



Zusätzlicher Hopfen 9.4

ExtraHop System-Benutzerhandbuch

© 2024 ExtraHop Networks, Inc. Alle Rechte vorbehalten.

Dieses Handbuch darf ohne vorherige schriftliche Genehmigung von ExtraHop Networks, Inc. weder ganz noch auszugsweise vervielfältigt, übersetzt oder in eine maschinenlesbare Form gebracht werden.

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

Veröffentlicht: 2024-02-12

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

Inhaltsübersicht

Über diesen Leitfaden	10
Kontaktiere uns	10
Einführung in das ExtraHop-System	11
Plattform-Architektur	11
Module	11
Lösungen	12
Komponenten	13
ExtraHop Cloud-Dienste	15
Intelligente Sensoranalytik	15
Sensortypen	15
Drahtdaten	15
Flow-Daten	16
Metriken, Datensätze und Pakete	16
Erkennung von Geräten	16
Erkennung von Bedrohungen	19
Im ExtraHop-System navigieren	21
Unterstützte Browser	21
Layout und Menü	21
Beginnen Sie mit der Datenanalyse	23
Erweiterte Workflows zur Anpassung Ihres ExtraHop-Systems	24
Greifen Sie auf Tastenkombinationen zu	25
Dashboards mit Tastenkombinationen verwalten	26
Zeitintervalle	27
Ändern Sie das Zeitintervall	27
Ändern Sie die angezeigte Zeitzone	28
Die neuesten Daten für ein Zeitintervall anzeigen	28
Granularität der Diagrammdaten ändern	29
Vergrößern Sie einen benutzerdefinierten Zeitraum	30
Frieren Sie das Zeitintervall ein, um einen benutzerdefinierten Zeitraum zu erstellen	31
Übersichtsseiten	33
Überblick über die Sicherheit	33
Bedrohungsinformationen	34
Standortauswahl und Bericht der Geschäftsleitung	34
Überblick über das Netzwerk	34
Straftäter bei Fahndungen	34
Erkennungskarte	34
Standortauswahl und Bericht der Geschäftsleitung	35
Perimeter im Überblick	35
Perimeterverkehr	35
Halo-Visualisierung	36
Kartenvisualisierung	37
Standortauswahl und Bericht der Geschäftsleitung	37

Armaturenbretter	38
Dashboards erstellen	38
Dashboards anzeigen	39
Dashboard-Daten exportieren und teilen	40
System-Dashboards	40
Dashboard zur Netzwerkaktivität	41
Dashboard zur Netzwerkleistung	42
Dashboard zur Erhöhung der Sicherheit	42
Dashboard mit generativen KI-Tools	44
Active Directory Directory-Dashboard	44
Systemintegritäts-Dashboard	46
Geräteerkennung	47
Datenfeed	48
Rekorde	50
Auslöser	50
Öffnen Sie Data Stream und Recordstore	52
SSL Zertifikate	54
Paketerfassung aus der Ferne (RPCAP)	55
Fortgeschrittene Gesundheitsmetriken	56
Status- und Diagnosetools in den Administrationseinstellungen	58
Dashboard zur Systemnutzung	58
Erstellen Sie ein Dashboard	59
Erstellen Sie das Dashboard-Layout	59
Bearbeiten Sie ein einfaches Diagramm	60
Bearbeiten Sie ein einfaches Textfeld-Widget	61
Fügen Sie Ihrem Dashboard weitere Widgets und Regionen hinzu	61
Tipps zur Bearbeitung von Diagrammen	61
Erstellen Sie ein Dashboard mit dynamischen Quellen	62
Ein Dashboard kopieren	63
Ein Dashboard-Layout bearbeiten	64
Bearbeiten Sie ein Diagramm mit dem Metric Explorer	65
Erstellen und bearbeiten Sie ein Basisdiagramm	65
Konfigurieren Sie erweiterte Optionen für die Datenanalyse und Diagrammanpassung	67
Filter für reguläre Ausdrücke	68
Ein Textfeld-Widget bearbeiten	72
Text in Markdown formatieren	73
Bilder in Markdown hinzufügen	74
Fügen Sie Metrikbeispiele in Markdown hinzu	74
Beispiele für metrische Abfragen für das Textfeld-Widget	76
Eine Dashboard-Region bearbeiten	79
Ändern Sie das Zeitintervall für eine Dashboard-Region	80
Dashboard-Eigenschaften bearbeiten	81
Präsentieren Sie ein Dashboard	81
Ein Dashboard teilen	82
Zugriff auf ein Dashboard entfernen	83
Eine Dashboard-Sammlung erstellen	83
Eine Dashboard-Sammlung teilen	84
Daten exportieren	85
Daten nach Excel exportieren	85
Daten nach CSV exportieren	85
Erstellen Sie eine PDF-Datei	85
Passen Sie das Format einer PDF-Datei an	86
Erstellen Sie einen geplanten Dashboard-Bericht	87
Erstellen Sie einen Dashboard-Bericht (Reveal (x) Enterprise)	87

Erstellen Sie einen Dashboard-Bericht (Reveal (x) 360)	89
Diagrammtypen	92
Erstellen Sie ein Diagramm	101
Ein Diagramm kopieren	102
Drilldown	103
Drilldown von einem Dashboard oder einer Protokollseite aus	103
Detaillierter Überblick über Netzwerkerfassung und VLAN-Metriken	104
Drilldown von einer Erkennung aus	105
Drilldown von einer Alarm aus	106
Untersuchen Sie detaillierte Metriken	107
Ein zweites Mal mit einem Schlüsselfilter aufschlüsseln	110
Detailmetriken zu einem Diagramm hinzufügen	112
Rate oder Anzahl in einem Diagramm anzeigen	114
Zeigen Sie den Durchschnittskurs in einem Diagramm an	115
Zeigen Sie die maximale Rate in einem Diagramm an	115
Perzentile oder einen Mittelwert in einem Diagramm anzeigen	116
Einen benutzerdefinierten Perzentilbereich anzeigen	117
Ausreißer in Histogramm- oder Heatmap-Diagrammen filtern	118
Metrikbeschriftungen in einer Diagrammlegende bearbeiten	118
Hinzufügen einer Dynamische Basislinie zu einem Diagramm	119
Hinzufügen einer statischen Schwellenwertlinie zu einem Diagramm	121
Gerätegruppenmitglieder in einem Diagramm anzeigen	122
Filter für reguläre Ausdrücke	124
Finden Sie alle Geräte, die mit externen IP-Adressen kommunizieren	127
Überwachen Sie ein Gerät auf externe IP-Adressverbindungen	128
Vergleichen Sie Zeitintervalle, um das Metrik Delta zu ermitteln	129
Vermögenswerte	131
Geräte	132
Navigationsgeräte	132
Seite „Geräteübersicht“	132
Geräte-Metriken	135
Angaben zur IP-Adresse	136
Geräte gruppieren	138
Maßgeschneiderte Geräte	139
Gerätegruppen	140
Gerätenamen und Rollen	140
Gerätenamen	140
Geräterollen	141
Finde ein Gerät	145
Finden Sie ein Gerät über eine globale Suche	145
Suchen Sie anhand von Details nach einem Gerät	146
Suchen Sie nach Geräten anhand der Protokollaktivität	149
Suchen Sie nach Geräten, auf die ein bestimmter Benutzer zugegriffen hat	151
Suche nach Peer-Geräten	153
Einen Gerätenamen ändern	155
Eine Geräterolle ändern	156
Gerätmodell ändern	158
Manuelles Identifizieren eines Gerät hoher Wert	159
Ein Geräte-Tag erstellen	160
Eine Gerätegruppe erstellen	160
Erstellen Sie eine dynamische Gerätegruppe	160
Erstellen Sie eine statische Gerätegruppe	165

