste basierend auf dem mit dem Dienst verknüpften IP-Adressbereich.

IP-Adresse oder CIDR-Block

Sie können eine einzelne IP-Adresse oder einen CIDR-Block von IP-Adressen angeben, um alle Teilnehmer innerhalb dieses Bereichs auszublenden. Wenn ein Team beispielsweise Penetrationstest in einem bestimmten Subnetz durchführt, können Sie eine Optimierungsregel mit den Subnetz-IP-Adressen erstellen, um einen Anstieg der Erkennungen im Zusammenhang mit Aufzählungs- und Hacking-Tools zu vermeiden.

Hinweis: Erkennungen werden basierend auf der IP-Adresse zum Zeitpunkt der Erkennung ausgeblendet. Da sich IP-Adressen für erkannte Geräte und externe Endpunkte dynamisch ändern können, ist die Angabe einer einzelnen IP-Adresse nur dann zuverlässig, wenn der Endpunkt eine statische IP-Adresse hat.

Hostname oder Domain

Sie können einen Hostnamen, Domainnamen oder Server Name Indication (SNI) angeben, um einen Teilnehmer auszublenden, der vom ExtraHop-System nicht erkannt wurde. Wenn Sie einen Domainnamen angeben, blendet die Tuning-Regel alle Subdomains aus. Wenn Sie beispielsweise eine Optimierungsregel mit vendor.com als Täter erstellen, blendet die Optimierungsregel Erkennungen mit example.vendor.com als Täter aus. Wenn Sie eine Subdomain wie example.vendor.com angeben, blendet die Tuning-Regel nur Erkennungen aus, bei denen der Teilnehmer mit genau dieser Subdomain endet. In diesem Beispiel wäre test.example.vendor.com versteckt, test.vendor.com jedoch nicht .

Hinweis: Tuning-Regeln verbergen erkannte Geräte nicht nach Hostnamen. Sie können erkannte Geräte als Optimierungsregelkriterien hinzufügen, indem Sie eine IP-Adresse, ein Gerät oder eine Gerätegruppe angeben.

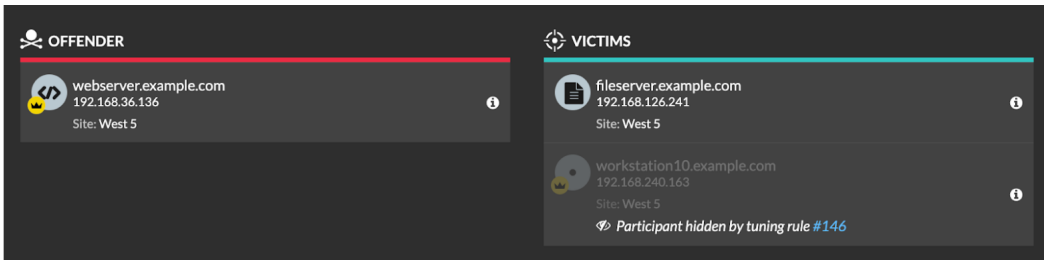
Netzwerk-Lokalität

Sie können eine angeben Netzwerklokalität um IP-Adressteilnehmer an diesem Ort zu verbergen.

Hinweis: Durch Tuning-Regeln werden nur Teilnehmer mit den spezifischen IP-Adressen ausgeblendet , die in der Netzwerklokalität enthalten sind. Wenn einem Gerät eine andere IP-Adresse außerhalb des CIDR-Blocks für den Netzwerkstandort zugewiesen wird, wird dieses Gerät nicht versteckt.

Hier sind einige wichtige Überlegungen zum Abstimmung von Teilnehmern:

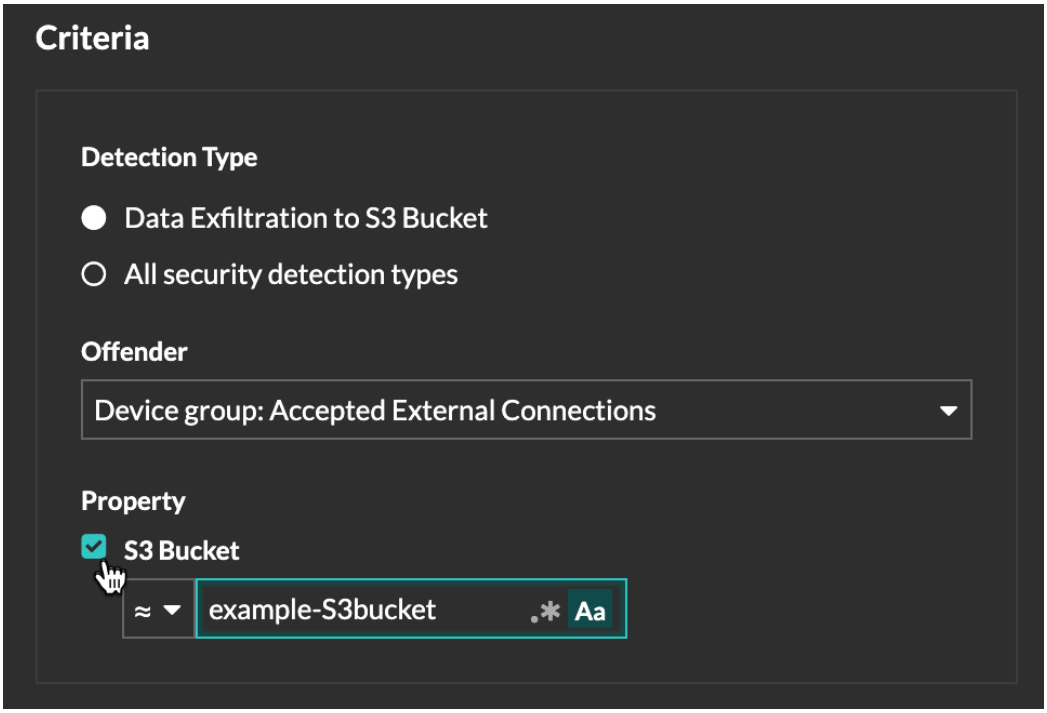
- Wenn die Teilnehmerkriterien für eine Optimierungsregel nur mit einem Teil der Teilnehmerliste einer Erkennung übereinstimmen, blendet das System die in der Optimierungsregel angegebenen Teilnehmer aus, ohne die gesamte Erkennung auszublenden.



- Teilnehmer, die als Optimierungskriterien angegeben sind, einschließlich CIDR-Blöcke und externe Scandienste, werden ausgeblendet, selbst wenn sie sich über ein Gateway oder einen Load Balancer verbinden.

Erkennungseigenschaften

Erstellen Sie eine Optimierungsregel, die Erkennungen anhand einer bestimmten Eigenschaft verbirgt. Sie können beispielsweise seltene SSH-Port-Erkennungen für eine einzelne Portnummer oder Erkennungen von Datenexfiltration in S3-Buckets für einen bestimmten S3-Bucket ausblenden.

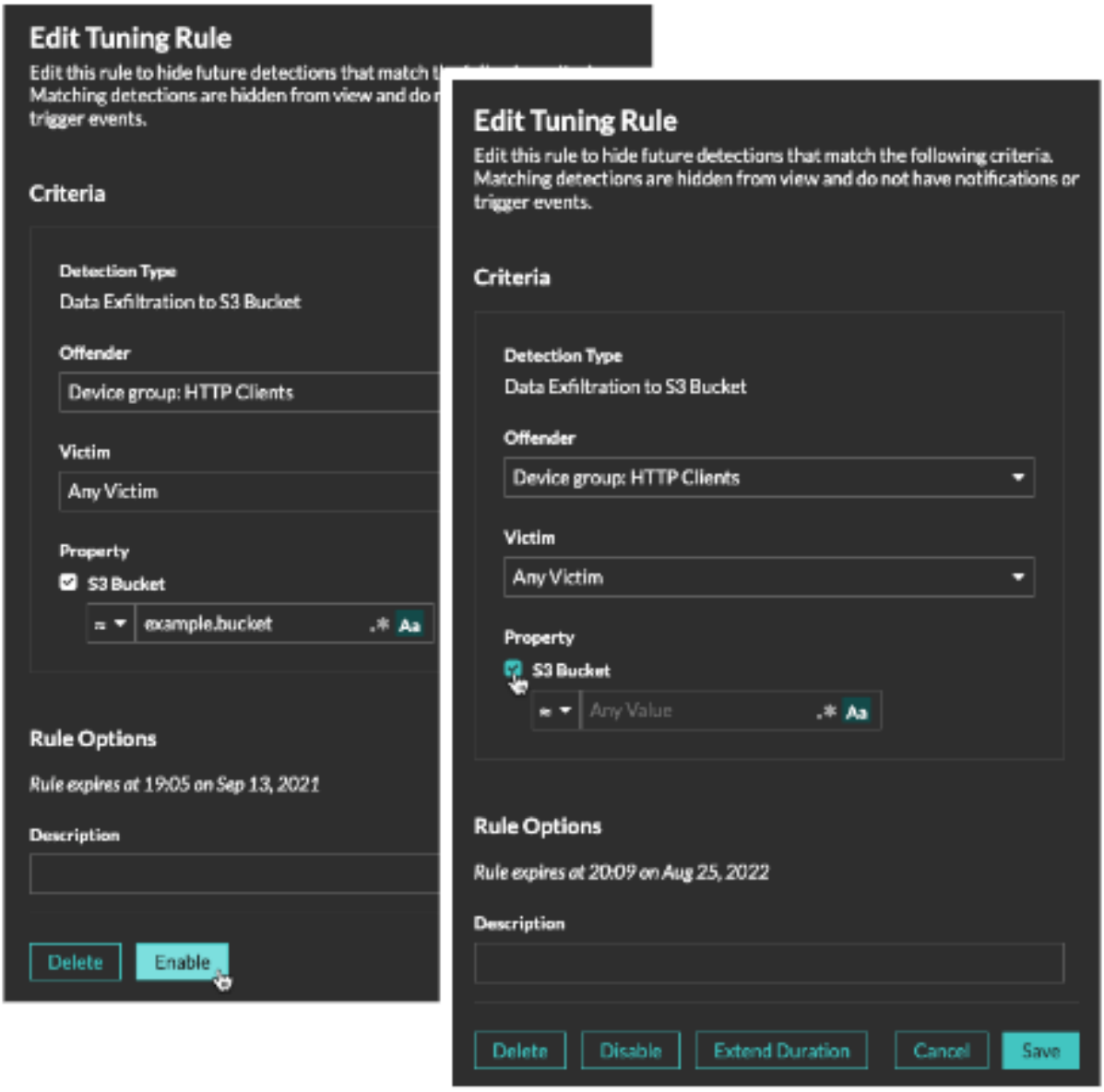


Tuning-Regeln verwalten

Sie können die Kriterien bearbeiten oder die Dauer einer Regel verlängern, eine Regel erneut aktivieren und eine Regel deaktivieren oder löschen.

Klicken Sie oben auf der Seite auf das Symbol Systemeinstellungen und wähle **Tuning-Regeln**.

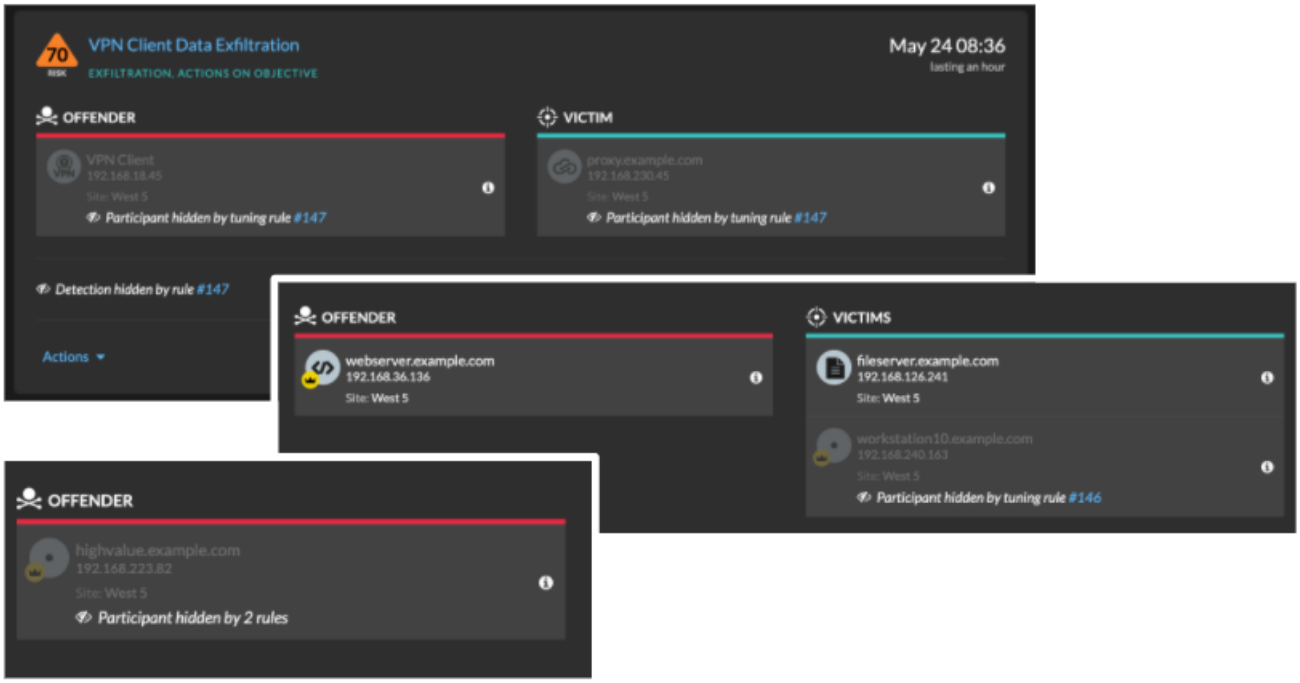
Klicken Sie auf eine Tuning-Regel in der Tuning-Regeln Tabelle zum Öffnen der Optimierungsregel bearbeiten tafel. Aktualisieren Sie Teilnehmer, Regelkriterien oder Eigenschaften, um den Geltungsbereich der Regel anzupassen. Klicken Sie auf die Schaltflächen am unteren Rand des Fensters, um eine Regel zu löschen, zu deaktivieren, zu aktivieren oder die Dauer einer Regel zu verlängern.



- Nachdem Sie eine Regel deaktiviert oder gelöscht haben, läuft die Regel sofort ab und die zugehörigen Auslöser und Benachrichtigungen werden fortgesetzt.
- Nachdem Sie eine Regel deaktiviert haben, bleiben zuvor ausgeblendete Erkennungen verborgen; laufende Erkennungen werden angezeigt.
- Beim Löschen einer Regel werden zuvor ausgeblendete Erkennungen angezeigt.
- Das ExtraHop-System löscht automatisch Erkennungen, die seit dem Startzeitpunkt der Erkennung 21 Tage lang auf dem System waren, die nicht andauern und die versteckt sind. Wenn eine neu erstellte oder bearbeitete Optimierungsregel eine Erkennung verbirgt, die diesen Kriterien entspricht, wird die betroffene Erkennung 48 Stunden lang nicht gelöscht.

Sie können das anwenden Versteckter Status zur Seite Erkennungen, um nur Erkennungen anzuzeigen, die derzeit versteckt durch eine Tuning-Regel.

Jede versteckte Erkennung oder jeder versteckte Teilnehmer enthält einen Link zur zugehörigen Optimierungsregel und zeigt den Benutzernamen des Benutzers an, der die Regel erstellt hat. Wenn die Erkennung oder der Teilnehmer durch mehrere Regeln verdeckt ist, wird die Anzahl der geltenden Regeln angezeigt.



Härteerkennungen filtern und abstimmen

Erkennungen in der Kategorie Härtung tragen dazu bei, das Risiko einer Ausnutzung zu verringern. Sie können eine große Anzahl von Härteerkennungen sortieren, indem Sie die Seite „Erkennungen“ filtern und Abstimmung.

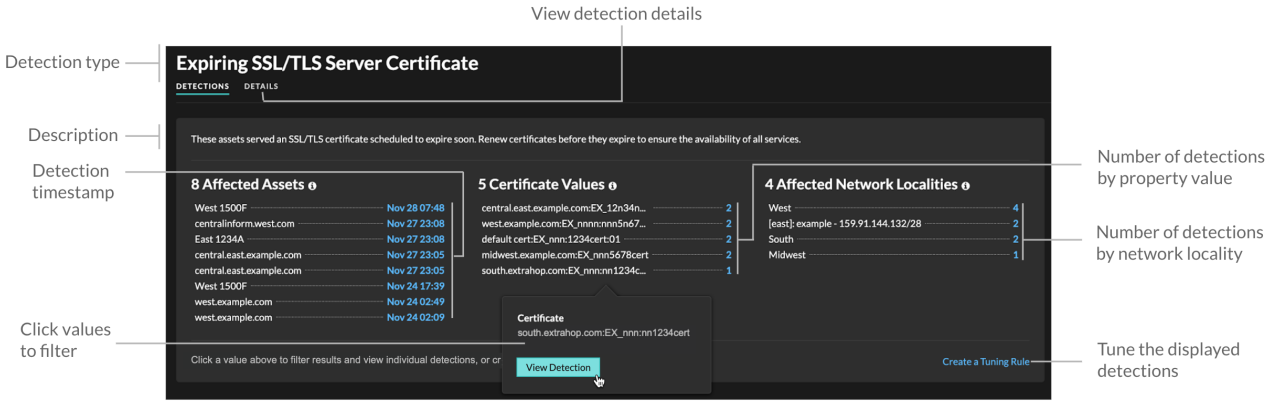
Bevor Sie beginnen

Benutzern muss Folgendes gewährt werden Privilegien um Erkennungen anzuzeigen und müssen über vollständige Schreibrechte oder höhere Rechte verfügen, um eine Optimierungsregel zu erstellen.

Erfahre mehr über Abstimmung von Erkennungen.

Erfahre mehr über Abstimmung von Best Practices.

Klicken Sie auf eine Härteerkennung aus dem Erkennungen Seite, um die Zusammenfassung anzusehen. In den Zusammenfassungen der Hardening-Erkennung werden der Entdeckungstyp, die Ressourcen, die an Erkennungen dieses Typs beteiligt sind, die Erkennungseigenschaften und die Netzwerkstandorte, an denen sich die betroffenen Geräte befinden, identifiziert.



Klicken Sie auf einen Asset-, Objekt- oder Netzwerkstandortwert, um einzelne Erkennungen anzuzeigen, die diesem Wert zugeordnet sind.

Betroffene Vermögenswerte

Eine Liste von Assets, die an Hardening-Erkennungen des ausgewählten Typs beteiligt sind. Die Liste der betroffenen Ressourcen ist nach dem letzten Zeitpunkt der Erkennung sortiert.

Immobilienwerte

Eine Liste der wichtigsten Eigenschaftswerte, die dem Erkennungstyp zugeordnet sind. Beispielsweise listet der Erkennungstyp Weak Cipher Suite die Verschlüsselungssammlungen auf, auf die bei Erkennungen verwiesen wird, und der Erkennungstyp Auslaufendes TLS-Serverzertifikat listet Zertifikate auf, deren Ablauf geplant ist. Die Liste der Eigenschaftswerte ist nach der Anzahl der Funde sortiert, die den Eigenschaftswert enthalten.

Betroffene Netzwerkstandorte

Eine Liste von Netzwerkstandorten, die Hardening-Erkennungen des ausgewählten Typs enthalten. Die Liste der betroffenen Netzwerkstandorte ist nach der Anzahl der Funde in der Netzwerklokalität sortiert.

Durch Filtern der Ergebnisse für eine einzelne Asset, Immobilie oder Lokalität können Sie Erkennungen identifizieren, die sich auf kritische Systeme auswirken oder eine Tuning-Regel erstellen Dadurch werden Erkennungen mit niedrigen Werten ausgeblendet, die den gefilterten Ergebnissen ähneln.

Erkennungsverfolgung aktivieren

Mit der Erkennungsverfolgung können Sie einem Benutzer eine Erkennung zuweisen, den Status festlegen und Notizen hinzufügen. Sie können Erkennungen direkt im ExtraHop-System, mit einem externen Ticketsystem eines Drittanbieters oder mit beiden Methoden verfolgen.

Hinweis Sie müssen die Ticketverfolgung auf allen angeschlossenen Sensoren aktivieren.

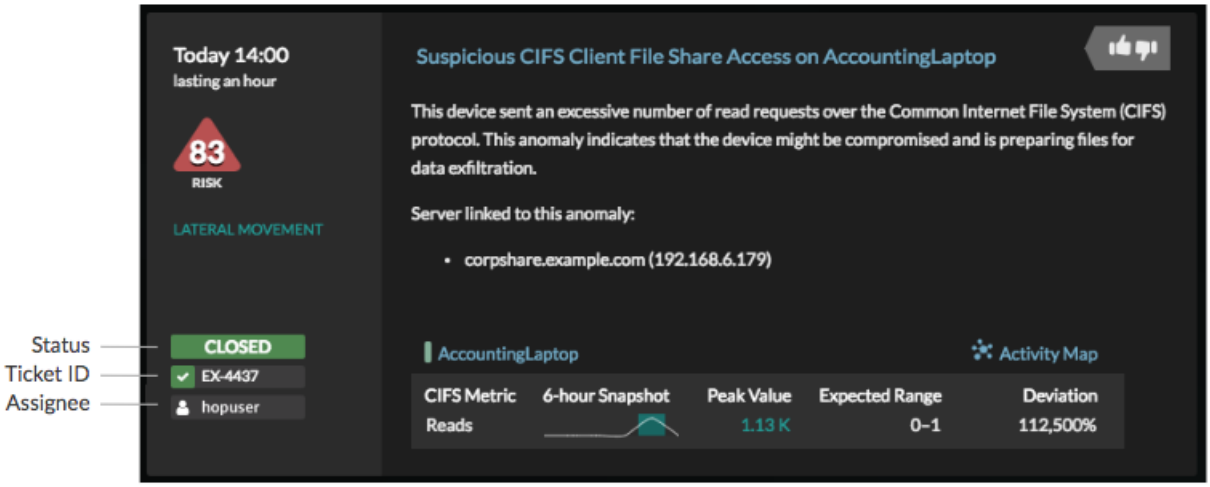
Bevor Sie beginnen

- Sie müssen Zugriff auf ein ExtraHop-System mit einem Benutzerkonto haben, das Administratorrechte.
- Nachdem Sie die externe Ticketverfolgung aktiviert haben, müssen Sie Ticket-Tracking von Drittanbietern konfigurieren indem Sie einen Auslöser schreiben, um Tickets in Ihrem Ticketsystem zu erstellen und zu aktualisieren, und dann Ticketaktualisierungen auf Ihrem ExtraHop-System über die REST-API aktivieren.
- Wenn Sie das externe Ticket-Tracking deaktivieren, werden zuvor gespeicherte Status- und Empfänger-Ticketinformationen in das ExtraHop-Erkennungs-Tracking umgewandelt. Wenn das Erkennungs-Tracking innerhalb des ExtraHop-Systems aktiviert ist, können Sie Tickets einsehen, die bereits existierten, als Sie das externe Ticket-Tracking deaktiviert haben, aber Änderungen an diesem externen Ticket werden nicht im ExtraHop-System angezeigt.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erkennungsverfolgung**.
3. Klicken Sie auf der Übersichtsseite auf **Systemeinstellungen** und klicken Sie dann **Die gesamte Verwaltung**.
4. Aus dem Einstellungen der Konsole Abschnitt, klicken **Erkennungsverfolgung**.
5. Wählen Sie eine oder beide der folgenden Methoden für die Nachverfolgung von Erkennungen aus:
   - Wählen **Ermöglichen Sie ExtraHop-Benutzern, Erkennungen aus dem ExtraHop-System heraus zu verfolgen**.
   - Wählen **Ermöglichen Sie externe Integrationen wie SOAR oder Ticket-Tracking-Systeme, um Erkennungen über die ExtraHop Rest API zu verfolgen** .

6. Optional: Nachdem Sie die Option zum Aktivieren externer Integrationen ausgewählt haben, geben Sie die URL-Vorlage für Ihr Ticketsystem an und fügen Sie die *$ Ticket_ID* variabel an der entsprechenden Stelle. Geben Sie beispielsweise eine vollständige URL ein, z. B. `https://jira.example.com/browse/$ticket_id`. Das *$ Ticket_ID* Die Variable wird durch die Ticket-ID ersetzt, die der Erkennung zugeordnet ist.

   Nachdem die URL-Vorlage konfiguriert ist, können Sie in einer Erkennung auf die Ticket-ID klicken, um das Ticket in einem neuen Browser-Tab zu öffnen.



Nächste Schritte
Wenn Sie externe Ticket-Tracking-Integrationen aktiviert haben, müssen Sie mit der folgenden Aufgabe fortfahren:

- Ticket-Tracking von Drittanbietern für Erkennungen konfigurieren

Ticket-Tracking von Drittanbietern für Erkennungen konfigurieren

Mit der Ticketverfolgung können Sie Tickets, Alarme oder Fälle in Ihrem Work-Tracking-System mit ExtraHop-Erkennungen verknüpfen. Jedes Ticketsystem von Drittanbietern, das Open Data Stream (ODS) - Anfragen annehmen kann, wie Jira oder Salesforce, kann mit ExtraHop-Erkennungen verknüpft werden.

Bevor Sie beginnen

- Das musst du haben hat in den Verwaltungseinstellungen die Option zum Nachverfolgen der Erkennung durch Dritte ausgewählt.
- Sie müssen Zugriff auf ein ExtraHop-System mit einem Benutzerkonto haben, das System- und Zugriffsadministrationsrechte.
- Sie müssen mit dem Schreiben von ExtraHop-Triggern vertraut sein. siehe Trigger und die Verfahren in Einen Auslöser erstellen.
- Sie müssen ein ODS-Ziel für Ihren Ticket-Tracking-Server erstellen. Weitere Informationen zur Konfiguration von ODS-Zielen finden Sie in den folgenden Themen : HTTP, Kafka, MongoDB, Syslog, oder Rohdaten.
- Sie müssen mit dem Schreiben von REST-API-Skripten vertraut sein und über einen gültigen API-Schlüssel verfügen, um die folgenden Verfahren ausführen zu können. siehe Generieren Sie einen API-Schlüssel.

Schreiben Sie einen Auslöser, um Tickets zu Erkennungen in Ihrem Ticketsystem zu erstellen und zu aktualisieren
Dieses Beispiel zeigt Ihnen, wie Sie einen Auslöser erstellen, der die folgenden Aktionen ausführt:

- Erstellen Sie jedes Mal, wenn eine neue Erkennung im ExtraHop-System erscheint, ein neues Ticket im Ticketsystem.
- Weisen Sie einem Benutzer mit dem Namen neue Tickets zu `escalations_team` im Ticketsystem.

- Wird jedes Mal ausgeführt, wenn eine Erkennung auf dem ExtraHop-System aktualisiert wird.
- Senden Sie Erkennungsaktualisierungen über einen HTTP Open Data Stream (ODS) an das Ticketsystem.

Das vollständige Beispielskript ist am Ende dieses Themas verfügbar.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Auslöser**.
3. klicken **Neu**.
4. Geben Sie einen Namen und eine optionale Beschreibung für den Auslöser an.
5. Wählen Sie in der Liste Ereignisse **ERKENNUNGSUPDATE**.

   Das Ereignis DETECTION_UPDATE wird jedes Mal ausgeführt, wenn eine Erkennung im ExtraHop-System erstellt oder aktualisiert wird.
6. Geben Sie im rechten Bereich Folgendes an Erkennungsklasse Parameter in einem JavaScript-Objekt. Diese Parameter bestimmen die Informationen, die an Ihr Ticketsystem gesendet werden.

   Der folgende Beispielcode fügt die Erkennungs-ID, die Beschreibung, den Titel, die Kategorien, die MITRE-Techniken und -Taktiken sowie die Risikoscore zu einem JavaScript-Objekt mit dem Namen hinzu `payload`:

```
const summary = "ExtraHop Detection: " + Detection.id + ": " +
 Detection.title;
const description = "ExtraHop has detected the following event on your
 network: " + Detection.description
const payload = {
    "fields": {
        "summary": summary,
        "assignee": {
            "name": "escalations_team"
        },
        "reporter": {
            "name": "ExtraHop"
        },
        "priority": {
            "id": Detection.riskScore
        },
        "labels": Detection.categories,
        "mitreCategories": Detection.mitreCategories,
        "description": description
    }
};
```

7. Definieren Sie als Nächstes die HTTP-Anforderungsparameter in einem JavaScript-Objekt unter dem vorherigen JavaScript-Objekt.

   Der folgende Beispielcode definiert eine HTTP-Anfrage für die im vorherigen Beispiel beschriebene Nutzlast: definiert eine Anfrage mit einer JSON-Payload:

```
const req = {
    'path': '/rest/api/issue',
    'headers': {
        'Content-Type': 'application/json'
    },
    'payload': JSON.stringify(payload)
};
```

   Weitere Hinweise zu ODS-Anforderungsobjekten finden Sie unter Offene Datenstromklassen.

8. Geben Sie abschließend die HTTP-POST-Anfrage an, die die Informationen an das ODS-Ziel sendet. Der folgende Beispielcode sendet die im vorherigen Beispiel beschriebene HTTP-Anfrage an ein ODS-Ziel namens Ticket-Server:

```
Remote.HTTP('ticket-server').post(req);
```

Der vollständige Triggercode sollte dem folgenden Beispiel ähneln:

```
const summary = "ExtraHop Detection: " + Detection.id + ": " +
 Detection.title;
const description = "ExtraHop has detected the following event on your
 network: " + Detection.description
const payload = {
    "fields": {
        "summary": summary,
        "assignee": {
            "name": "escalations_team"
        },
        "reporter": {
            "name": "ExtraHop"
        },
        "priority": {
            "id": Detection.riskScore
        },
        "labels": Detection.categories,
        "mitreCategories": Detection.mitreCategories,
        "description": description
    }
};

const req = {
    'path': '/rest/api/issue',
    'headers': {
        'Content-Type': 'application/json'
    },
    'payload': JSON.stringify(payload)
};

Remote.HTTP('ticket-server').post(req);
```

Ticketinformationen über die REST-API an Erkennungen senden
Nachdem Sie einen Auslöser konfiguriert haben, um Tickets für Erkennungen in Ihrem Ticket-Tracking-System zu erstellen, können Sie die Ticketinformationen in Ihrem ExtraHop-System über die REST-API aktualisieren.

Ticketinformationen werden bei Erkennungen auf der Seite „Entdeckungen“ im ExtraHop-System angezeigt. Weitere Informationen finden Sie in der Erkennungen Thema.

Das folgende Python-Beispielskript entnimmt Ticketinformationen aus einem Python-Array und aktualisiert die zugehörigen Erkennungen auf dem ExtraHop-System.

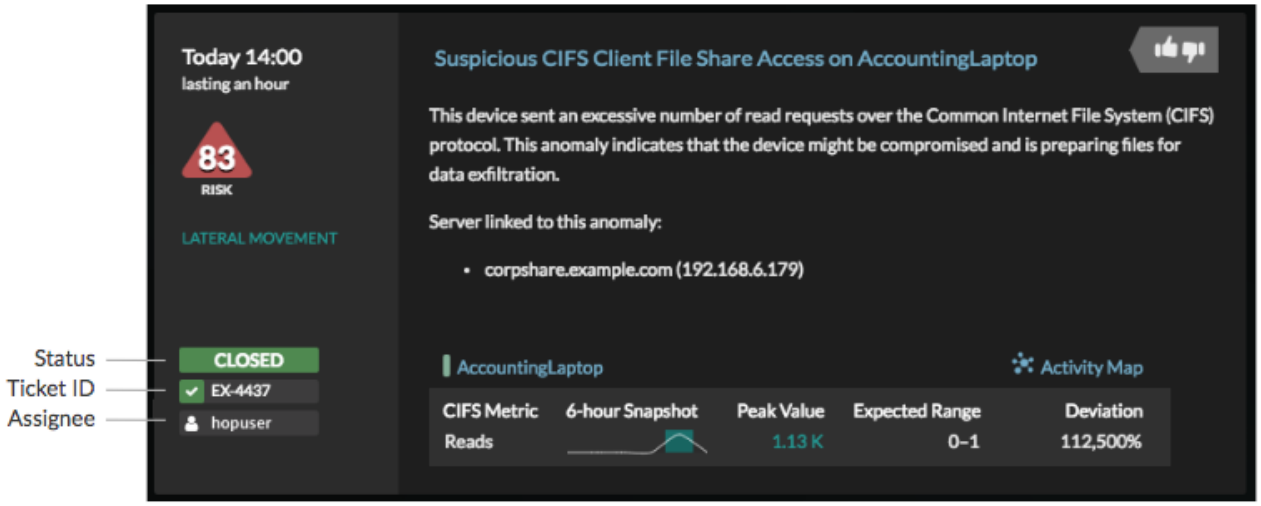
```
#!/usr/bin/python3

import json
import requests
import csv

API_KEY = '123456789abcdefghijklmnop'
HOST = 'https://extrahop.example.com/'

# Method that updates detections on an ExtraHop system
def updateDetection(detection):
```

```
    url = HOST + 'api/v1/detections/' + detection['detection_id']
    del detection['detection_id']
    data = json.dumps(detection)
    headers = {'Content-Type': 'application/json',
               'Accept': 'application/json',
               'Authorization': 'ExtraHop apikey=%s' % API_KEY}
    r = requests.patch(url, data=data, headers=headers)
    print(r.status_code)
    print(r.text)

# Array of detection information
detections = [
                {
                    "detection_id": "1",
                    "ticket_id": "TK-16982",
                    "status": "new",
                    "assignee": "sally",
                    "resolution": None,
                },
                {
                    "detection_id": "2",
                    "ticket_id": "TK-2078",
                    "status": None,
                    "assignee": "jim",
                    "resolution": None,
                },
                {
                    "detection_id": "3",
                    "ticket_id": "TK-3452",
                    "status": None,
                    "assignee": "alex",
                    "resolution": None,
                }
            ]

for detection in detections:
    updateDetection(detection)
```

Hinweis: Wenn das Skript eine Fehlermeldung zurückgibt, dass die TLS-Zertifikatsüberprüfung fehlgeschlagen ist, stellen Sie sicher, dass Ihrem Sensor oder Ihrer Konsole wurde ein vertrauenswürdiges Zertifikat hinzugefügt. Alternativ können Sie das hinzufügen `verify=False` Option zur Umgehung der Zertifikatsüberprüfung. Diese Methode ist jedoch nicht sicher und wird nicht empfohlen. Der folgende Code sendet eine HTTP GET-Anfrage ohne Zertifikatsüberprüfung:

```
requests.get(url, headers=headers, verify=False)
```

Nachdem die Ticketverfolgung konfiguriert wurde, werden Ticketdetails im linken Bereich der Erkennungsdetails angezeigt, ähnlich der folgenden Abbildung:



Status

Der Status des Tickets, das mit der Erkennung verknüpft ist. Das Ticket-Tracking unterstützt die folgenden Status:

- Neu
- Im Gange
- geschlossen
- Mit ergriffenen Maßnahmen geschlossen
- Geschlossen, ohne dass Maßnahmen ergriffen wurden

Ticket-ID

Die ID des Tickets in Ihrem Work-Tracking-System, das mit der Erkennung verknüpft ist. Wenn Sie eine Vorlagen-URL konfiguriert haben, können Sie auf die Ticket-ID klicken, um das Ticket in Ihrem Work-Tracking-System zu öffnen.

Abtretungsempfänger

Der Benutzername, der dem Ticket zugewiesen wurde, das mit der Erkennung verknüpft ist. Graue Benutzernamen weisen auf ein Konto hin, das kein ExtraHop-Konto ist.

Untersuchen Sie Sicherheitserkennungen

Wenn eine interessante Erkennung auftritt, sollten Sie untersuchen, ob das erkannte Verhalten auf ein Problem mit niedriger Priorität oder auf ein potenzielles Sicherheitsrisiko hindeutet. Sie können Ihre Untersuchung direkt von der Erkennungskarte aus starten, die Links zu Daten im gesamten ExtraHop-System enthält.