Benutzerdefiniertes Gerät erstellen	166
Benutzerdefiniertes Gerät löschen oder deaktivieren	167
Remote-Sites für benutzerdefinierte Geräte konfigurieren	168
Geben Sie Netzwerkstandorte und vertrauenswürdige Domänen an	169
Geben Sie eine Netzwerklokalität an	169
Eine vertrauenswürdige Domain hinzufügen	170
Prioritäten der Analyse	171
Geräte und Gruppen priorisieren	171
Analysestufen vergleichen	172
Transfermanagement von Analyseprioritäten	173
Priorisieren Sie Gruppen für Erweiterte Analyse	173
Priorisieren Sie Gruppen für die Standardanalyse	176
Ein Gerät zur Beobachtungsliste hinzufügen	178
Ein Gerät von der Beobachtungsliste entfernen	179
Karten mit Aktivitäten	181
Navigiere durch Aktivitätskarten	181
Grundriss	181
Beschriftungen und Icons	184
Kreis- und Liniengröße	185
Farbe	186
Schritte und Filter zu einer Map hinzufügen	189
Aktivitätskarten verwalten	191
Bewährte Methoden für die Untersuchung von Aktivitätsdiagramm Map-Daten	191
Erstellen Sie eine Aktivitätsdiagramm	192
Erstellen Sie eine grundlegende Aktivitätsdiagramm	192
Fügen Sie Verbindungen hinzu und filtern Sie Geräte zu Ihrer Karte	194
Fügen Sie eine weitere Ebene von Geräteverbindungen hinzu	195
Geräte einbeziehen oder ausschließen	196
Speichern und teilen Sie eine Aktivitätsdiagramm	197
Zugriff auf eine Aktivitätsdiagramm entfernen oder ändern	198
Eine gespeicherte Aktivitätsdiagramm laden und verwalten	198
Erkennungen	200
Erkennungen anzeigen	200
Zusammenfassung	200
Sortierung von Erkennungen in der Übersichtsansicht	201
Gruppierung von Erkennungen in der Übersichtsansicht	201
Triage	203
MITRE karte	203
Tabelle „Untersuchungen“	204
Erkennungen filtern	204
Durch Erkennungen navigieren	207
Erkennungskatalog	213
Ermittlungen	213
Auffinden von Erkennungen im ExtraHop-System	216
Optimierung von Erkennungen	216
Eine Erkennung teilen	217
Bestätigen Sie Erkennungen	218
Eine Untersuchung erstellen	218
Eine Regel für Erkennungsbenachrichtigungen erstellen	219
Referenz zur Webhook-Benachrichtigung	220
Nutzlast JSON	221

Variablen	221
Webhook-Beispiele	224
Eine Erkennung verfolgen	228
Eine Erkennung von einer Erkennungskarte aus verfolgen	230
Verfolgen Sie eine Gruppe von Erkennungen anhand einer Erkennungsübersicht	230
CrowdStrike-Geräte aus einer Erkennung eindämmen	231
Erstellen Sie eine benutzerdefinierte Erkennung	234
Erstellen Sie einen Auslöser, um benutzerdefinierte Erkennungen zu generieren	235
Erstellen Sie einen benutzerdefinierten Erkennungstyp	239
Benutzerdefinierte Erkennungen anzeigen	239
Beispiel für einen benutzerdefinierten Erkennungsauslöser	240
Erkennungen optimieren	241
Parameter abstimmen	242
Tuning-Regeln	242
Versteckte Entdeckungen anzeigen	242
Optimierte Vorgehensweisen	243
Unterdrücken Sie Erkennungen mit Optimierungsparametern	244
Geben Sie Optimierungsparameter für Erkennungen und Metriken an	244
Fügen Sie einen Tuning-Parameter oder eine vertrauenswürdige Domain von einer Erkennungskarte hinzu	246
Eine vertrauenswürdige Domain hinzufügen	247
Erkennungen mit Optimierungsregeln ausblenden	248
Eine Optimierungsregel erstellen	248
Eine Optimierungsregel von einer Erkennungskarte hinzufügen	248
Eine Optimierungsregel aus einer Härtungserkennung hinzufügen	249
Fügen Sie auf der Seite „Tuning-Regeln“ eine Tuning-Regel hinzu	249
Kriterien für Optimierungsregeln	250
Tuning-Regeln verwalten	251
Härtungserkennungen filtern und optimieren	253
Ticket-Tracking für Erkennungen konfigurieren	254
Aktivieren Sie die Ticketverfolgung und geben Sie eine URL-Vorlage an	254
Schreiben Sie einen Auslöser, um Tickets zu Erkennungen in Ihrem Ticketsystem zu erstellen und zu aktualisieren	255
Senden Sie Ticketinformationen über die REST-API an Erkennungen	257
Untersuchen Sie Sicherheitserkennungen	258
Beginne deine Untersuchung	259
Verfeinern Sie Ihre Untersuchung	259
Untersuchen Sie Leistungserkennungen	262
Beginne deine Untersuchung	262
Verfeinern Sie Ihre Untersuchung	263
Bedrohungsinformationen	267
Benachrichtigungsregel Bedrohungsübersicht Bedrohungsinformationen erstellen	267
Bedrohungsinformationen	269
Sammlungen von Bedrohungen	269
Untersuchung von Bedrohungen	269
Bedrohungssammlungen verwalten	273
Von ExtraHop kuratierte Bedrohungssammlungen aktivieren oder deaktivieren	273
Laden Sie eine Bedrohungssammlung hoch	274

Alerts	275
Benachrichtigungen konfigurieren	275
Benachrichtigungen anzeigen	275
Einen Schwellenwertalarm konfigurieren	276
Konfigurieren Sie eine Trendwarnung	278
Hinzufügen einer Benachrichtigung zu einer Warnungskonfiguration	283
Eine Alarm hinzufügen (Reveal (x) Enterprise)	283
Eine Alarm hinzufügen (Reveal (x) 360)	284
Einer Alarm ein Ausschlussintervall hinzufügen	284
Rekorde	286
In Datensätzen navigieren	286
Filtern Sie Ihre Datensätze mit einer einfachen Abfrage	288
Datensätze im ExtraHop-System finden	291
Aufzeichnungen sammeln	292
Flow-Aufzeichnungen sammeln	293
Sammeln Sie L7-Datensätze mit einem Auslöser	293
Sammeln Sie benutzerdefinierte Datensätze	294
Einen Auslöser schreiben und zuweisen	294
Erstellen Sie ein benutzerdefiniertes Datensatzformat, um Ihre Datensatzergebnisse in einer Tabelle anzuzeigen	296
Fragen Sie nach Ihrem benutzerdefinierten Datensatztyp ab	297
Einstellungen für das Aufzeichnungsformat	297
Datensätze mit einem erweiterten Filter abfragen	299
Filtern Sie Ihre Datensätze mit erweiterten Abfragerregeln	299
Datensatzabfragen für benutzerdefinierte Metriken aktivieren	301
Pakete	304
Konfigurieren Sie eine globale PCAP	306
Analysieren Sie eine Paketerfassungsdatei	307
Stellen Sie den Offline-Aufnahmemodus ein	307
Bringen Sie das System in den Live-Aufnahmemodus zurück	307
Pakete mit der Berkeley-Paketfilter-Syntax filtern	308
Fügen Sie einen Filter mit BPF-Syntax hinzu	308
Unterstützte BPF-Syntax	308
Speichern Sie SSL-Sitzungsschlüssel in verbundenen Paketspeichern	310
Laden Sie Sitzungsschlüssel mit Paketerfassungen herunter	310
Sehen Sie sich die entschlüsselte Nutzlast in Wireshark an	311
Auslöser	312
Einen Auslöser erstellen	314
Trigger-Einstellungen konfigurieren	314
Schreiben Sie ein Trigger-Skript	315
Erweiterte Trigger-Optionen	317
Triggerleistung überwachen	321
Überprüfen Sie die Triggerausgabe im Debug-Log	321
Die Leistung eines einzelnen Auslöser anzeigen	322
Die Leistung aller Trigger auf dem System anzeigen	323
Bündel	325
Installiere ein Paket	325
Ein Paket erstellen	326

Geomaps

Generieren Sie eine Geomap

328

330

Anlage

Protokollmodule

Unterstützte Browser

Allgemeine Akronyme

Tastenkürzel

331

331

332

332

333

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 wichtigsten Systemkomponenten und -funktionen Ihnen helfen, auf Erkennungen, Metriken, Transaktionen und Pakete über den Datenverkehr in Ihrem Netzwerk zuzugreifen.