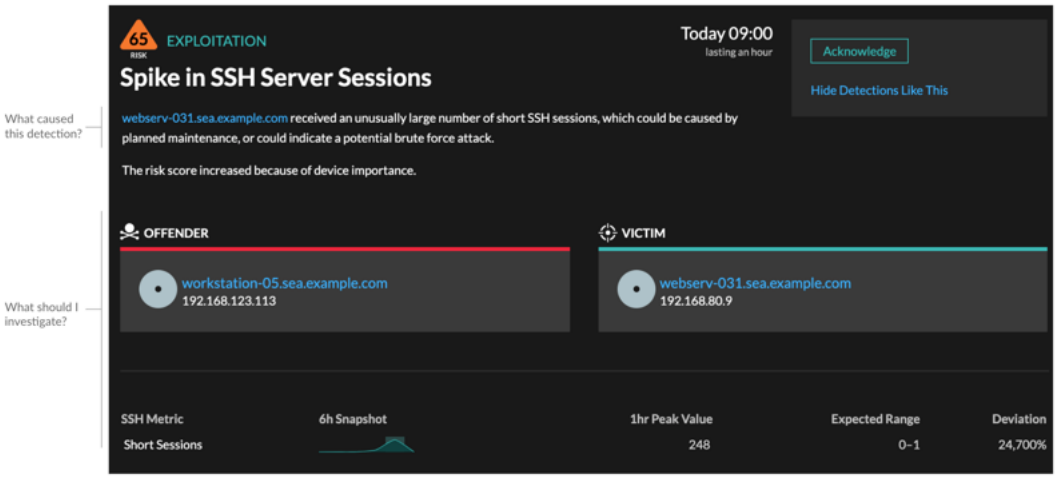
Es gibt eine Reihe von Tools, die Ihnen beim Filtern helfen können Ihre Ansicht, um die Erkennungen zu sehen, die Sie für die Untersuchung priorisieren möchten. Halten Sie zunächst nach den folgenden Trends Ausschau:

- Gab es zu ungewöhnlichen oder unerwarteten Zeiten Erkennungen, z. B. bei Benutzeraktivitäten am Wochenende oder außerhalb der Geschäftszeiten?
- Erscheinen irgendwelche Erkennungen in großen Clustern auf der Timeline?
- Werden Erkennungen für hochwertige Endgeräte angezeigt?
- Gibt es Entdeckungen mit hohen Risikowerten?
- Sind Geräte, die an der Erkennung beteiligt sind, auch an anderen Erkennungen beteiligt?

- Werden anhand einer Bedrohungssammlung im Zusammenhang mit der Erkennung Indikatoren für eine Gefährdung identifiziert?

Beginne deine Untersuchung

Lesen Sie den Titel und die Zusammenfassung der Erkennung, um zu erfahren, was die Erkennung verursacht hat.



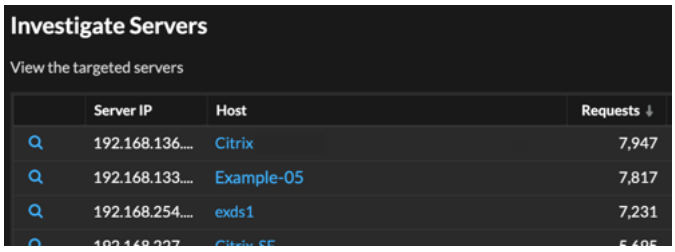
Verfeinern Sie Ihre Untersuchung

Erkennungsdetailkarten enthalten verwandte Daten zur Erkennung. Die Verfügbarkeit der Daten hängt von den Geräten und Metriken ab, die mit der Erkennung verknüpft sind. Nachdem Sie auf einen Link geklickt haben, können Sie zur Erkennungskarte zurückkehren, indem Sie im Navigationspfad auf den Erkennungsnamen klicken. Jede Untersuchungsoption wird in den folgenden Abschnitten beschrieben.

Überprüfen Sie die Ermittlungsdaten

Die meisten Daten, die Sie benötigen, um eine Erkennung zu verstehen, zu validieren und zu untersuchen, werden auf der Erkennungsdetailseite angezeigt: Tabellen mit relevanten Metrikdaten, Aufzeichnungstransaktionen und Links zu Rohpaketen.

Klicken Sie auf einen Hostnamen, um zur Seite Geräteübersicht zu gelangen, oder klicken Sie mit der rechten Maustaste, um ein Diagramm mit diesem Gerät als Quelle und den relevanten Messwerten zu erstellen.

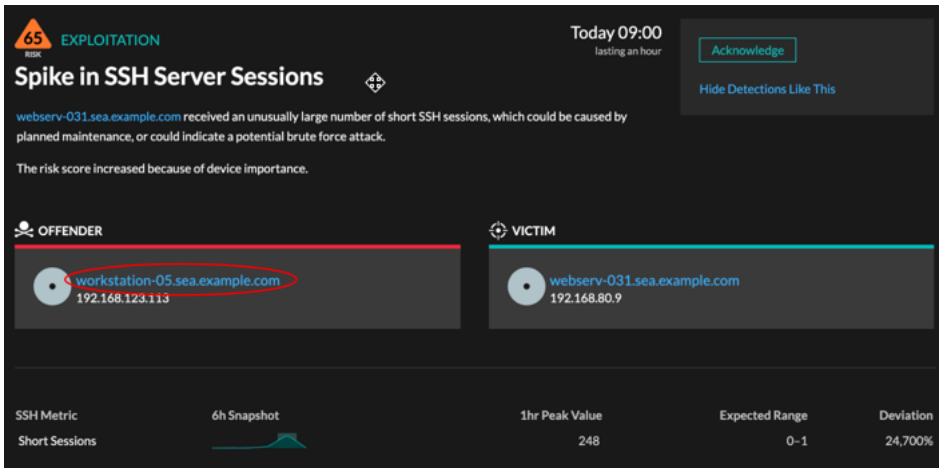


Name des Geräts

Klicken Sie auf einen Gerätenamen, um zur Seite Geräteübersicht zu gelangen, die die Rolle, Benutzer und Tags enthält, die diesem Gerät zugeordnet sind. Klicken Sie im linken Bereich auf einen Protokollnamen,

um alle mit dem Gerät verknüpften Protokollmetriken anzuzeigen. Auf der Protokollseite erhalten Sie ein vollständiges Bild davon, was dieses Gerät zum Zeitpunkt der Erkennung getan hat.

Wenn Sie beispielsweise einen Reconnaissance-Scan erkennen, können Sie Erkennung, ob dem Gerät, das mit dem Scan verknüpft ist, die Rolle Vulnerability Scanner zugewiesen wurde.



Verfügbarkeit

Links zu Gerätenamen sind nur für Geräte verfügbar, die vom ExtraHop-System automatisch erkannt wurden. Remote-Geräte, die sich außerhalb Ihres Netzwerk befinden, werden durch ihre IP-Adressen dargestellt.

Karte der Aktivitäten

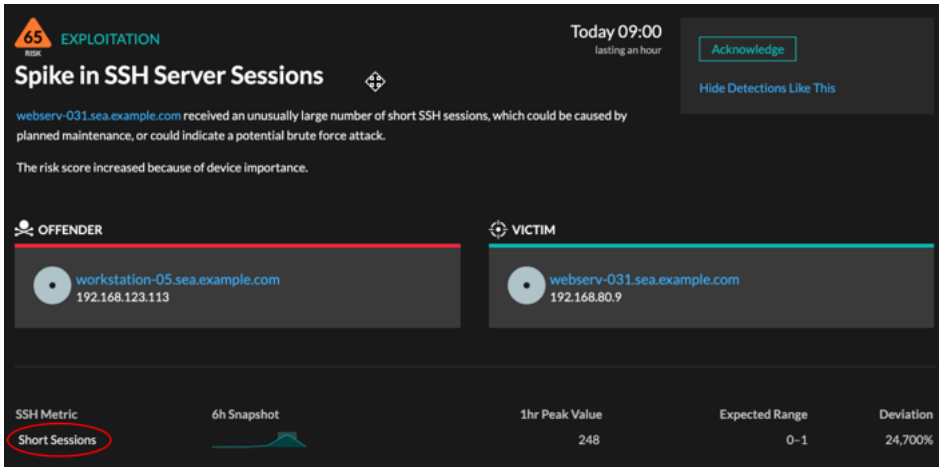
Klicken Sie auf das Activity Map-Symbol neben einem Gerätenamen, um die Geräteverbindungen nach Protokoll während der Erkennung anzuzeigen. Wenn Sie beispielsweise eine laterale Bewegung Bewegungserkennung erhalten, können Sie herausfinden, ob das verdächtige Gerät über ein Fernsteuerungsprotokoll Verbindungen zu anderen Clients, IT-Servern oder Domänencontrollern in Ihrem Netzwerk hergestellt hat.

Verfügbarkeit

Eine Aktivitätsdiagramm ist verfügbar, wenn ein einzelner Client oder Server mit ungewöhnlichen L7-Protokollaktivitäten verknüpft ist, z. B. einer hohen Anzahl von HTTP-Fehlern oder DNS-Anforderungs-Timeouts.

Detaillierter Metrik Drilldown

Klicken Sie auf einen Link zur Detail-Metrik, um einen Metrikwert genauer zu betrachten. Eine Metrik-Detailseite wird angezeigt , auf der Messobjektwerte nach einem Schlüssel aufgelistet sind, z. B. Client-IP-Adresse, Server-IP-Adresse, Methode oder Fehler. Wenn bei Ihnen beispielsweise ein Reconnaissance Scan erkannt wird, können Sie einen Drilldown durchführen, um herauszufinden, welche Client-IP-Adressen während der Erkennung mit der ungewöhnlich hohen Anzahl von 404-Statuscodes verknüpft waren.

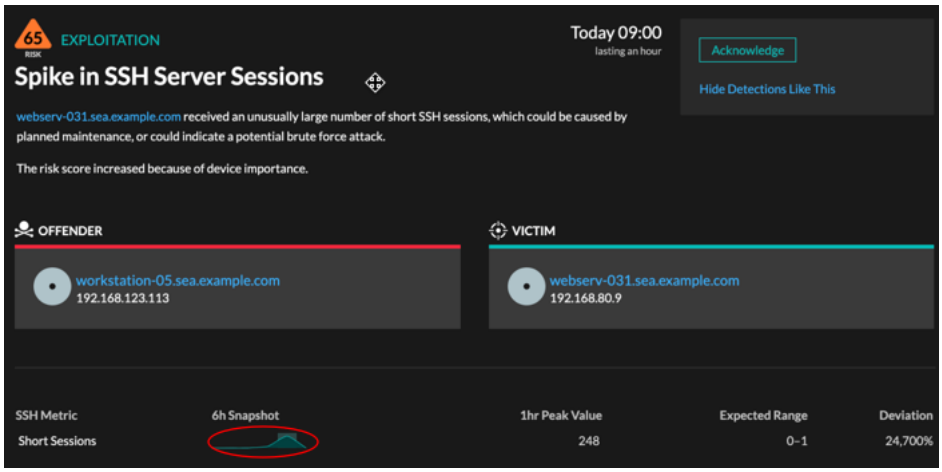


Verfügbarkeit

Die Drilldown-Option ist verfügbar für Erkennungen im Zusammenhang mit Topnset detaillierte Metriken.

Sparkline

Klicken Sie auf die Sparkline, um ein Diagramm zu erstellen, das die Quelle, das Zeitintervall und die Drilldown-Details der Erkennung enthält. Dieses Diagramm können Sie dann zur Überwachung zu einem Dashboard hinzufügen. Wenn Sie beispielsweise eine ungewöhnliche Anzahl von Remotesitzungen feststellen, erstellen Sie ein Diagramm mit SSH-Sitzungen für diesen Server und fügen Sie dieses Diagramm dann einem Dashboard zur Sitzungsverwaltung hinzu.



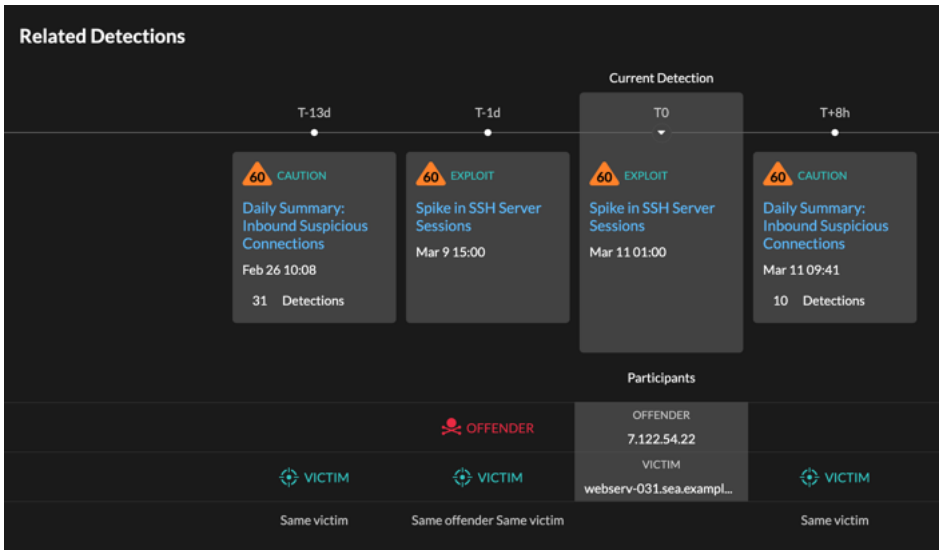
Verfügbarkeit

Die Sparkline-Option ist für Erkennungen verfügbar, die mit Metriken verknüpft waren und eine Dauer von über einer Stunde hatten. Für 1-Sekunden-Metriken ist eine Sparkline verfügbar, wenn die Dauer über 30 Sekunden lag.

Verwandte Erkennungen

Klicken Sie auf eine verwandte Erkennung , um Informationen über verdächtiges Verhalten und neu auftretende Angriffe bei mehreren Erkennungen mit gemeinsamen Teilnehmern zu erhalten. Beispielsweise könnte ein Opfer an der aktuellen Erkennung, das an einer späteren Erkennung als Täter teilnimmt, darauf hinweisen, dass das Gerät kompromittiert ist. Sie können zugehörige Erkennungsdetails anzeigen, um

festzustellen, ob die Erkennungsereignisse ähnlich sind, und um zu sehen , welche anderen Geräte beteiligt sind.



Verfügbarkeit

Die entsprechende Zeitleiste für Erkennungen ist verfügbar, wenn es Erkennungen gibt, bei denen dieselben Opfer- oder Täterteilnehmer wie bei der aktuellen Erkennung aufgetreten sind. Ähnliche Erkennungen sind möglicherweise vor oder nach der aktuellen Erkennung aufgetreten.

Bedrohungsinformationen

Klicken Sie auf ein rotes Kamerasymbol um detaillierte Bedrohungsinformationen zu einem Bedrohungsindikator abzurufen.

Bedrohungsinformationen liefern bekannte Daten über verdächtige IP-Adressen, Hostnamen und URIs, die Ihnen helfen können , Risiken für Ihr Unternehmen zu identifizieren. Diese Datensätze, sogenannte Bedrohungssammlungen, sind standardmäßig in Ihrem RevealX-System und aus kostenlosen und kommerziellen Quellen in der Sicherheits-Community verfügbar.

Verfügbarkeit

Bedrohungsinformationen müssen auf Ihrem RevealX-System aktiviert sein, bevor Sie diese Indikatoren sehen können.

Untersuchen Sie Leistungserkennungen

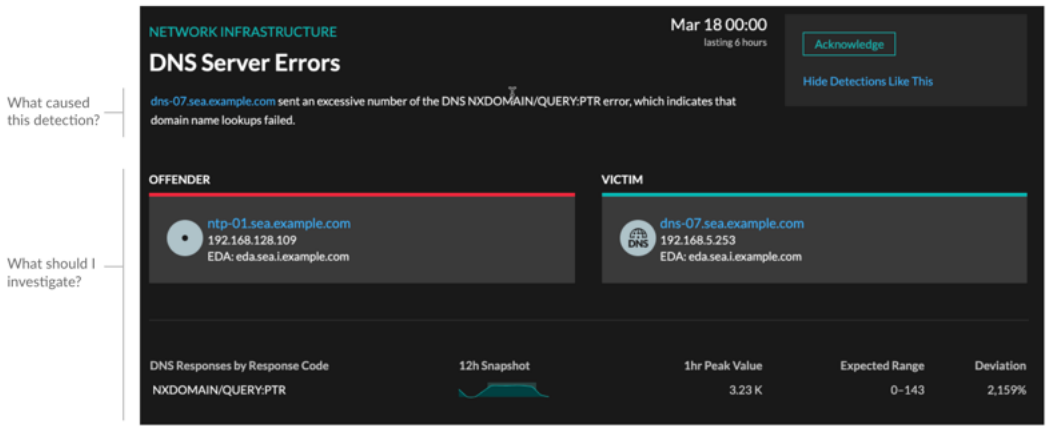
Wenn eine interessante Erkennung auftritt, sollten Sie untersuchen, ob das erkannte Verhalten auf ein Problem mit niedriger Priorität oder auf ein potenzielles Problem hindeutet. Sie können Ihre Untersuchung direkt von der Erkennungskarte aus starten, die Links zu Daten im gesamten ExtraHop-System enthält.

Es gibt eine Reihe von Tools, die Ihnen beim Filtern helfen können Ihre Ansicht, um die Erkennungen zu sehen, denen Sie bei der Untersuchung Priorität einräumen möchten. Halten Sie zunächst nach den folgenden Trends Ausschau:

- Gab es zu ungewöhnlichen oder unerwarteten Zeiten Erkennungen, z. B. bei Benutzeraktivitäten am Wochenende oder außerhalb der Geschäftszeiten?
- Erscheinen irgendwelche Erkennungen in großen Clustern auf der Timeline?
- Werden Erkennungen für hochwertige Endgeräte angezeigt?
- Sind Geräte, die an der Erkennung beteiligt sind, auch an anderen Erkennungen beteiligt?

Beginne deine Untersuchung

Lesen Sie den Titel und die Zusammenfassung der Erkennung, um zu erfahren, was die Erkennung verursacht hat.



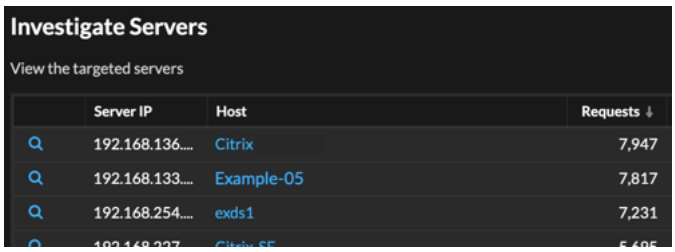
Verfeinern Sie Ihre Untersuchung

Karten mit Erkennungsdetails enthalten zugehörige Daten zur Erkennung. Die Verfügbarkeit der Daten hängt von den Geräten und Metriken ab, die mit der Erkennung verknüpft sind. Nachdem Sie auf einen Link geklickt haben, können Sie zur Erkennungskarte zurückkehren, indem Sie im Navigationspfad auf den Namen der Erkennung klicken. Jede Untersuchungsoption wird in den folgenden Abschnitten beschrieben.

Ermittlungsdaten überprüfen

Die meisten Daten, die Sie benötigen, um eine Erkennung zu verstehen, zu validieren und zu untersuchen, werden auf der Erkennungsdetailseite angezeigt: Tabellen mit relevanten Metrikdaten, Datensatztransaktionen und Links zu Rohpaketen.

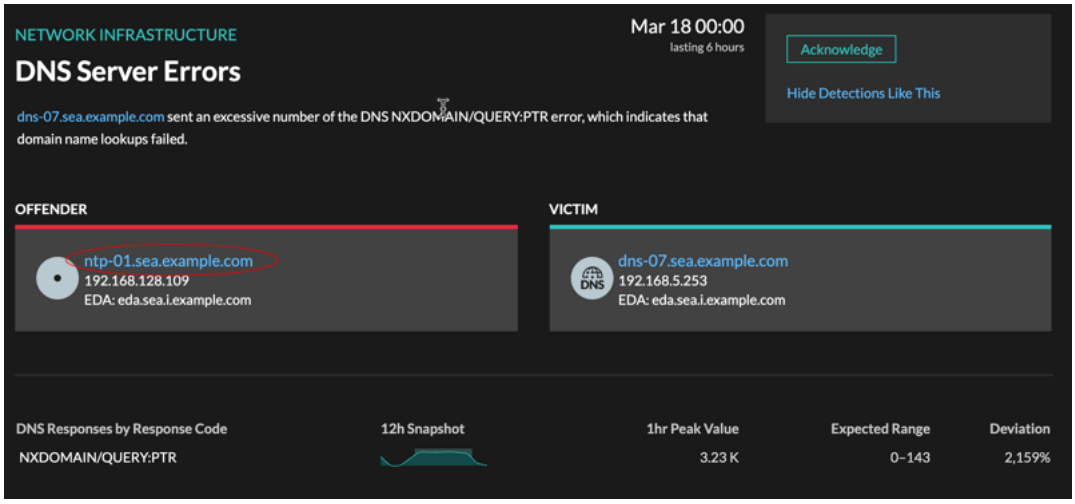
Klicken Sie auf einen Hostnamen, um zur Seite „Geräteübersicht“ zu gelangen, oder klicken Sie mit der rechten Maustaste, um ein Diagramm mit diesem Gerät als Quelle und den entsprechenden Messwerten zu erstellen.



Name des Geräts

Klicken Sie auf einen Gerätenamen, um zur Seite „Geräteübersicht“ zu gelangen, die die Rolle, Benutzer und Tags enthält, die mit diesem Gerät verknüpft sind. Klicken Sie im linken Bereich auf einen Protokollnamen, um alle mit dem Gerät verknüpften Protokollmetriken anzuzeigen. Auf der Protokollseite erhalten Sie einen vollständigen Überblick darüber, was dieses Gerät zum Zeitpunkt der Erkennung getan hat.

Wenn Sie beispielsweise feststellen, dass Datenbanktransaktionen fehlschlagen, können Sie sich über andere Aktivitäten im Zusammenhang mit dem Server informieren, der die Datenbank-Instance hostet.



Verfügbarkeit

Links zu Gerätenamen sind nur für Geräte verfügbar, die vom ExtraHop-System automatisch erkannt wurden. Remote-Geräte, die sich außerhalb Ihres Netzwerk befinden, werden durch ihre IP-Adressen dargestellt.

Karte der Aktivitäten

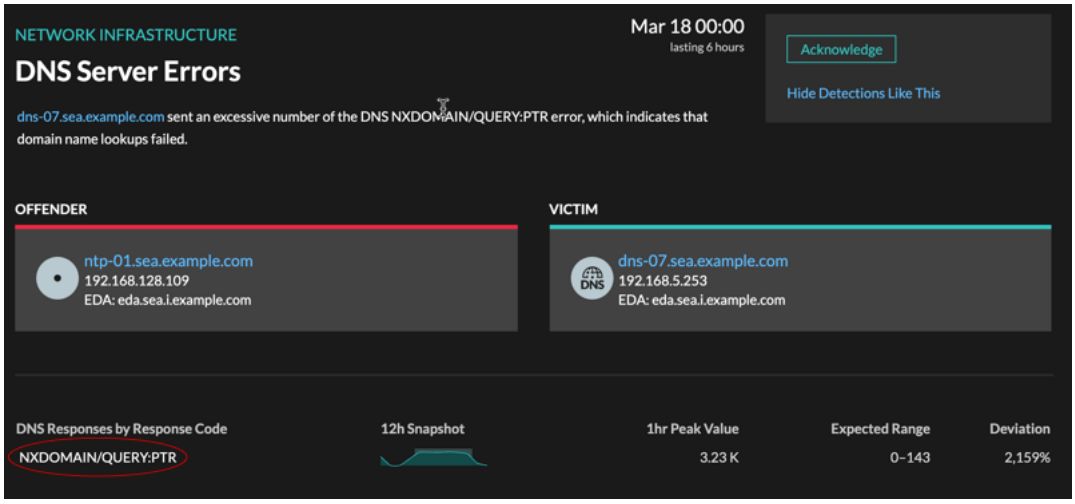
Klicken Sie auf das Activity Map-Symbol neben einem Gerätenamen, um die Geräteverbindungen nach Protokoll während der Erkennung anzuzeigen. Wenn Sie beispielsweise eine Erkennung von LDAP-Authentifizierungsfehlern erhalten, können Sie eine Aktivitätsdiagramm erstellen, um zu erfahren, welche Geräte während der Erkennung mit einem LDAP-Server verbunden waren.

Verfügbarkeit

Eine Aktivitätsdiagramm ist verfügbar, wenn ein einzelner Client oder Server mit ungewöhnlichen L7-Protokollaktivitäten in Verbindung gebracht wird, z. B. einer hohen Anzahl von HTTP-Fehlern oder Timeouts bei DNS-Anfragen.

Detaillierter Metrik Drilldown

Klicken Sie auf einen Link zur Detail-Metrik, um einen Metrikwert aufzuschlüsseln. Es wird eine Seite mit Detail-Metrik angezeigt , auf der Metrikwerte nach einem Schlüssel aufgelistet sind, z. B. Client-IP-Adresse, Server-IP-Adresse, Methode oder Fehler. Wenn Sie beispielsweise eine Authentifizierungserkennung für einen LDAP-Server erhalten, können Sie im Detail herausfinden, welche Client-IP-Adressen die ungültigen Anmeldedaten übermittelt haben, die zur Gesamtzahl der LDAP-Fehler beigetragen haben.

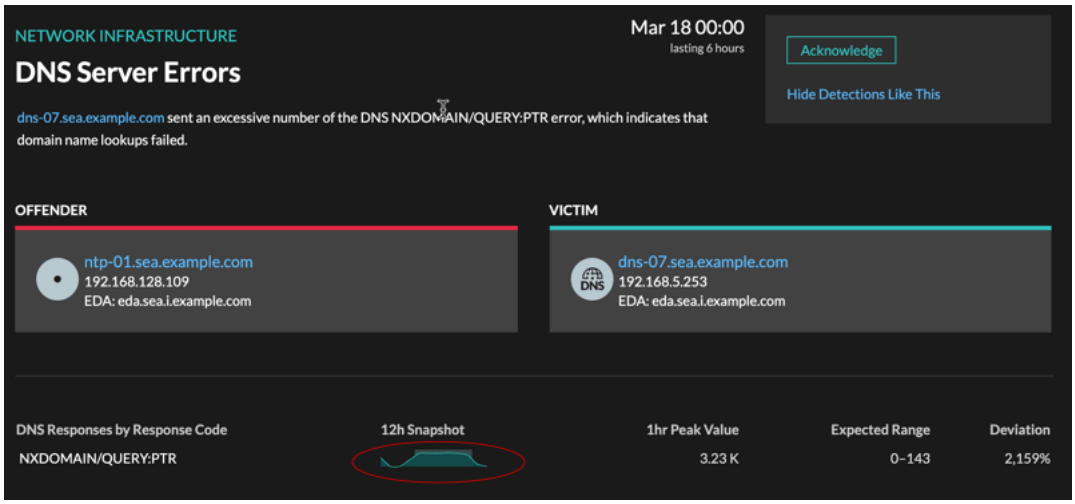


Verfügbarkeit

Die Drilldown-Option ist für Erkennungen verfügbar, die mit Topnset detaillierte Metriken.

Sparkline

Klicken Sie auf die Sparkline, um ein Diagramm zu erstellen, das die Quelle, das Zeitintervall und die Drilldown-Details der Erkennung enthält. Sie können es dann einem Dashboard zur zusätzlichen Überwachung hinzufügen. Wenn Sie beispielsweise Probleme mit dem Erkennung feststellen, können Sie ein Diagramm mit den 500 vom Server gesendeten Statuscodes erstellen und dieses Diagramm dann zu einem Dashboard über die Leistung der Website hinzufügen.



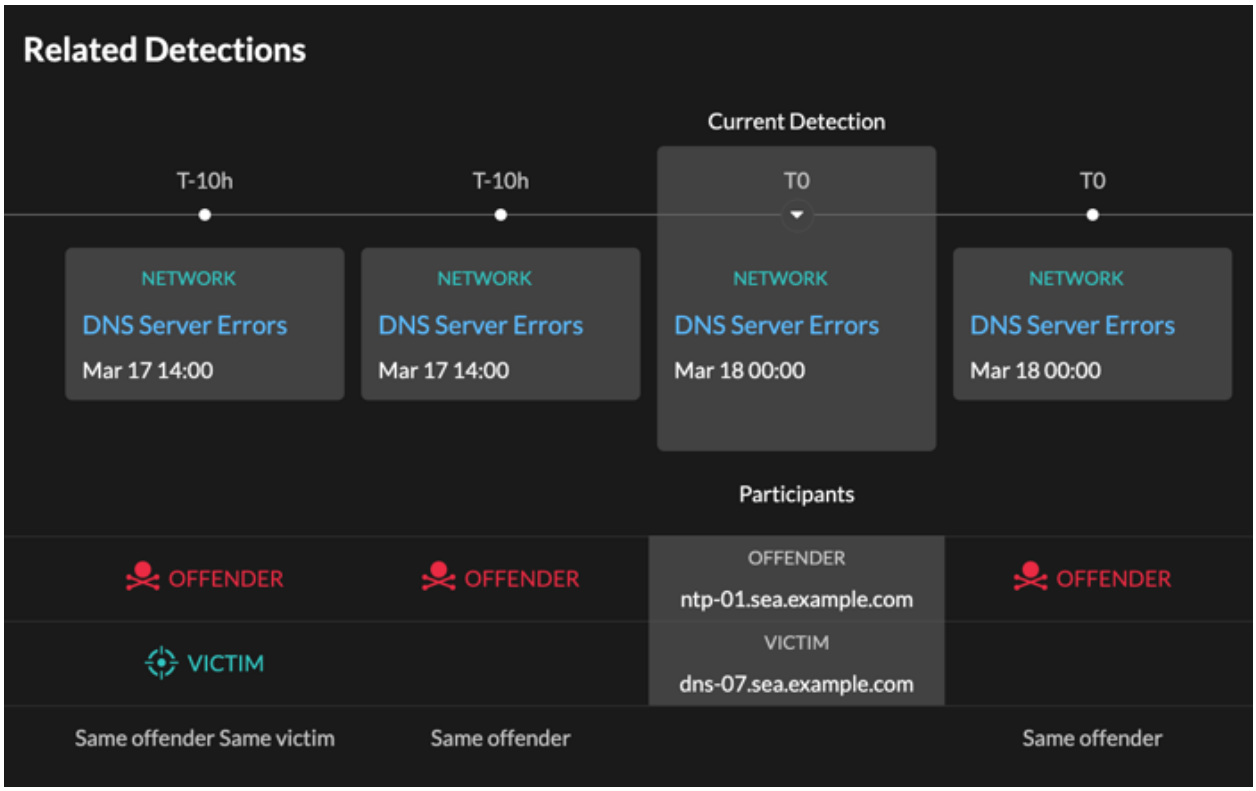
Verfügbarkeit

Die Sparkline-Option ist für Erkennungen verfügbar, die mit Metriken verknüpft waren.

Verwandte Erkennungen

Klicken Sie auf eine entsprechende Erkennung, um Informationen zu Netzwerk-, Anwendung- und Infrastrukturproblemen bei mehreren Erkennungen mit gemeinsamen Teilnehmern zu erhalten. Beispielsweise ist ein als Täter identifiziertes Gerät die wahrscheinliche Quelle eines Problems, z. B. ein Datenbankserver, der eine übermäßige Anzahl von Antwortfehlern sendet. Ein Gerät, das als Opfer identifiziert wurde, ist in der Regel negativ von dem Problem betroffen, z. B. bei Clients, bei denen langsame oder fehlgeschlagene Datenbanktransaktionen auftreten. Sie können zugehörige Erkennungsdetails

anzeigen, um festzustellen, ob die Erkennungsereignisse ähnlich sind, um zu sehen, welche anderen Geräte beteiligt sind, und um Metrikdaten einzusehen.



Verfügbarkeit

Die zugehörige Erkennungszeitleiste ist verfügbar, wenn es Erkennungen gibt, an denen dieselben Opfer- oder Täterteilnehmer wie an der aktuellen Erkennung beteiligt sind. Ähnliche Erkennungen sind möglicherweise vor oder nach der aktuellen Erkennung aufgetreten.

Bedrohungsinformationen

Bedrohungsinformationen bieten Hinweise zu potenziellen Bedrohungen für Ihr Netzwerk.

Bedrohungsinformationen beziehen sich auf die folgenden Ereignisse:

- Branchenweite Sicherheitsereignisse, bei denen das ExtraHop-System Erkennungen im Zusammenhang mit bekannten Sicherheitslücken entdeckt.
- Sicherheitsanalyse-Briefings, die auf Ihr Netzwerk zugeschnittene Machine-Learning-Analysen bieten.
- (Nur RevealX 360.) Rückblickende Informationen zur Bedrohungsanalyse, in denen neue Bedrohungsindikatoren in aktualisierten, von Extrahop kuratierten Bedrohungsinformationen erkannt werden.

Bedrohungsinformationen enthalten Hinweise auf Scans, Exploits und Bedrohungsindikatoren (Kompromittierungsindikatoren), die im Zusammenhang mit der Bedrohung stehen. Die Informationen in jedem Briefing variieren je nach Art der Bedrohung. Die Informationen im Zusammenhang mit dem Briefing werden in der Cloud aktualisiert, sobald Details über das Kompromittierungsindikatoren, potenzielle Angriffsvektoren und bekannte Risiken bekannt werden.

Bedrohungsinformationen finden Sie in der oberen linken Ecke des Überblick über die Sicherheit Seite. Klicken Sie auf einen beliebigen Titel, um zur Detailseite für dieses Briefing zu gelangen. Die Detailseite wird aktualisiert, sobald weitere Informationen gefunden werden.

Hier sind einige Möglichkeiten, wie Sie den Überblick über Bedrohungsinformationen behalten können:

- Eine Benachrichtigungsregel Bedrohungsübersicht Bedrohungsinformationen erstellen um E-Mails zu erhalten, wenn eine neue Bedrohungsübersicht erscheint.
- klicken **Untersuchung erstellen** von der Detailseite aus, um die mit dem Briefing verbundenen Entdeckungen zu einer Untersuchung hinzuzufügen.
- klicken **Archiv-Briefing** von der Detailseite aus, wenn Sie das Briefing nicht mehr überwachen möchten; das Briefing wird automatisch wiederhergestellt und eine Benachrichtigungs-E-Mail wird gesendet, wenn das Briefing aktualisiert wird. Ältere Briefings finden Sie im Abschnitt Archiviert auf der Seite Threat Briefing. klicken **Briefing wiederherstellen** auf der Detailseite, um das Briefing wieder in den aktiven Bereich der Seite Threat Briefing zu verschieben.

Eine Benachrichtigungsregel Bedrohungsübersicht Bedrohungsinformationen erstellen

Sie können eine Benachrichtigungsregel erstellen, die eine Empfängerliste per E-Mail sendet, wenn eine neue Bedrohungsinformation veröffentlicht oder automatisch wiederhergestellt wird. Briefings werden automatisch wiederhergestellt, wenn sie mit Inhaltsänderungen oder neuen Erkennungen aktualisiert werden.

Bevor Sie beginnen

- Benutzern muss der Zugriff auf das NDR-Modul gewährt werden und sie müssen Vollzugriff haben Privilegien oder höher, um die Aufgaben in diesem Handbuch abzuschließen.
- Das ExtraHop-System muss verbunden mit ExtraHop Cloud Services um Benachrichtigungen per E-Mail zu senden.
- E-Mail-Benachrichtigungen werden von no-reply@notify.extrahop.com gesendet. Stellen Sie sicher, dass Sie diese Adresse zu Ihrer Liste der zulässigen Absender hinzufügen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann auf **Regeln für Benachrichtigungen**.

3. Klicken Sie **Erstellen**.
4. Klicken Sie **Lagebesprechung über Bedrohungen**.
5. Geben Sie im Feld Name einen eindeutigen Namen für die Benachrichtigungsregel ein.
6. Fügen Sie im Feld Beschreibung Informationen zur Benachrichtigungsregel hinzu.
7. Geben Sie einzelne E-Mail-Adressen an, getrennt durch ein Komma.
8. In der Optionen Abschnitt, der **Benachrichtigungsregel aktivieren** Das Kontrollkästchen ist standardmäßig aktiviert. Deaktivieren Sie das Kontrollkästchen, um die Benachrichtigungsregel zu deaktivieren.
9. Klicken Sie **Speichern**.