Workflows zur Überwachung der Netzwerkleistung ermöglichen es Ihnen, zu überwachen, wie Dienste und Geräte miteinander interagieren und wie Transaktionen über die Daten Verbindungsschicht (L2) zur Anwendungsebene (L7) in Ihrem Netzwerk Fluss. Mit Workflows zur Netzwerkerkennung und -reaktion können Sie Daten untersuchen, die von Leistungseinbußen bis hin zu verdächtigem Verhalten erkannt wurden. Außerdem erhalten Sie einen Überblick darüber, welche Geräte an den Taktiken, Techniken und Verfahren (TTPs) (TTPs) von MITRE ATT&CK beteiligt waren, die mit fortschrittlichen, mehrstufigen Angriffskampagnen verbunden sind.

Plattform-Architektur

Das ExtraHop-System ist mit modularen Komponenten maßgeschneidert, die in Kombination Ihren individuellen Umwelтанforderungen 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 Benutzern rollenbasierten Zugriff auf das NDR-Modul, das NPM-Modul oder beide gewähren.

Überwachung der Netzwerkleistung

Das NPM-Modul ermöglicht es privilegierten Benutzern, die folgenden Arten von Systemaufgaben auszuführen.

- 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 Benachrichtigungen.
- Leistungserkennungen anzeigen.

Netzwerkerkennung und Reaktion

Das NDR-Modul ermöglicht es privilegierten Benutzern, die folgenden Arten von Systemaufgaben auszuführen.

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

Benutzer, denen Zugriff auf beide Module gewährt wurde, dürfen all diese Aufgaben ausführen. Weitere Informationen zur Migration von Benutzern zum rollenbasierten Zugriff mit diesen Modulen finden Sie im Migrationsleitfaden.

Zusätzliche Module sind auch für spezielle Anwendungsfälle verfügbar:

Paketforensik

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

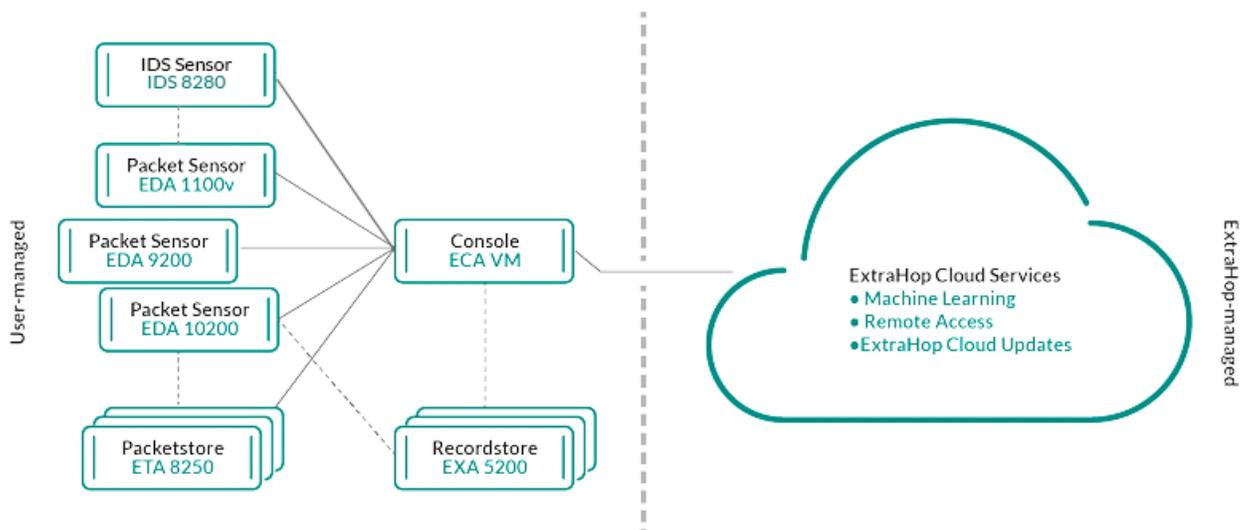
Systeme zur Erkennung von Eindringlingen

Das IDS-Modul muss mit dem NDR-Modul kombiniert werden und ermöglicht Erkennungen, die auf branchenüblichen IDS-Signaturen basieren.

Lösungen

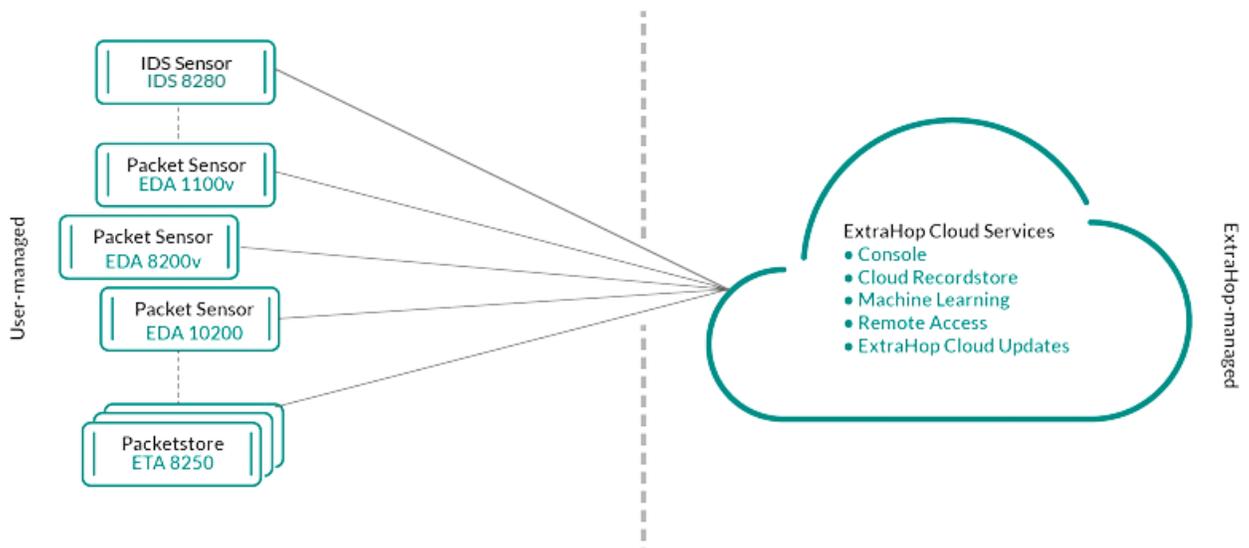
Reveal (x) Enterprise

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



Enthülle (x) 360

Reveal (x) 360 ist eine Software-as-a-Service (SaaS) -Lösung, die Folgendes umfasst Sensoren und Packetstores und beinhaltet einen cloudbasierten Recordstore, einen Konsole und Zugriff auf ExtraHop Cloud Services.



Komponenten

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

Paketsensoren

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

Sensoren des Intrusion Detection Systems (Intrusion Detection System) lassen sich in Paketsensoren integrieren, 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 Reveal (x) 360- oder Reveal (x) Enterprise-Umgebungen verfügbar.

Durchflusssensoren

Flow-Sensoren sind nur für Reveal (x) 360 verfügbar und erfassen ausschließlich VPC-Flow-Logs, sodass Sie den von AWS SaaS-Diensten verwalteten Traffic sehen können.

Plattenläden

Plattenläden lassen sich mit Sensoren integrieren und Konsolen zu [Transaktions- und Flussdatensätze speichern](#) das kann im gesamten ExtraHop-System abgefragt werden. Recordstores können als eigenständige physische oder virtuelle Optionen bereitgestellt und als Drittanbieterverbindungen zu Splunk oder BigQuery von Reveal (x) Enterprise unterstützt werden. Sie sind in Paketen mit NPM- und NDR-Modulen erhältlich.

Paketläden

Packetstores integrieren sich mit Sensoren und Konsolen zur Verfügung stellen [kontinuierliche PCAP](#) und ausreichend Speicherplatz für tiefere Untersuchungen und forensische Bedürfnisse. Packetstores können als eigenständige physische oder virtuelle Optionen bereitgestellt werden und sind als Zusatzmodul für Packet Forensics 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 Reveal (x) Enterprise bereitgestellt werden und sind in Reveal (x) 360 enthalten.

Die folgende Tabelle gibt einen Überblick über die Optionen, die für jede Lösung verfügbar sind.

	Reveal (x) Enterprise		Enthülle (x) 360	
	Körperlich	Virtuell/Cloud	Körperlich	Virtuell/Cloud
Paketsensor	EDA 1200	EDA 100 V AWS	EDA 1200	EDA 100 V AWS
	EDA 620		EDA 620	
	EDA 820	EDA 1100v Azurblau	EDA 820	EDA 1100v Azurblau
	EDA 920	EDA 100 V GCP	EDA 920	EDA 100 V GCP
	EDA 10200	EDA 1100 V Linux KVM	EDA 10200	EDA 1100 V Linux KVM
		EDA 1100 v VMWare		EDA 1100 v VMWare
		EDA 6100 v VMWare		EDA 6100 v VMWare

	Reveal (x) Enterprise		Enthülle (x) 360	
		EDA 6100 v AWS ↗		EDA 6100 v AWS ↗
		EDA 6100v Azurblau ↗		EDA 6100v Azurblau ↗
		EDA 820 v AWS ↗		EDA 820 v AWS ↗
		Reveal (x) Ultra 1 Gbit/s und 10 Gbit/s AWS ↗		Reveal (x) Ultra 1 Gbit/s und 10 Gbit/s AWS ↗
		Reveal (x) Ultra GCP mit 1 Gbit/s ↗		Reveal (x) Ultra GCP mit 1 Gbit/s ↗
IDS-Sensor	Intrusion Detection System 8280 ↗	N/A	Intrusion Detection System 8280 ↗	N/A
Durchflusssensor	N/A	N/A	N/A	EFC 1291 v ↗
Paketspeicher	ETA 6150 ↗	ETA 150 V AWS ↗	ETA 6150 ↗	ETA 150 V AWS ↗
	ETA 8250 ↗	ETA 1150v Azurblau ↗	ETA 8250 ↗	ETA 1150v Azurblau ↗
		ETA 1150 V GCP ↗		ETA 1150 V GCP ↗
		ETA 1150v VMWare ↗		ETA 1150v VMWare ↗
		ETA 6150v VMWare ↗		ETA 6150v VMWare ↗
				In Ultra- Abonnements enthalten
Plattenladen	EXA 5200 ↗	EXA 5100 v AWS ↗	N/A	In Premium- und Ultra- Abonnements enthalten
		EXA 5100v Azurblau ↗		
		EXA 5100 v Hyper-V ↗		
		EXA 5100 v Linux KVM ↗		
		EXA 5100v VMWare ↗		
Konsole	N/A	ECA AWS ↗	N/A	In allen Abos enthalten
		ECA Azurblau ↗		
		ECA GCP ↗		
		ECA Hyper-V ↗		
		ECA Linux KVM ↗		

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 in Bottom-up-Workflows untersuchen und anpassen können, wie Sie Ihre Netzwerkdaten sammeln, anzeigen und teilen. Fortgeschrittene Benutzer können sowohl Verwaltungs- als auch Benutzeraufgaben automatisieren und Skripten erstellen über [ExtraHop REST-API](#) [↗](#) und passen Sie die Datenerfassung an über die [ExtraHop-Trigger-API](#) [↗](#), das ist ein JavaScript-IDE-Tool.

Das Herzstück des ExtraHop-Systems ist ein intelligentes Sensor, das Metrik Daten über Ihr Netzwerk erfasst, speichert und analysiert – und bietet je nach Bedarf unterschiedliche Ebenen der Datenanalyse, -erfassung und -speicherung. Sensoren sind mit Speicher ausgestattet, der einen Metrik-Lookback für 30 Tage unterstützt. Beachten Sie, dass der tatsächliche Lookback je nach Verkehrsmustern, Transaktionsraten, Anzahl der Endpunkte und Anzahl der aktiven Protokolle variiert.

Konsolen fungieren als Kommandozentrale mit Verbindungen zu mehreren Sensoren, Plattenläden und Paketläden, die auf Rechenzentren und Zweigstellen verteilt sind. Alle Reveal (x) 360-Bereitstellungen beinhalten eine Konsole; Reveal (x) Enterprise kann virtuelle oder Cloud-Varianten bereitstellen.

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

In den folgenden Abschnitten werden die wichtigsten Funktionskomponenten des ExtraHop-Systems und ihr 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.

Drahtdaten

Paketsensoren beobachten passiv unstrukturierte Pakete über einen Port Mirror oder Tap und speichern die Daten im lokalen Datenspeicher. Die Paketdaten durchlaufen eine Echtzeit-Stream-Verarbeitung, bei der die Pakete in strukturierte wire data umgewandelt werden. Dabei werden die folgenden Phasen durchlaufen:

1. TCP-Zustandsmaschinen werden neu erstellt, um eine vollständige Stream-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 anhand ihrer Aktivität erkannt und klassifiziert.
 - Metriken werden generiert und mit Protokollen und Quellen verknüpft, und die Metrik Daten werden dann zu Metrik Zyklen 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 ein Satz von Paketen, die Teil einer einzelnen Verbindung zwischen zwei Endpunkten sind. Durchfluss Sensoren sind für **Reveal (x) 360** verfügbar und bieten kontinuierliche Netzwerktransparenz auf der Grundlage von VPC-Flow-Protokollen, um AWS-Umgebungen zu schützen. VPC-Flussprotokolle ermöglichen es Ihnen, Informationen über den IP-Verkehr zu und von Netzwerkschnittstellen in Ihrer VPC zu erfassen. Sie werden als Flow-Protokolldatensätze aufgezeichnet. Dabei handelt es sich um Protokollereignisse, die aus Feldern bestehen, die den Verkehrsfluss beschreiben. Diese Protokoll Daten ermöglichen es Ihnen, mit fortschrittlichen Erkennungen durch maschinelles Lernen nach Bedrohungen zu suchen.

Flow-Logs werden aufgenommen, dedupliziert und dann in Flows gruppiert. Die Datenflüsse 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 erkannt und anhand ihrer Aktivität klassifiziert, die über bestimmte Ports beobachtet wird.
- Grundlegende L2-L4-Metriken werden generiert und zu Metrikzyklen zusammengefasst.
- ExFlow-Datensatztypen werden generiert und veröffentlicht.

Metriken, Datensätze und Pakete

ExtraHop-Sensoren erfassen und speichern mehrere Tiefen der Netzwerkkommunikation 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.