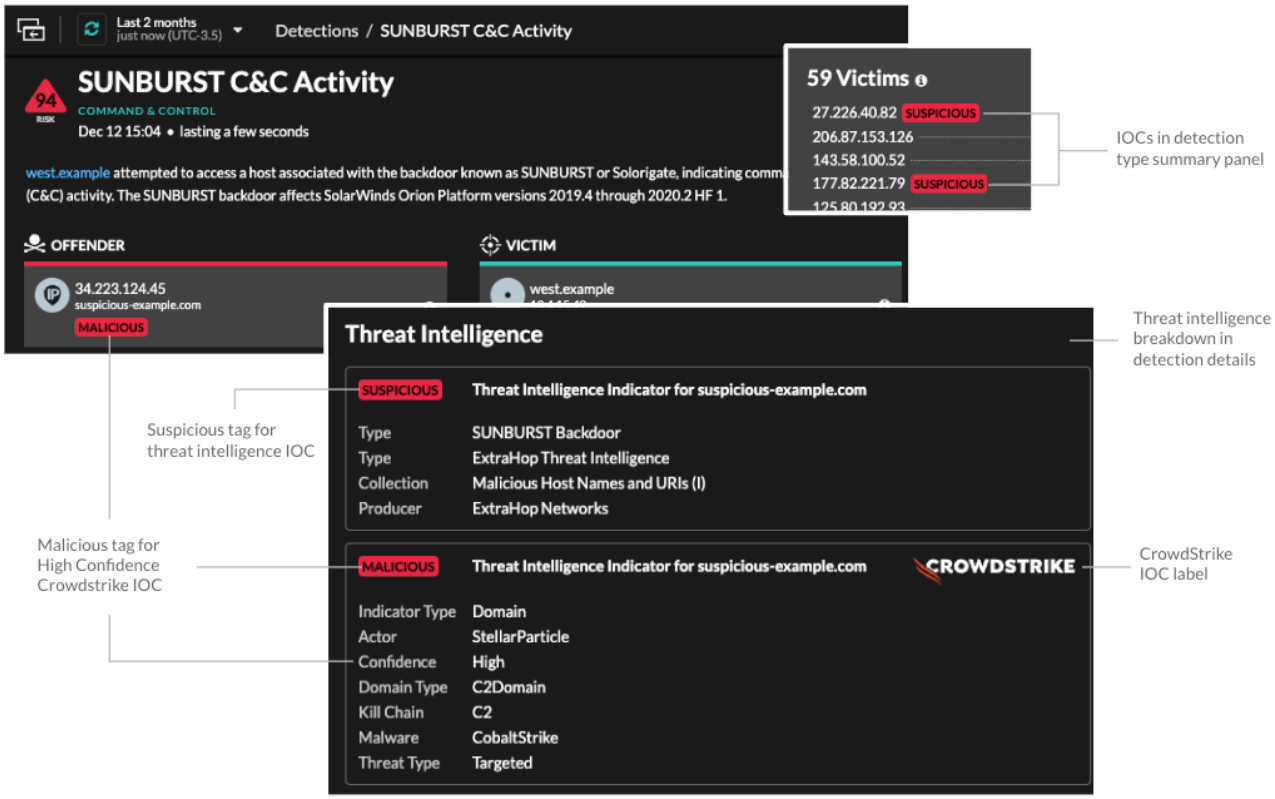
Bedrohungsinformationen

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

Video: Sehen Sie sich die entsprechende Schulung an: Bedrohungsinformationen

Bedrohungsinformationsdatensätze, sogenannte Bedrohungssammlungen, enthalten Listen verdächtiger Endpunkte, die als Indicators of Compromise (IOCs) bezeichnet werden.

Teilnehmer, die einer Bedrohungssammlung entsprechen, werden in Erkennungen, Erkennungszusammenfassungen, Systemdiagrammen und Aufzeichnungen als Verdächtig markiert. (Bei Crowdstrike-IOCs, bei denen das Konfidenzniveau hoch ist, wird der Teilnehmer als bösartig markiert.) Aufzeichnungen, die den verdächtigen Eintrag enthalten, sind mit einem Kamerasymbol gekennzeichnet. . In vielen Fällen führt eine Übereinstimmung des Indikators auch zu einer Erkennung der verdächtigen Verbindung.



Sammlungen von Bedrohungen

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

Integrierte Bedrohungssammlungen

Kuratierte Bedrohungssammlungen von ExtraHop und CrowdStrike Falcon sind standardmäßig in Ihrem ExtraHop-System verfügbar. Integrierte Sammlungen werden alle 6 Stunden aktualisiert. Du kannst integrierte Bedrohungssammlungen aktivieren oder deaktivieren von der Threat Intelligence-Seite.

STIX-Datei-Uploads

Wichtig: STIX-Datei-Uploads sind jetzt veraltet und werden voraussichtlich im März 2025 entfernt.

Kostenlose und kommerzielle Sammlungen, die von der Sicherheits-Community angeboten werden und in Structured Threat Information eXpression (STIX) als komprimierte TAR-Dateien wie .TGZ oder TAR.GZ formatiert sind, können manuell hochgeladen 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.

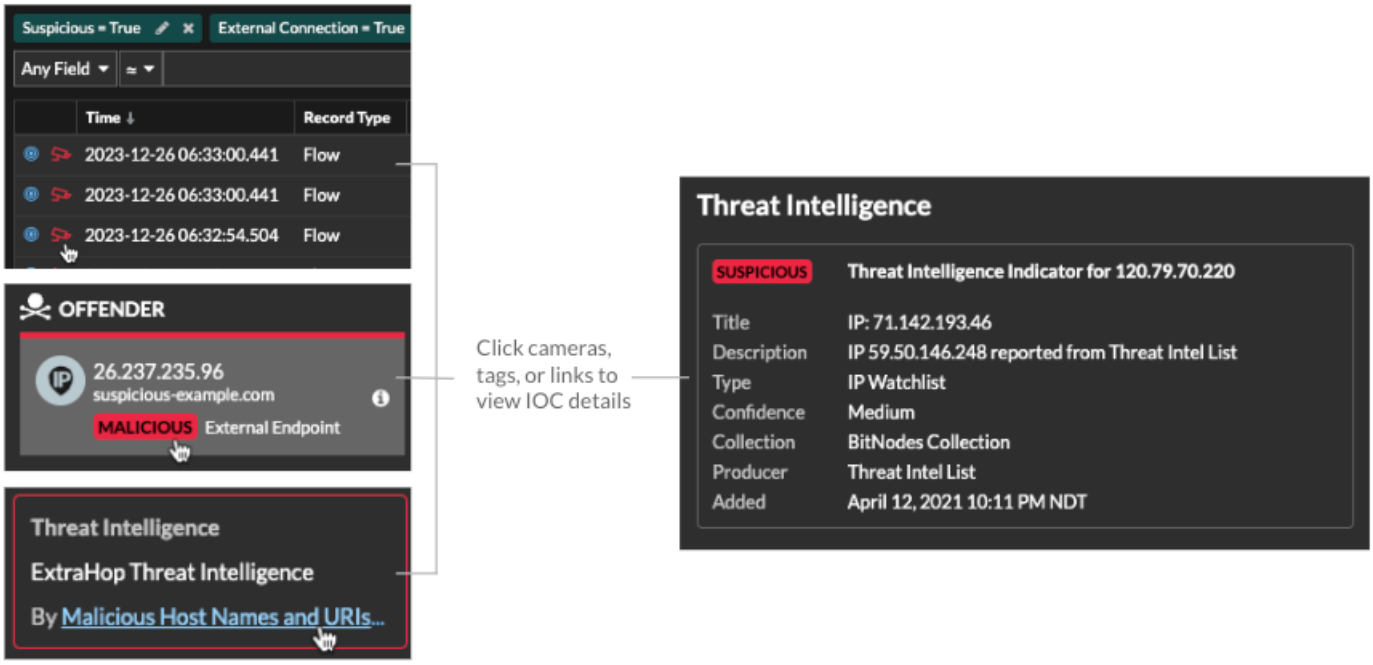
TAXII füttern

Bedrohungssammlungen können über das TAXII-Protokoll (Trusted Automated Exchange of Intelligence Information) von einer zuverlässigen Quelle in Ihre Umgebung übertragen werden. Ein TAXII-Feed kann einen konsistenten Strom aktualisierter Bedrohungsindikatoren liefern. Du kannst füge einen TAXII-Feed hinzu aus dem Bedrohungsinformationen Seite.

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 Ihnen, Ihre STIX-Datei-Uploads auf qualitativ hochwertige Bedrohungsdaten zu beschränken, die sich auf eine bestimmte Art von Eindringlingen konzentrieren, z. B. eine Sammlung für Malware und eine andere Sammlung für Botnets. Ebenso empfehlen wir, TAXII-Feeds auf zuverlässige und qualitativ hochwertige Quellen zu beschränken.

Untersuchung von Bedrohungen

Nachdem das RevealX-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 Bösartig 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.



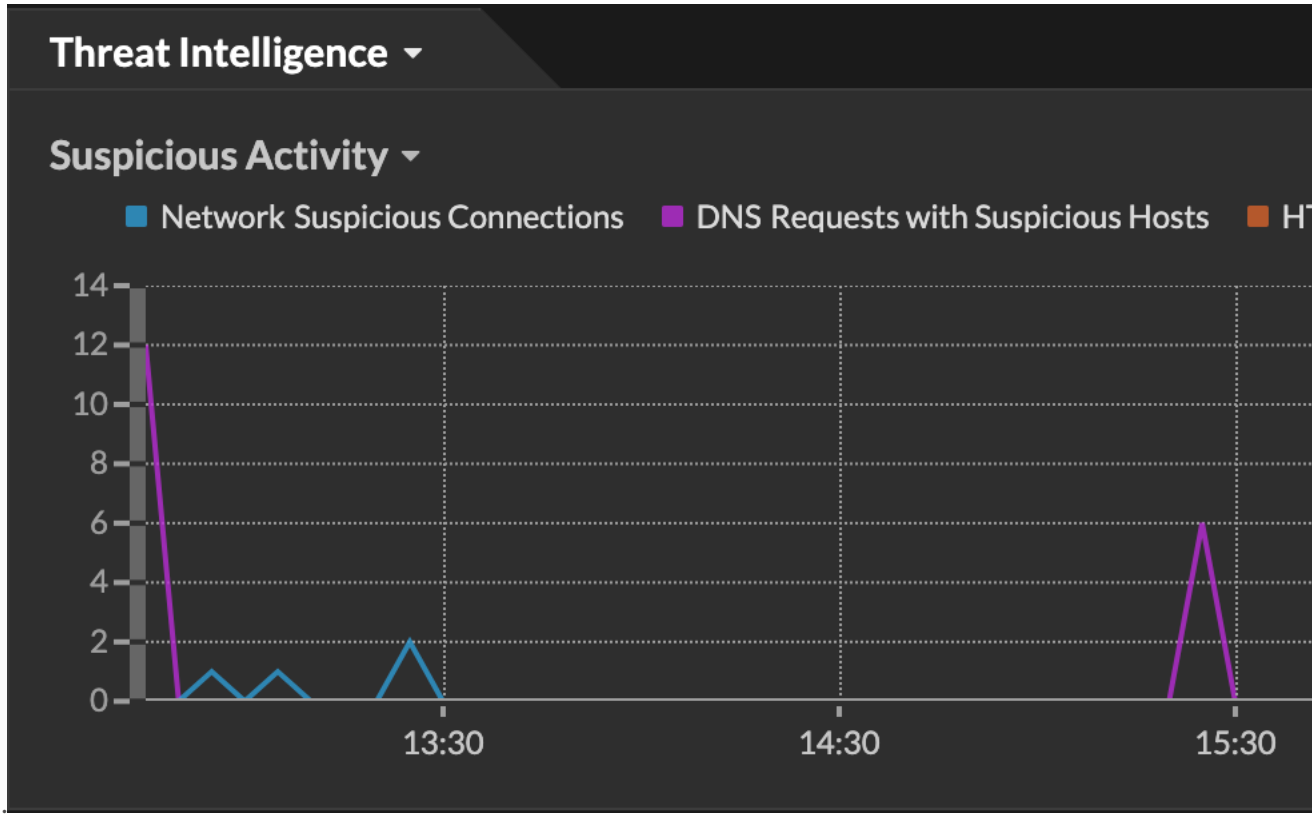
- Wenn die Bedrohungssammlung hinzugefügt oder aktualisiert wird, nachdem das System die verdächtige Aktivität beobachtet hat, werden Bedrohungsinformationen erst dann auf diese IP-Adresse, diesen Hostnamen oder URI angewendet, wenn die verdächtige Aktivität erneut auftritt.

- (Nur RevealX 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 RevealX-System, an denen die Bedrohungsindikatoren angezeigt werden, die in Ihren Bedrohungssammlungen gefunden wurden:

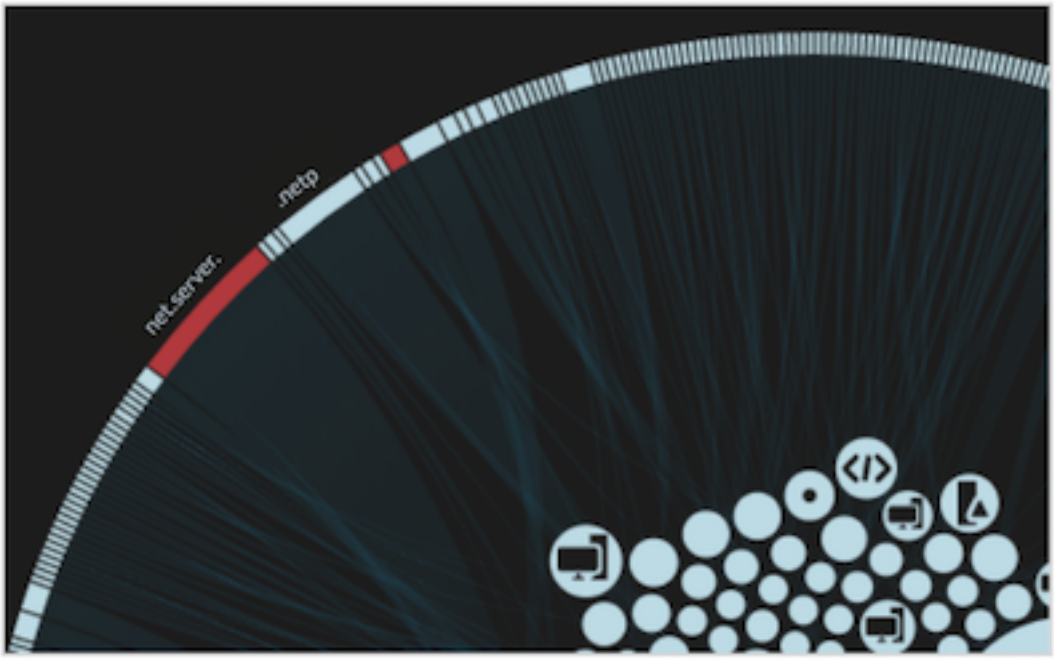
Dashboard zur Erhöhung der Sicherheit

Das Region „Bedrohungsinformationen“ enthält Kennzahlen 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 verwandte Transaktionen abfragen.



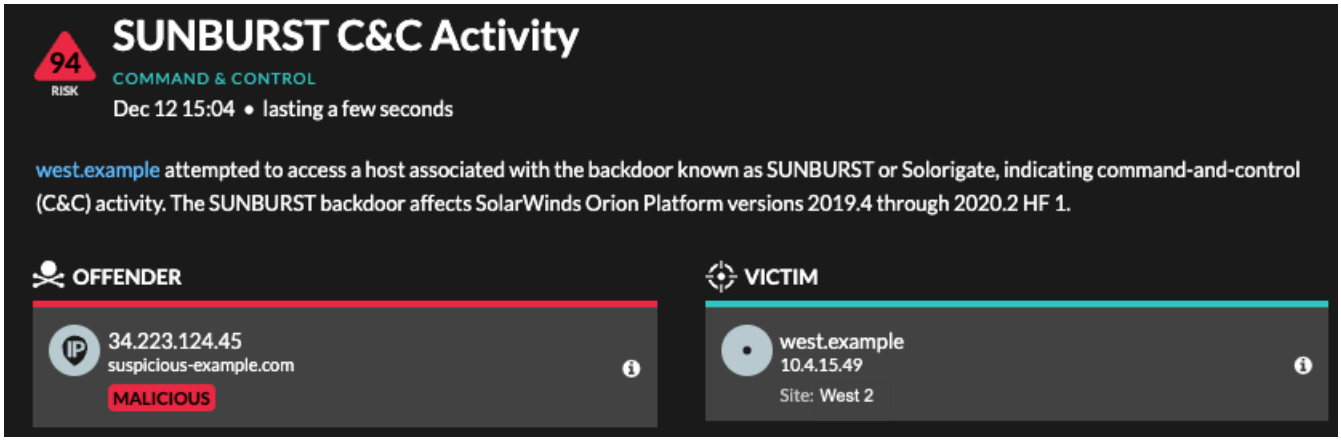
Perimeter im Überblick

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



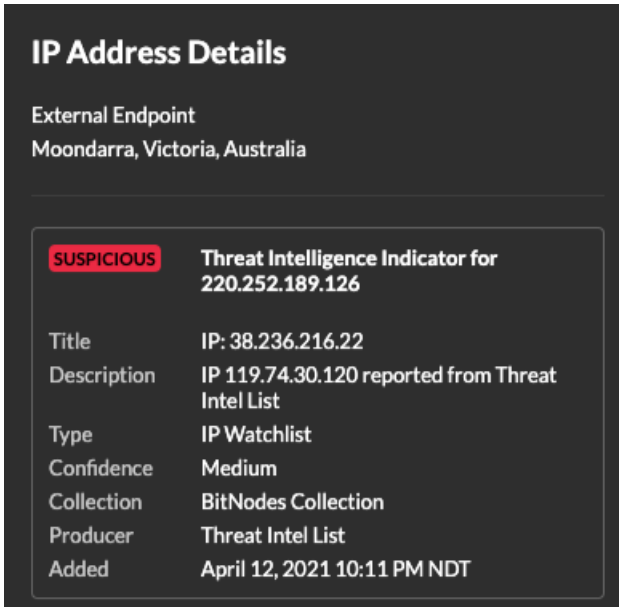
Erkennungen

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



Angaben zur IP-Adresse

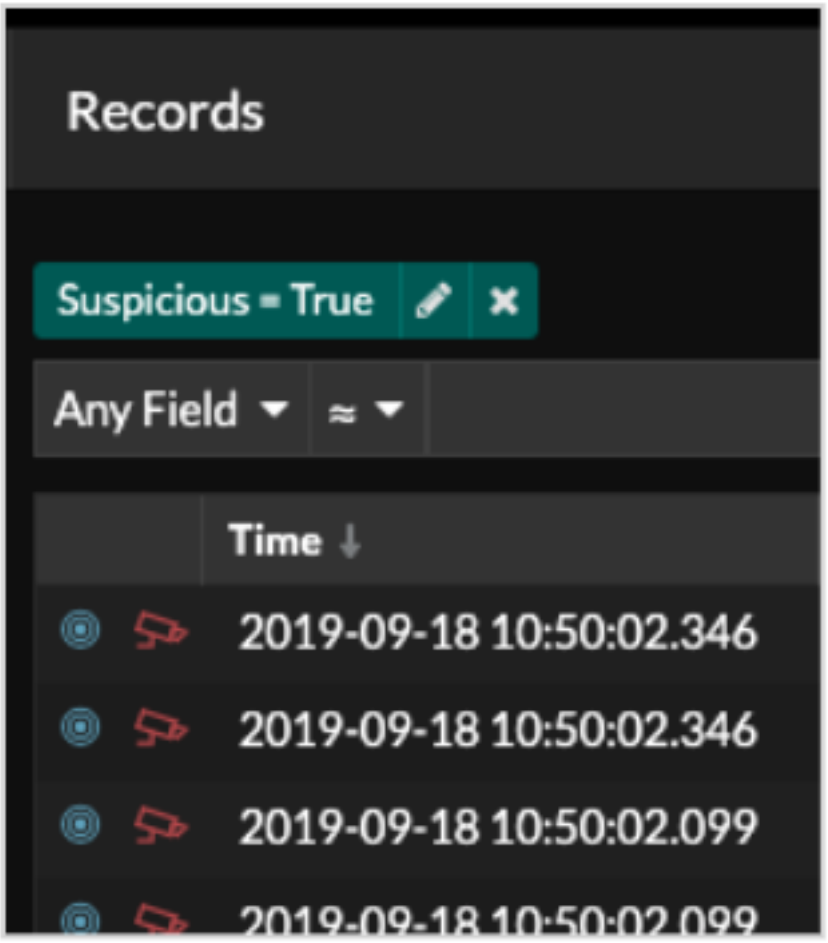
Auf den IP-Adressdetailseiten werden vollständige Bedrohungsinformationen zu IP-Adressindikatoren für kompromittierte IP-Adressen angezeigt.



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.



Bedrohungssammlungen verwalten

ExtraHop RevealX kann sich bewerben Bedrohungsinformationen zu Ihrer Netzwerkaktivität auf der Grundlage von Bedrohungssammlungen, die von Extrahop, CrowdStrike oder anderen kostenlosen und kommerziellen Quellen bereitgestellt werden.

Bevor Sie beginnen

- Erfahre mehr über Bedrohungsinformationen.
- Das musst du haben System- und Zugriffsadministrationsrechte auf jeder Konsole und jedem Sensor zur Verwaltung von Bedrohungssammlungen.
- Wenn Ihre ExtraHop-Bereitstellung eine Konsole umfasst, empfehlen wir Ihnen Transfermanagement Verbinden Sie alle angeschlossenen Sensoren mit der Konsole, um die integrierten Bedrohungssammlungen in Ihrem gesamten System zu aktivieren oder zu deaktivieren.

Integrierte Bedrohungssammlungen aktivieren oder deaktivieren

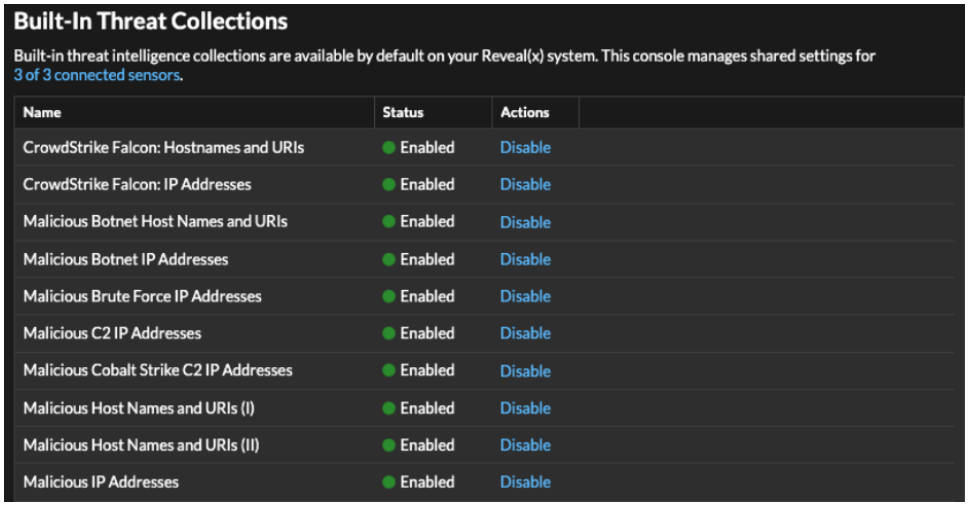
Integrierte Bedrohungssammlungen von ExtraHop und CrowdStrike identifizieren Anzeichen für eine Gefährdung im gesamten System.

Aktivierte Bedrohungssammlungen aktualisieren automatisch Systeme , die mit ExtraHop Cloud Services verbunden sind. Sie können die Konnektivität auf der ExtraHop Cloud-Dienste Seite in den Administrationseinstellungen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.

2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Bedrohungsinformationen**.
3. Klicken Sie in der Tabelle Integrierte Bedrohungssammlungen auf **Aktiviere** oder **Deaktiviert** in der Spalte Aktionen.

   Das System sucht automatisch alle 6 Stunden nach Updates für ExtraHop- und CrowdStrike-Bedrohungssammlungen.



Laden Sie eine Bedrohungssammlung hoch

Laden Sie Bedrohungssammlungen aus kostenlosen und kommerziellen Quellen hoch, um im gesamten ExtraHop-System Anzeichen für eine Gefährdung zu identifizieren. Da Bedrohungsdaten häufig (manchmal täglich) aktualisiert werden, müssen Sie möglicherweise eine Bedrohungssammlung mit den neuesten Daten aktualisieren. Wenn Sie eine Bedrohungssammlung mit neuen Daten aktualisieren, wird die Sammlung gelöscht und ersetzt und nicht an eine bestehende Sammlung angehängt.

Wichtig: STIX-Datei-Uploads sind jetzt veraltet und werden voraussichtlich im März 2025 entfernt.

Sie müssen Bedrohungssammlungen einzeln auf Ihre Konsole und auf alle angeschlossenen Sensoren hochladen.

Im Folgenden finden Sie einige Überlegungen zum Hochladen von Bedrohungssammlungen.

- Benutzerdefinierte Bedrohungssammlungen müssen in Structured Threat Information eXpression (STIX) als komprimierte TAR-Dateien wie .TGZ oder TAR.GZ formatiert werden. RevealX unterstützt derzeit Uploads der STIX-Dateiversionen 1.0 - 1.2.
- Sie können Bedrohungssammlungen direkt auf RevealX 360 hochladen, um sie selbst zu verwalten Sensoren. Wenden Sie sich an den ExtraHop-Support, um eine Bedrohungssammlung auf ExtraHop-Managed hochzuladen Sensoren.
- Die maximale Anzahl an Observables, die eine Bedrohungssammlung enthalten kann, hängt von Ihrem Sensorspeicher und Ihrer Lizenz ab. Um sicherzustellen, dass Uploads innerhalb der Grenzen Ihrer Sensoren und Ihrer Lizenz erfolgreich sind, empfehlen wir, Sammlungen in Dateien mit weniger als 3.000 Observables mit einer Gesamtgröße von weniger als 1 Million Observables aufzuteilen. Weitere Informationen zu Lizenz- und Plattformbeschränkungen für das Hochladen von Bedrohungssammlungen erhalten Sie von Ihrem ExtraHop-Vertreter.
- Du kannst Laden Sie STIX-Dateien über die REST-API hoch.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Bedrohungsinformationen**.
3. Klicken Sie **Benutzerdefinierte Sammlungen verwalten**.

4. Klicken Sie **Neue Kollektion hochladen**.
5. Geben Sie in das Feld Sammlungs-ID eine eindeutige Sammlungs-ID ein. Die ID darf nur alphanumerische Zeichen enthalten und Leerzeichen sind nicht zulässig.
6. Klicken Sie **Wählen Sie eine Datei** und wähle eine `.tgz` Datei, die eine STIX enthält.
7. Geben Sie einen Anzeigenamen in das Feld Anzeigename ein.
8. Klicken Sie **Sammlung hochladen**.
9. Wiederhole diese Schritte für alle Konsolen und jeder ist verbunden Sensor.

Einen TAXII-Feed hinzufügen

Bedrohungssammlungen können über das TAXII-Protokoll (Trusted Automated Exchange of Intelligence Information) in Ihre Umgebung übertragen werden.

TAXII-Feeds können in ihrer Qualität oder Relevanz für Ihre Umgebung variieren. Um die Genauigkeit zu gewährleisten und das Rauschen zu reduzieren, empfehlen wir, nur Feeds aus zuverlässigen Quellen hinzuzufügen, die qualitativ hochwertige Bedrohungsdaten liefern.

Bevor Sie beginnen

- TAXII-Feed-Indikatoren werden von ExtraHop Cloud Services verarbeitet. Das ExtraHop-System muss verbunden mit ExtraHop Cloud Services um einen TAXII-Feed hinzuzufügen.
- TAXII-Feeds können nur von Benutzern mit NDR-Modulzugriff und Verwaltung von einer Konsole aus verwaltet werden Privilegien.
- TAXII-Feed-Indikatoren werden nur an angeschlossene Sensoren geliefert, auf denen die Firmware-Versionen 9.6.0 und höher ausgeführt werden.
- RevealX unterstützt derzeit TAXII-Feeds für die TAXII-Versionen 2.0 - 2.1, die die STIX-Dateiversionen 2.0 - 2.1 enthalten

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Bedrohungsinformationen**.
3. Klicken Sie im TAXII-Feed-Bereich auf **TAXII Feed hinzufügen**.
4. Geben Sie im Feld Name einen eindeutigen Namen für den TAXII-Feed ein.
5. Geben Sie im Feld TAXII Server Discovery URL die Discovery-URL für Ihren TAXII-Feed-Anbieter ein.
6. Wählen Sie im Drop-down-Menü TAXII-Version die TAXII-Protokollversion des Feeds aus.
7. Wählen Sie einen Authentifizierungstyp aus.
   - Keine Authentifizierung
   - Grundlegende Authentifizierung

     Geben Sie den Benutzernamen und das Passwort für den Ziel-Feed ein.
8. Geben Sie ein Zertifikat für den Zielfeed an.
   - Kein Zertifikat
   - Basiszertifikat

     Kopieren Sie den Inhalt der PEM-kodierten Zertifikatskette und fügen Sie ihn in das Feld für das Basiszertifikat ein. Es muss ein gültiger Vertrauenspfad vom Zertifikat zu einem vertrauenswürdigen Stammverzeichnis existieren.
9. Klicken Sie **Verbindung testen** um URL -, Authentifizierung- und Zertifikatseinstellungen zu bestätigen.
10. Klicken Sie **Weiter**.
11. Wählen Sie aus dem Drop-down-Menü Sammlungen zur Anreicherung die Bedrohungssammlungen aus , die zu einem verdächtigen Tag führen, wenn ein Indikator übereinstimmt.
12. Wählen Sie aus dem Drop-down-Menü Sammlungen für Erkennungserstellung die Bedrohungssammlungen aus, die zu einer Erkennung führen, wenn ein Indikator zutrifft .

Hinweis Sie können eine Sammlung sowohl der Anreicherung als auch der Erkennungserstellung zuweisen. Wenn eine Sammlung nicht der Anreicherungsoption zugewiesen ist, wird die Sammlung während der Umfrage nicht aktualisiert und Indikatoren aus der Sammlung werden nicht in Ihrem System angezeigt.

13. Geben Sie im Feld Maximaler Lookback die Anzahl der Tage in der Vergangenheit ein, an denen Sie Indikatoren aus der Bedrohungssammlung akzeptieren möchten.

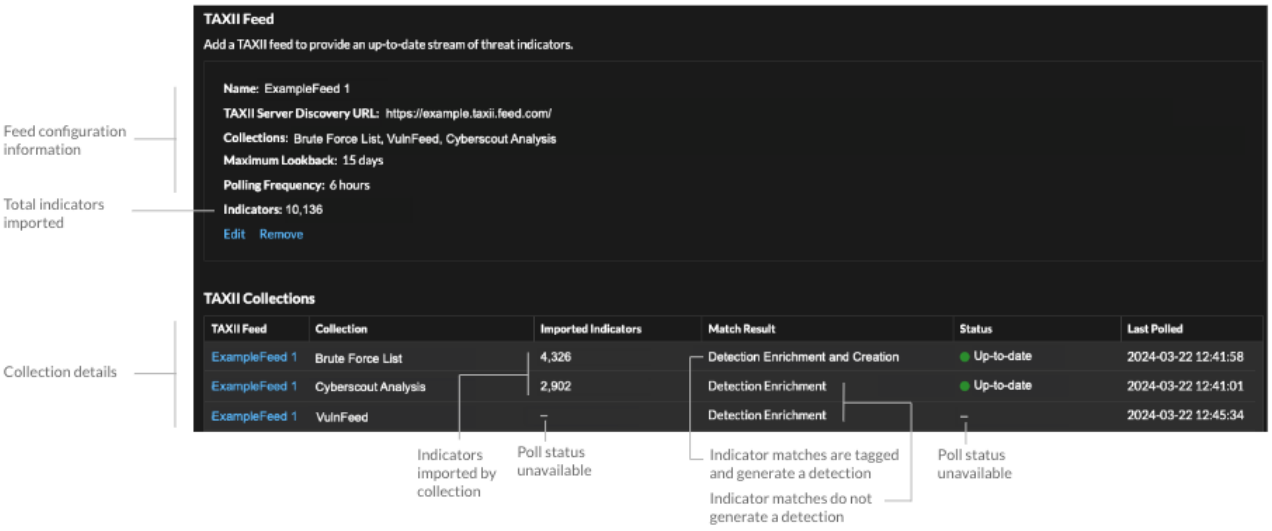
    Sie können diesen Wert auf eine Zahl zwischen 1 und 15 Tagen festlegen. Der Feed akzeptiert nur Indikatoren, die während dieser Lookback-Periode erstellt wurden.

14. Geben Sie im Feld Abfragehäufigkeit die Anzahl der Stunden zwischen der Abfrage des TAXII-Feeds nach Updates zur Bedrohungssammlung ein.

    Sie können diesen Wert auf eine Zahl zwischen 1 und 24 Stunden festlegen.

15. Klicken Sie **Speichern**.

Informationen zur TAXII-Feed-Konfiguration werden im Abschnitt TAXII-Feed der Threat Intelligence-Seite angezeigt, einschließlich des angegebenen Lookback-Zeitraums, der Abfragehäufigkeit und der Gesamtzahl der im Feed enthaltenen Indikatoren. Die Tabelle TAXII Collections enthält Details zu den einzelnen Sammlungen im Feed.



Hier sind einige Überlegungen zu TAXII-Feeds:

- Die Zeit, die für die Abfrage der TAXII-Feed- und Prozessindikatoren benötigt wird, basiert auf der Anzahl der Indikatoren im Feed. Als Referenz: Die Abfrage eines Feeds mit 500.000 Indikatoren im angegebenen Lookback-Zeitraum kann eine Stunde oder länger dauern.
- Indikatortypen, die vom ExtraHop-System nicht erkannt werden, gutartige Endpunktindikatoren und als gesperrt markierte Indikatoren werden bei der Umfrage aus dem Feed entfernt.
- In der TAXII-Sammeltabelle wird der Abholstatus mit einem Bindestrich (-) angezeigt, bis die Abholung auf dem neuesten Stand ist. Wenn dieser Status nicht auf aktuell gesetzt wird, testen Sie Ihre Verbindung zum TAXII-Server und überprüfen Sie dann Ihren TAXII-Feed-Anbieter, um sicherzustellen, dass die Sammlung noch im Feed vorhanden ist, dass Ihre Anmeldedaten Zugriff auf die Sammlung gewähren und dass Sie die vom Anbieter festgelegten Abfragelimits nicht überschritten haben. Ein teilweiser Aktualisierungsstatus wird angezeigt, wenn eine Sammlung während der Abfrage nicht vollständig aktualisiert wird. Teilaktualisierungen können erfolgen, wenn die Abfrage unerwartet unterbrochen wurde oder wenn ein Ratenlimit des Anbieters erreicht wurde.

Warnmeldungen

Mithilfe von Warnmeldungen können Sie leicht erkennen, wenn wichtige Ereignisse in Ihrem Netzwerk auftreten oder ob Bereiche sich nicht wie erwartet verhalten, z. B. Verstöße gegen den Softwarelizenzvertrag (SLA) oder langsame Datenbankreaktionszeiten.

Video: Sehen Sie sich die entsprechende Schulung an: Warnmeldungen

Konfigurierte Warnbedingungen bestimmen, wann eine Alarm generiert wird. Warnbedingungen sind eine Kombination aus Einstellungen, z. B. einem Zeitintervall, einem Metrikwert und Metrik Berechnungen, die für zugewiesene Datenquellen durchgeführt werden. Schwellenwert- oder Trendwarnungen basieren auf dem Wert der überwachten Metrik.

Benachrichtigungen konfigurieren

Konfigurieren Sie eine Alarm, um bestimmte Bedingungen zu überwachen und Warnmeldungen zu generieren, wenn diese Bedingungen in den zugewiesenen Datenquellen erfüllt sind.

Schwellenwertwarnungen

Schwellenwertbasierte Warnmeldungen werden generiert, wenn eine überwachte Metrik innerhalb eines bestimmten Zeitintervalls einen definierten Wert überschreitet.

Erstellen Sie eine Schwellenwarnung, um Ereignisse wie Fehlerraten, die einen angenehmen Prozentsatz überschreiten, oder Verstöße gegen SLAs zu überwachen. Erfahren Sie, wie Sie einen Schwellenwertalarm konfigurieren.

Trendwarnungen

Trendbasierte Warnmeldungen werden generiert, wenn eine überwachte Metrik von den vom System beobachteten normalen Trends abweicht. Trendwarnungen sind komplexer als Schwellenwertwarnungen und eignen sich zur Überwachung von Metriktrends wie ungewöhnlich hohen Round-Trip-Zeiten oder ungewöhnlich geringem Datenverkehr auf Speicherservern, was auf ein fehlgeschlagenes Backup hindeuten könnte.

Erstellen Sie eine Trendwarnung, um zu überwachen, wenn eine Metrik vom normalen Verhalten abweicht und wo Schwellenwerte schwer zu definieren sind. Erfahren Sie, wie Sie eine Trendwarnung konfigurieren.

Darüber hinaus können Sie eine Alarm mit den folgenden Optionen konfigurieren:

- Legen Sie ein Ausschlussintervall fest um Warnmeldungen während bestimmter Zeiträume zu unterdrücken, z. B. während eines Wartungsfensters.
- Benachrichtigungen konfigurieren um eine E-Mail zu erhalten, wenn eine Alarm generiert wird.

Benachrichtigungen anzeigen

Auf der Seite Alerts wird eine Liste aller Alerts angezeigt, die während des angegebenen Zeitintervalls generiert wurden.

Wählen Sie einen der Filter oben auf der Seite aus, um die Liste anzupassen, oder klicken Sie auf einen Warnungsnamen , um Details zu der Alarm anzuzeigen.

Art der Quelle

Filtern Sie Benachrichtigungen, die Anwendungen oder Geräten zugewiesen sind.

Schweregrad

Filtern Sie Warnmeldungen nach Schweregrad.