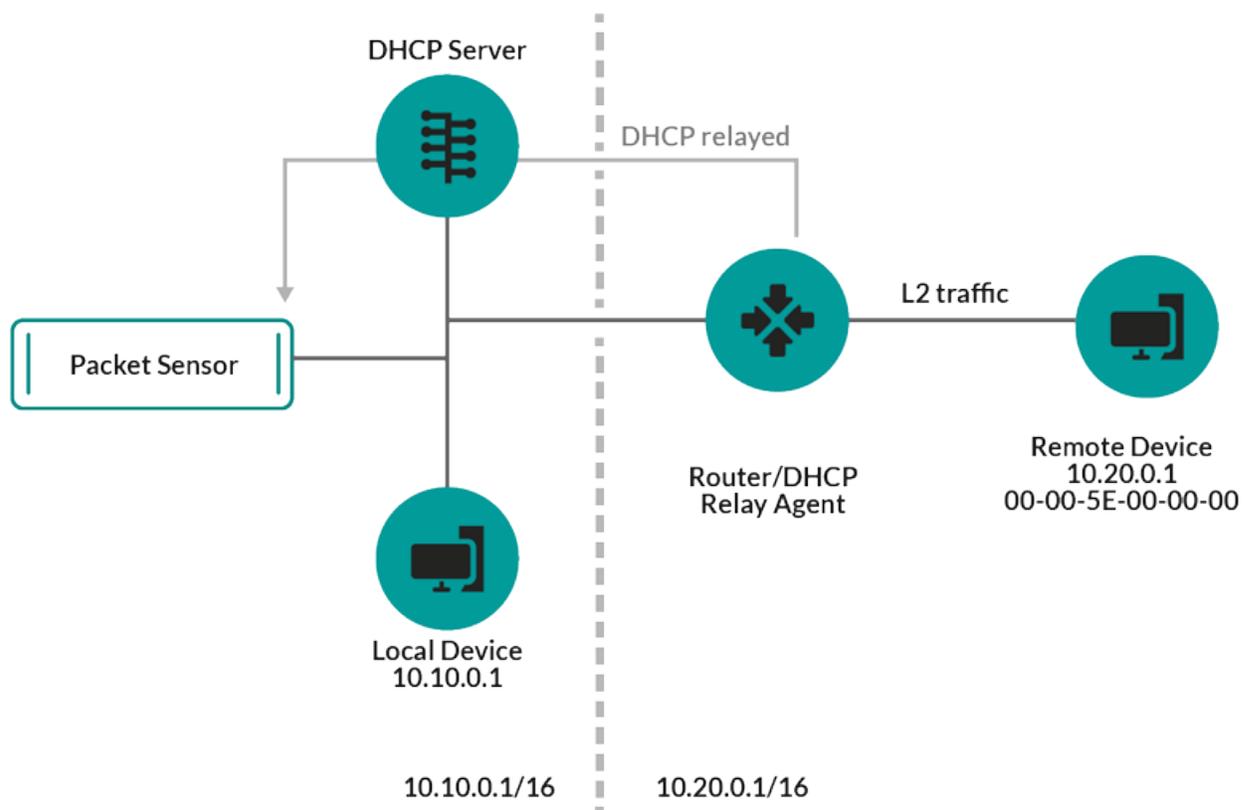


Abbildung 1: Sowohl die MAC-Adresse als auch die IP-Adresse werden für das entferntes Gerät erkannt.

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.)

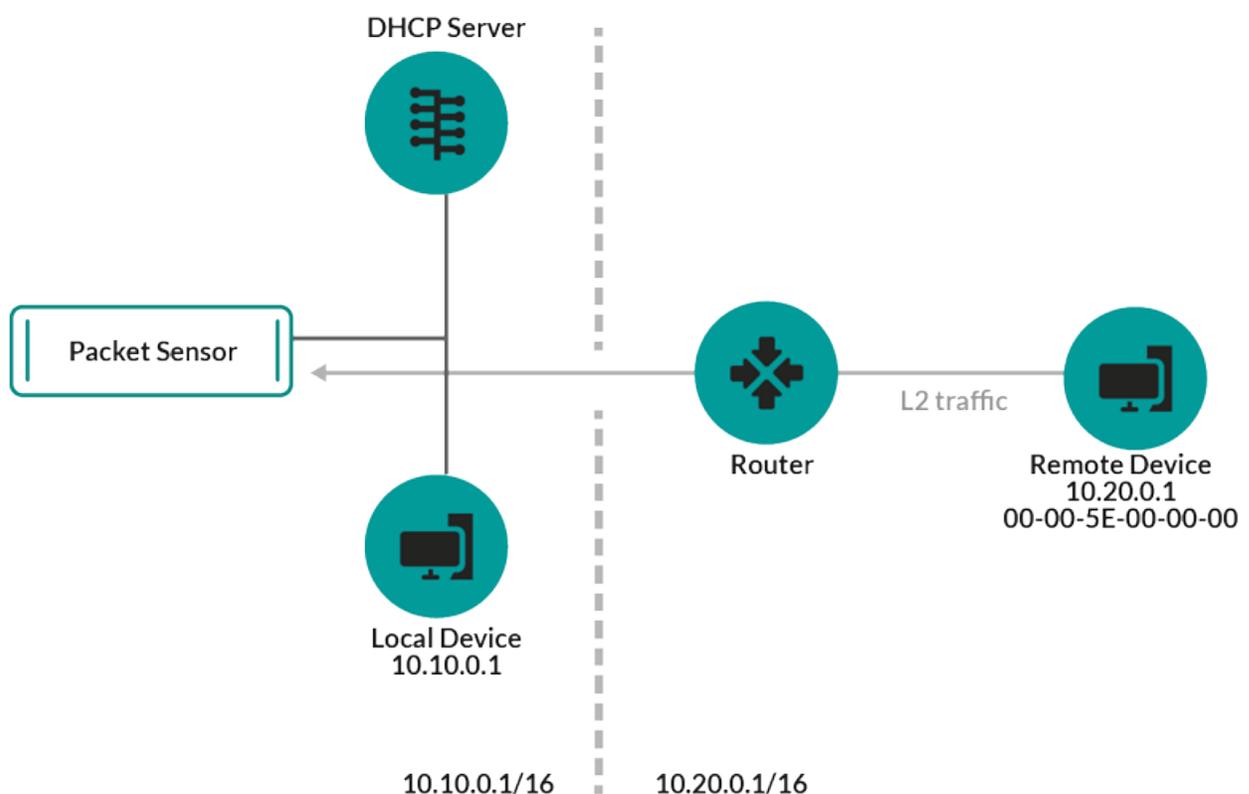


Abbildung 2: Für das entferntes Gerät wird nur die IP-Adresse erkannt.

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.)

Erkennung von Bedrohungen

Das ExtraHop-System bietet sowohl maschinelles Lernen als auch regelbasiertes Lernen **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 eine proaktive Bedrohungssuche.

Tuning der Erkennung

[Reduzieren Sie das Rauschen und lassen Sie nur kritische Erkennungen sichtbar werden](#) indem Sie Details zu Ihrem 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) im System als internes Gerät klassifiziert.

Da einige Netzwerkumgebungen jedoch IP-Adressen enthalten, die nicht nach RFC1918 stammen, als Teil ihres internen Netzwerk können Sie [die interne oder externe Klassifizierung für IP-Adressen ändern](#) von der Seite Network Localities.

Bedrohungsinformationen

Das ExtraHop-System beinhaltet ein kuratiertes [Bedrohungsinformationen](#) Feed, der über die Cloud aktualisiert wird, sobald neue Bedrohungen entdeckt werden. Du kannst auch [Bedrohungssammlungen hinzufügen](#) von einem Drittanbieter oder über einen Partner [Integrationen mit ExtraHop Reveal \(x\) 360](#).

Bedrohungsinformationen

[Bedrohungsinformationen](#) Informationen über drohende Bedrohungen bereitstellen, die auf Netzwerke abzielen. Aktualisierte 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

Reveal (x) 360 bietet mehrere Integrationen von Drittanbietern, die das Erkennung- und Reaktionsmanagement verbessern und einen besseren Einblick in den Netzwerkverkehr bieten können.

[Cortex XSOAR](#)

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

[CrowdStrike](#)

Importieren Sie Bedrohungsinformationen aus CrowdStrike Falcon X, sehen Sie sich Details zu CrowdStrike-Geräten an und speichern Sie diese Geräte aus dem ExtraHop-System.

[CrowdStrike Falcon Logwaage](#)

Geben Sie Filterkriterien für ExtraHop-Sicherheitserkennungen an und exportieren Sie die Ergebnisse nach CrowdStrike Falcon LogScale.

Microsoft 365 [↗](#)

Importieren Sie Microsoft 365-Erkennungen und -Ereignisse, überwachen Sie Microsoft 365-Metriken in integrierten Dashboards und zeigen Sie Details zu Risikoereignissen in Datensätzen an.

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.

QRadar [↗](#)

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

Splunk [↗](#)

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

Splunk SOAR [↗](#)

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

Im ExtraHop-System navigieren

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.

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 Hauptbereichen 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 einschätzen, sich über Protokollaktivitäten und Geräteverbindungen informieren und eingehenden und ausgehenden 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.

Dashboards

klicken **Dashboards** 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.

Alerts

klicken **Alerts** 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 Navigation auf oberster Ebene zeigt die **Erkennungen** Speisekarte. klicken **Erkennungen** um anhand Ihrer wire data identifizierte Erkennungen einzusehen. Sie können auf gespeicherte Erkennungen zugreifen, auch wenn Sensor ist vom Machine Learning-Dienst getrennt.



Hinweis: Erkennungen durch maschinelles Lernen erfordern eine [Verbindung zu ExtraHop Cloud Services](#).

Vermögenswerte

klicken **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, in der Navigation auf oberster Ebene wird das Menü Datensätze angezeigt. klicken **Rekorde** um alle gespeicherten Datensätze für das aktuelle Zeitintervall abzufragen. Aufzeichnungen sind strukturierte Informationen über Transaktionen, Nachrichten und Netzwerkflüsse.

Pakete

Wenn Ihr ExtraHop-System mit einem konfiguriert ist Packetstore, in der Navigation auf oberster Ebene wird das Menü Pakete angezeigt. klicken **Pakete** um alle gespeicherten Pakete für das aktuelle Zeitintervall abzufragen.

Globales Suchfeld

Geben Sie den Namen eines beliebigen Geräts (Hostname oder IP-Adresse, Anwendung oder 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. Die aktuellsten und umfassendsten ExtraHop-Dokumentationen finden Sie auf [ExtraHop-Dokumentationswebsite](#).

Symbol „Systemeinstellungen“

Greifen Sie auf Systemkonfigurationsoptionen wie Auslöser, Benachrichtigungen, Dashboard-Berichte und benutzerdefinierte Geräte zu und klicken Sie, um das ExtraHop-System und die Version

anzuzeigen. klicken **Hinweise zum System** um eine Liste der Funktionen in der aktuellsten Version und allen [Systemhinweise](#) wie z. B. ablaufende Lizenzen oder verfügbare Firmware-Upgrades.

Benutzeroptionssymbol

Loggen Sie sich ein und melden Sie sich von Ihrem Sensor oder Konsole, ändern Sie Ihr Passwort, wählen Sie das Anzeigedesign, [eine Sprache festlegen](#), 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 im Pfad auf einen Seitennamen, um zu dieser Seite zurückzukehren.

Dropdownmenü „Befehl“

Klicken Sie hier, um auf bestimmte Aktionen für die Seite zuzugreifen, die Sie gerade betrachten. Zum Beispiel, wenn Sie klicken **Armaturenbrett** oben auf der Seite das Befehlsmenü  bietet Aktionen zum Ändern von 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 Geräteiname](#) 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

Alerts 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

Auslöser 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](#)

Greifen Sie auf Tastenkombinationen zu

Mithilfe von Tastenkombinationen können Sie schnell im ExtraHop-System navigieren und Dashboards mit wenigen Tastenschlägen verwalten.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Geben Sie eine der folgenden Tastenkombinationen ein:

Tastenkombinationen	Aktion
?	Hilfemenü für Tastenkombinationen ein- oder ausblenden
G dann S	Gehe zu Dashboards
G dann A	Gehe zu Alerts
G dann P	Gehe zu Anwendungsmetriken
G dann N	Gehe zu Netzwerkmetriken
G dann D	Gehe zu Gerätekenzahlen
G dann G	Gehe zu Protokollmetriken
/	Weltweite Suche
O dann H	Zwischen den letzten Seiten wechseln
J	Wählen Sie das nächste Element auf den letzten Seiten
K	Wählen Sie das vorherige Element auf den letzten Seiten
O dann M	Metric Explorer öffnen
G dann E	Gehe zu den Systemeinstellungen
G dann T	Gehe zu Triggers
G dann H	Hilfe öffnen
O dann Q	Systeminformationen anzeigen
STRG+S	Widget-Konfiguration speichern
O dann L	Layoutmodus bearbeiten umschalten
O dann P	Dashboard-Eigenschaften anzeigen
C dann D	Kopieren Sie das aktuelle Dashboard
D dann D	Das aktuelle Dashboard löschen
O dann S	Beschreibungen umschalten
STRG+UMSCHALTTASTE+F	Präsentationsmodus umschalten
N dann D	Neues Dashboard erstellen
N dann F	Einen neuen Ordner erstellen
O dann D	Dock bearbeiten umschalten

Tastenkombinationen	Aktion
P dann P	Drucken oder als PDF exportieren
S dann R	Dashboard-Berichte öffnen (nur Konsolen)
Strg+Klick oder Befehlstaste+Klick	Öffnen Sie bestimmte Links zu Seiten und Ansichten in einem neuen Browser-Tab. Diese Funktion funktioniert in bestimmten Kontextmenüs und Listen-Widgets nicht. Sie können gegebenenfalls auch Seiten in einem neuen Tab über Ihre Browsermenüs öffnen.

Dashboards mit Tastenkombinationen verwalten

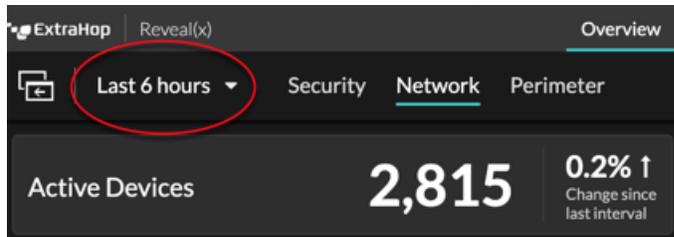
Die folgenden Tastenkombinationen gelten nur für Dashboards.

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

Tastenkombinationen	Aktion
O dann L	Layoutmodus bearbeiten umschalten
O dann P	Dashboard-Eigenschaften anzeigen
C dann D	Kopieren Sie das aktuelle Dashboard
D dann D	Das aktuelle Dashboard löschen
O dann S	Beschreibungen umschalten
Strg+Aufwärtspfeil+F	Präsentationsmodus umschalten
N dann D	Neues Dashboard erstellen
N dann F	Einen neuen Ordner erstellen
O dann D	Dock-Bearbeitungsmodus umschalten

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**.



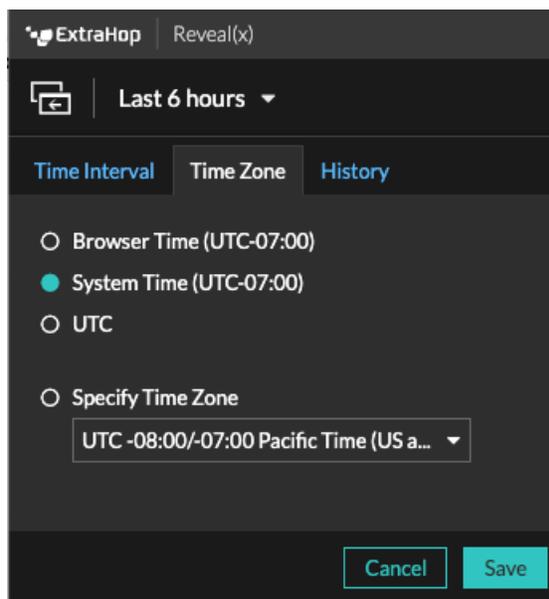
Hinweis Sie können das Zeitintervall auch über den **Geschichte** Klicken Sie auf die Registerkarte, indem Sie aus bis zu fünf aktuellen Zeitintervallen auswählen, die in einer vorherigen Anmeldesitzung festgelegt wurden.

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 Reveal (x) 360:

- Das Ändern der angezeigten Zeitzone wirkt sich auf die Datums- und Zeitstempel aus, die Sie im ExtraHop-System sehen, gilt jedoch nicht für geplante Dashboard-Berichte oder exportierte Dashboards.
- Wenn Sie Ihre Zeitzone ändern, wird die in den Administrationseinstellungen konfigurierte Standardanzeigezeit außer Kraft gesetzt. siehe [Systemzeit](#) (für ExtraHop Performance und Reveal (x) Enterprise) oder [Konfigurieren Sie die Systemzeit](#) (für Reveal (x) 360) für weitere Informationen.

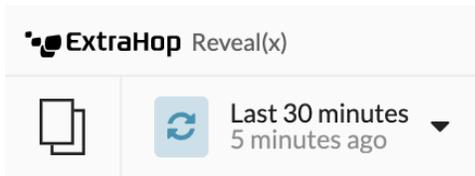


1. <extrahop-hostname-or-IP-address>Melden Sie sich über https://beim ExtraHop-System an.
2. Klicken Sie in der oberen linken Ecke der Seite auf den Zeitselektor.
3. klicken **Zeitzone**.
4. Wählen Sie eine der folgenden Optionen aus:
 - **Browser-Zeit**
 - **Systemzeit**
 - **UTC**
 - **Zeitzone angeben** und wählen Sie dann eine Zeitzone aus der Drop-down-Liste aus.
5. klicken **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	<p>Ein 1-Sekunden-Rollup ist nur für benutzerdefinierte Metriken und für die folgenden integrierten Metriken verfügbar:</p> <ul style="list-style-type: none"> • Netzwerkquelle: <ul style="list-style-type: none"> • Netzwerk-Bytes (Gesamtdurchsatz) • Netzwerkpakete (Gesamtpakete) • Maximale Netzwerk-Bytes pro Millisekunde • Maximale Netzwerkpakete pro Millisekunde • Gerätequelle: <ul style="list-style-type: none"> • Netzwerk-Bytes (kombinierter