Art der Warnung

Filtern Sie nach Schwellenwert-, Trend- oder Erkennungswarnungen.

Wichtig: Erkennungswarnungen sind veraltet und werden in einer zukünftigen Freigabe entfernt. Um Benachrichtigungen über Entdeckungen zu erhalten, eine Benachrichtigungsregel erstellen.

Seite

Filtern Sie nach verbundenen Websites. (Nur erhältlich bei einem Konsole.)

Auf der Seite „Benachrichtigungen“ werden die folgenden Informationen zu jeder Alarm angezeigt:

Schweregrad

Ein farbcodierter Indikator für den Schweregrad der Alarm. Sie können die folgenden Schweregrad festlegen: Notfall, Warnung, Kritisch, Fehler, Warnung, Hinweis, Info und Debug.

Name der Warnung

Der Name der konfigurierten Alarm. Klicken Sie auf den Namen der Alarm, um die Warnungsdetails anzuzeigen.

Quelle

Der Name der Quelle, in der die Warnbedingungen aufgetreten sind. Klicken Sie auf den Quellnamen, um zur Seite mit der Quellübersicht zu gelangen.

Zeit

Der Zeitpunkt, zu dem die Warnbedingungen zuletzt eingetreten sind.

Art der Warnung

Zeigt einen Trend- oder Schwellenwertalarm an.

Weitere Informationen zum Anzeigen von Benachrichtigungen finden Sie in den folgenden Themen

- Fügen Sie einem Dashboard ein Warnmeldungs-Widget hinzu
- Häufig gestellte Fragen zu Warnungen

Einen Schwellenwertalarm konfigurieren

Konfigurieren Sie eine Schwellenwertalarm, um zu überwachen, wenn eine bestimmte Metrik eine definierte Grenze überschreitet. Sie können beispielsweise eine Alarm generieren, wenn ein HTTP 500-Statuscode innerhalb eines Zeitraums von zehn Minuten mehr als 100 Mal beobachtet wird.

Bevor Sie beginnen
Du musst haben volle Schreibrechte oder höher.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Alerts**.
3. klicken **Erstellen**.
4. Geben Sie einen eindeutigen Namen für die Alert-Konfiguration in der **Name** Feld.
5. In der **Beschreibung** Feld, fügen Sie Informationen zur Alarm hinzu.

   Hinweis: Warnungsbeschreibungen unterstützen Markdown, eine einfache Formatierungssyntax, die Klartext in HTML konvertiert. Weitere Informationen finden Sie in der Häufig gestellte Fragen zu Warnungen.
6. In der **Art der Warnung** Abschnitt, klicken **Schwellenwertalarm**.
7. In der **Zugewiesene Quellen** Feld, geben Sie den Namen eines Gerät, einer Gerätegruppe oder einer Anwendung ein und wählen Sie dann aus den Suchergebnissen aus.

Um nach einer Standort, einem Flussnetz oder einer Flussschnittstelle zu suchen, wählen Sie diesen Quelltyp aus dem Drop-down-Menü oben in den Suchergebnissen aus.

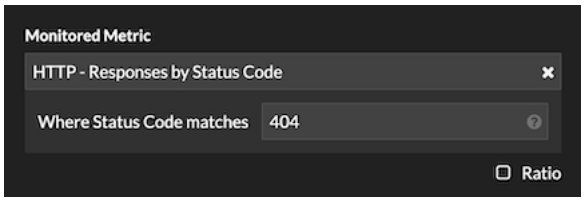
8. Optional: klicken **Quelle hinzufügen** um die Alarm mehreren Quellen zuzuweisen. Mehrere Quellen müssen vom gleichen Typ sein, z. B. nur Geräte und Gerätegruppen oder nur Anwendungen.

   Hinweis Weisen Sie einer Gerätegruppe eine Alarm zu, um Zuweisungen an mehrere Geräte effizient zu verwalten.

9. In der **Überwachte Metrik** Feld, geben Sie den Namen einer Metrik ein und wählen Sie dann aus den Suchergebnissen aus.

   Die Metrik muss mit den zugewiesenen Quellen kompatibel sein. Wenn Sie die Alarm beispielsweise einer Anwendung zuweisen, können Sie keine Gerätemetrik auswählen.

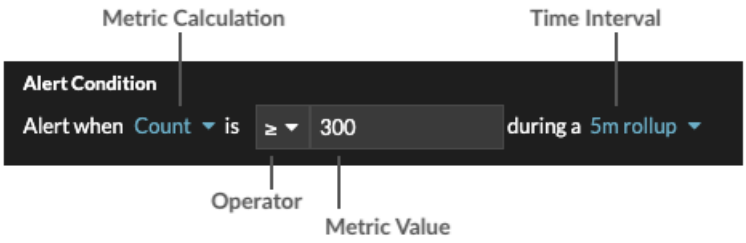
   Hinweis Wenn Sie eine auswählen Detailmetrik, Sie können einen Schlüsselwert angeben. Sie könnten beispielsweise HTTP — Antworten nach Statuscode auswählen und dann 404 als Schlüsselwert angeben. Eine Alarm wird nur generiert, wenn HTTP-Antworten mit 404-Statuscodes auftreten.



10. Optional: Um den Wert einer Metrik geteilt durch eine sekundäre Metrik zu überwachen, klicken Sie auf **Verhältnis** und wählen Sie dann eine sekundäre Metrik aus.

    Sie können beispielsweise den Prozentsatz der HTTP-Fehler überwachen, die bei Antworten auftreten, indem Sie HTTP-Antwortfehler durch HTTP-Antworten dividieren.

11. Geben Sie im Abschnitt Warnbedingung die Bedingungen für die Generierung einer Warnung an.



    a) Wählen Sie eine Metrikberechnung aus, um anzugeben, wie der Metrikwert innerhalb des Zeitintervalls berechnet werden soll. Die verfügbaren Optionen hängen vom Datentyp ab.

Zählen	• Zählen • Rate pro Sekunde • Rate pro Minute

	• Preis pro Stunde
Datensatz	• Minimum • 25. Perzentil • Median • 75. Perzentil • Maximal
Probenset	• Gemein • +1 bis +7 Standardabweichungen • -1 bis -7 Standardabweichungen
Maximum, Snapshot	Keine Messung; der Prüfer vergleicht den tatsächlichen Metrik Wert.

b) Wählen Sie einen Operator aus, um anzugeben, wie die Metrikberechnung mit dem Metrikwert verglichen werden soll.
c) Geben Sie den Metrikwert an, der mit der Metrikberechnung verglichen werden soll.
d) Wählen Sie das Zeitintervall aus, in dem der Metrikwert beobachtet und die Metrikdaten aggregiert oder zusammengefasst werden. Sie können ein Zeitintervall von 30 Sekunden bis zu 30 Minuten wählen.

Um beispielsweise eine Alarm zu generieren, wenn innerhalb von 5 Minuten mehr als 300 HTTP-Antwortfehler auftreten, geben Sie die folgenden Bedingungen an:

- Metrische Berechnung: Anzahl
- Betreiber: >
- Metrischer Wert: 300
- Zeitintervall: 5 m Rollup

12. Optional: Im Bereich Benachrichtigungen eine E-Mail-Benachrichtigung zu einer Alarm hinzufügen um E-Mails oder SNMP-Traps zu erhalten, wenn eine Alarm generiert wird.
13. Klicken Sie im Abschnitt Status auf eine Option, um die Alarm zu aktivieren oder zu deaktivieren.
14. Optional: Ein Ausschlussintervall hinzufügen um Warnmeldungen zu bestimmten Zeiten zu unterdrücken.
15. klicken **Speichern**.

Konfigurieren Sie eine Trendwarnung

Konfigurieren Sie eine Trendwarnung, um zu überwachen, wenn eine bestimmte Metrik von normalen Trends abweicht. Trendwarnungen sind nützlich, um Metriktrends wie ungewöhnlich hohe Round-Trip-Zeiten oder ungewöhnlich wenig Traffic auf Speicherservern zu überwachen, was auf ein fehlgeschlagenes Backup hindeuten könnte. Sie können beispielsweise eine Trendwarnung konfigurieren, die Warnmeldungen generiert, wenn ein Anstieg (75. Perzentil) der HTTP-Webserver-Verarbeitungszeit länger als 10 Minuten dauert und wenn der Metrikwert der Verarbeitungszeit um 100% über dem Trend liegt.

Bevor Sie beginnen
Du musst volle Schreibrechte oder höher.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Warnmeldungen**.
3. klicken **Erstellen**.

4. Geben Sie einen eindeutigen Namen für die Alert-Konfiguration in der **Name** Feld.
5. In der **Beschreibung** Feld, fügen Sie Informationen zur Alarm hinzu.

   Hinweis Warnungsbeschreibungen unterstützen Markdown, eine einfache Formatierungssyntax, die Klartext in HTML konvertiert. Weitere Informationen finden Sie in der Häufig gestellte Fragen zu Warnungen.
6. In der **Art der Warnung** Abschnitt, klicken **Trendwarnung**.
7. In der **Zugewiesene Quellen** Feld, geben Sie den Namen eines Gerät, einer Gerätegruppe oder einer Anwendung ein und wählen Sie dann aus den Suchergebnissen aus.

   Um nach einer Standort, einem Flussnetz oder einer Flussschnittstelle zu suchen, wählen Sie diesen Quelltyp aus dem Drop-down-Menü oben in den Suchergebnissen aus.
8. Optional: klicken **Quelle hinzufügen** um die Alarm mehreren Quellen zuzuweisen. Mehrere Quellen müssen vom gleichen Typ sein, z. B. nur Geräte und Gerätegruppen oder nur Anwendungen.

   Hinweis Weisen Sie einer Gerätegruppe eine Alarm zu, um Zuweisungen an mehrere Geräte effizient zu verwalten.
9. In der **Überwachte Metrik** Feld, geben Sie den Namen einer Metrik ein und wählen Sie dann aus den Suchergebnissen aus.

   Die Metrik muss mit den zugewiesenen Quellen kompatibel sein. Wenn Sie die Alarm beispielsweise einer Anwendung zuweisen, können Sie keine Gerätemetrik auswählen.

   Wenn Sie eine Datensatzmetrik wie HTTP Server Processing Time auswählen, müssen Sie eine der folgenden Datenaggregationsmethoden angeben:

Zusammenführen	Aggregieren Sie alle Metrik Datensatzwerte und wenden Sie das Trendgewichtungsmodell auf eine Obermenge von Daten an. Beispielsweise enthält ein aggregiertes 30-Sekunden-Rollup oder ein Metrik Zyklus einen einzelnen Datensatz für jedes 30-Sekunden-Intervall. Daher umfasst ein 30-minütiges Intervall 60 Datensätze.
Gemein	Aggregieren Sie den Mittelwert jedes Metrik Datensatzes.
Perzentil	Aggregieren Sie das Perzentil jedes Metrik-Datasets auf der Grundlage des Werts, den Sie angeben für **Perzentil**.
Absolute Standardabweichung	Aggregieren Sie den Metrik Datensatz auf seine Standardabweichung als Konstante.
Relative Standardabweichung	Aggregieren Sie den Metrik Datensatz auf seine Standardabweichung relativ zum Mittelwert.

10. Optional: Um den Wert einer Metrik geteilt durch eine sekundäre Metrik zu überwachen, klicken Sie auf **Verhältnis** und wählen Sie dann eine sekundäre Metrik aus.

    Teilen Sie beispielsweise HTTP-Antwortfehler durch HTTP-Antworten auf, um Trends beim Prozentsatz der HTTP-Fehler zu beobachten.

11. Geben Sie im Abschnitt Trenddefinition an, wie der Trend berechnet wird:
    a) Wählen Sie aus der Drop-down-Liste Trendgewichtungsmodell ein Modell aus. Das Gewichtungsmodell aggregiert historische Metrikwerte, um einen Trend zu berechnen.

Gemein	Berechnen Sie einen Trend, indem Sie den Durchschnitt aller Metrik Werte gleichmäßig gewichtet bilden.
Minimaler Wert	Berechnet einen Trend anhand der Kennzahlen mit dem niedrigsten Wert.
Medianwert	Berechnet einen Trend aus den mittleren historischen Metrikwerten.
Maximaler Wert	Berechnen Sie einen Trend anhand der wertvollsten Kennzahlen.
Perzentil	Berechnen Sie anhand des Perzentils jeder Metrik einen Trend auf der Grundlage des Werts, den Sie angeben für **Perzentilwert**.
Absolute Standardabweichung	Berechnen Sie einen Trend, indem Sie die Standardabweichung als konstanten Wert mit dem aktuellen Trend vergleichen. Aus dem **Art der Abweichung** Drop-down-Liste, wählen Sie einen Typ aus: • Stichprobenbasiert • Bevölkerungsbezogen
Relative Standardabweichung	Berechnen Sie einen Trend, indem Sie die Standardabweichung als Wert relativ zum Mittelwert des aktuellen Trends vergleichen. Aus dem **Art der Abweichung** Drop-down-Liste, wählen Sie einen Typ aus: • Stichprobenbasiert • Bevölkerungsbezogen
Lineare Regression	Berechnet einen linearen Trend auf der Grundlage früherer Metrikwerte.
Polynomielle Regression 2. Grades	Berechnen Sie einen quadratischen Trend, indem Sie eine Kurve mit der folgenden Gleichung projizieren: `y=ax^2+bx+c`
Einzelner exponentieller Mittelwert	Berechnet einen Trend, indem der Durchschnitt gewichtsbasierter Metrikwerte gebildet wird. In der **Aktuelle Berechnung des Wertgewichts** Feld, geben Sie eine große Zahl an, um den neuesten Metrik Werten mehr Gewicht zu

	geben, oder geben Sie eine kleine Zahl an, um den ältesten Metrik Werten mehr Gewicht zu geben.
Doppelter exponentieller Mittelwert	Berechnet einen Trend, indem der Durchschnitt gewichtsbasierter Metrikwerte gebildet wird. In der **Aktuelle Berechnung des Wertgewichts** Feld, geben Sie eine große Zahl an, um den neuesten Metrik Werten mehr Gewicht zu geben, oder geben Sie eine kleine Zahl an, um den ältesten Metrik Werten mehr Gewicht zu geben. Beachten Sie, dass Berechnungen mit doppelten exponentiellen Mittelwerten für die Vorhersage des Trendverlaufs genauer sind.
Statischer Wert	Berechnet einen Trend auf der Grundlage eines statischen Metrikwerts im Vergleich zu einer Metrikberechnung. Geben Sie einen statischen Wert an und wählen Sie eine Metrikberechnung aus: • Preis pro Stunde • Rate pro Minute • Zählen Dieses Modell ist nützlich, um konstante Linien für SLAs zu zeichnen.
Trimean	Berechnet einen Trend auf der Grundlage des gewichteten Durchschnitts der Metrikwerte 25., 50. und 75. Perzentil.
Time Delta	Berechnen Sie einen Trend, indem Sie aktuelle Metrikwerte mit historischen Daten vergleichen.
Gewonnener Mittelwert	Berechnen Sie einen Trend, indem Sie Metrikwerte mit bestimmten niedrigen und hohen Prozentwerten abrufen und sie durch die niedrigsten und höchsten verbleibenden Werte ersetzen. Metrikwerte über dem 90. Perzentil werden beispielsweise zu demselben Wert wie dem 90. Perzentil, und Metrikwerte unter dem 10. Perzentil werden zu demselben Wert wie dem 10. Perzentil. Aus dem **Winsorisierung** Drop-down-Liste, wählen Sie ein Prozentpaar aus: • 5/95. Perzentil • 10/90. Perzentil • 25/75. Perzentil

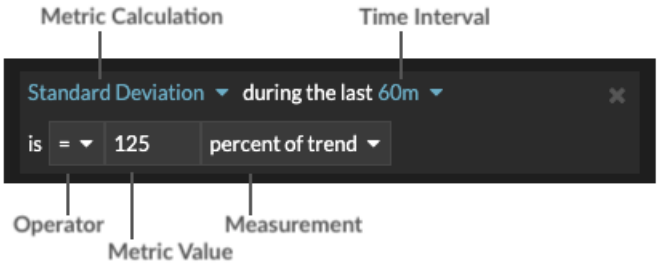
b) Aus dem **Trendfenster** Dropdownliste, wählen Sie ein Berechnungsfenster aus.

Gleiche Stunde der Woche	Berechnen Sie einen Trend, indem Sie die Kennzahlen vergleichen, die jede Woche aus demselben einstündigen Fenster stammen.
Gleiche Stunde des Tages	Berechnen Sie einen Trend, indem Sie die Messwerte vergleichen, die jeden Tag aus demselben einstündigen Fenster stammen.
Gleitender Minutendurchschnitt	Berechnen Sie einen Trend, indem Sie den Durchschnitt der Metrikwerte ermitteln, die jede Minute innerhalb eines bestimmten Zeitraums ab dem aktuellen Zeitpunkt erfasst wurden.
Gleitender Stundendurchschnitt	Berechnen Sie einen Trend, indem Sie den Durchschnitt der Metrikwerte ermitteln, die jede Stunde innerhalb eines bestimmten Zeitraums ab dem aktuellen Zeitpunkt erfasst wurden.

c) In der **Rückblick auf den Trend** Feld, geben Sie das Zeitfenster der historischen Daten an, die das ExtraHop-System zur Berechnung des Trends überprüft. Gültige Lookback-Werte werden durch das ausgewählte Trendfenster bestimmt.

- Geben Sie einen Wert zwischen 1 und 45 Tagen an, wenn Gleiche Stunde des Tages ausgewählt ist.
- Geben Sie einen Wert zwischen 1 und 15 Wochen an, wenn Gleiche Stunde der Woche ausgewählt ist.
- Geben Sie einen Wert zwischen 1 und 48 Stunden an, wenn der gleitende Stundendurchschnitt ausgewählt ist.
- Geben Sie einen Wert zwischen 1 und 999 Minuten an, wenn der gleitende Minutendurchschnitt ausgewählt ist.

12. Geben Sie im Abschnitt Warnbedingung die Bedingungen für die Generierung einer Warnung an.



a) Aus dem **Alle abgleichen** Wählen Sie in der Dropdownliste eine Option aus, um eine Alarm zu generieren, wenn alle, eine oder keine der Warnungsbedingungen erfüllt sind.

b) Wählen Sie eine Metrikberechnung aus, um anzugeben, wie der Metrikwert innerhalb des Zeitintervalls berechnet werden soll.

Gemein	Berechnet den Mittelwert der Metrik.
Median	Berechnet den 50. Perzentilwert der Metrik.
25. Perzentil	Berechnet den 25. Perzentilwert der Metrik.
75. Perzentil	Berechnet den 75. Perzentilwert der Metrik.

Standardabweichung	Berechnet die Standardabweichung im Vergleich zur Metrik. Die Standardabweichung ist das Ausmaß der Abweichung vom Trend.
Zählen	Geben Sie die absolute Summe der Metrik an. Es ist keine Messung erforderlich.

c) Wählen Sie das Zeitintervall aus, in dem der Metrikwert beobachtet wird. Sie können ein Intervall von 30 Sekunden bis zu 30 Minuten wählen.
d) Wählen Sie einen Operator aus, um anzugeben, wie die Metrikberechnung mit dem Metrikwert verglichen wird.
e) Geben Sie den Metrikwert an, der mit der Metrikberechnung verglichen werden soll.
f) Geben Sie an, wie der Metrik Wert gemessen werden soll.

- Prozent des Trends
- Absolut
- Pro Sekunde
- Pro Minute

g) Optional: klicken **Bedingung hinzufügen** um weitere Bedingungskriterien hinzuzufügen, oder klicken Sie auf **Bedingungsgruppe hinzufügen** zu den Kriterien für den besten Zustand.

Um beispielsweise eine Alarm zu generieren, wenn die Standardabweichung der beobachteten Metrik über ein 60-Minuten-Intervall einem Trendwert von 25% entspricht, geben Sie die folgenden Bedingungen an:

- Metrische Berechnung: Standardabweichung
- Zeitintervall: 60 m
- Betreiber: =
- Metrischer Wert: 125
- Messung: Prozent des Trends

13. Optional: Im Bereich Benachrichtigungen eine E-Mail-Benachrichtigung zu einer Alarm hinzufügen um E-Mails oder SNMP-Traps zu erhalten, wenn eine Alarm generiert wird.
14. Klicken Sie im Abschnitt Status auf eine Option, um die Alarm zu aktivieren oder zu deaktivieren.
15. Optional: Ein Ausschlussintervall hinzufügen um Warnmeldungen zu bestimmten Zeiten zu unterdrücken.
16. klicken **Speichern**.

Hinzufügen einer Benachrichtigung zu einer Warnungskonfiguration

Konfigurieren Sie eine Alarm so, dass eine Benachrichtigung gesendet wird, wenn die Warnbedingung erfüllt ist.

Eine Alarm hinzufügen (RevealX Enterprise)

Sie können einer Warnungskonfiguration eine Benachrichtigung hinzufügen, die eine E-Mail an eine angegebene E-Mail-Adresse oder E-Mail-Gruppe sendet, wenn die Alarm auftritt. Die E-Mail enthält Warnungsdetails und einen Link zum Anzeigen der Warnquelle. Sie können auch Benachrichtigungen an einen SNMP-Listener senden.

Bevor Sie beginnen

- Das musst du haben volle Schreibrechte oder höher.
- Ihr ExtraHop-System muss konfiguriert, um Benachrichtigungen zu senden.
- Wenn Sie möchten, dass eine Alarm an mehrere E-Mail-Adressen gesendet wird, eine E-Mail-Gruppe konfigurieren.
- Wenn Sie Benachrichtigungen über SNMP senden möchten, den SNMP-Listener konfigurieren.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Warnmeldungen**.
3. Klicken Sie in der Tabelle Warnungen auf die gewünschte Alarm.
4. Geben Sie im Abschnitt Benachrichtigungen die E-Mail-Gruppen und Adressen an, die beim Auftreten der Alarm benachrichtigt werden sollen.
   - klicken **Wählen Sie eine E-Mail-Benachrichtigungsgruppe** und klicken Sie auf eine oder mehrere E-Mail-Gruppen.
   - Geben Sie einzelne E-Mail-Adressen ein. Mehrere Adressen müssen durch ein Komma getrennt werden.
5. Optional: klicken **SNMP-Trap senden** um Benachrichtigungen an einen SNMP-Listener zu senden.
6. Optional: Fügen Sie der E-Mail-Benachrichtigung zusätzliche Messwerte hinzu.

   Die E-Mail enthält den Wert dieser Metriken zum Zeitpunkt des Auftretens der Warnung.
   a) klicken **Erweiterte Optionen anzeigen**.
   b) Aus dem Zusätzliche Metriken in E-Mail-Benachrichtigungen Abschnitt, klicken Sie **Metrik hinzufügen**.
   c) Geben Sie in das Suchfeld den Namen einer Metrik ein und wählen Sie dann die Metrik aus den Suchergebnissen aus.

      Die Metrik muss mit dem zugewiesenen Quelltyp und der überwachten Metrik kompatibel sein, z. B. mit Geräten und Gerätemetriken.
7. klicken **Speichern**.

Eine Alarm hinzufügen (RevealX 360)

Sie können einer Warnungskonfiguration eine Benachrichtigung hinzufügen, die eine E-Mail an eine oder mehrere angegebene E-Mail-Adressen sendet, wenn die Alarm auftritt. Die E-Mail enthält Warnungsdetails und einen Link zum Anzeigen der Warnungsquelle.

Bevor Sie beginnen
Das musst du haben volle Schreibrechte oder höher.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Warnmeldungen**.
3. Klicken Sie in der Tabelle Warnungen auf die gewünschte Alarm.
4. Geben Sie im Abschnitt Benachrichtigungen die E-Mail-Adressen an, die benachrichtigt werden sollen, wenn die Alarm auftritt.

   Geben Sie einzelne E-Mail-Adressen ein. Mehrere Adressen müssen durch ein Komma getrennt werden.
5. Optional: Fügen Sie der E-Mail-Benachrichtigung zusätzliche Metriken hinzu.

   Die E-Mail enthält den Wert dieser Metriken zum Zeitpunkt des Auftretens der Warnung.
   a) Klicken Sie **Erweiterte Optionen anzeigen**.
   b) Klicken Sie im Abschnitt Zusätzliche Metriken in E-Mail-Benachrichtigungen auf **Metrik hinzufügen**.
   c) Geben Sie in das Suchfeld den Namen einer Metrik ein und wählen Sie dann die Metrik aus den Suchergebnissen aus.

      Die Metrik muss mit dem zugewiesenen Quelltyp und der überwachten Metrik kompatibel sein, z. B. mit Geräten und Gerätemetriken.
6. Klicken Sie **Speichern**.

Einer Alarm ein Ausschlussintervall hinzufügen

Mit Ausschlussintervallen können Sie eine oder mehrere Benachrichtigungen in bestimmten Zeiträumen unterdrücken. Sie können beispielsweise eine Alarm außerhalb der Geschäftszeiten, am Wochenende oder während Wartungsfenstern unterdrücken.

Erstellen Sie ein neues Ausschlussintervall, wenn Sie eine Alarm erstellen oder bearbeiten. Nachdem Sie ein Ausnahmeintervall erstellt haben, können Sie es auf bestehende und neue Benachrichtigungen anwenden.

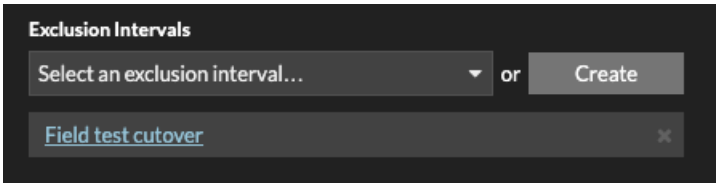
Bevor Sie beginnen
Du musst volle Schreibrechte oder höher.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Warnmeldungen**.
3. Klicken Sie in der Tabelle Benachrichtigungen auf die gewünschte Alarm.
4. Klicken Sie im Abschnitt Warnung bearbeiten auf **Erweiterte Optionen anzeigen**.
5. Fügen Sie im Abschnitt Ausschlussintervalle ein vorhandenes Intervall hinzu oder erstellen Sie ein neues.

Option	Description
Ein vorhandenes Ausschlussintervall hinzufügen	1. Klicken Sie auf die Dropdownliste Ausschlussintervall und wählen Sie ein Intervall aus. 2. Wiederholen Sie diesen Vorgang, um der Alarm ein zusätzliches Intervall hinzuzufügen.
Neues Ausschlussintervall erstellen	1. klicken **Erstellen**. 2. Geben Sie einen eindeutigen Namen für das Ausschlussintervall in der **Name** Feld. 3. In der **Beschreibung** Feld, fügen Sie Informationen über das Intervall hinzu. 4. Geben Sie im Abschnitt Ausschließen ein Intervall und einen Zeitraum ein: • klicken **Jeden Tag von** um ein täglich wiederkehrendes Intervall festzulegen. • klicken **Jede Woche von** um ein wöchentlich wiederkehrendes Intervall festzulegen. • klicken **Benutzerdefinierter Zeitbereich** um ein einmaliges Intervall festzulegen. 5. Optional: Wählen Sie im Abschnitt Zuweisungen eine globale Zuweisungsoption aus: • klicken **Allen Alerts zuweisen** um das Intervall zu allen bestehenden und zukünftigen Alert-Konfigurationen hinzuzufügen. • klicken **Allen Trends zuordnen** um die Metrik Aktivität während des Intervalls von den Trendberechnungen auszuschließen.

Option	Description
	6. klicken **Speichern** um das Intervall zu erstellen und es der Alarm hinzuzufügen.

Hinweis: Klicken Sie in der Liste der hinzugefügten Ausschlussintervalle auf einen Intervallnamen, um die Eigenschaften zu bearbeiten, oder klicken Sie auf das Symbol Entfernen (X), um das Intervall aus der Alarm zu entfernen.



6. klicken **Speichern** und dann klicken **Erledigt**.

Aufzeichnungen

Datensätze sind strukturierte Informationen über Transaktions-, Nachrichten- und Netzwerkflüsse, die generiert und vom ExtraHop-System an einen Recordstore gesendet werden. Nachdem Ihre Aufzeichnungen gesammelt und gespeichert wurden, können Sie sie im gesamten ExtraHop-System abfragen.

Aufzeichnungen werden auf zwei Protokollebenen gesammelt: L3 und L7. L3- (oder Fluss-) Datensätze zeigen Transaktionen auf Netzwerkebene zwischen zwei Geräten über das IP-Protokoll. L7-Datensätze zeigen Transaktionen, die nachrichtenbasiert (wie ActiveMQ, DNS und DHCP), transaktional (wie HTTP, SMB und NFS) und sitzungsbasiert (wie TLS und ICA) sind.

Wenn Sie beispielsweise fünfzig HTTP 503-Fehler hätten, würden die zugehörigen HTTP-Transaktionen Details über die URL, den Server, den Client, der die Anfrage gesendet hat, usw. enthalten. Diese Details können Ihnen helfen, das zugrunde liegende Problem zu identifizieren.

Video: Sehen Sie sich die entsprechende Schulung an: Aufzeichnungen

Bevor du anfängst

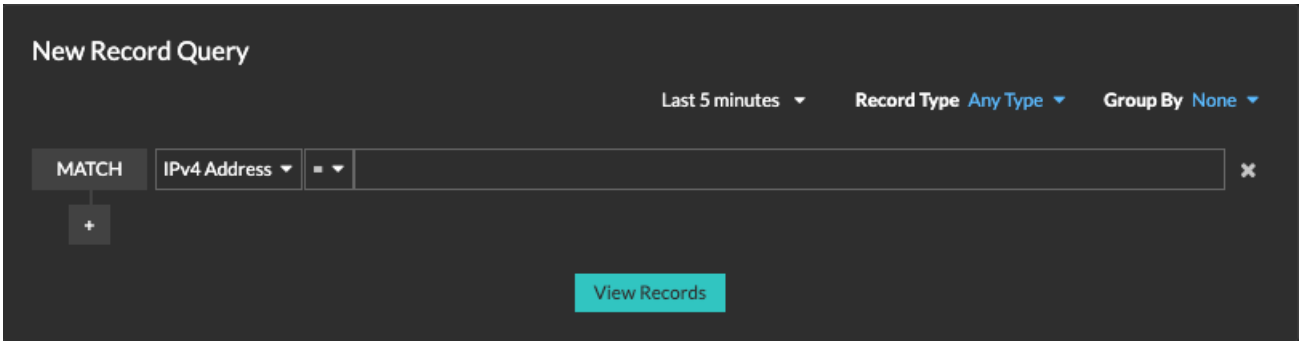
- Sie müssen einen konfigurierten Recordstore haben, z. B. ExtraHop Recordstore, Splunk, Google BigQuery, oder CrowdStrike Falcon LogScale.
- Sie können nur einen Recordstore für das ExtraHop-System konfigurieren.
- Ihr ExtraHop-System muss für das Sammeln und Speichern konfiguriert sein Flussaufzeichnungen oder L7-Datensätze.

In Datensätzen navigieren

Auf der Hauptseite „Datensätze“ werden mehrere Möglichkeiten zur Abfrage von gespeicherten Datensätzen angezeigt. klicken **Rekorde** aus dem oberen Menü, um loszulegen.

Standardsuche

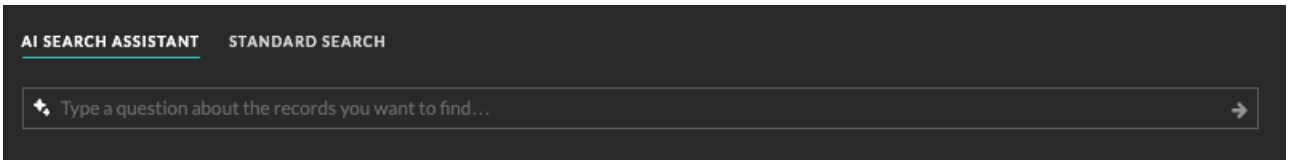
Fragen Sie mit einer Standardsuche nach Datensätzen ab, um einen komplexen Filter zu erstellen, indem Sie die Operatoren „AND“ und „OR“ mit zusätzlichen Filteroptionen wie Datensatztyp und Zeitintervall kombinieren . Erfahren Sie mehr über das Abfragen von Datensätzen mit einer Standardsuche.



KI-Suchassistent

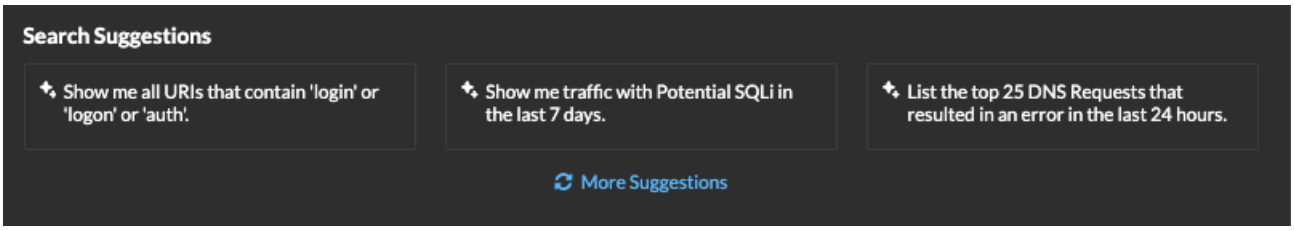
AI Search Assistant hilft Ihnen bei der Suche nach Datensätzen mit Fragen, die in natürlicher, alltäglicher Sprache verfasst sind, sodass Sie im Vergleich zur Erstellung einer Standardsuchabfrage mit denselben Kriterien schnell komplexe Abfragen erstellen können. Der AI Search Assistant muss

von Ihrem ExtraHop-Administrator aktiviert werden.Erfahren Sie mehr über das Abfragen von Datensätzen mit dem AI Search Assistant.



Vorschläge für die Suche

Das ExtraHop-System bietet mehrere Suchvorschläge mit vorgefertigten Filtern , mit denen Sie häufig verwendete Datensatzsuchen effizienter durchführen können. Klicken Sie auf eine vorgeschlagene Suche, um die Abfrage anzuwenden und sofort Datensätze anzuzeigen, oder klicken Sie auf **Weitere Vorschläge** für mehr Optionen.



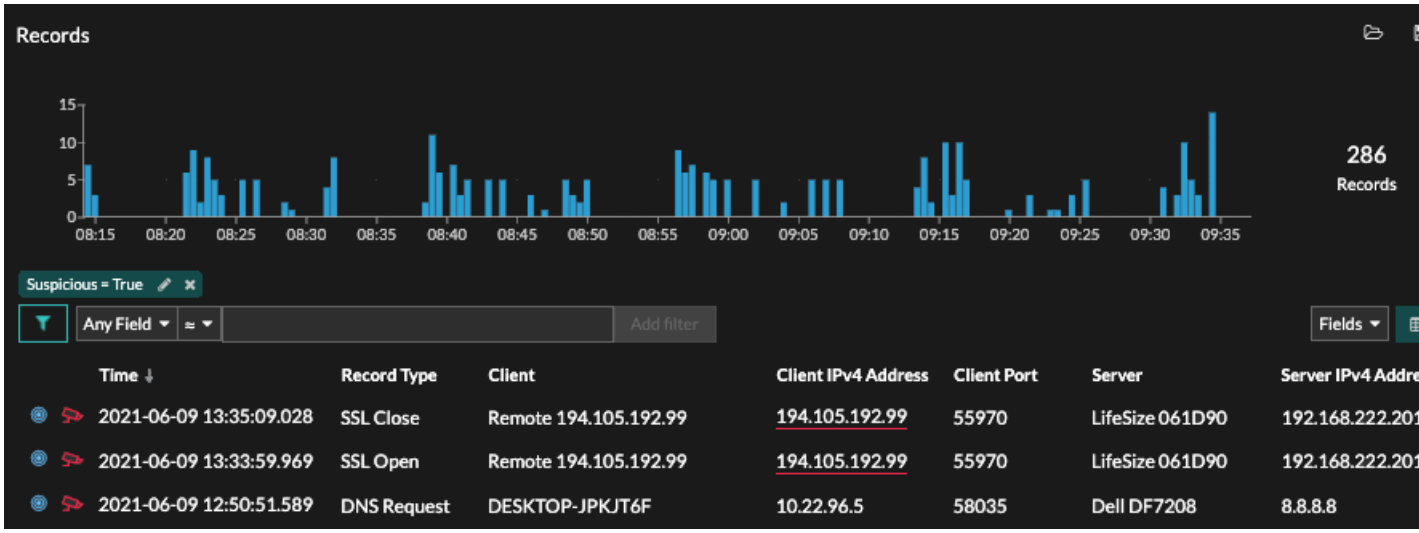
Gespeicherte Abfragen

Sie können auch eine zuvor gespeicherte Abfrage aus der Liste auf der Seite Datensätze auswählen und sofort Datensätze anzeigen, oder Sie können auf das Ordnersymbol klicken in der oberen rechten Ecke der Seite, um alle gespeicherten Abfragen anzuzeigen.

Hinweis: Um eine Datensatzabfrage für eine benutzerdefinierte Metrik zu erstellen, müssen Sie zunächst die Datensatzbeziehung definieren, indem Sie Verknüpfung der benutzerdefinierten Metrik mit einem Datensatztyp.

Ergebnisse einer Datensatzabfrage anzeigen

Nachdem Sie die Abfrage abgeschickt haben, werden die Ergebnisse auf der Hauptseite „Datensätze “ angezeigt.



Hinweis: Eine Abfrage kann Millionen von Datensätzen basierend auf dem Zeitintervall und den Filterkriterien zurückgeben. Wenn eine Abfrage die maximale Anzahl von Abfrageergebnissen überschreitet, wird eine gekürzte Anzahl von Datensätzen angezeigt (nur ExtraHop-Recordstore). Beispielsweise führen Abfragen aus dem Standardfilter Beliebiges Feld häufig zu einer sehr großen Anzahl von Ergebnissen und können sich auf die Leistung auswirken.

Hier sind einige Möglichkeiten, wie Sie die Ergebnisse von Datensatzabfragen aufschlüsseln können:

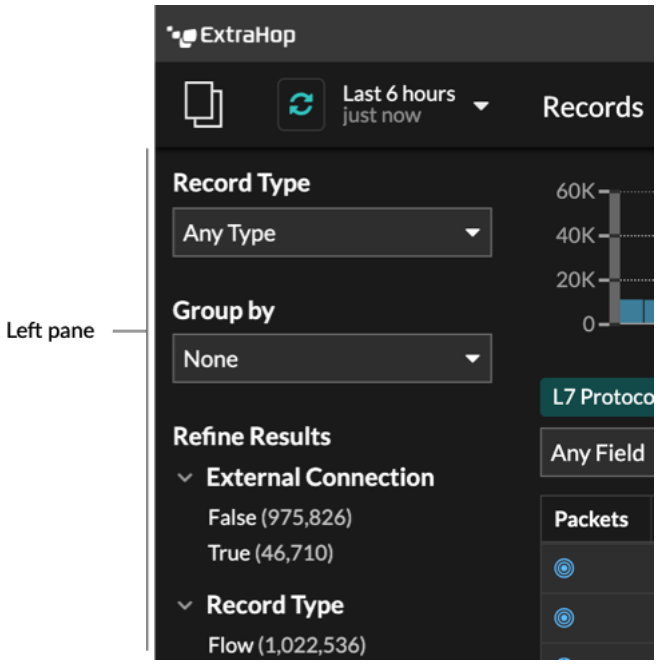
- Zeigen Sie im Datensatzdiagramm mit der Maus auf ein Zeitintervall, um die Anzahl der Datensätze anzuzeigen, oder klicken und ziehen Sie über das Diagramm, um die Ergebnisse der Datensatzabfrage auf ein bestimmtes Zeitintervall einzugrenzen.
- Klicken Sie auf einen Hostnamen oder eine IP-Adresse, um Details zum Gerät oder Externer Endpunkt anzuzeigen.
- Datensätze, die verdächtige IP-Adressen, Hostnamen und URIs enthalten, werden mit einem roten Kamerasymbol angezeigt. Klicken Sie auf das Kamerasymbol, um es anzuzeigen Bedrohungsinformationen für's Datensatz.
- Klicken Sie auf ein Paketsymbol, um eine zu starten Paketabfrage das wird durch diesen Datensatz gefiltert.
- Datensatzergebnisse werden standardmäßig in einer Tabelle angezeigt. Klicken Sie auf die Tabellenansicht oder die ausführliche Ansicht  Symbole zum Umschalten der Anzeige.
- Eine Abfrage wird automatisch angehalten, wenn die Anzahl der gescannten oder zurückgegebenen Datensatzbytes extrem groß ist. Wenn die Abfrage angehalten ist, zeigt sie die neuesten Datensätze an. klicken **Abfrage fortsetzen** um die Suche fortzusetzen.
- Klicken Sie auf **Felder** Dropdownliste, um der Datensatzansicht zusätzliche Datensatzinformationen hinzuzufügen.
- Klicken und ziehen Sie in der Tabellenansicht die Spaltenüberschriften, um die Datensatzinformationen anzuordnen.
- Bewerben einfach oder erweiterte Filter um potenzielle Probleme zu finden, z. B. zu lange Bearbeitungszeiten oder ungewöhnliche Antwortgrößen.

Verfeinern Sie Ihren Datensatzabfragefilter

Es gibt eine Reihe von Möglichkeiten, Ihren Datensatzabfragefilter zu verfeinern, um genau die Datensätze zu finden, nach denen Sie suchen. Die folgenden Abschnitte beschreiben jede Methode und zeigen Beispiele, mit denen Sie sich zunächst vertraut machen können.

Filtern der Datensatzergebnisse aus dem linken Bereich

Nachdem alle verfügbaren Datensätze für das gewählte Zeitintervall auf der Seite Datensätze angezeigt wurden, können Sie im linken Bereich filtern, um Ihre Ergebnisse zu verfeinern.



Das **Typ des Datensatzes** Das Drop-down-Menü zeigt eine Liste aller Datensatztypen an, für deren Erfassung und Speicherung Ihr ExtraHop-System konfiguriert ist. Ein Datensatztyp bestimmt, welche Daten gesammelt und im Recordstore gespeichert werden.

Hinweis: Da Sie einen Auslöser schreiben müssen, um Datensätze zu sammeln, benötigen Sie eine Möglichkeit, den Typ der zu sammelnden Daten zu identifizieren. Es gibt integrierte Datensatztypen, die alle verfügbaren bekannten Felder für ein Protokoll sammeln. Sie können mit einem integrierten Datensatztyp (z. B. HTTP) beginnen und einen Auslöser schreiben, der nur die Felder für dieses Protokoll erfasst, die für Sie von Bedeutung sind (wie URI und Statuscode). Fortgeschrittene Benutzer können auch einen benutzerdefinierten Datensatztyp erstellen, wenn sie proprietäre Informationen sammeln müssen, die über einen integrierten Datensatztyp nicht verfügbar sind.

Das **Gruppieren nach** In der Dropdownliste finden Sie eine Liste von Feldern, nach denen Sie den Datensatztyp weiter filtern können.

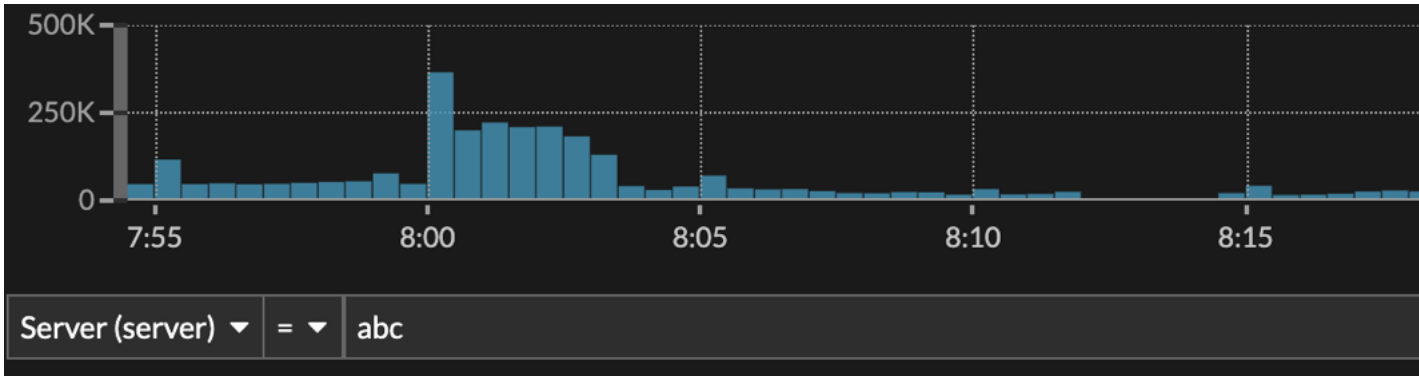
Das **Ergebnisse verfeinern** Dieser Abschnitt zeigt Ihnen eine Liste gängiger Datensatzfilter für den ausgewählten Datensatztyp mit der Anzahl der Datensätze, die dem Filter in Klammern entsprechen.

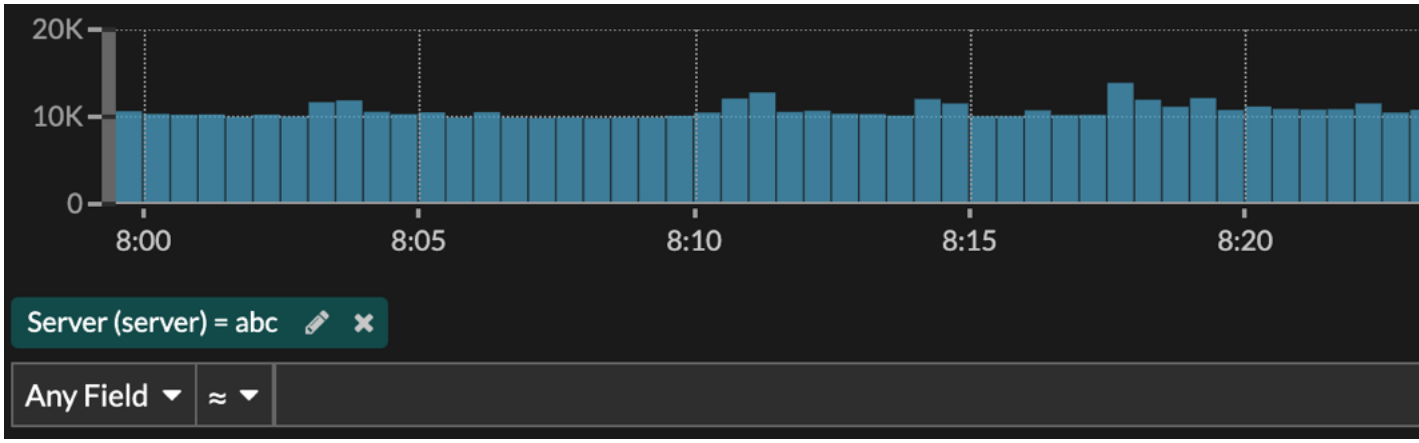
Filterung der Datensatzergebnisse durch das Dreifeld

Klicken Sie auf das Stiftsymbol um einen vorhandenen Filter zu bearbeiten, oder klicken Sie auf die Schaltfläche Advance Filter hinzufügen um einen neuen Filter hinzuzufügen.

In der **Anzeigename des Filters** Feld, Sie können einen beschreibenden Namen angeben, um den allgemeinen Zweck der Abfrage zu identifizieren.

Wählen Sie eine Kriterienoption aus dem Dropdownmenü aus (die Standardoption ist IPv4-Adresse), wählen Sie einen Operator aus (z. B. das Gleichheitszeichen (=)), und geben Sie dann den Suchwert ein. Klicken Sie **Filter hinzufügen**, und der Filter wird über der Filterleiste hinzugefügt.





Ihre Ergebnisse zeigen nur Datensätze, die dem Filter entsprechen.

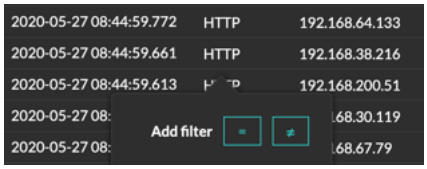
Die folgenden Operatoren können basierend auf dem ausgewählten Feldnamen ausgewählt werden:

Betreiber	Beschreibung
=	Ist gleich
≈	Ist nicht gleich
≈	Beinhaltet Wenn Datensätze in einem ExtraHop-Recordstore gespeichert sind, entspricht der Include-Operator ganzen Wörtern, die durch Leerzeichen und Satzzeichen getrennt sind. Beispielsweise würde eine Suche nach „www.extra“ auf „www.extra.com“, aber nicht auf „www.extrahop.com“ passen. Bei allen anderen Datensatzspeichern entspricht der Include-Operator Teilzeichenfolgen, einschließlich Leerzeichen und Satzzeichen. Beispielsweise würde eine Suche nach „www.extra“ mit „www.extrahop.com“ übereinstimmen, aber eine Suche nach „www extra“ würde nicht mit „www.extrahop.com“ übereinstimmen. Regex- und Platzhalterzeichen werden nicht unterstützt.

Betreiber	Beschreibung
≈/	Schließt aus Wenn Datensätze in einem ExtraHop-Recordstore gespeichert sind, entspricht der Ausschlussoperator ganzen Wörtern, die durch Leerzeichen und Satzzeichen getrennt sind. Beispielsweise würde eine Suche nach „extra“ zwar „www.extra.com“ ausschließen, aber nicht „www.extrahop.com“. Bei allen anderen Datensatzspeichern entspricht der Operator excludes Teilzeichenfolgen, einschließlich Leerzeichen und Satzzeichen. Beispielsweise würde eine Suche nach „www.extra“ „www.extrahop.com“ ausschließen, aber eine Suche nach „www extra“ würde „www.extrahop.com“ nicht ausschließen. Regex - und Platzhalterzeichen werden nicht unterstützt.
<	Weniger als
≤	Weniger als oder gleich
>	Größer als
≥	Größer als oder gleich
beginnt mit	Beginnt mit
existiert	Existiert
geht nicht	Existiert nicht

Direktes Filtern aus Datensatzergebnissen

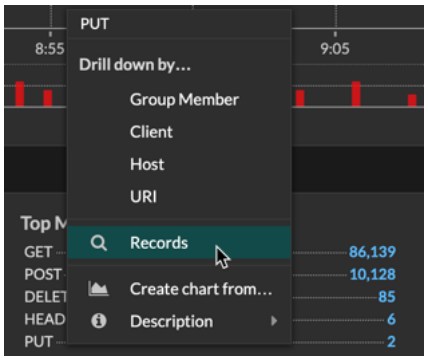
Sie können jeden Feldeintrag auswählen, der in Ihren Datensatzergebnissen entweder in der Tabellenansicht oder in der ausführlichen Ansicht angezeigt wird, und dann auf den Popup-Operator klicken, um den Filter hinzuzufügen. Filter werden unter der Diagrammzusammenfassung angezeigt (mit Ausnahme des Feld Datensatztyp, das im linken Bereich geändert wurde).



Datensätze im ExtraHop-System finden

- Geben Sie einen Suchbegriff in das globale Suchfeld oben auf dem Bildschirm ein und klicken Sie auf Datensätze durchsuchen, um eine Abfrage für alle gespeicherten Datensätze zu starten.
- Klicken Sie auf einer Geräteübersichtsseite auf **Rekorde** um eine nach diesem Gerät gefilterte Abfrage zu starten.
- Klicken Sie auf einer Übersichtsseite für Gerätegruppe auf **Aufzeichnungen ansehen** um eine nach dieser Gerätegruppe gefilterte Abfrage zu starten.

- Klicken Sie auf einer Erkennungskarte auf Datensätze anzeigen, um eine Abfrage zu starten, die mit den Transaktionen gefiltert wird, die mit der Erkennung verknüpft sind.
- Klicken Sie auf das Datensatzsymbol aus einem Diagramm-Widget, wie in der folgenden Abbildung dargestellt.



- Klicken Sie auf das Datensatzsymbol neben einer Detail-Metrik, nachdem Sie sich eine Top-Level-Metrik genauer angesehen haben. Klicken Sie beispielsweise nach der Aufschlüsselung der HTTP-Antworten nach Server auf das Symbol Datensätze, um eine Abfrage für Datensätze zu erstellen, die eine bestimmte Server-IP-Adresse enthalten.

Abfrage nach gespeicherten Datensätzen

Sie können Datensätze, die im Recordstore gespeichert sind, mit einer Standardsuche oder mit AI Search Assistant abfragen.

- Erfahren Sie mehr über das Abfragen von Datensätzen mit einer Standardsuche.
- Erfahren Sie mehr über das Abfragen von Datensätzen mit dem AI Search Assistant.
- Informationen zum Abfragen eines bestimmten Datensatz finden Sie in unserer exemplarischen Vorgehensweise für Fehlende Webressourcen entdecken.
- Du kannst auch automatisiere diese Aufgabe über die REST-API.

Nächste Schritte

Hinweis: Um eine Datensatzabfrage für eine benutzerdefinierte Metrik zu erstellen, müssen Sie zunächst die Datensatzbeziehung definieren, indem Sie Verknüpfung der benutzerdefinierten Metrik mit einem Datensatztyp.

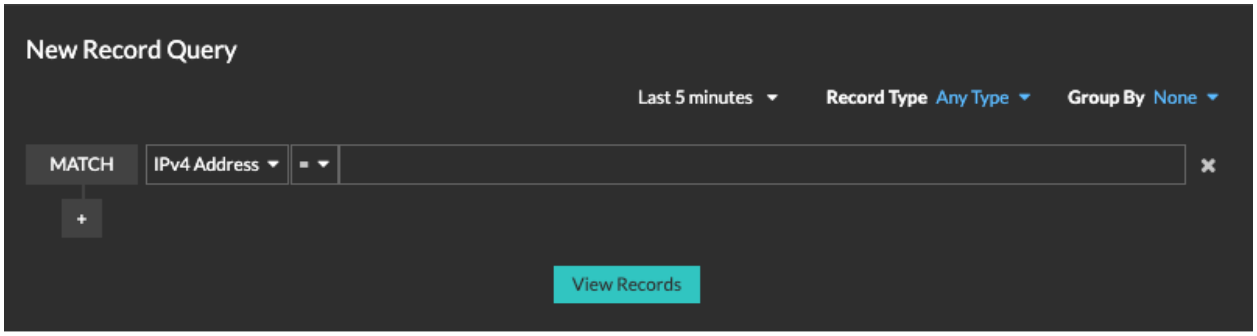
Datensätze mit einer Standardsuche abfragen

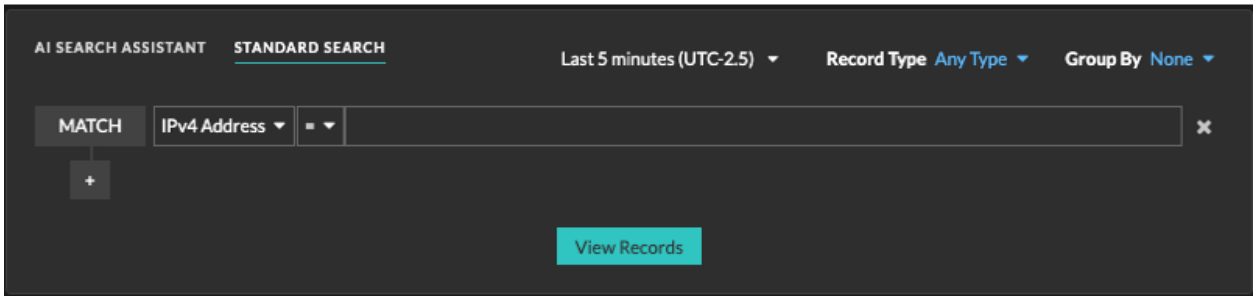
Auf der Seite „Datensätze“ können Sie einen komplexen Filter für die Suche nach Datensätzen erstellen.

Hier sind einige wichtige Dinge, die Sie über Datensatzabfragen mit der Standardsuche wissen sollten:

- Sie können mehrere Kriterien mit den Operatoren OR (Match Any), AND (Match All) und NOT angeben.
- Sie können Filter gruppieren und innerhalb jeder Gruppe auf vier Ebenen verschachteln.
- Sie können eine Filtergruppe bearbeiten, nachdem Sie sie erstellt haben, um die Suchergebnisse zu verfeinern.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Aufzeichnungen**.
   Wenn AI Search Assistant nicht aktiviert ist, wird der Abschnitt Neue Datensatzabfrage angezeigt.
   Wenn AI Search Assistant aktiviert ist, klicken Sie auf **Standardsuche**.



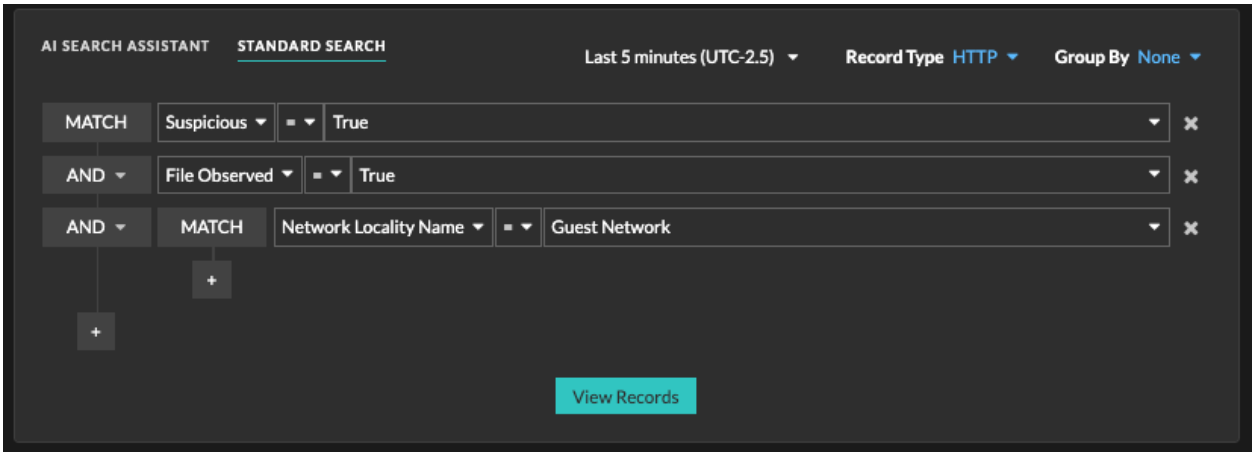


3. Wählen Sie das Zeitintervall aus, nach dem Sie suchen möchten.

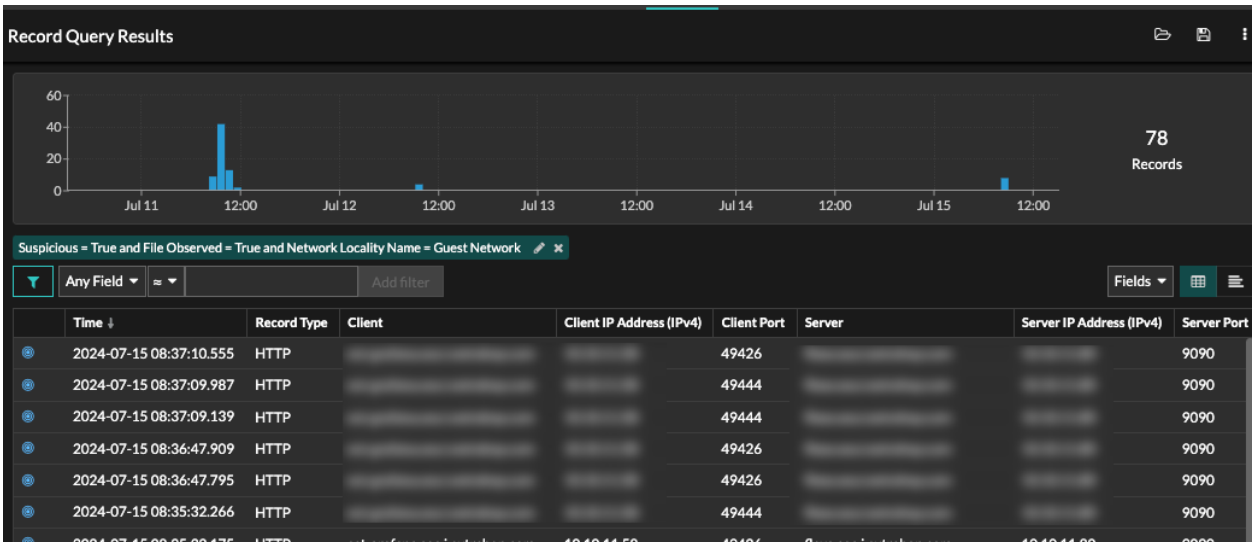
   Das Zeitintervall, das Sie auswählen, ändert die in der globaler Zeitwähler.
4. Aus dem **Datensatztyp** Wählen Sie im Drop-down-Menü einen oder mehrere der Datensatztypen aus, für deren Erfassung und Speicherung Ihr ExtraHop-System konfiguriert ist.
5. Aus dem **Gruppieren nach** Wählen Sie im Dropdownmenü eine Option aus, um anzugeben, wie Sie die Ergebnisse gruppieren möchten. Die angezeigten Optionen sind mit den von Ihnen ausgewählten Datensatztypen verknüpft.

   Wenn Sie beispielsweise HTTP-Datensätze nach Client gruppieren, werden in der Ergebnistabelle die Clients angezeigt, die in den Datensatztransaktionen gefunden wurden, sortiert nach der Häufigkeit, mit der dieser Client gefunden wurde.
6. Wählen Sie im Dropdownmenü Filterkriterien (die Standardeinstellung ist IPv4-Adresse) die ersten Kriterien aus, denen der Filter entsprechen soll. Die angezeigten Optionen sind mit den von Ihnen ausgewählten Datensatztypen verknüpft.
7. Optional: Klicken Sie auf das Plus-Symbol und wählen Sie **Filter hinzufügen** oder **Filtergruppe hinzufügen** um weitere Kriterien auf der obersten oder sekundären Ebene des Filters anzugeben.

   Eine neue Filtergruppe fügt dem Ergebnis des ursprünglichen Filters Kriterien hinzu. Wenn Sie beispielsweise nach HTTP-Transaktionen suchen, die verdächtig waren und Dateien enthielten, können Sie eine Filtergruppe hinzufügen, um die Ergebnisse auf Datensätze einzugrenzen, die einer bestimmten Netzwerklokalität zugeordnet sind.



8. Klicken Sie **Aufzeichnungen ansehen**.
   Die Ergebnisse der Aufzeichnungen werden auf der Hauptseite „Aufzeichnungen“ angezeigt.



Nächste Schritte

- Du kannst Abfrageergebnisse anzeigen und aufschlüsseln.
- Du kannst verfeinern Sie Ihren Datensatzabfragefilter.
- Sie können auf das Symbol Speichern klicken von oben rechts auf der Seite, um Ihren Filter für ein anderes Mal zu speichern.
- Sie können auf ein Paketsymbol neben einem Datensatz klicken, um einen zu starten Paketabfrage das nach diesem Datensatz gefiltert wird, oder klicken Sie auf den Abfrage-Link am Ende der Tabelle, um eine Paketabfrage für alle angezeigten Datensätze zu starten.

Datensätze mit AI Search Assistant abfragen

Mit dem AI Search Assistant können Sie nach Datensätzen mit Fragen suchen, die in natürlicher, alltäglicher Sprache verfasst sind. So können Sie im Vergleich zur Erstellung einer Standardsuchabfrage mit denselben Kriterien schnell komplexe Abfragen erstellen.

Wenn Sie beispielsweise abfragen: „Gab es in den letzten 7 Tagen verdächtige HTTP-Transaktionen mit Dateien?“ , die folgende AI Search Assistant-Abfrage wird angezeigt:

```
Time Interval = Last 2 days and Record Type = [HTTP]
```

```
Suspicious = True and File Observed = True
```

Hier sind einige Dinge, die Sie bei der Suche nach Geräten mit AI Search Assistant beachten sollten:

- Eingabeaufforderungen werden denselben Datensatzfilterkriterien zugeordnet, die Sie beim Erstellen einer Standardsuche angeben.
- Eingabeaufforderungen können absolute und relative Zeitbereiche enthalten, z. B. „Zeige mir Traffic mit potenziellem SQLi in den letzten 7 Tagen“. Das aktuelle Jahr wird verwendet, wenn für ein Datum kein Jahr enthalten ist.
- Die Eingabeaufforderungen sollten so klar und präzise wie möglich sein. Wir empfehlen Ihnen, einige Variationen zu schreiben, um Ihre Ergebnisse zu maximieren.
- Das ExtraHop-System ist möglicherweise nicht in der Lage, eine Abfrage zu verarbeiten, die Anfragen nach Datensatzinformationen enthält, die außerhalb der verfügbaren Filter liegen.
- Das ExtraHop-System kann Benutzeranweisungen zur Produktverbesserung speichern. Wir empfehlen, dass Sie in Ihren Eingabeaufforderungen keine urheberrechtlich geschützten oder vertraulichen Daten angeben.
- Sie können die Abfragefilterkriterien bearbeiten, um die Suchergebnisse zu verfeinern.

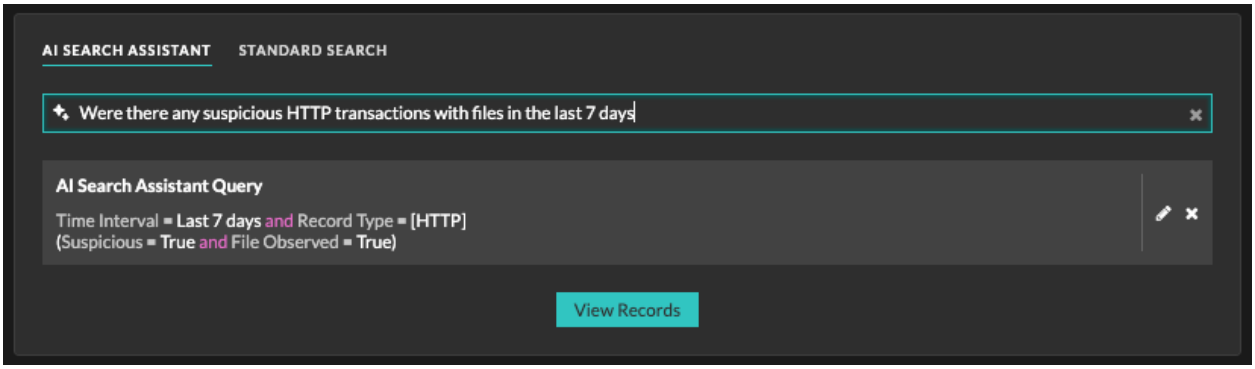
Bevor Sie beginnen

- Ihr ExtraHop-System muss verbunden mit ExtraHop Cloud Services.
- Der AI Search Assistant muss von Ihrem ExtraHop-Administrator aktiviert werden.

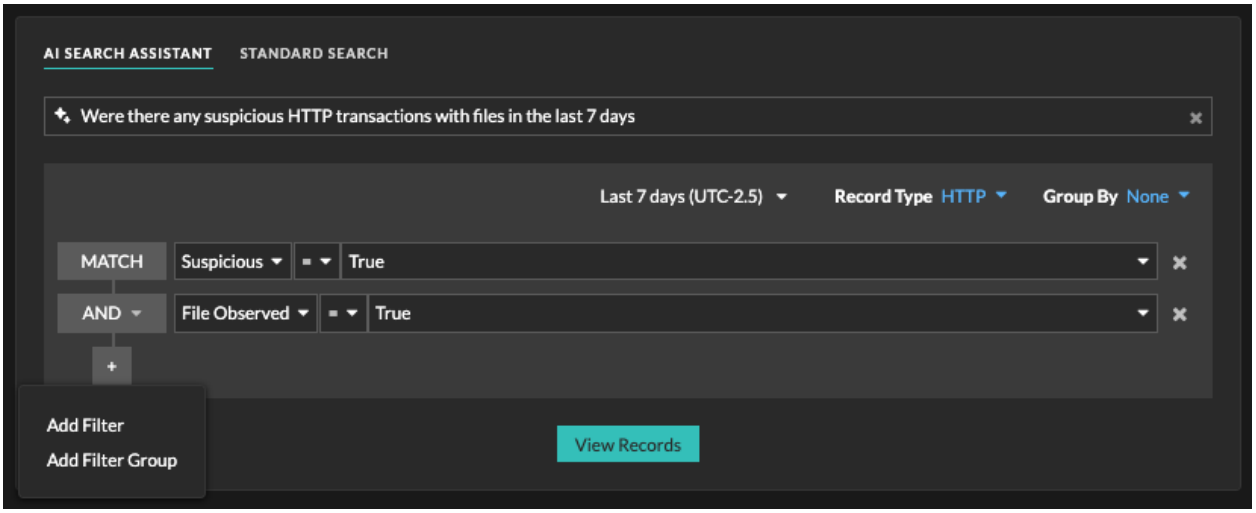
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Rekorde**.
3. Schreiben Sie eine Aufforderung in das Feld AI Search Assistant und drücken Sie die EINGABETASTE.

   Hinweis: Klicken Sie auf das Suchaufforderungsfeld, um eine aktuelle Abfrage oder eine vorgeschlagene Suche auszuwählen.

   Der AI Search Assistant-Abfragefilter wird angezeigt.



4. Optional: Klicken Sie im Abschnitt AI Search Assistant Query auf das Bearbeitungssymbol um Ihre Abfragefilterkriterien zu verfeinern.



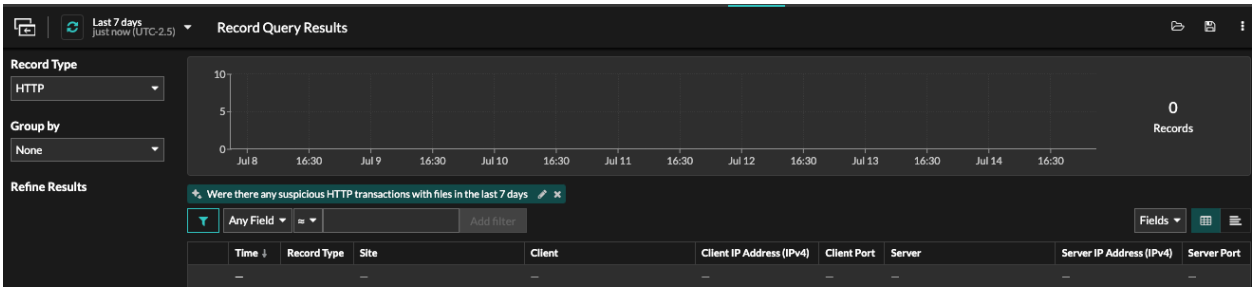
a) Bearbeiten Sie in der obersten Zeile das Zeitintervall, **Datensatztyp** oder **Gruppieren nach** Optionen.

b) Klicken Sie auf das Plus-Symbol und wählen Sie **Filter hinzufügen** oder **Filtergruppe hinzufügen** um weitere Kriterien auf der obersten oder sekundären Ebene des Filters anzugeben.

Eine neue Filtergruppe fügt dem Ergebnis des ursprünglichen Filters Kriterien hinzu. Wenn Sie beispielsweise nach verdächtigen HTTP-Datensätzen suchen, die Dateien enthielten, können Sie eine Filtergruppe hinzufügen, um die Ergebnisse auf Datensätze einzugrenzen, die einer bestimmten Netzwerklokalität zugeordnet sind.

c) Klicken Sie **Erledigt**.

5. Klicken Sie **Aufzeichnungen ansehen**.
Die Ergebnisse der Aufzeichnungen werden auf der Hauptseite „Aufzeichnungen“ angezeigt. Der Anzeigename des AI Search Assistant-Filters ist die Eingabeaufforderung, die Sie eingegeben haben und die über dem Dreifeld angezeigt wird.



Nächste Schritte

- Du kannst Abfrageergebnisse anzeigen und aufschlüsseln.
- Du kannst verfeinern Sie Ihren Datensatzabfragefilter.
- Sie können auf das Symbol Speichern klicken von oben rechts auf der Seite, um Ihren Filter für ein anderes Mal zu speichern.
- Sie können auf ein Paketsymbol neben einem Datensatz klicken, um einen zu starten Paketabfrage das nach diesem Datensatz gefiltert wird, oder klicken Sie auf den Abfrage-Link am Ende der Tabelle, um eine Paketabfrage für alle angezeigten Datensätze zu starten.

Aufzeichnungen sammeln

Bestimmte Datensatztypen sind standardmäßig für die Erfassung aktiviert. Sie können die Arten von Datensätzen, die gesammelt und an Ihren Recordstore gesendet werden, aus dem Ordner hinzufügen oder entfernen Einstellungen//Aufzeichnungen Seite. Diese Datensätze enthalten hauptsächlich Informationen über Nachrichten, Transaktionen und Sitzungen, die über gängige L7-Protokolle wie DNS, HTTP und TLS gesendet wurden.

Wenn Sie nur bestimmte Details von Transaktionen sammeln möchten, können Sie benutzerdefinierte Datensätze über den ExtraHop-Trigger-API.

Hinweis: Du kannst verwalte diese Einstellungen zentral von einer Konsole aus.

Erfahre mehr über ExtraHop Records.

Bevor Sie beginnen
Sie müssen einen konfigurierten Recordstore haben, z. B. einen ExtraHop Recordstore, Splunk, oder Google BigQuery.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Schallplattensammlung**.
3. Auf dem Rekorde Seite, aktivieren Sie das Kontrollkästchen neben den Transaktionstypen, die Sie erfassen und im Datensatzspeicher speichern möchten, und klicken Sie dann auf **Aktiviere**.
4. klicken **Rekorde** aus dem Hauptmenü, und klicken Sie dann auf **Aufzeichnungen ansehen** um eine Abfrage zu starten.