Zeitintervall	Aggregations-Rollup (falls verfügbar)	Hinweise
		<p>eingehender und ausgehender Durchsatz pro Gerät)</p> <ul style="list-style-type: none"> • 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	—

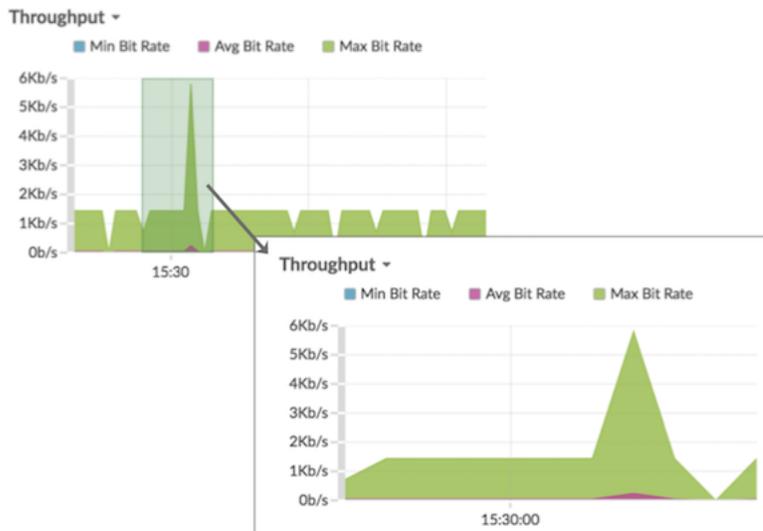
 **Hinweis** Wenn Sie über einen erweiterten Datenspeicher verfügen, der für 24-Stunden-Metriken konfiguriert ist, zeigt ein bestimmtes Zeitintervall von 30 Tagen oder länger einen 24-Stunden-Aggregations-Rollup an.

Vergrößern Sie einen benutzerdefinierten Zeitraum

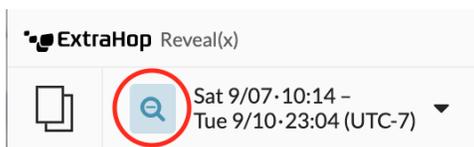
Sie können über ein Diagramm klicken und ziehen, um interessante Metrikaktivitäten zu vergrößern. Dieser benutzerdefinierte Zeitraum wird dann auf das gesamte ExtraHop-System angewendet. Dies ist nützlich, um andere Metrik Aktivitäten zu untersuchen, die gleichzeitig aufgetreten sind.

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.



- 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.

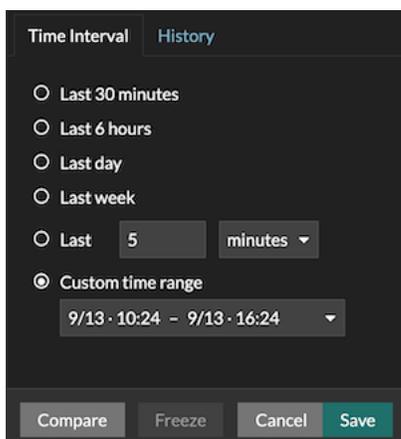


Hinweis Auf einer Dashboard-Seite können Sie den benutzerdefinierten Zeitbereich für das Zoomen auf eine bestimmte Region beschränken. Klicken Sie auf die Kopfzeile der Region und wählen Sie **Region Zeitsелеktor verwenden**, und vergrößern Sie dann ein Diagramm. Jedes Diagramm oder Widget in dieser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

- Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
- Klicken Sie auf die Zeitauswahl in der oberen linken Ecke der Seite.
- Wählen Sie ein voreingestelltes Zeitintervall.
- 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 ausgehenden 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 hervorgehoben werden. Diese Diagramme können Ihnen dabei helfen, das Ausmaß der Sicherheitsrisiken einzuschätzen, Untersuchungen ungewöhnlicher Aktivitäten einzuleiten und Sicherheitsbedrohungen zu mindern. Erkennungen werden je nach Metrik alle 30 Sekunden oder jede Stunde analysiert.

Für Triage empfohlen

Dieses Diagramm zeigt Ihnen eine Liste der Erkennungen, die ExtraHop auf der Grundlage einer kontextuellen Analyse Ihrer Umgebung empfiehlt. Klicken Sie auf eine Erkennung, um die [Erkennungskarte](#) in [Triage-Ansicht](#) auf der Seite Erkennungen.

Erkennungstypen

Dieses Diagramm zeigt die Anzahl der verschiedenen Erkennungstypen, die in den Kategorien Attack, Hardening und Operations während des ausgewählten Zeitintervalls aufgetreten sind. Wenn Sie das Zeitintervall ändern, können Sie sehen, wie viele Erkennungstypen während dieser Zeit aufgetreten sind. Klicken Sie auf eine Zahl, um die Seite Erkennungen zu öffnen, die gefiltert ist, sodass die Erkennungen für jeden Typ in der ausgewählten Erkennungskategorie angezeigt werden.

Erkennungen nach Angriffskategorie

Dieses Diagramm bietet einen schnellen Überblick über die Arten von Angriffen, denen Ihr Netzwerk ausgesetzt sein könnte, und zeigt die Anzahl der Erkennungen an, die in jeder Kategorie während des ausgewählten Zeitintervalls aufgetreten sind. Aktionen bei objektiven Erkennungen sind nach Typ sortiert, damit Sie die schwerwiegendsten Erkennungen priorisieren können. Klicken Sie auf eine beliebige Zahl, um eine gefilterte Ansicht der Erkennungen zu öffnen, die der ausgewählten Zahl entsprechen [Angriffskategorie](#).

Häufige Straftäter

Dieses Diagramm zeigt die 20 Geräte oder Endgeräte, die bei einer oder mehreren Erkennungen als Täter gehandelt haben. Das ExtraHop-System berücksichtigt die Anzahl der verschiedenen Angriffskategorien und Erkennungstypen sowie die Risikobewertung der Erkennungen, die mit den einzelnen Gerät verknüpft sind, um festzustellen, welche Geräte als häufige Angreifer gelten.

Die Größe des Gerätesollensymbols 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 [Geräteeigenschaften](#).

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 der Geschäftsleitung

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

Seitenauswahl

Klicken Sie oben auf der Seite auf die Site-Auswahl, um Daten für eine oder mehrere Websites in Ihrer Umgebung anzuzeigen. Sehen Sie sich den kombinierten Datenverkehr in Ihren Netzwerken an oder konzentrieren Sie sich auf einen einzelnen Standort, um Gerätedaten schnell zu finden. Die Seitenauswahl gibt an, wann alle oder einige Websites offline sind. Da Daten von Offline-Websites nicht verfügbar sind, zeigen die mit Offline-Websites verknüpften Diagramme und Geräteseiten möglicherweise keine oder nur begrenzte Daten an. Der Site-Selector ist nur verfügbar von Konsole.

(nur NDR-Modul) Executive Report

Klicken **Bericht für die Geschäftsleitung erstellen** um eine PDF-Datei zu erstellen. Der Executive Report bietet eine Zusammenfassung der wichtigsten Erkennungen und Risiken für Ihr Netzwerk in der letzten Woche. Der Executive Report enthält nur Informationen für die ausgewählten Standorte.

Überblick über das Netzwerk

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

Erkennungskategorie umschalten

Sie können zwischen den angezeigten Ansichten hin- und herschalten **Alle Angriffserkennungen** oder **Alle Leistungserkennungen**, abhängig von den aktivierten Modulen und Ihrem Modulzugriff.

Straftäter bei Fahndungen

Diese Liste zeigt Straftäter, sortiert nach der Anzahl der Erkennungen, bei denen das Gerät oder der Endpunkt als Täter gehandelt hat.