   Wenn Sie keine Aufzeichnungen sehen, warten Sie ein paar Minuten und versuchen Sie es erneut. Wenn nach fünf Minuten keine Aufzeichnungen angezeigt werden, überprüfen Sie Ihre Konfiguration oder wenden Sie sich an ExtraHop-Unterstützung.

Flow-Aufzeichnungen sammeln

Sie können automatisch alle Datenflussdatensätze erfassen und speichern, bei denen es sich um Kommunikation auf Netzwerkebene zwischen zwei Geräten über ein IP-Protokoll handelt. Wenn Sie diese Einstellung aktivieren, aber keine IP-Adressen oder Portbereiche hinzufügen, werden alle erkannten Flussdatensätze erfasst. Die Konfiguration von Flow-Datensätzen für die automatische Erfassung ist ziemlich einfach und kann eine gute Möglichkeit sein, die Konnektivität zu Ihrem Recordstore zu testen.

Bevor Sie beginnen
Sie müssen Zugriff auf ein ExtraHop-System haben mit System- und Zugriffsadministrationsrechte.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Rekorde Abschnitt, klicken Sie **Automatische Flussaufzeichnungen**.
3. Wählen Sie die **Aktiviert** Ankreuzfeld.
4. In der Intervall veröffentlichen Feld, geben Sie eine Zahl zwischen 60 und 21600 ein.

   Dieser Wert bestimmt, wie oft Datensätze aus einem aktiven Fluss an den Recordstore gesendet werden. Der Standardwert ist 1800 Sekunden.
5. In der IP Adresse Feld, geben Sie eine einzelne IP-Adresse oder einen IP-Adressbereich im IPv4-, IPv6- oder CIDR-Format ein.
6. Klicken Sie auf das grüne Plus (**+**) Symbol.

   Sie können einen Eintrag entfernen, indem Sie auf das rote Löschen klicken (**X**) Symbol.
7. In der Portbereiche Feld, geben Sie einen einzelnen Port oder Portbereich ein, und klicken Sie dann auf das grüne Plus (**+**) Symbol.

8. Klicken Sie **Speichern**.

   Flow-Datensätze, die Ihre Kriterien erfüllen, werden jetzt automatisch an Ihren konfigurierten Recordstore gesendet. Warten Sie ein paar Minuten, bis die Aufzeichnungen gesammelt sind.
9. Klicken Sie im ExtraHop-System auf **Rekorde** aus dem Hauptmenü, und klicken Sie dann auf **Aufzeichnungen ansehen** um eine Abfrage zu starten.

   Wenn Sie keine Aufzeichnungen sehen, warten Sie ein paar Minuten und versuchen Sie es erneut. Wenn nach fünf Minuten keine Aufzeichnungen angezeigt werden, überprüfen Sie Ihre Konfiguration oder wenden Sie sich an ExtraHop-Unterstützung.

Sammle L7-Datensätze mit einem Auslöser

L7-Protokolle können über eine globale Triggerfunktion als Datensatz festgeschrieben (gesammelt und gespeichert) werden. L7-Datensätze enthalten Nachrichten, Transaktionen und Sitzungen, die über gängige L7-Protokolle wie DNS, HTTP und TLS gesendet werden.

In den folgenden Schritten erfahren Sie, wie Sie Datensätze für jedes Gerät sammeln, das eine HTTP-Antwort sendet oder empfängt.

Erfahre mehr über ExtraHop Records.

Zuerst schreiben wir einen Auslöser, um Informationen aus dem eingebauten HTTP-Recordtyp mit der commitRecord () -Methode zu sammeln, die auf allen verfügbar ist Protokollklassen. Die grundlegende Trigger-Syntax lautet `<protocol>.commitRecord()`. Dann weisen wir den Auslöser einem Server zu. Schließlich werden wir überprüfen, ob die Aufzeichnungen an den Recordstore gesendet werden.

Bevor Sie beginnen

- Sie müssen einen konfigurierten Recordstore haben, z. B. ExtraHop Recordstore, Splunk, oder Google BigQuery
- Diese Anweisungen setzen eine gewisse Vertrautheit mit ExtraHop-Auslöser, die Erfahrung mit JavaScript erfordern. Alternativ können Sie L7-Datensatzsammlung konfigurieren durch das ExtraHop-System.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen, und klicken Sie dann auf **Trigger**.
3. Klicken Sie **Erstellen**.
4. In der Trigger erstellen Bereich, vervollständigen Sie Ihre Informationen, ähnlich wie im folgenden Beispiel:

   • **Name:** `HTTP-Antworten`

   • **Beschreibung:** `Dieser Auslöser sammelt HTTP-Antworten.`
5. Markieren Sie das Kästchen neben **Debug-Log aktivieren**.
6. Wählen Sie aus der Dropdownliste Ereignisse **HTTP_RESPONSE**.
7. In der **Zuweisungen** Textfeld, suchen Sie nach einem aktiven Webserver, für den Sie Datensätze sammeln möchten, und wählen Sie den Server aus.
8. Geben Sie im rechten Bereich den folgenden Beispielcode ein:

```
HTTP.commitRecord();
debug ("committing HTTP responses");
```

   Dieser Code generiert Datensätze für den HTTP-Datensatztyp, wenn `HTTP_RESPONSE` Ereignis tritt ein und entspricht dem integrierten Datensatzformat für HTTP.
9. Klicken Sie **Speichern**.

Nächste Schritte

Warten Sie einige Minuten, bis die Datensätze erfasst sind, und überprüfen Sie dann im nächsten Schritt, ob Ihre Aufzeichnungen erfasst werden, indem Sie auf **Aufzeichnungen** aus dem Hauptmenü und dann auf **Aufzeichnungen ansehen** um eine Abfrage zu starten.

Wenn Sie nach 5 Minuten keine HTTP-Einträge sehen, klicken Sie auf **Debug-Protokoll** Tabulatortaste unten auf der Seite im Trigger-Editor, um zu sehen, ob es Fehler gibt, die Sie beheben können. Wenn der Auslöser läuft, wird die Meldung „Committing HTTP Responses“ angezeigt. Wenn nach dem Ausführen des Auslöser keine Datensätze angezeigt werden, wenden Sie sich an ExtraHop-Unterstützung.

Sammeln Sie benutzerdefinierte Datensätze

Sie können die Art der Datensatzdetails, die Sie generieren und in einem Recordstore speichern, anpassen, indem Sie einen Auslöser schreiben. Wir empfehlen, dass Sie auch ein Datensatzformat erstellen, um zu steuern, wie die Datensätze im ExtraHop-System angezeigt werden.

Bevor Sie beginnen

- Diese Anweisungen setzen eine gewisse Vertrautheit mit ExtraHop voraus Auslöser.
- Wenn Sie mit einem Google BigQuery-Datensatzspeicher verbunden sind, gilt für benutzerdefinierte Datensätze ein Limit von 300.

Im folgenden Beispiel erfahren Sie, wie Sie nur Datensätze für HTTP-Transaktionen speichern, die zu einem 404-Statuscode führen. Zunächst schreiben wir einen Auslöser, um Informationen aus dem integrierten HTTP-Datensatztyp zu sammeln. Dann weisen wir den Auslöser einem Server zu. Schließlich erstellen wir ein Datensatzformat, um ausgewählte Datensatzfelder in der Tabellenansicht für unsere Datensatzabfrageergebnisse anzuzeigen.

Einen Auslöser schreiben und zuweisen

Beachten Sie, dass der Auslöser auf jedem erstellt werden muss Sensor von denen Sie diese Arten von Datensätzen sammeln möchten. Sie können den Auslöser auf einem erstellen Konsole um Ihre benutzerdefinierten Datensätze von allen verbundenen zu sammeln Sensoren.

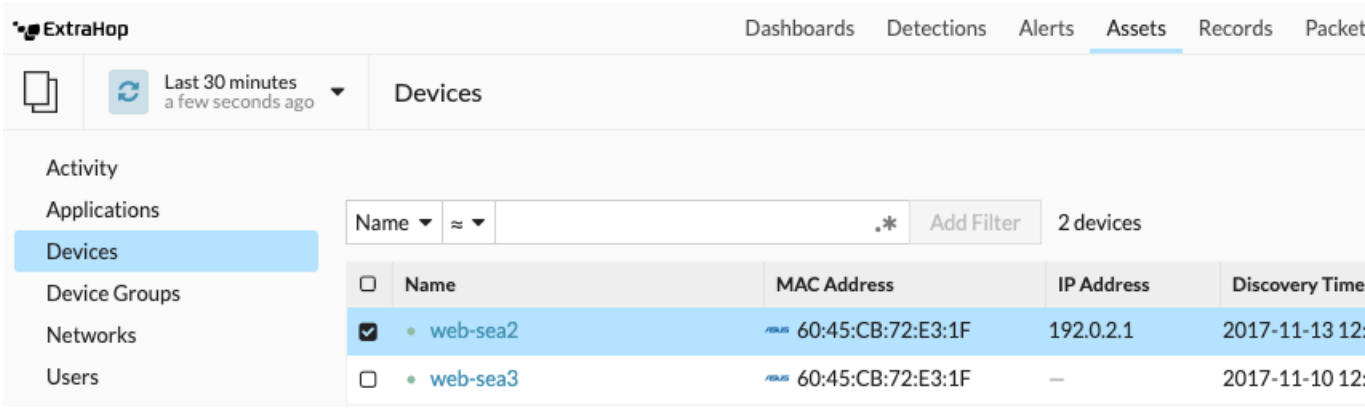
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen, und klicken Sie dann **Auslöser**.
3. klicken **Erstellen**.
4. In der Trigger erstellen Fenster, vervollständigen Sie Ihre Informationen, ähnlich dem folgenden Beispiel:
   - **Name:** `HTTP 404-Fehler`
   - **Beschreibung:** `Verfolgen Sie 404-Fehler auf dem primären Server.`
   - **Debug-Log aktivieren:** Markieren Sie das Kontrollkästchen, um das Debuggen zu aktivieren.
   - **Ereignisse:** `HTTP_RESPONSE`
5. Klicken Sie auf **Herausgeber** Tab, um die Trigger-Spezifikationen zu schreiben.

   Die folgende Abbildung zeigt eine Beispielkonfiguration, die nur Datensätze sammelt, wenn ein 404-Statuscode erkannt wird. Wir haben auch einen Namen festgelegt (`web 404`) für diese Datensatztypen, um sie in einer Datensatzabfrage zu identifizieren, und es wurden identifizierende Informationen für das Debuggen hinzugefügt.

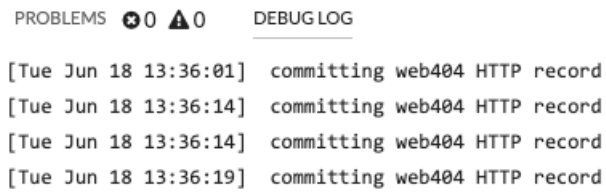
```
1  if (HTTP.statusCode === 404) {
2      commitRecord("web404", HTTP.record);
3      debug("committing web404 HTTP record");
4  }
```

Weisen Sie den Auslöser in den nächsten Schritten einem Gerät oder einer Gerätegruppe zu, für die Sie 404-Statuscodes überwachen möchten.

6. klicken **Vermögenswerte** aus dem oberen Menü.
7. klicken **Geräte** und klicken Sie dann auf **Aktive Geräte** Diagramm.
8. Wählen Sie das Kontrollkästchen für ein Gerät aus der Liste aus. Für unser Beispiel wählen wir einen Server namens `web2-sea`.
9. Klicken Sie auf das Symbol „Auslöser zuweisen“, wählen Sie den Trigger aus, den Sie in den vorherigen Schritten erstellt haben, und klicken Sie dann auf **Trigger zuweisen**. In der folgenden Abbildung haben wir unseren Server ausgewählt, `web2-sea`.



Nachdem Sie den Auslöser zugewiesen haben, kehren Sie zurück zum **Systemeinstellungen > Trigger** Seite und wählen Sie den Auslöser aus, den Sie erstellt haben. Stellen Sie zunächst sicher, dass Ihr Gerät aktiv ist. Klicken Sie dann auf **Debug-Protokoll** Klicken Sie auf die Registerkarte, um zu sehen, ob der Auslöser Ihre Datensätze festschreibt. Im folgenden Beispiel haben wir bewusst nicht verfügbare Webseiten besucht, um 404-Fehler zu generieren.



Erstellen Sie ein benutzerdefiniertes Datensatzformat, um Ihre Datensatzergebnisse in einer Tabelle anzuzeigen

Datensatzformate sind die empfohlene Methode, um Ihre Datensätze nur mit den Feldern anzuzeigen, die Sie sehen möchten. Ohne ein benutzerdefiniertes Datensatzformat werden die Felder für Ihren benutzerdefinierten Datensatz in keiner auswählbaren Liste angezeigt, z. B. in der Liste Gruppieren nach.

Der schnellste Weg, ein benutzerdefiniertes Datensatzformat zu erstellen, besteht darin, das Schema beim Lesen aus einem integrierten Datensatzformat zu kopieren und in ein neues Datensatzformat einzufügen. Wenn Sie über mehrere Sensoren verfügen, müssen Sie das benutzerdefinierte Datensatzformat auf jeder Appliance erstellen, auf der die Aufzeichnungsergebnisse angezeigt werden. Sie können das Datensatzformat auf einer Konsole erstellen, um einen benutzerdefinierten Datensatz auf allen angeschlossenen Sensoren zu formatieren.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Formate aufzeichnen**.

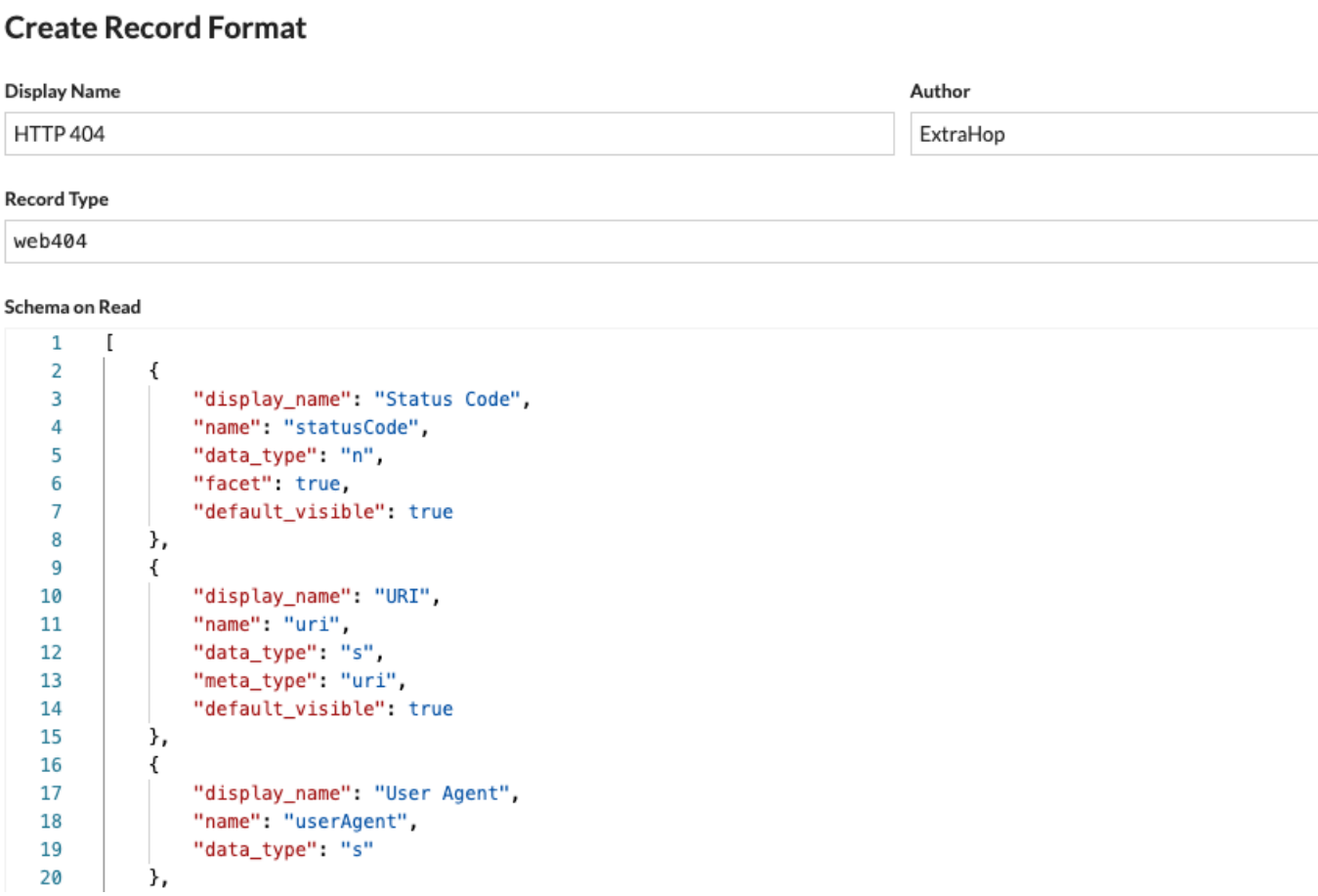
3. Klicken Sie auf den Datensatztyp, den Sie kopieren möchten. In unserem Beispiel kopieren wir das HTTP-Datensatzformat.
4. Kopieren Sie den Inhalt in das Textfeld unten Schema beim Lesen.
5. klicken **Neues Datensatzformat**.
6. Füllen Sie die folgenden Felder aus:

   • **Name anzeigen:** Geben Sie einen eindeutigen Namen für Ihr Datensatzformat ein.

   • **Autor:** Identifizieren Sie den Autor für das Datensatzformat.

   • **Art des Datensatzes:** Geben Sie dieselbe Datensatztyp-ID ein, die Sie im Auslöser erstellt haben. In unserem Beispiel ist dieser Wert `web404`.

   • **Schema beim Lesen:** Fügen Sie den kopierten Inhalt aus Schritt 4 in das Textfeld ein. Bearbeiten Sie das Feld, um alle unerwünschten Felder zu löschen. Für unser Beispiel in der Abbildung unten haben wir nur die folgenden Felder beibehalten: Client, Server, Methode, Statuscode, URI und Verarbeitungszeit.



Fragen Sie nach Ihrem benutzerdefinierten Datensatztyp ab

1. klicken **Rekorde** aus dem oberen Menü.
2. Klicken Sie auf **Beliebiger Datensatztyp** Drop-down-Liste und wählen Sie Ihr neu erstelltes Datensatzformat aus.
3. klicken **Aufzeichnungen ansehen**.
4. Klicken Sie auf **Ausführliche Ansicht** Ikone.
5. klicken **Felder** und dann klicken **Alles auswählen**.

Alle vom Auslöser gesammelten Informationen zu diesen Datensätzen werden in den Abfrageergebnissen angezeigt.

Einstellungen für das Aufnahmeformat

Das Einstellungen für das Aufnahmeformat Auf dieser Seite wird eine Liste aller integrierten und benutzerdefinierten Aufnahmeformate angezeigt, die auf Ihren ExtraHop-Sensoren oder der ExtraHop-Konsole verfügbar sind. Wenn Sie ein benutzerdefiniertes Datensatzformat erstellen müssen, empfehlen wir Ihnen, das Schema zu kopieren und einzufügen, wenn Sie Informationen aus einem integrierten Datensatzformat lesen. Fortgeschrittene Benutzer möchten möglicherweise ein benutzerdefiniertes Datensatzformat mit ihren eigenen Feld-Wert-Paaren erstellen und sollten das in diesem Abschnitt bereitgestellte Referenzmaterial verwenden.

Aufzeichnungsformate bestehen aus den folgenden Einstellungen:

Name anzeigen

Der Name, der für das Datensatzformat im ExtraHop-System angezeigt wird. Wenn für den Datensatz kein Datensatzformat vorhanden ist, wird der Datensatztyp angezeigt.

Autor

(Optional) Der Autor des Datensatzformat. Alle integrierten Aufnahmeformate werden angezeigt `ExtraHop` als Autor.

Typ des Datensatzes

Ein eindeutiger alphanumerischer Name, der den Informationstyp identifiziert, der im zugehörigen Datensatzformat enthalten ist. Der Datensatztyp verknüpft das Datensatzformat mit den Datensätzen, die an den Recordstore gesendet werden. Integrierte Datensatzformate haben einen Datensatztyp, der mit einer Tilde (~) beginnt. Benutzerdefinierte Datensatzformate können keinen Datensatztyp haben, der mit einer Tilde (~) oder einem At-Symbol (@) beginnt.

Schema beim Lesen

Ein JSON-formatiertes Array mit mindestens einem Objekt, das aus einem Feldnamen und einem Wertepaar besteht. Jedes Objekt beschreibt ein Feld im Datensatz und jedes Objekt muss eine eindeutige Kombination aus Name und Datentyp für dieses Datensatzformat haben. Sie können die folgenden Objekte für ein benutzerdefiniertes Datensatzformat erstellen:

Name

Der Name des Feldes.

Anzeigename

Der Anzeigename für das Feld. Wenn der `display_name` Feld ist leer, das `name` Feld wird angezeigt.

Beschreibung

(Optional) Beschreibende Informationen zum Datensatzformat. Dieses Feld ist auf die Seite mit den Datensatzformateinstellungen beschränkt und wird in keiner Datensatzabfrage angezeigt.

Standard_sichtbar

(Optional) Wenn gesetzt auf `true`, dieses Feld wird im ExtraHop-System standardmäßig als Spaltenüberschrift in der Tabellenansicht angezeigt.

Facette

(Optional) Wenn gesetzt auf `true`, Facetten für dieses Feld werden im ExtraHop-System angezeigt. Facetten sind eine kurze Liste der häufigsten Werte für das Feld, auf die geklickt werden kann, um einen Filter hinzuzufügen.

datentyp

Die Abkürzung, die den in diesem Feld gespeicherten Datentyp identifiziert. Die folgenden Datentypen werden unterstützt:

Datentyp	Abkürzung	Beschreibung
Anwendung	`app`	ExtraHop-Anwendungs-ID (Zeichenfolge)
boolesch	`b`	Boolescher Wert
Gerät	`dev`	ExtraHop Geräte-ID (Zeichenfolge)
Flussschnittstelle	`fint`	Flow-Schnittstellen-ID
Flussnetz	`fnet`	Flow-Netzwerk-ID
IPv4	`addr4`	Eine IPv4-Adresse im Quad-Format mit Punkten. Filter, die größer oder kleiner sind, werden unterstützt.
IPv6	`addr6`	Eine IPv6-Adresse. Nur zeichenfolgenorientierte Filter werden unterstützt.
Nummer	`n`	Zahl (Ganzzahl oder Gleitkomma)
Schnur	`s`	Generische Zeichenfolge

meta_type

Die Unterklassifizierung des Datentyps, die weiter bestimmt, wie die Informationen im ExtraHop-System angezeigt werden. Die folgenden Metatypen werden für jeden der zugehörigen Datentypen unterstützt:

Datentyp	Metatyp
Schnur	• `domain` • `uri` • `user`
Zahl	• `bytes` • `count` • `expiration` • `milliseconds` • `packets` • `timestamp`

Datensatzabfragen für benutzerdefinierte Metriken aktivieren

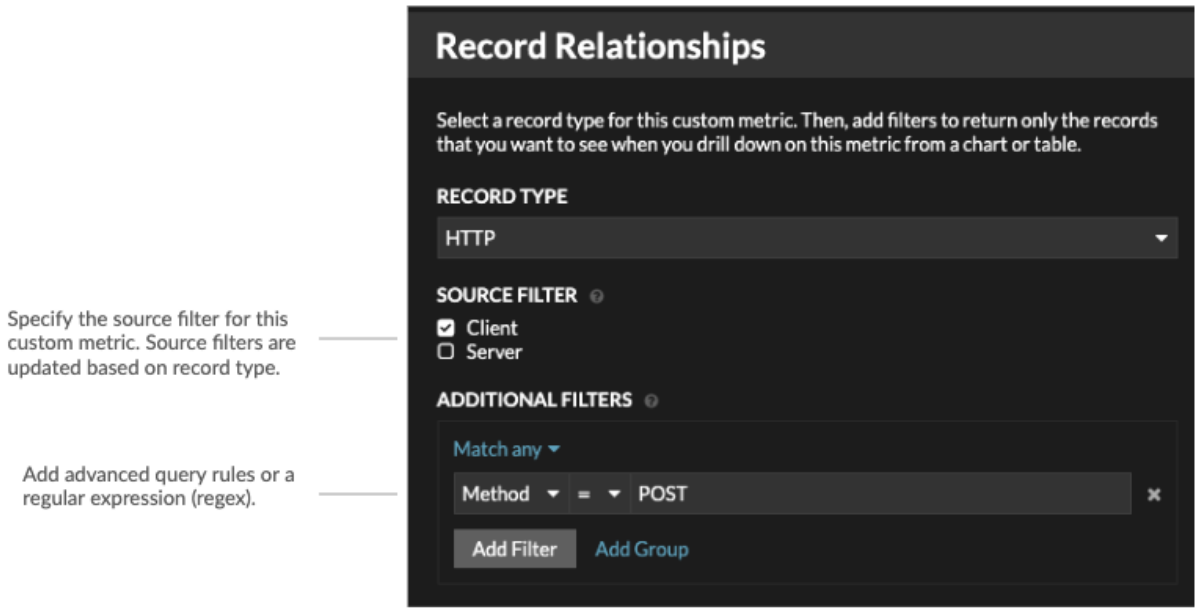
Benutzerdefinierte Metriken werden in der Regel erstellt, um spezifische Informationen über Ihre Umgebung zu sammeln. Sie können Einstellungen konfigurieren, mit denen Sie Datensätze auf Transaktionsebene, die einer benutzerdefinierten Metrik zugeordnet sind, abfragen und abrufen können. Im Metrikkatalog können Sie im Bereich Datensatzbeziehungen eine benutzerdefinierte Metrik einem Datensatztyp zuordnen. Wenn Sie nach Datensätzen aus dieser benutzerdefinierten Metrik abfragen würden, würden Sie Ergebnisse für alle Datensätze dieses Datensatztyps zurückgeben, unabhängig von den anderen Attributen, die für Ihre benutzerdefinierte Metrik konfiguriert sind. Wir empfehlen Ihnen, Filter hinzuzufügen, um aussagekräftige Ergebnisse für Ihre Datensatzabfragen zurückzugeben.

Wenn Sie im Metrikkatalog einen Quellfilter einrichten, filtern Sie Datensätze automatisch nach der Quelle, von der Sie einen Drilldown durchgeführt haben. Wenn Sie beispielsweise ein Kontrollkästchen neben Server aktivieren, wenn Sie Datensätze für diese benutzerdefinierte Metrik von einem Webserver mit dem Namen abfragen `example-web-sea`, Ihrer Abfrage wird automatisch ein Filter hinzugefügt, der nur Ergebnisse für Transaktionen zurückgibt, bei denen `example-web-sea` fungiert als Server.

Durch das Einstellen erweiterter Filter filtern Sie Datensätze automatisch nach den angegebenen Kriterien. Erweiterte Filter sind komplex und können auf vier Ebenen verschachtelt werden.

Bevor Sie beginnen
Erstellen Sie eine benutzerdefinierte Metrik

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Metrischer Katalog**.
3. Geben Sie in der oberen linken Ecke den Namen der benutzerdefinierten Metrik ein und klicken Sie dann in den Ergebnissen auf den Namen der benutzerdefinierten Metrik.
   Die Parameter für die benutzerdefinierte Metrik werden im rechten Bereich angezeigt.
4. Scrollen Sie im rechten Bereich nach unten zum Abschnitt Datensatzbeziehungen und klicken Sie auf die Dropdownliste DATENSATZTYP.
5. Klicken Sie in der Liste auf einen oder mehrere Datensatztypen und klicken Sie dann auf eine Stelle außerhalb der Liste , um Ihre Auswahl zu übernehmen. Zusätzliche Optionen zum Filtern von Datensatzfeldern werden unter den ausgewählten Datensatztypen angezeigt.



6. Optional: Aktivieren Sie im Abschnitt QUELLFILTER das Kontrollkästchen neben dem Quelltyp, z. B. Client oder Anwendung. Diese Quellen werden basierend auf den ausgewählten Datensatztypen dynamisch aktualisiert.
7. Optional: Geben Sie im Feld ZUSÄTZLICHE FILTER mehrere Kriterien mit den Operatoren OR (Beliebige Übereinstimmung), UND (Alle erfüllen) und KEINE an, um ein erweiterter Abfragefilter oder geben Sie ein regulärer Ausdruck (Regex) um Datensätze nach benutzerdefinierten Detailmetriken zu filtern.
8. klicken **Aktualisiere**.

Mit der benutzerdefinierten Metrik können Sie jetzt von jedem Diagramm oder jeder Detailseite aus nach Datensätzen abfragen.

Nächste Schritte

- Erstellen Sie eine Datensatzabfrage für Ihre benutzerdefinierte Metrik, indem Sie in einem Diagramm auf die Metrik klicken und dann auf **Rekorde**.

Pakete

Ein Netzwerkpaket ist eine kleine Datenmenge, die über TCP/IP-Netzwerke (Transmission Control Protocol/Internet Protocol) gesendet wird. Das ExtraHop-System ermöglicht es Ihnen, diese Pakete kontinuierlich mit einer Trace-Appliance zu sammeln, zu durchsuchen und herunterzuladen. Dies kann nützlich sein, um Netzwerkeinbrüche und andere verdächtige Aktivitäten zu erkennen.

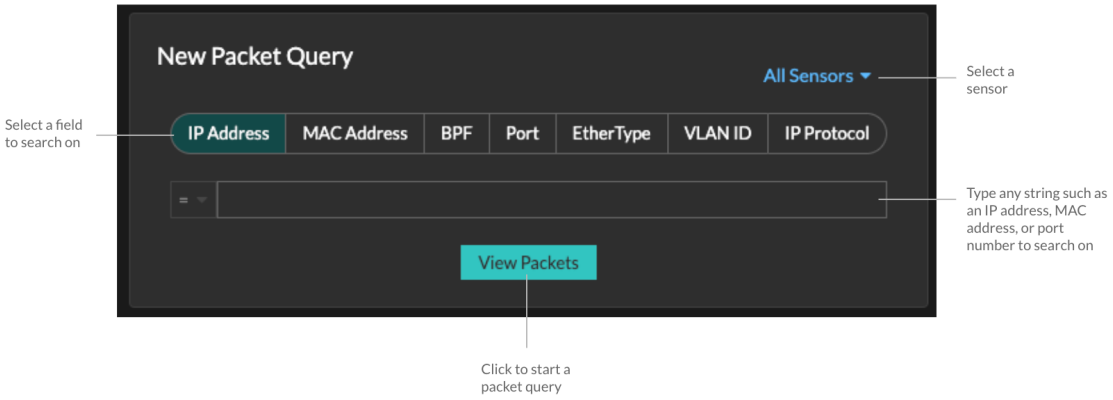
Sie können auf der Seite Pakete im ExtraHop-System nach Paketen suchen und diese herunterladen und über Paketsuche Ressource in der ExtraHop REST-API. Heruntergeladene Pakete können dann mit einem Drittanbieter-Tool wie Wireshark analysiert werden.

Hinweis: Wenn Sie keine Trace-Appliance haben, können Sie Pakete trotzdem über löst aus. siehe Initiieren Sie präzise Paketerfassungen, um Bedingungen ohne Fenster zu analysieren für ein Beispiel.

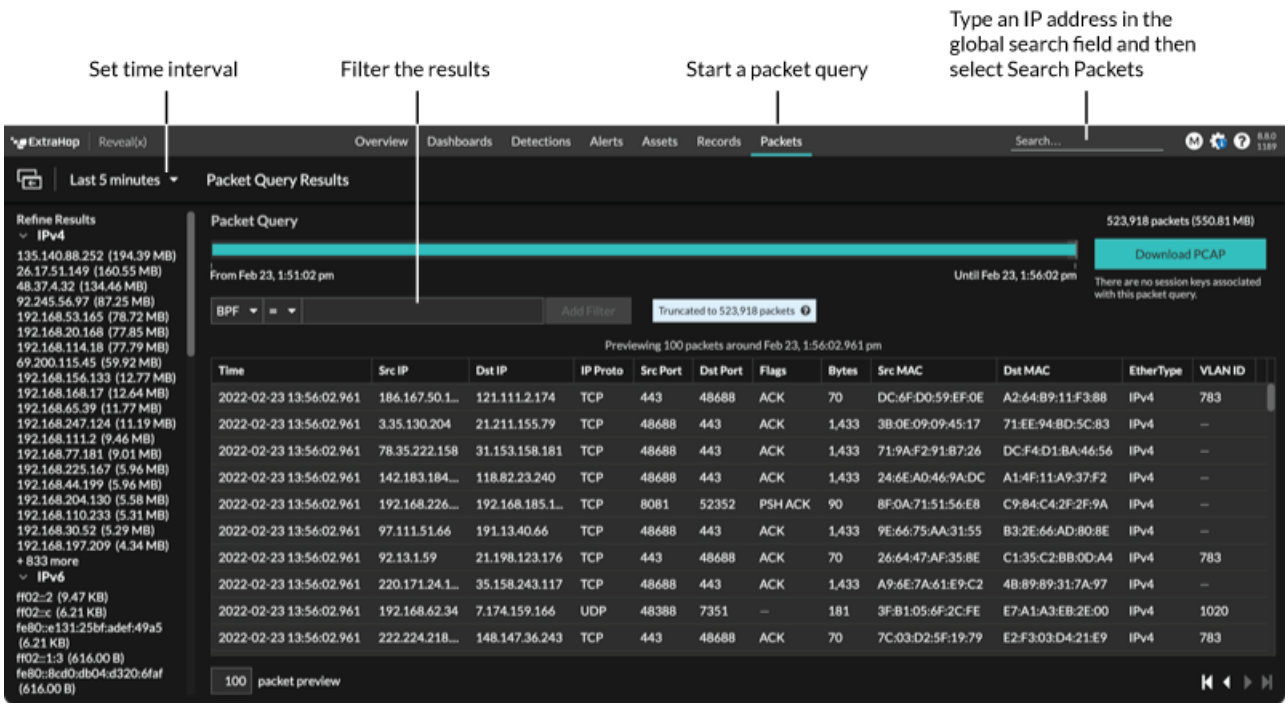
Video: Sehen Sie sich die entsprechende Schulung an: Pakete

In Paketen navigieren

Klicken Sie **Pakete** aus dem oberen Menü, um eine neue Paketabfrage zu erstellen. Auf der Seite Neue Paketabfrage können Sie einen Filter angeben.



Die Ergebnisse erscheinen auf der Hauptseite Pakete Seite. Starten Sie eine weitere Paketabfrage, indem Sie auf **Pakete** wieder aus dem Hauptmenü.



Wenn Sie das Zeitintervall ändern, beginnt die Abfrage erneut. An beiden Enden des grauen Balkens wird ein Zeitstempel angezeigt, der durch das aktuelle Zeitintervall bestimmt wird. Die Uhrzeit auf der rechten Seite zeigt den Startpunkt der Abfrage an und die Uhrzeit auf der linken Seite zeigt den Endpunkt der Abfrage an. Der blaue Balken gibt den Zeitraum an, in dem das System Pakete gefunden hat. Sie können einen Zeitraum in der blauen Leiste durch Ziehen vergrößern, um eine Abfrage für das ausgewählte Zeitintervall erneut auszuführen.

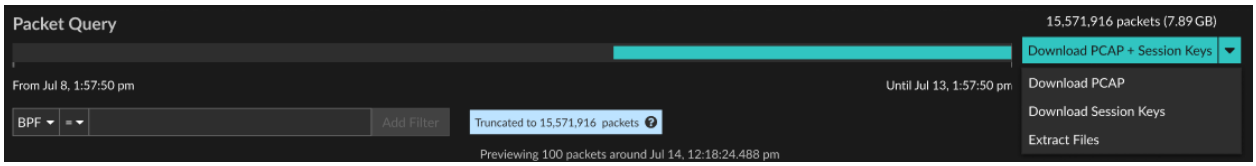
Hinweis: Pakete mit der Berkeley-Paketfilter-Syntax filtern.

Hinweis: Sie können nur Pakete anzeigen, die den von Ihrem ExtraHop-Administrator gewährten Rechten entsprechen. Wenn Sie Ihre erwarteten Abfrageergebnisse nicht sehen, wenden Sie sich an Ihren ExtraHop-Administrator.

Pakete werden heruntergeladen

Sie können die Abfrageergebnisse zusammen mit den TLS-Sitzungsschlüsseln und den Paketen zugehörigen Dateien zur Analyse in eine Paketerfassungsdatei (PCAP-Datei) herunterladen.

Download-Optionen sind im Drop-down-Menü oben rechts verfügbar. Klicken Sie auf eine Option, damit Ihr Browser die Datei auf Ihren lokalen Computer herunterladen kann.



Hier sind einige Überlegungen zum Herunterladen von Paketen und Extrahieren von Dateien:

- Die im Dropdownmenü angezeigten Download-Optionen hängen von Ihren Abfrageergebnissen ab. Wenn den Paketen beispielsweise keine Sitzungsschlüssel zugeordnet sind, werden möglicherweise nur Optionen zum Herunterladen von PCAP und zum Extrahieren von Dateien angezeigt.
- Downloads enthalten nur Pakete, die den von Ihrem ExtraHop-Administrator gewährten Rechten entsprechen. Wenn Sie beispielsweise zwei Sensoren abfragen, aber von Ihrem Administrator

eingeschränkter Zugriff auf einen der Sensoren zugewiesen wurde, enthält Ihr Download nur die Paket-Header des Sensor mit beschränktem Zugriff.

- Wenn du Sitzungsschlüssel herunterladen, können Sie die Paketerfassungsdatei in einem Tool wie Wireshark öffnen, das die Sitzungsschlüssel anwenden und die entschlüsselten Pakete anzeigen kann.
- Dateiextraktion (auch bekannt als File Carving) ist verfügbar, wenn Dateien in Paketen mit HTTP- oder SMB-Einträgen beobachtet werden.

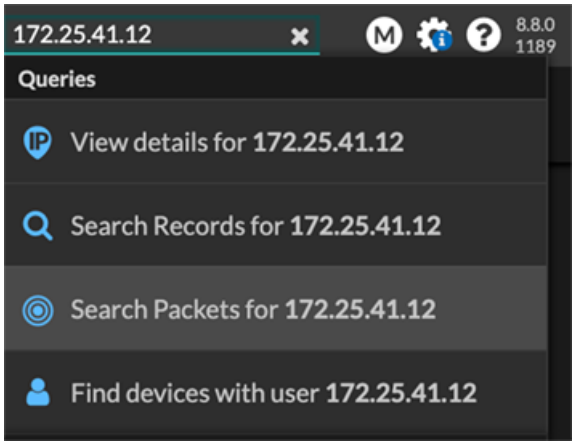
  Hinweis: Auf der Seite „ Datensätze“ können Sie nach HTTP- oder SMB-Datensatztypen suchen und nach beobachteter Datei filtern. Klicken Sie auf das Paketsymbol neben dem Datensatz, der Dateien enthält, die Sie extrahieren möchten.
- Extrahierte Dateien werden in einer ZIP-Datei heruntergeladen und enthalten unverschlüsselten Originalinhalt, der schädliche Daten enthalten kann. Zum Öffnen der entpackten ZIP-Dateien ist ein Passwort erforderlich. Das Passwort ist in der RevealX Enterprise oder RevealX 360 Administrationseinstellungen und können von Ihrem ExtraHop-Administrator abgerufen werden.
- Wenn Sie Ihre erwarteten Download-Optionen nicht sehen, wenden Sie sich an Ihren ExtraHop-Administrator. Sie haben keinen oder nur eingeschränkten Zugriff auf Sensoren, die Ihnen nicht über die Sensorzugriffskontrolle zugewiesen wurden. Darüber hinaus können Ihre Download-Optionen durch Modulzugriff und Benutzerrechte eingeschränkt werden. Der Modulzugriff und die für jede Download-Option erforderlichen Rechte werden in der folgenden Tabelle beschrieben:

Option herunterladen	Modul erforderlich	Rechte für Paketforensik erforderlich
PCAP+-Sitzungsschlüssel herunterladen	NDR oder NPM	Pakete und Sitzungsschlüssel
PCAP herunterladen	NDR oder NPM	Nur Pakete
PCAP-Header herunterladen	NDR oder NPM	Nur Paket-Header
PCAP-Slices herunterladen	NDR oder NPM	Nur Paketsegmente
Sitzungsschlüssel herunterladen	NDR oder NPM	Pakete und Sitzungsschlüssel
Dateien extrahieren	NDR	Nur Pakete oder Pakete und Sitzungsschlüssel

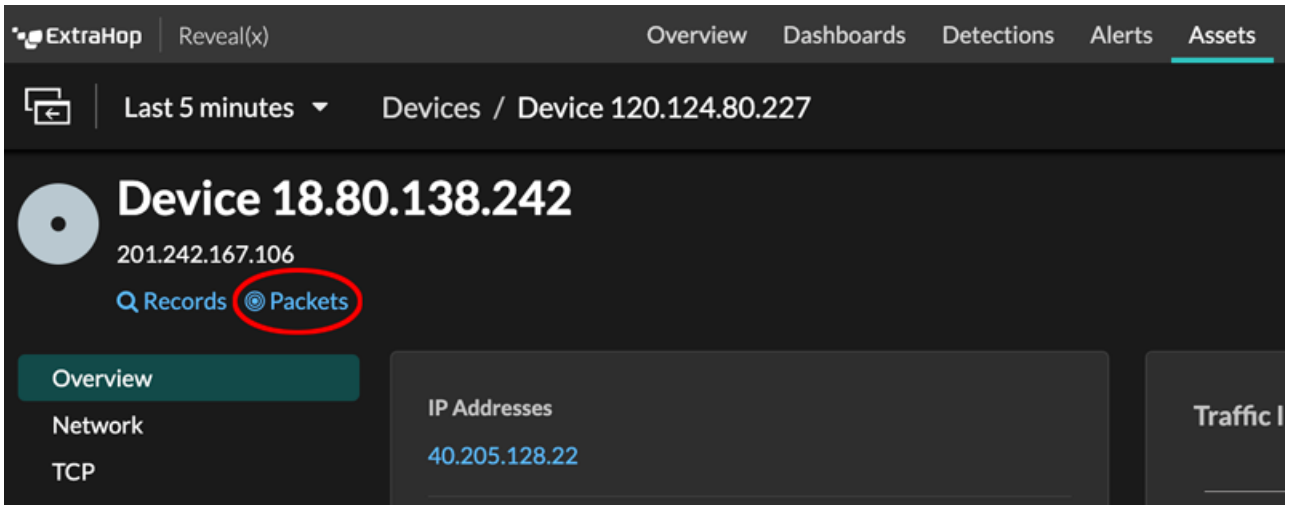
Pakete im ExtraHop-System abfragen

Die Seite Pakete bietet zwar schnellen Zugriff, um alle Pakete abzufragen, aber es gibt Indikatoren und Links, über die Sie im gesamten ExtraHop-System eine Paketabfrage starten können.

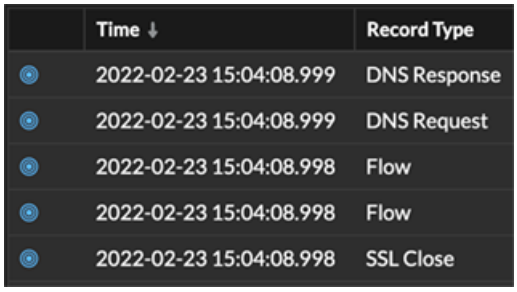
- Geben Sie eine IP-Adresse in das globale Suchfeld ein und wählen Sie dann das Symbol Pakete durchsuchen .



- Klicken Sie **Pakete** auf einer Geräteseite.

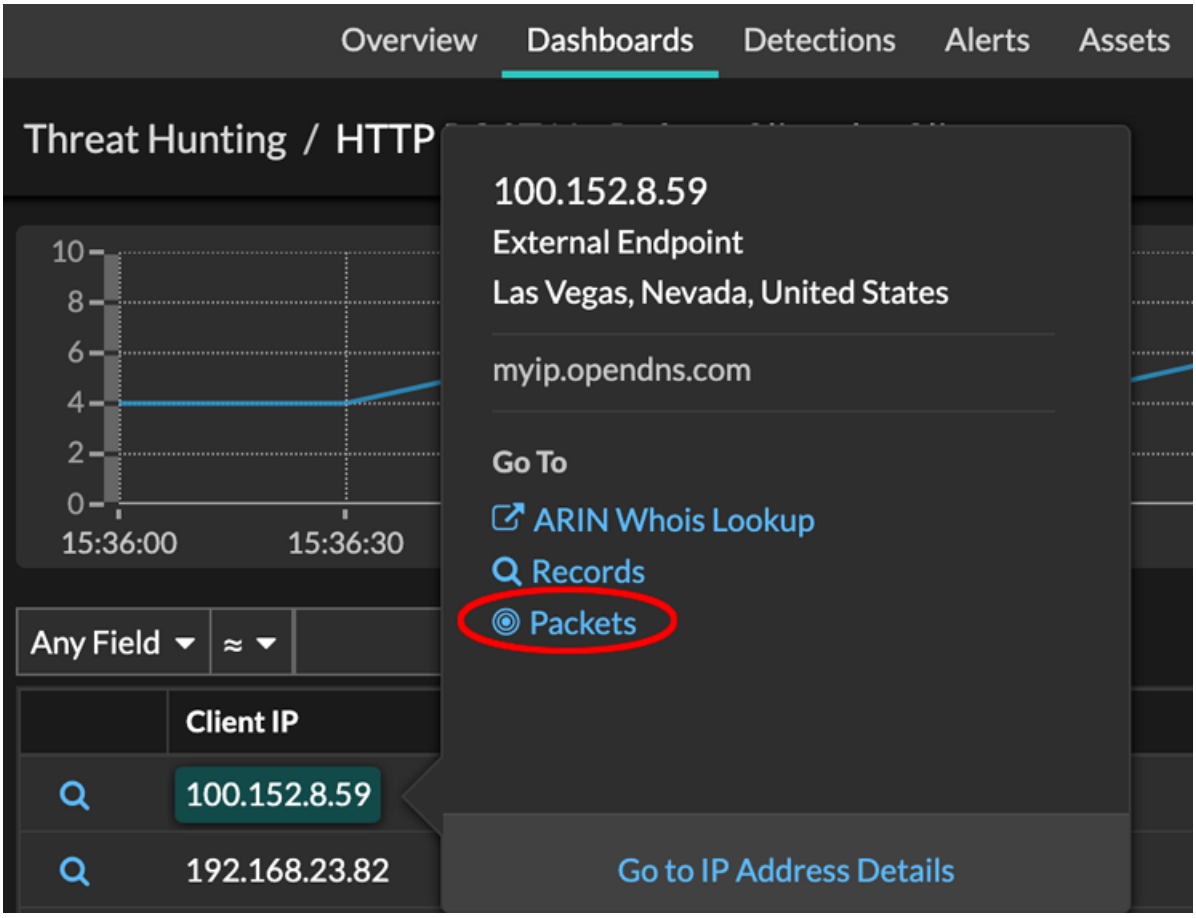


- Klicken Sie auf das Paketsymbol neben einem beliebigen Datensatz auf der Ergebnisseite einer Datensatzabfrage.



	Time ↓	Record Type
	2022-02-23 15:04:08.999	DNS Response
	2022-02-23 15:04:08.999	DNS Request
	2022-02-23 15:04:08.998	Flow
	2022-02-23 15:04:08.998	Flow
	2022-02-23 15:04:08.998	SSL Close

- Klicken Sie in einem Diagramm mit Metriken für Netzwerkbytes oder Pakete nach IP-Adresse auf eine IP-Adresse oder einen Hostnamen, um ein Kontextmenü aufzurufen. Klicken Sie dann auf das Paketsymbol um das Gerät und das Zeitintervall abzufragen.



Konfigurieren Sie eine globale PCAP

Eine globale PCAP erfasst jedes Paket, das an das ExtraHop-System gesendet wird, für die Dauer, die den Kriterien entspricht.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Paketerfassung Abschnitt, klicken **Globale Paketerfassung**.

   Bei der Konfiguration der PCAP müssen Sie nur die gewünschten Kriterien für die Paketerfassung angeben.
3. In der Name Feld, geben Sie einen Namen ein, um die Paketerfassung zu identifizieren.
4. In der Max. Pakete Feld, geben Sie die maximale Anzahl der zu erfassenden Pakete ein.
5. In der Max. Byte Feld, geben Sie die maximale Anzahl der zu erfassenden Byte ein.
6. In der Max. Dauer (Millisekunden) Feld, geben Sie die maximale Dauer der PCAP in Millisekunden ein.

   ExtraHop empfiehlt den Standardwert 1000 (1 Sekunde). Der Maximalwert beträgt bis zu 60000 Millisekunden (1 Minute).
7. In der Schnappschuss Feld, geben Sie die maximale Anzahl der pro Frame kopierten Byte ein.

   Der Standardwert ist 96 Byte, aber Sie können diesen Wert auf eine Zahl zwischen 1 und 65535 setzen.
8. Klicken Sie **Starten**.

Hinweis: Notieren Sie sich den Zeitpunkt, zu dem Sie mit der Erfassung beginnen, um das Auffinden der Pakete zu erleichtern.

9. Klicken Sie **Stopp** um die Paketerfassung zu stoppen, bevor eine der Höchstgrenzen erreicht wird.

Laden Sie Ihre PCAP herunter.

- Klicken Sie auf RevealX Enterprise-Systemen auf **Pakete** aus dem Hauptmenü und dann auf **PCAP herunterladen**.

  Um das Auffinden Ihrer PCAP zu erleichtern, klicken und ziehen Sie auf die Zeitleiste der Paketabfrage, um den Zeitraum auszuwählen, in dem Sie die PCAP gestartet haben.
- Klicken Sie auf ExtraHop Performance-Systemen auf das Symbol Systemeinstellungen, klicken **Die gesamte Verwaltung**, und klicken Sie dann auf **Paketerfassungen anzeigen und herunterladen** im Abschnitt Paketerfassung.

Analysieren Sie eine Paketerfassungsdatei

Der Offline-Erfassungsmodus ermöglicht es Administratoren, eine mit einer Paketanalyse-Software wie Wireshark oder tcpdump aufgezeichnete Capture-Datei in das ExtraHop-System hochzuladen und zu analysieren.

Hier sind einige wichtige Überlegungen, bevor Sie den Offline-Aufnahmemodus aktivieren:

- Wenn die Erfassung in den Offline-Modus versetzt wird, wird der Systemdatenspeicher zurückgesetzt. Alle zuvor aufgezeichneten Metriken werden aus dem Datenspeicher gelöscht. Wenn das System in den Online-Modus versetzt wird, wird der Datenspeicher erneut zurückgesetzt.
- Im Offline-Modus werden keine Metriken von der Erfassungsoberfläche erfasst, bis das System wieder in den Online-Modus versetzt wird.
- Es werden nur Erfassungsdateien im PCAP-Format unterstützt. Andere Formate wie pcpapng werden nicht unterstützt.

Stellen Sie den Offline-Aufnahmemodus ein

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.
3. klicken **Offline-Capture-Datei**.
4. Wählen **Upload** und dann klicken **Speichern**.
5. klicken **OK** um das Zurücksetzen des Datenspeichers zu bestätigen.
   Der Erfassungsvorgang wird gestoppt, der Erfassungsstatus wird auf Offline gesetzt und der Datenspeicher wird von allen Daten gelöscht. Wenn das System die Erfassung in den Offline-Modus versetzt hat, Offline-Capture-Datei Seite erscheint.
6. klicken **Wählen Sie Datei**, navigieren Sie zu der Capture-Datei, die Sie hochladen möchten, wählen Sie die Datei aus, und klicken Sie dann auf **Öffnen**.
7. klicken **Upload**.
   Das ExtraHop-System zeigt die Seite mit den Offline-Capture-Ergebnissen an , wenn die Capture-Datei erfolgreich hochgeladen wurde.
8. klicken **Ergebnisse ansehen** um die Paketerfassungsdatei so zu analysieren, als ob sich das System im Live-Capture-Modus befindet.

Bringen Sie das System in den Live-Aufnahmemodus zurück

1. In der Konfiguration des Systems Abschnitt, klicken **Aufnehmen (offline)**.
2. klicken **Capture neu starten**.
3. Wählen **Lebe**, und klicken Sie dann auf **Speichern**.

Das System entfernt die Leistungskennzahlen, die aus der vorherigen Erfassungsdatei gesammelt wurden, und bereitet den Datenspeicher für die Echtzeitanalyse über die Erfassungsoberfläche vor.

Pakete mit der Berkeley-Paketfilter-Syntax filtern

Suchen Sie nach Paketen mit der Berkeley Packet Filter (BPF) -Syntax allein oder in Kombination mit den integrierten Filtern.

Berkeley-Paketfilter sind eine einfache Schnittstelle zu Datenverbindungsebenen und ein leistungsstarkes Tool für die Analyse der Erkennung von Eindringlingen. Die BPF-Syntax ermöglicht es Benutzern, Filter zu schreiben, die schnell nach bestimmten Paketen suchen, um die wichtigsten Informationen zu sehen.

Das ExtraHop-System erstellt einen synthetischen Paket-Header aus den Paketindexdaten und führt dann die BPF-Syntaxabfragen für den Paket-Header aus, um sicherzustellen, dass Abfragen viel schneller sind als das Scannen der gesamten Paketnutzlast. Beachten Sie, dass ExtraHop nur eine Teilmenge der BPF-Syntax unterstützt. siehe Unterstützte BPF-Syntax.

Die BPF-Syntax besteht aus einem oder mehreren Primitiven, denen ein oder mehrere Qualifikatoren vorangestellt sind. Primitive bestehen normalerweise aus einer ID (Name oder Nummer), der ein oder mehrere Qualifikatoren vorangestellt sind. Es gibt drei verschiedene Arten von Qualifikationsspielen:

Art

Qualifikatoren, die angeben, auf welchen Typ sich der ID-Name oder die ID-Nummer bezieht. Zum Beispiel `host`, `net`, `port`, und `portrange`. Wenn es kein Qualifikationsmerkmal gibt, `host` wird angenommen.

dir

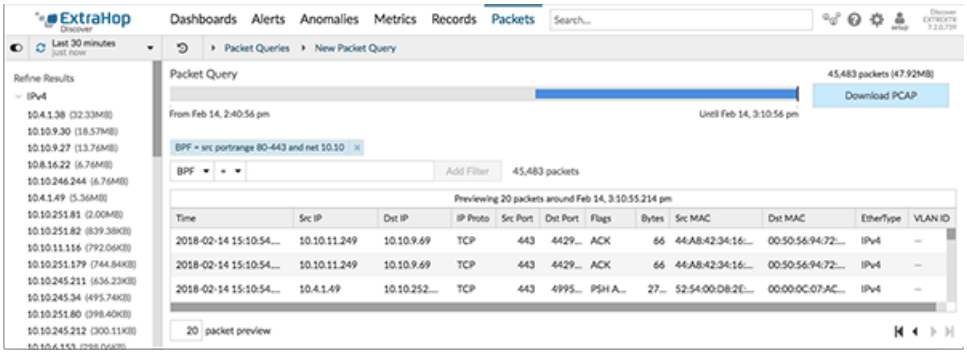
Qualifier, die eine bestimmte Übertragungsrichtung zu und/oder von einer ID angeben. Mögliche Richtungen sind `src`, `dst`, `src and dst`, und `src or dst`. Zum Beispiel `dst net 128.3`.

Proto

Qualifikatoren, die die Übereinstimmung auf das jeweilige Protokoll beschränken. Mögliche Protokolle sind `ether`, `ip`, `ip6`, `tcp`, und `udp`.

Fügen Sie einen Filter mit BPF-Syntax hinzu

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie im oberen Menü auf **Pakete**.
3. Wählen Sie im Bereich Dreifeld-Filter **BPF**, und geben Sie dann Ihre Filtersyntax ein. Geben Sie beispielsweise `src portrange 80-443 and net 10.10`.
4. klicken **PCAP herunterladen** um die PCAP mit Ihren gefilterten Ergebnissen zu speichern.



Unterstützte BPF-Syntax

Das ExtraHop-System unterstützt die folgende Teilmenge der BPF-Syntax zum Filtern von Paketen.

Hinweis

- ExtraHop unterstützt nur numerische IP-Adresssuchen. Hostnamen sind nicht erlaubt.
- Indizierung in Header, `[...]`, wird nur unterstützt für `tcpflags` und `ip_offset`. Zum Beispiel `tcp[tcpflags] & (tcp-syn|tcp-fin) != 0`

- ExtraHop unterstützt sowohl numerische als auch hexadezimale Werte für VLAN-ID-, EtherType- und IP-Protokollfelder. Stellen Sie Hexadezimalwerten 0x voran, z. B. 0x11.

Primitiv	Beispiele	Beschreibung
`[src|dst] host <host ip>`	`host 203.0.113.50` `dst host 198.51.100.200`	Entspricht einem Host als IP-Quelle, Ziel oder einer der beiden. Diese Host-Ausdrücke können in Verbindung mit anderen Protokollen wie ip, arp, rarp oder ip6 angegeben werden.
`ether [src|dst] host <MAC>`	`ether host 00:00:5E:00:53:00` `ether dst host 00:00:5E:00:53:00`	Entspricht einem Host als Ethernet-Quelle, Ziel oder einer der beiden.
`vlan <ID>`	`vlan 100`	Entspricht einem VLAN. Gültige ID-Nummern sind `0-4095`. Die VLAN-Prioritätsbits sind Null. Wenn das ursprüngliche Paket mehr als ein VLAN-Tag hatte, hat das synthetische Paket, mit dem der BPF übereinstimmt, nur das innerste VLAN-Tag.

`[src|dst] portrange <p1>-<p2>`
oder
`[tcp|udp] [src|dst] portrange <p1>-<p2>`
	`src portrange 80-88`
	`tcp dst portrange 1501-1549`
		Ordnet Pakete zu oder von einem Port im angegebenen Bereich zu. Protokolle können auf einen Portbereich angewendet werden, um bestimmte Pakete innerhalb des Bereichs zu filtern.

`[ip|ip6][src|dst] proto <protocol>`	`proto 1`
	`src 10.4.9.40 and proto ICMP`
	`ip6 and src fe80::aebc:32ff:fe84:70b7 and proto 47`
	`ip and src 10.4.9.40 and proto 0x0006`
		Entspricht anderen IPv4- oder IPv6-Protokollen als TCP und UDP. Das Protokoll kann eine Zahl oder ein Name sein.

`[ip|ip6][tcp|udp] [src|dst] port <port>`	`udp and src port 2005` `ip6 and tcp and src port 80`	Entspricht IPv4- oder IPv6-Paketen an einem bestimmten Port.

`[src|dst] net <network>`	`dst net 192.168.1.0`
	`src net 10`
	`net 192.168.1.0/24`
		Ordnet Pakete zu oder von einer Quelle oder einem Ziel oder beidem zu, die sich in einem Netzwerk befinden. Eine IPv4-Netzwerknummer kann als einer der folgenden Werte angegeben werden:
		• Gepunktetes Viereck (x.x.x.x)

Primitiv	Beispiele	Beschreibung
		• Dreifach gepunktet (x.x.x) • Gepunktetes Paar (x.x) • Einzelne Zahl (x)

`[ip|ip6] tcp tcpflags & (tcp-[ack|fin|syn|rst|push|urg|)`	`tcp[tcpflags] & (tcp-ack) !=0`
	`tcp[13] & 16 !=0`
	`ip6 and (ip6[40+13] & (tcp-syn) != 0)`
		Entspricht allen Paketen mit dem angegebenen TCP-Flag

Fragmentierte IPv4-Pakete (ip_offset! = 0)	`ip[6:2] & 0x3fff != 0x0000`	Stimmt mit allen Paketen mit Fragmenten überein.

Speichern Sie TLS-Sitzungsschlüssel in verbundenen Paketspeichern

Wenn die Weiterleitung von Sitzungsschlüsseln auf einem ExtraHop-System konfiguriert ist, das mit einem Packetstore verbunden ist, kann das ExtraHop-System verschlüsselte Sitzungsschlüssel zusammen mit den gesammelten Paketen speichern.

Bevor Sie beginnen
Erfahre mehr über Entschlüsseln von Paketen mit gespeicherten Schlüsseln.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.
3. Klicken Sie **Speicher für SSL-Sitzungsschlüssel**.
4. Wählen **SSL-Sitzungsschlüsselspeicher aktivieren**.
5. Klicken Sie **Speichern**.

Nächste Schritte

Weitere Hinweise zum Herunterladen von Sitzungsschlüsseln finden Sie unter Laden Sie Sitzungsschlüssel mit Paket herunter.

Laden Sie Sitzungsschlüssel mit Paket herunter

Sie können die PCAP Next Generation (pcapng) -Datei herunterladen, die alle erfassten TLS-Sitzungsschlüssel und verschlüsselten Pakete enthält. Anschließend können Sie die Paketerfassungsdatei in einem Tool wie Wireshark öffnen, das die Sitzungsschlüssel anwenden und die entschlüsselten Pakete anzeigen kann.

Bevor Sie beginnen

- Sie müssen über einen konfigurierten Packetstore oder eine Paketerfassungsdiskette verfügen, bevor Sie Pakete und Sitzungsschlüssel von einem herunterladen können Sensor oder ein Konsole. Sehen Sie unsere Bereitstellungsanleitungen um loszulegen.
- Das Konsole muss für TLS Shared Secrets lizenziert sein.
- Das TLS-Sitzungsschlüsselspeicher Die Einstellung muss am Sensor aktiviert sein.
- RevealX Enterprise-Benutzer müssen entweder über Systemzugriff und Administration verfügen Privilegien oder eingeschränkte Rechte mit Zugriff auf Pakete und Sitzungsschlüssel. RevealX 360-Benutzer müssen Zugriff auf Pakete und Sitzungsschlüssel haben.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.

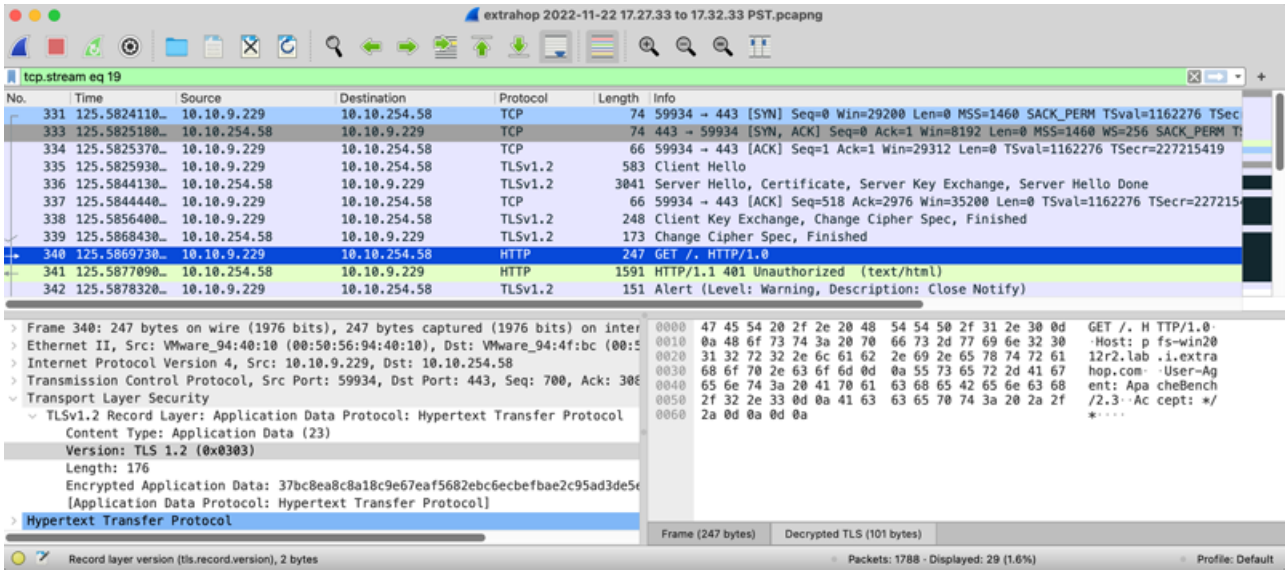
2. Klicken Sie im oberen Menü auf **Pakete**.
3. Optional: Wenden Sie Filter an, um die Paketabfrage zu verfeinern.
4. Wenn die Abfrage abgeschlossen ist, klicken Sie auf **PCAP+-Sitzungsschlüssel herunterladen**.
5. Klicken Sie **PCAP+-Sitzungsschlüssel herunterladen**.
   Die PCAPNG-Datei wird automatisch auf Ihren Computer heruntergeladen, und der Vorgang zum Herunterladen des Sitzungsschlüssels wird im Audit-Log.

   Wenn für die heruntergeladene PCAP keine Sitzungsschlüssel verfügbar sind, wird **PCAP+-Sitzungsschlüssel herunterladen** Die Schaltfläche wird nicht angezeigt.

Sehen Sie sich die entschlüsselte Nutzlast in Wireshark an

1. Starten Sie die Wireshark-Anwendung.
2. Öffnen Sie die heruntergeladene Paketerfassungsdatei (pcapng) in Wireshark.

Wenn ein SSL-verschlüsselter Frame ausgewählt ist, wird **Entschlüsseltes SSL** Die Registerkarte wird am unteren Rand des Wireshark-Fensters angezeigt. Klicken Sie auf die Registerkarte, um die entschlüsselten Informationen in der PCAP als Klartext anzuzeigen.



Trigger

Trigger bestehen aus benutzerdefiniertem Code, der bei Systemereignissen automatisch über die ExtraHop Trigger API ausgeführt wird. Sie können über die Trigger-API einen Trigger, bei dem es sich um einen JavaScript-Block handelt, schreiben, um benutzerdefinierte Wire-Data-Ereignisse und -Metriken zu extrahieren, zu speichern und zu visualisieren, die für Ihr Unternehmen, Ihre Infrastruktur, Ihr Netzwerk, Ihre Kunden und Geschäftsanwendungen spezifisch sind.

Zu den gängigsten Workflows, die Sie über Trigger ausführen können, gehören die folgenden Operationen:

- Erstellen Sie eine Anwendung Container, in dem Metriken für bestimmte Geräte gesammelt werden. Anwendungscontainer erweitern die gerätebasierten Ansichten, die das ExtraHop-System standardmäßig erstellt.
- Erstellen benutzerdefinierte Metriken und speichern Sie sie im ExtraHop-Datenspeicher. Zum Beispiel User-Agent-Daten, die von einem generiert wurden HTTP Anfrage ist keine in das ExtraHop-System integrierte Metrik. Die ExtraHop Auslöser API bietet jedoch eine User-Agent-HTTP-Eigenschaft , mit der Sie einen Trigger schreiben können, der User-Agent-Daten als benutzerdefinierte Metrik sammelt.
- Generieren Aufzeichnungen und schreiben Sie sie zur langfristigen Speicherung und zum Abrufen in einen Datenspeicher.
- Senden Sie Daten an Syslog-Verbraucher wie Splunk oder an Datenbanken von Drittanbietern wie MongoDB oder Kafka, durch eine Datenstrom öffnen.
- Führen Sie eine Universal Payload Analysis (UPA) durch, um auf TCP- und UDP-Payloads zuzugreifen und diese von nicht unterstützten zu analysieren Protokolle.
- Initiieren Sie Paketerfassungen, um einzelne Datenflüsse auf der Grundlage benutzerdefinierter Kriterien Datensatz. Ihr ExtraHop-System muss für die PCAP lizenziert sein, um auf diese Funktion zugreifen zu können.

Um alle Auslöser anzuzeigen, klicken Sie auf **Systemeinstellungen** Symbol und klicken Sie dann **Trigger**. Auf der Seite „Auslöser“ können Sie einen Auslöser erstellen oder wählen Sie das Häkchen neben einem Auslöser, um Bearbeiten Sie die Triggerkonfiguration oder modifizieren Sie das Trigger-Skript.

Einen Auslöser planen

Das Schreiben eines Auslöser zur Erfassung benutzerdefinierter Metriken ist eine leistungsstarke Methode, um Ihre Anwendungs - und Netzwerkleistung zu überwachen. Trigger verbrauchen jedoch Systemressourcen und können die Systemleistung beeinträchtigen, und ein schlecht geschriebener Auslöser kann zu unnötiger Systemlast führen. Bevor Sie einen Auslöser erstellen, evaluieren Sie, was Ihr Auslöser erreichen soll, ermitteln Sie, welche Ereignisse und Geräte erforderlich sind, um die benötigten Daten zu extrahieren, und ermitteln Sie, ob bereits eine Lösung existiert.

- Identifizieren Sie die spezifischen Informationen, die Sie sammeln müssen, indem Sie die folgenden Arten von Fragen stellen:
  - Wann laufen meine TLS-Zertifikate ab?
  - Erhält mein Netzwerk Verbindungen über nicht autorisierte Ports?
  - Wie viele langsame Transaktionen hat mein Netzwerk?
  - Welche Daten möchte ich über einen offenen Datenstrom an Splunk senden?
- Überprüfen Sie die Metrischer Katalog um festzustellen, ob bereits eine integrierte Metrik vorhanden ist, die die benötigten Daten extrahiert. Integrierte Metriken belasten das System nicht zusätzlich.
- Identifizieren Sie welches System Veranstaltungen produzieren Sie die Daten, die Sie sammeln möchten. Beispielsweise kann ein Auslöser, der die Aktivität von Cloud-Anwendungen in Ihrer Umgebung überwacht, bei HTTP-Antworten und beim Öffnen und Schließen von TLS-Verbindungen ausgeführt werden. Eine vollständige Liste der Systemereignisse finden Sie in der ExtraHop Trigger API-Referenz.

- Machen Sie sich mit den API-Methoden und Eigenschaften vertraut, die in der ExtraHop Trigger API-Referenz . Bevor Sie beispielsweise mit der Planung Ihres Auslöser zu weit gehen, überprüfen Sie die Referenz, um sicherzustellen, dass die Eigenschaft, die Sie extrahieren möchten, verfügbar ist, oder um herauszufinden, welche Eigenschaften in einem Standard-SMB-Datensatz erfasst sind.
- Legen Sie fest, wie Sie die vom Auslöser gesammelten Daten visualisieren oder speichern möchten. Zum Beispiel können Sie Metriken auf einem Dashboard oder von Protokoll, Sie können Datensätze an den Recordstore senden.
- Stellen Sie fest, ob bereits ein Auslöser existiert, der Ihren Anforderungen entspricht oder leicht geändert werden kann. Beginnen Sie nach Möglichkeit immer mit einem bereits vorhandenen Auslöser. Suchen Sie in den folgenden Ressourcen nach einem vorhandenen Auslöser:
  - Bestehende Trigger auf der Seite „Trigger“
  - Die ExtraHop Community-Foren

Trigger bauen

Wenn Sie feststellen, dass Sie einen neuen Auslöser erstellen müssen, machen Sie sich mit den folgenden Aufgaben vertraut, die abgeschlossen werden müssen:

- Konfiguriere den Auslöser um Details wie den Triggernamen und ob das Debuggen aktiviert ist, bereitzustellen. Geben Sie vor allem an, bei welchen Systemereignissen der Auslöser ausgeführt wird. Wenn Sie beispielsweise möchten, dass Ihr Auslöser jedes Mal ausgeführt wird, wenn eine SSH-Verbindung geöffnet wird, geben Sie an `SSH_OPEN` als Triggerereignis.
- Schreiben Sie das Trigger-Skript, das die Anweisungen angibt, die der Auslöser ausführt, wenn ein für den Auslöser konfiguriertes Systemereignis eintritt. Das Trigger-Skript kann Anweisungen für eine einfache Aufgabe wie das Erstellen einer benutzerdefinierten Metrik zur Geräteanzahl namens „slow_rsp“ oder für komplexere Aufgaben wie die Überwachung und Erfassung von Statistiken über die Cloud-Anwendungen bereitstellen, auf die in Ihrer Umgebung zugegriffen wird.

Nachdem der Auslöser abgeschlossen ist und ausgeführt wird, ist es wichtig zu überprüfen, ob der Auslöser erwartungsgemäß funktioniert.

- Das Debug-Log anzeigen für die erwartete Ausgabe von Debug-Anweisungen im Trigger-Skript. Das Protokoll zeigt auch alle Laufzeitfehler und Ausnahmen an, die Sie beheben müssen.
- Überwachen Sie die Leistungskosten indem die Anzahl der vom Auslöser verbrauchten Zyklen verfolgt wird.
- Überprüfe die Diagramme zum Systemstatus für Trigger-Ausnahmen, Ausfälle aus der Trigger-Warteschlange und unerwartete Aktivitäten.
- Prüfen Sie, ob das Trigger-Skript den Leitfaden zu bewährten Methoden für Triggers.

Navigiere durch Trigger

Die Seite „Trigger“ enthält eine Liste der aktuellen Trigger mit den folgenden Informationen:

Name
Der benutzerdefinierte Name des Auslöser.

Autor
Der Name des Benutzers, der den Auslöser geschrieben hat. Standard-Trigger zeigen ExtraHop für dieses Feld an.

Beschreibung
Die benutzerdefinierte Beschreibung des Auslöser.

Zuweisungen
Die Geräte oder Gerätegruppen, denen der Auslöser zugewiesen ist.

Status
Ob der Auslöser aktiviert ist. Wenn der Auslöser aktiviert ist, wird auch die Anzahl der Gerätezuweisungen angezeigt.

Debug-Protokoll

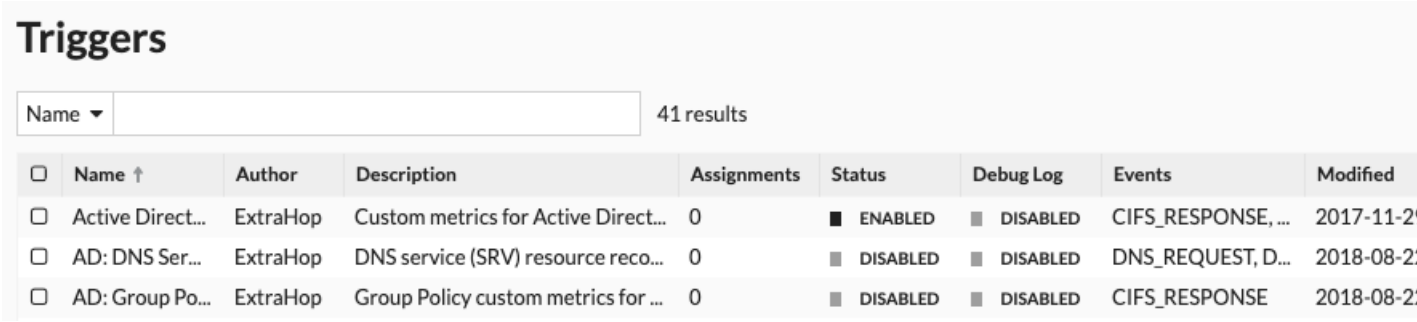
Ob Debugging aktiviert ist. Wenn das Debuggen aktiviert ist, werden die Ausgaben von Debug-Anweisungen im Triggerskript im Debug-Log-Ausgabe.

Ereignisse

Die Systemereignisse, die zur Ausführung des Auslöser führen, wie `HTTP_RESPONSE`.

Geändert

Das letzte Mal, dass der Auslöser geändert wurde.



Einen Auslöser erstellen

Trigger bieten erweiterte Funktionen Ihres ExtraHop-Systems. Mit Triggern können Sie benutzerdefinierte Metriken erstellen, Datensätze generieren und speichern oder Daten an ein Drittanbietersystem senden. Da Sie das Trigger-Skript schreiben, steuern Sie die Aktionen, die der Auslöser bei bestimmten Systemereignissen ausführt.

Um einen Auslöser zu erstellen, müssen Sie eine Trigger-Konfiguration erstellen, das Trigger-Skript schreiben und den Auslöser dann einer oder mehreren Metrikquellen zuweisen. Der Auslöser wird erst ausgeführt, wenn alle Aktionen abgeschlossen sind.

Bevor Sie beginnen
Melden Sie sich beim ExtraHop-System mit einem Benutzerkonto an, das über die vollständige Schreibberechtigung verfügt Privilegien erforderlich, um Trigger zu erstellen.

Wenn du mit Triggern noch nicht vertraut bist, Machen Sie sich mit dem Trigger-Planungsprozess vertraut, mit deren Hilfe Sie den Fokus Ihres Auslöser eingrenzen oder feststellen können, ob Sie überhaupt einen Auslöser erstellen müssen. Führen Sie dann den Prozess zum Erstellen eines Auslöser durch, indem Sie den Exemplarische Vorgehensweise für Trigger.

Trigger-Einstellungen konfigurieren

Der erste Schritt beim Erstellen eines Auslöser besteht darin, einen Triggernamen anzugeben, festzustellen, ob Debugging aktiviert ist, und vor allem zu identifizieren, bei welchen Systemereignissen der Auslöser ausgeführt wird.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Auslöser**.
3. klicken **Erstellen**.
4. Geben Sie die folgenden Einstellungen für die Trigger-Konfiguration an:

   Name

   Ein Name für den Auslöser.

   Autor

   Der Name des Benutzers, der den Auslöser geschrieben hat. Standard-Trigger zeigen ExtraHop an.

Beschreibung

Eine optionale Beschreibung des Auslöser.

Zuweisungen

Die Geräte oder Gerätegruppen, denen der Auslöser zugewiesen ist. Ein Auslöser wird erst ausgeführt, wenn er einem Gerät zugewiesen ist, und der Auslöser sammelt Metrikdaten nur von den Geräten, denen er zugewiesen ist.

Warnung: Das Ausführen von Triggern auf nicht benötigten Geräten und Netzwerken erschöpft die Systemressourcen. Minimiere die Auswirkungen auf die Leistung, indem du einen Auslöser nur den spezifischen Quellen zuweist, aus denen du Daten sammeln musst.

Wichtig: Trigger mit den folgenden Ereignissen werden immer dann ausgeführt, wenn das Ereignis eintritt. Trigger, die nur bei diesen Ereignissen ausgeführt werden, können Geräten oder Gerätegruppen nicht zugewiesen werden.

- ALERT_RECORD_COMMIT
- ERKENNUNGSUPDATE
- METRIC_CYCLE_BEGIN
- ENDE DES METRISCHEN ZYKLUS
- METRIC_RECORD_COMMIT
- NEUE_ANWENDUNG
- NEUES_GERÄT
- SITZUNG ABLAUFEN
- TIMER_30 SEK

Debug-Log aktivieren

Ein Kontrollkästchen, das das Debuggen aktiviert oder deaktiviert. Wenn Sie dem Trigger-Skript Debug-Anweisungen hinzufügen, können Sie mit dieser Option Debug-Ausgabe anzeigen im Debug-Log, wenn der Auslöser ausgeführt wird.

Ereignisse

Die Ereignisse, bei denen der Auslöser ausgeführt wird. Der Auslöser wird immer dann ausgeführt, wenn eines der angegebenen Ereignisse auf einem zugewiesenen Gerät eintritt. Daher müssen Sie Ihrem Auslöser mindestens ein Ereignis zuweisen. Sie können in das Feld klicken oder mit der Eingabe eines Veranstaltungsnamens beginnen, um eine gefilterte Liste der verfügbaren Ereignisse anzuzeigen.

Erweiterte Optionen

Erweiterte Trigger-Optionen variieren je nach den ausgewählten Ereignissen. Wenn Sie zum Beispiel die `HTTP_RESPONSE` Ereignis, Sie können die Anzahl der Nutzdatenbytes festlegen, die bei diesen Ereignissen zwischengespeichert werden sollen.

Schreiben Sie ein Trigger-Skript

Das Triggerskript gibt die Anweisungen an, die der Auslöser ausführt, wenn ein für den Auslöser konfiguriertes Systemereignis eintritt.

Bevor Sie beginnen

Wir empfehlen Ihnen, das zu öffnen ExtraHop Trigger API-Referenz, das die Ereignisse, Methoden und Eigenschaften enthält, die Sie für Ihren Auslöser benötigen. Ein Link ist auch im Trigger-Editor-Fenster im ExtraHop-System verfügbar.

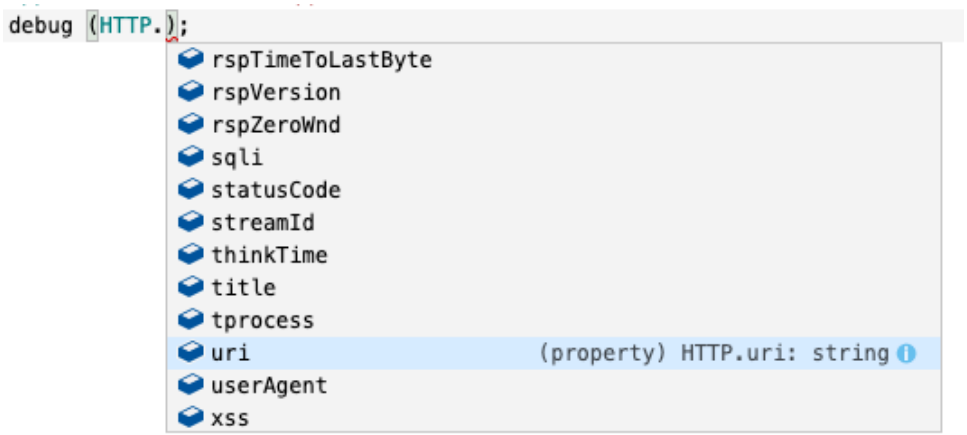
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen, und klicken Sie dann auf **Auslöser**.
3. klicken **Erstellen**.

4. Geben Sie im rechten Bereich das Triggerskript in JavaScript-ähnlicher Syntax mit Ereignissen, Methoden und Eigenschaften aus dem ExtraHop Trigger API-Referenz.

   Die folgende Abbildung zeigt ein Beispielskript, das auf der Registerkarte Editor eingegeben wurde:

```
1  if (HTTP.uri.match("seattle")){
2      Application("Seattle App").commit();
3      debug (HTTP.uri);
4  }
```

   Der Editor bietet eine Autocomplete-Funktion, die eine Liste von Eigenschaften und Methoden anzeigt, die auf dem ausgewählten Klassenobjekt basieren. Geben Sie beispielsweise einen Klassennamen und dann einen Punkt (.) ein, um eine Liste der verfügbaren Eigenschaften und Methoden anzuzeigen, wie in der folgenden Abbildung dargestellt:

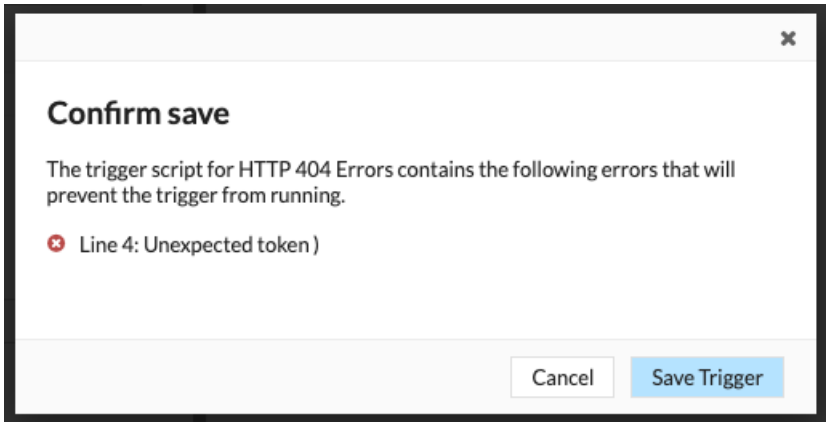


5. klicken **Speichern**.

   Der Editor bietet eine Syntaxvalidierung Ihres Skripts. Wenn Sie den Auslöser speichern, ruft der Validator alle ungültigen Aktionen, Syntaxfehler oder veralteten Elemente im Skript auf. Falls verfügbar, zeigt der Validator Ersetzungen für veraltete Elemente an.

   Warnung: Um eine schlechte Triggerleistung, falsche Ergebnisse oder einen Auslöser zu vermeiden, der nicht funktioniert, wird dringend empfohlen, den Code zu korrigieren oder das veraltete Element zu ersetzen.

   Die folgende Abbildung zeigt ein Beispiel für eine vom Syntaxvalidator generierte Fehlermeldung:



Erweiterte Trigger-Optionen

Sie müssen Trigger so konfigurieren, dass sie bei mindestens einem Ereignis ausgeführt werden. Je nach ausgewähltem Ereignis werden im Bereich „Trigger erstellen“ erweiterte Konfigurationsoptionen angezeigt. Wählen Sie zum Beispiel die HTTP_RESPONSE Ereignis ermöglicht es Ihnen, die Anzahl der Payload-Bytes festzulegen, die bei jedem Auftreten dieses Ereignis im System zwischengespeichert werden sollen.

In der folgenden Tabelle werden die verfügbaren erweiterten Optionen und die Ereignisse beschrieben, die jede Option unterstützen.

Option	Beschreibung	Unterstützte Ereignisse
Zu erfassende Byte pro Paket	Gibt die Anzahl der Byte an, die pro Paket erfasst werden sollen. Die Erfassung beginnt mit dem ersten Byte im Paket. Geben Sie diese Option nur an , wenn das Trigger-Skript die PCAP durchführt. Ein Wert von 0 gibt an, dass die Erfassung alle Byte in jedem Paket sammeln soll.	Alle Ereignisse außer der folgenden Liste werden unterstützt: • ALERT_RECORD_COMMIT • METRIC_CYCLE_BEGIN • METRIC_CYCLE_END • FLOW_REPORT • NEW_APPLICATION • NEW_DEVICE • SESSION_EXPIRE
L7-Nutzdaten-Bytes in den Puffer	Gibt die maximale Anzahl von Nutzdatenbytes an, die gepuffert werden sollen. **Hinweis:** Wenn mehrere Trigger für dasselbe Ereignis ausgeführt werden, bestimmt der Auslöser mi dem höchsten Wert für L Payload Bytes to Buffer die maximale Nutzlast für dieses Ereignis für jeden Auslöser.	• CIFS_REQUEST • CIFS_RESPONSE • HTTP_REQUEST • HTTP_RESPONSE • ICA_TICK • LDAP_RESPONSE
Byte aus der Zwischenablage	Gibt die Anzahl der Byte an, die bei einer Übertragung in die	• ICA_TICK

Option	Beschreibung	Unterstützte Ereignisse
	Citrix-Zwischenablage gepuffert werden sollen.	
Metrischer Zyklus	Gibt die Länge des Metrik Zyklus an, ausgedrückt in Sekunden. Der einzig gültige Wert ist `30sec`.	• `METRIC_CYCLE_BEGIN` • `METRIC_CYCLE_END` • `METRIC_RECORD_COMMIT`
Metrische Typen	Gibt den Metriktyp anhand des Rohmetriknamens an, z. B. `extrahop.device.http_server`. Geben Sie mehrere Metriktypen in einer kommagetrennten Liste an.	• `ALERT_RECORD_COMMIT` • `METRIC_RECORD_COMMIT`
Auslöser bei jedem Flow-Turn ausführen	Aktiviert die PCAP auf jedem Fluss drehen. Die Per-Turn-Analyse analysiert kontinuierlich die Kommunikation zwischen zwei Endpunkten, um einen einzelnen Nutzdatenpunkt aus dem Datenfluss zu extrahieren. Wenn diese Option aktiviert ist, werden alle angegebenen Werte für **Übereinstimmende Zeichenfolge für den Client** und **Passende Zeichenfolge für den Server** Optionen werden ignoriert.	• `SSL_PAYLOAD` • `TCP_PAYLOAD`
Portbereich des Clients	Gibt den Portbereich des Client an. Gültige Werte liegen zwischen 0 und 65535.	• `SSL_PAYLOAD` • `TCP_PAYLOAD` • `UDP_PAYLOAD`
Client-Bytes in den Puffer	Gibt die Anzahl der Client-Bytes an, die gepuffert werden sollen. Der Wert dieser Option kann nicht auf 0 gesetzt werden, wenn der Wert von **Server-Bytes zum Puffer** Die Option ist ebenfalls auf 0 gesetzt.	• `SSL_PAYLOAD` • `TCP_PAYLOAD`
Suchzeichenfolge für den Client-Puffer	Gibt die Formatzeichenfolge an, die angibt, wann mit dem Puffern der Client-Daten begonnen werden soll. Gibt bei einer Zeichenkettenübereinstimmung das gesamte Paket zurück.	• `SSL_PAYLOAD` • `TCP_PAYLOAD` • `UDP_PAYLOAD`

Option	Beschreibung	Unterstützte Ereignisse
	Sie können die Zeichenfolge als Text oder Hexadezimalzahlen angeben. Zum Beispiel beide `ExtraHop` und `\x45\x78\x74\x72\x61\x48\x6F\x70` sind gleichwertig. Hexadezimalzahlen unterscheiden nicht zwischen Groß- und Kleinschreibung. Jeder für diese Option angegebene Wert wird ignoriert , wenn **Pro Spielzug** oder **Auslöser auf allen UDPs ausführen** Die Option Pakete ist aktiviert.	
Server-Port-Bereich	Gibt den Serverportbereich an. Gültige Werte liegen zwischen 0 und 65535.	• SSL_PAYLOAD • TCP_PAYLOAD • UDP_PAYLOAD
Server-Bytes in Puffer	Gibt die Anzahl der Server-Bytes an, die gepuffert werden sollen. Der Wert dieser Option kann nicht auf 0 gesetzt werden, wenn der Wert von **Client-Bytes zum Puffer** Die Option ist ebenfalls auf 0 gesetzt.	• SSL_PAYLOAD • TCP_PAYLOAD
Suchzeichenfolge für Serverpuffer	Gibt die Formatzeichenfolge an, die angibt, wann mit dem Puffern der Serverdaten begonnen werden soll. Sie können die Zeichenfolge als Text oder Hexadezimalzahlen angeben. Zum Beispiel beide `ExtraHop` und `\x45\x78\x74\x72\x61\x48\x6F\x70` sind gleichwertig. Hexadezimalzahlen unterscheiden nicht zwischen Groß- und Kleinschreibung. Jeder für diese Option angegebene Wert wird ignoriert , wenn **Pro Spielzug** oder **Auslöser**	• SSL_PAYLOAD • TCP_PAYLOAD • UDP_PAYLOAD

Option	Beschreibung	Unterstützte Ereignisse
	auf allen UDPs ausführen Option ist aktiviert.	
Auslöser für alle UDP-Pakete ausführen	Ermöglicht die Erfassung aller UDP-Datagramme.	• `UDP_PAYLOAD`
FLOW_CLASSIFY für ablaufende, nicht klassifizierte Flows ausführen	Ermöglicht die Ausführung des Ereignis nach Ablauf, um Metriken zu sammeln für Flüsse die vor Ablauf nicht klassifiziert wurden.	• `FLOW_CLASSIFY`
Externe Typen	Gibt die Typen von externen Daten an, die der Auslöser verarbeitet. Der Auslöser wird nur ausgeführt, wenn die Payload ein Typfeld mit einem der angegebenen Werte enthält. Geben Sie mehrere Typen in einer kommagetrennten Liste an.	1. `EXTERNAL_DATA`

Triggerleistung überwachen

Nachdem Sie einen Auslöser erstellt haben, stellen Sie sicher, dass er wie erwartet ausgeführt wird, ohne Fehler oder unnötigen Ressourcenverbrauch. Wenn Ihr Trigger-Skript eine Debug-Anweisung enthält, überprüfen Sie das Debug-Log auf die Debug-Ausgabe. Sie können auch das Debug-Log auf Fehler und Ausnahmen überprüfen. Sie können Leistungsinformationen für einen einzelnen Auslöser und mehrere Systemstatusdiagramme anzeigen, die die kollektiven Auswirkungen all Ihrer Trigger auf das System angeben.

Informationen zu den Schritten, die Sie ausführen müssen, um einen Auslöser zu erstellen, finden Sie unter Einen Auslöser erstellen.

Überprüfen Sie die Triggerausgabe im Debug-Log

Nachdem Sie einen Auslöser erstellt oder bearbeitet haben, können Sie den Debug-Protokoll Registerkarte, um zu überprüfen, ob der Auslöser wie erwartet und ohne Probleme ausgeführt wird. Das Debug-Log zeigt Debug-Ausgaben, Fehler und Ausnahmen an. Diese Registerkarte wird erst angezeigt, nachdem der Auslöser gespeichert wurde.

Wenn ein Auslöser eine Debug-Anweisung enthält, wird die Ausgabe dieser Anweisung im Trigger-Debug-Log angezeigt. Stellen Sie sicher, dass die protokollierte Ausgabe erwartet wird. Wenn Sie keine Ergebnisse sehen, überprüfen Sie, ob das Debuggen auf der Konfiguration Registerkarte.

Beachten Sie, dass die Debug-Ausgabe mit der Protokollierung beginnt, sobald der Auslöser zugewiesen und gespeichert wurde. Das Protokoll kann jedoch keine Daten anzeigen, die vor der Zuweisung und Speicherung des Auslöser aufgetreten sind.

Die folgenden Schritte zeigen Ihnen, wie Sie auf das Debug-Log zugreifen können:

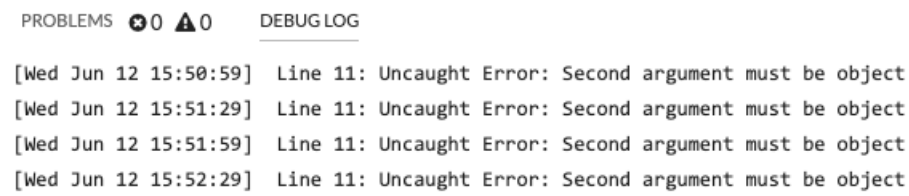
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen, und klicken Sie dann **Auslöser**.
3. Klicken Sie auf den Namen des Auslöser, den Sie anzeigen möchten.
4. klicken **Trigger-Skript bearbeiten**.
5. Klicken Sie auf **Debug-Protokoll** Tabulatur.

Im folgenden Beispiel überwacht der Auslöser HTTP-Verbindungen auf ausgewählten Geräten und gibt URIs zurück, die „Seattle“ enthalten.

```
if (HTTP.uri.match("seattle")){
    Application("Seattle App").commit();
    debug(HTTP.uri);
}
```

Wenn eine Übereinstimmung auftritt, wird der URI, der die Übereinstimmung enthält, in das Debug-Log geschrieben, wie in der folgenden Abbildung dargestellt:

Das Debug-Log zeigt auch alle auftretenden Laufzeitfehler oder Ausnahmen an, unabhängig davon, ob das Debuggen auf der Registerkarte Konfiguration aktiviert ist oder nicht. Sie sollten Ausnahmen korrigieren, wenn sie auftreten, um die Leistungseinbußen auf Ihr System zu minimieren.

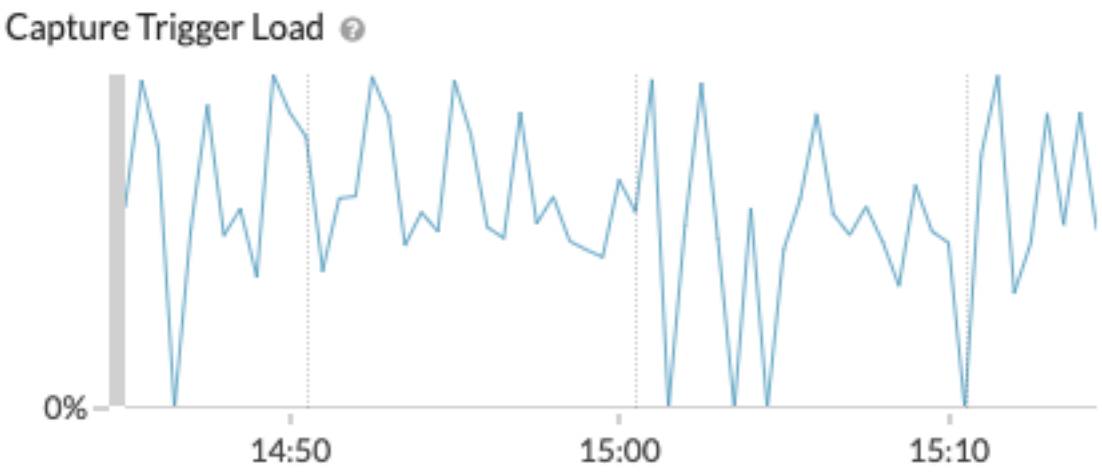


Die Leistung eines einzelnen Auslöser anzeigen

Nachdem Sie einen Auslöser erstellt oder bearbeitet haben, können Sie den Leistung Registerkarte, um eine grafische Darstellung der Auswirkungen des Auslöser auf die Leistung auf Ihre Umgebung anzuzeigen. Diese Registerkarte wird erst angezeigt, nachdem der Auslöser gespeichert wurde.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen, und klicken Sie dann **Auslöser**.
3. Klicken Sie auf den Auslöser, den Sie anzeigen möchten.
4. Scrollen Sie im Bereich Trigger bearbeiten nach unten zum Diagramm Capture Trigger Load.

Auf der Registerkarte wird ein Trigger-Leistungsdiagramm angezeigt, in dem die Anzahl der Zyklen aufgezeichnet wird, die der Auslöser innerhalb eines bestimmten Zeitintervalls verbraucht hat.



Nächste Schritte
Wenn die Wirkung des Auslöser stark ist, bewerten Sie den Zweck des Auslöser neu und ziehen Sie die folgenden Optionen in Betracht:

- Stellen Sie sicher, dass der Auslöser nur die erforderlichen Aufgaben ausführt und nur auf den erforderlichen Geräten oder Netzwerken ausgeführt wird.
- Suchen Sie in der Tabelle unten nach Ausnahmen Capture Trigger Load, besuchen Sie die Gesundheit des Systems Seite, die zusätzliche Leistungskennzahlen für Auslöser enthält, z. B. die Anzahl der laufenden Trigger, die Triggerlast und Trigger-Ausnahmen.
- Beurteilen Sie die Effizienz des Trigger-Skripts und suchen Sie nach Tipps zur Trigger-Optimierung in der Leitfaden mit bewährten Methoden für Trigger.

Die Leistung aller Trigger auf dem System anzeigen

Nachdem Sie einen Auslöser erstellt haben, können Sie sich mehrere Diagramme zur Systemintegrität ansehen, die die Gesamtauswirkung all Ihrer Trigger auf das System aufzeigen. Sie können diese Diagramme auf Probleme hin überwachen, die sich auf die Systemleistung auswirken oder zu falschen Daten führen.

Die Gesundheit des Systems Diese Seite enthält mehrere Diagramme, die einen Überblick über die Trigger bieten, die auf dem ExtraHop-System ausgeführt werden.

1. Klicken Sie auf das Symbol Systemeinstellungen, und klicken Sie dann **Gesundheit des Systems**.
2. Sehen Sie sich die folgenden Diagramme an:

Option	Description
Trigger wird von Trigger ausgeführt	Zeigt alle Trigger an, die auf dem System ausgeführt werden. Wenn der Auslöser, den Sie gerade erstellt oder geändert haben, nicht aufgeführt ist, liegt möglicherweise ein Problem mit dem Triggerskript vor.
Trigger wird ausgeführt	Zeigt Auslöseraktivitätsschübe an, die auf ineffizientes Verhalten eines oder mehrerer Trigger hinweisen könnten. Wenn Aktivitätsausbrüche angezeigt werden, sehen Sie sich das Diagramm Auslöser Executes by Auslöser an, um alle Trigger zu finden, die überdurchschnittlich viele Ressourcen verbrauchen. Dies kann darauf hindeuten, dass der Trigger über ein schlecht optimiertes Script verfügt, das die Leistung beeinträchtigt.

Option	Description
Ausnahmen nach Trigger auslösen	Zeigt alle Ausnahmen an, die durch Trigger verursacht wurden. Ausnahmen tragen wesentlich zu Problemen mit der Systemleistung bei und sollten sofort behoben werden.
Drops auslösen	Zeigt die Anzahl der Trigger an, die aus der Trigger-Warteschlange gelöscht wurden. Eine häufige Ursache für gelöschte Trigger ist ein lang andauernder Auslöser, der den Ressourcenverbrauch dominiert. Ein gesundes System sollte zu jeder Zeit 0 Tropfen enthalten.
Last auslösen	Verfolgt die Nutzung aller verfügbaren Ressourcen durch Trigger. Eine hohe Belastung beträgt ungefähr 50%. Achten Sie auf Verbrauchsspitzen, die darauf hindeuten können , dass ein neuer Auslöser eingeführt wurde oder dass bei einem vorhandenen Auslöser Probleme auftreten.

Anhand der folgenden Diagramme können Sie überwachen, ob Ihre Datenspeicher-Trigger, auch Bridge-Trigger genannt, ordnungsgemäß ausgeführt werden:

- Der Datenspeicher-Trigger wird ausgeführt
- Datenspeicher lösen Ausnahmen per Auslöser
- Auslösung des Datenspeicher-Triggers

Bündel

Ein Paket ist ein benutzerdefinierter Satz von Systemkonfigurationen, die gespeichert werden können und hochgeladen zu einem ExtraHop-System.

Video: Sehen Sie sich die entsprechende Schulung an: Bündel

Die folgenden Systemanpassungen können als Teil eines Paket gespeichert werden:

- Warnmeldungen
- Anwendungen
- Armaturenbretter
- Benutzerdefinierte Erkennungen
- Dynamische Gerätegruppen
- Abfragen aufzeichnen
- Formate aufzeichnen
- Trigger

Erfahre mehr über das Erstellen und Teilen von Paketen mit dem Leitfaden für bewährte Methoden im Bundle.

Installiere ein Paket

ExtraHop-Pakete ermöglichen es Ihnen, dem ExtraHop-System vorkonfigurierte Anpassungen hinzuzufügen.

Bevor Sie beginnen

- Sie müssen Vollschreiben oder höher haben Privilegien um ein Paket hochzuladen.
- Sie müssen mindestens über eine persönliche Schreibfähigkeit verfügen Privilegien um ein Paket herunterzuladen und zu installieren.
- Sie benötigen eine JSON-Bundle-Datei. Sie können ein Paket aus dem ExtraHop-System herunterladen, indem Sie zu **Systemeinstellungen > Bundles**, wählen Sie das Paket aus und klicken Sie dann auf **Paket herunterladen** aus dem rechten Bereich.

Nachdem Sie ein Paket heruntergeladen haben, können Sie das Paket hochladen und auf Ihrem System installieren.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen.
3. Klicken Sie **Bündel**.
4. Klicken Sie **Paket hochladen**.
5. In der Paket hochladen Bereich, klicken Sie **Wählen Sie Datei**, und wählen Sie dann die Bundle-JSON-Datei aus, die Sie hochladen möchten.

   Es werden Details zum Paketinhalt angezeigt, einschließlich der mindestens erforderlichen Firmware-Version.
6. Wählen Sie im Abschnitt Installationsoptionen die folgenden Kontrollkästchen aus:
   a) (Nur Konsole) Wählen Sie die Standort aus, auf der Sie das Paket installieren möchten.

      Hinweis: Bundle-Anpassungen wie Warnungen und Auslöser werden den ausgewählten Websites hinzugefügt. Sie können Anpassungen jedoch nur über das ExtraHop-System anzeigen, aktivieren und konfigurieren, auf dem das Paket installiert wurde .
   b) Wählen Sie die **Inbegriffene Aufgaben anwenden** Ankreuzfeld.

Diese Option weist das Paket den im Paket enthaltenen Metrikquellen zu. In den meisten Fällen ist es am besten, die Standardzuweisungen anzuwenden.

c) Wählen Sie die **Bestehenden Inhalt überschreiben** Ankreuzfeld.

Diese Option überschreibt alle Objekte, die denselben Namen wie Objekte im Paket haben. Wenn Sie bereits Systemobjekte mit demselben Namen haben , die Sie beibehalten möchten, müssen Sie diese Objekte umbenennen, um zu verhindern, dass sie mit den Objekten im Paket überschrieben werden.

7. Klicken Sie **Installieren**.

Nächste Schritte

- Aktiviere alle löst aus im Bundle enthalten.
- Konfiguriere alle Warnungen im Paket, um relevante E-Mail-Adressen zu benachrichtigen.

Ein Paket erstellen

Sie können Systemkonfigurationen in einer Bundle-Datei speichern und diese Datei dann auf andere ExtraHop-Systeme hochladen.

Bevor Sie beginnen
Sie müssen Vollschreiben oder höher haben Privilegien um ein Paket zu erstellen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Bündel**.
3. Auf dem Bündel Seite, klicken **Erstellen**.
4. Vervollständigen Sie die folgenden Informationen:

Name

Weisen Sie dem Paket einen Namen zu.

Autor

Geben Sie den Ersteller des Paket an. Dieser Name wird auf das Autorenfeld aller Objekte im Paket angewendet. Wenn Sie keinen Autor angeben, behält jedes Bundle-Objekt seine Autoreneinstellung bei.

Minimale ExtraHop-Version

Geben Sie die früheste Version der ExtraHop-Firmware an, auf der das Paket ausgeführt werden kann. Wir empfehlen Ihnen, die aktuelle Version der ExtraHop-Firmware anzugeben. Die Angabe der aktuellen Version verhindert, dass Ihr Paket versehentlich auf einem System installiert wird, das das Paket nicht unterstützt.

Hinweis: Wenn Sie versuchen, ein Paket zu installieren, für das eine neuere Firmware-Version erforderlich ist, wird eine Warnmeldung angezeigt. Diese Warnung hindert Sie jedoch nicht daran, das Paket hochzuladen und anzuwenden.

Beschreibung (optional)

Geben Sie eine Beschreibung des Paket ein.

Zum Paket hinzufügen

Wählen Sie im Dropdownmenü die Systemkonfigurationen aus, die Sie dem Paket hinzufügen möchten, z. B. Trigger, Dashboards und Warnungen. Sie können mehrere Artikel auswählen, um sie dem Paket hinzuzufügen.

Hinweis: Mit den folgenden Hotkeys können Sie schnell mehrere Bundle-Konfigurationen auswählen:

OPTION + Klick (Mac), ALT + Klick (Windows)

Wählen Sie alle Elemente aus, außer dem, auf den Sie geklickt haben.

UMSCHALTTASTE+Klick

Deaktivieren Sie alle Elemente außer dem, auf das Sie geklickt haben.

5. Klicken Sie **Speichern**.

   Sie können die von Ihnen erstellte Bundle-JSON-Datei herunterladen, indem Sie das Paket aus der Liste auswählen und dann auf **Paket herunterladen** aus dem rechten Bereich.

Nächste Schritte

- Installieren Sie Ihr Paket auf einem anderen ExtraHop-System

Anlage

Protokollmodule

Das ExtraHop-System bietet Metriken über die folgenden Arten von Protokollmodulen:

Typ des Moduls	Protokolle
L2-L3 Metriken	• Multicast • IP • IPv6 • ICMP • ICMP v6
L4-Metriken	• TCP • UDP
Benennung	DNS
Verzeichnisdienste	LDAP
Netz	• HTTP/HTTPS • AMF • TLS
Middleware	• MS-RPC • Memcache • IBMMQ
Datenbank	• IBM DB2 • IBM Informix • Microsoft SQL Server • MongoDB • MySQL • Orakel • PostgreSQL • Sybase ASE • Sybase IQ
Aufbewahrung	• iSCSI • SMB • NFS
Dateiübertragung	FTP
Post	SMTP
Citrix VDI	• ICA • CGP
Branchenspezifische Protokolle	• Durchmesser • FIX

Typ des Moduls	Protokolle
	• HL7 • RADIUS • SMPP • Telnet
Entschlüsselung	Irgendein Protokoll verschlüsselt über einen Ende-zu-Ende-TLS-Kanal, kann mit dem TLS-Entschlüsselungsmodul entschlüsselt werden.

Weitere Informationen zu den ExtraHop-Protokollmodulen finden Sie unter extrahop.com.

Unterstützte Browser

Die folgenden Browser sind mit allen ExtraHop-Systemen kompatibel. Wenden Sie die von Ihrem Browser bereitgestellten Barrierefreiheits- und Kompatibilitätsfunktionen an, um über technische Hilfsmittel auf Inhalte zuzugreifen.

- Firefox
- Google Chrome
- Microsoft Edge
- Safari

Wichtig: Internet Explorer 11 wird nicht mehr unterstützt. Wir empfehlen Ihnen, die neueste Version aller unterstützten Browser zu installieren.

Allgemeine Akronyme

Die folgenden gängigen Akronyme für Computer- und Netzwerkprotokolle werden in diesem Handbuch verwendet.

Akronym	Vollständiger Name
AAA	Authentifizierung, Autorisierung und Abrechnung
AMF	Format der Aktionsnachricht
CIFS	Gemeinsames Internet-Dateisystem
CLI	Befehlszeilenschnittstelle
CPU	Zentrale Verarbeitungseinheit
DB	Datenbank
DHCP	Dynamisches Host-Konfigurationsprotokoll
DNS	Domainnamensystem
ERSPAN	Gekapselter Remote-Switching-Port-Analysator
FIX	Austausch von Finanzinformationen
FTP	FTP
HTTP	Hypertext-Übertragungsprotokoll
IBMMQ	Nachrichtenorientierte IBM Middleware
ICA	Unabhängige Computerarchitektur

Akronym	Vollständiger Name
IP	Internet-Protokoll
iSCSI	Internetschnittstelle für kleine Computersysteme
L2	Ebene 2
L3	Schicht 3
L7	Schicht 7
LDAP	Leichtes Verzeichniszugriffsprotokoll
MAC	Medienzugriffskontrolle
MIB	Informationsbasis für das Management
NFS	NFS
NVRAM	Nichtflüchtiger Direktzugriffsspeicher
RADIUS	Benutzerdienst für Fernauthentifizierung mit Einwahl
RPC	Prozeduraufruf per Fernzugriff
RPCAP	Paketerfassung aus der Ferne
RSS	Größe des Resident-Sets
SMPP	Kurznachricht Peer-to-Peer-Protokoll
SMTP	Einfaches Nachrichtenübertragungsprotokoll
SNMP	Einfaches Netzwerkmanagement-Protokoll
SPAN	Analysator für geschaltete Anschlüsse
SSD	Solid-State-Laufwerk
SSH	Sichere Shell
SSL	Sichere Socket-Schicht
TACACS+	Zutrittskontrollsystem für Terminalzugriffssteuerungen Plus
TCP	TCP
TLS	Sicherheit auf Transportebene
UI	Benutzerschnittstelle
VLAN	VLAN
VM	Virtuelle Maschine