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

- Klicken Sie in der Liste auf ein Gerät oder einen Endpunkt, um die zugehörigen Erkennungen in der Erkennungsübersicht hervorzuheben und die Geräteeigenschaften anzuzeigen und auf Links zuzugreifen [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 um zum Erkennungen Seite, [gefiltert nach Erkennungskategorie und gruppiert nach Quelle](#).
- Wählen Sie den **Erkennungen ohne Opfer anzeigen** Kontrollkästchen, um Erkennungen anzuzeigen, an denen kein beteiligtes Opfer Teilnehmer ist. Beispielsweise schließen SSL/TLS-Scans und bestimmte Warnmeldungen bei verdächtigen Aktivitäten 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 der Geschäftsleitung

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

Seitenauswahl

Klicken Sie oben auf der Seite auf die Site-Auswahl, um Daten für eine oder mehrere Websites in Ihrer Umgebung anzuzeigen. Sehen Sie sich den kombinierten Datenverkehr in Ihren Netzwerken an oder konzentrieren Sie sich auf einen einzelnen Standort, um Gerätedaten schnell zu finden. Die Seitenauswahl gibt an, wann alle oder einige Websites offline sind. Da Daten von Offline-Websites nicht verfügbar sind, zeigen die mit Offline-Websites verknüpften Diagramme und Geräteseiten möglicherweise keine oder nur begrenzte Daten an. Der Site-Selector ist nur verfügbar von Konsole.

(nur NDR-Modul) Executive Report

Klicken **Bericht für die Geschäftsleitung erstellen** um eine PDF-Datei zu erstellen. Der Executive Report bietet eine Zusammenfassung der wichtigsten Erkennungen und Risiken für Ihr Netzwerk in der letzten Woche. Der Executive Report enthält nur Informationen für die ausgewählten Standorte.

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 ausläuft.

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 Rate anzuzeigen, mit der Daten von externen Endpunkten eingehend übertragen werden, und eine Aufschlüsselung nach Standort oder Konversation vornehmen.

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 vornehmen.

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 Zählendiagramm zeigt die Anzahl der Verbindungen, 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 Reveal (x) 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 ausgehenden 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 ausgehenden 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 der Geschäftsleitung

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

Seitenauswahl

Klicken Sie oben auf der Seite auf die Site-Auswahl, um Daten für eine oder mehrere Websites in Ihrer Umgebung anzuzeigen. Sehen Sie sich den kombinierten Datenverkehr in Ihren Netzwerken an oder konzentrieren Sie sich auf einen einzelnen Standort, um Gerätedaten schnell zu finden. Die Seitenauswahl gibt an, wann alle oder einige Websites offline sind. Da Daten von Offline-Websites nicht verfügbar sind, zeigen die mit Offline-Websites verknüpften Diagramme und Geräteseiten möglicherweise keine oder nur begrenzte Daten an. Der Site-Selector ist nur verfügbar von Konsole.

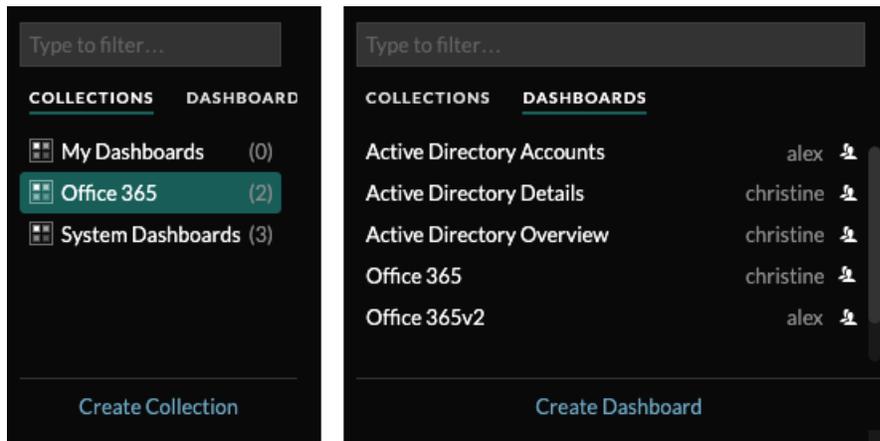
(nur NDR-Modul) Executive Report

Klicken **Bericht für die Geschäftsleitung erstellen** um eine PDF-Datei zu erstellen. Der Executive Report bietet eine Zusammenfassung der wichtigsten Erkennungen und Risiken für Ihr Netzwerk in der letzten Woche. Der Executive Report enthält nur Informationen für die ausgewählten Standorte.

Armaturenbretter

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

Dashboards und Sammlungen befinden sich im Dashboard-Dock.



Klicken **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 wem 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 **Armaturenbretter** um eine alphabetische Liste aller Dashboards anzuzeigen, die Ihnen gehören oder die mit Ihnen geteilt wurden, einschließlich der 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 gelöscht 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.

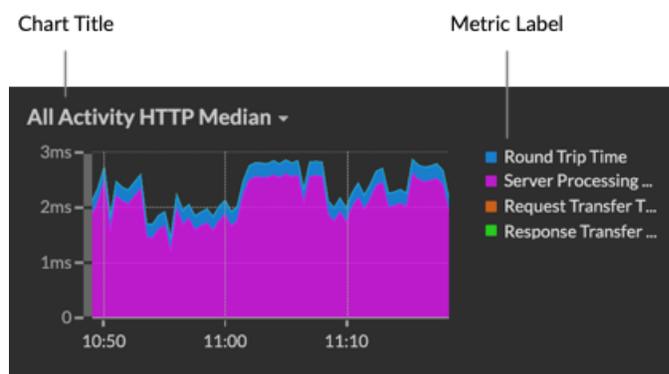
Erfahren Sie, wie Sie Ihr Netzwerk überwachen können, indem Sie [Durchführen einer Dashboard-Komplettlösung](#).

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 [Systemintegritäts-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 Network 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.

 **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 Reveal (x) -Abonnement beinhaltet keine Bedrohungsinformationen.
- Sie haben die Bedrohungsinformationen für Ihr ExtraHop Reveal (x) -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.

SSL - Sitzungen

Beobachten Sie die Anzahl der aktiven SSL-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 SSL-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.

SSL - Zertifikate

Beobachten Sie, welche SSL-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 Kataloge und Gruppenrichtlinien verfolgen.

Jedes Diagramm im Active Directory Directory-Dashboard enthält Visualisierungen von Active Directory-Kontodaten, die über die [ausgewähltes Zeitintervall](#), nach Region organisiert.

Das Active Directory Directory-Dashboard ist ein integriertes System-Dashboard, das Sie nicht bearbeiten, löschen oder zu einer gemeinsam genutzten 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 für Sie relevante Kennzahlen zu überwachen.



Hinweis Von einer Konsole aus können Sie das Active Directory Directory-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.

Die folgenden Informationen fassen jede Region und ihre Diagramme zusammen.

Zusammenfassung des Benutzerkontos

Sehen Sie sich die Anzahl der Active Directory Directory-Konten in Ihrer Umgebung in den folgenden Diagrammen an:

- **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 Servicezugriffsanfrage gesendet haben.

Fehler bei der Authentifizierung

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

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

Details zu Authentifizierungsfehlern

Einzelheiten zu Active Directory Directory-Konten, bei denen Authentifizierungsfehler auftraten, finden Sie in den folgenden Diagrammen:

- **Benutzerkonten:** Benutzernamen, die Benutzerkonten zugeordnet sind, bei denen die Anmeldung fehlgeschlagen ist. In diesem Diagramm wird auch angezeigt, wie oft jedes Benutzerkonto aufgrund eines ungültigen Passworts oder eines abgelaufenen Kontos einen Fehler erhalten hat.
- **Computerkonten:** Client-IP-Adressen und Hostnamen, die Benutzerkonten zugeordnet sind, bei denen die Anmeldung fehlgeschlagen ist. In diesem Diagramm wird auch angezeigt, wie oft jedes Benutzerkonto aufgrund eines ungültigen Passworts oder eines abgelaufenen Kontos einen Fehler erhalten hat.

Service zur Erteilung von Tickets

Sehen Sie sich die Transaktionsdaten im Zusammenhang mit dem Kerberos-Ticketgewährungsdienst in den folgenden Diagrammen an:

- **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 unbekanntem SPN-Fehler, die von dem SPN aufgeführt wurden, der den Fehler gesendet hat.
- **Unbekannte SPN-Fehler vom Client:** Anzahl der unbekanntem 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 mit der Gruppenrichtlinie verknüpften CIFS/SMB-Transaktionsdaten in den folgenden Diagrammen:

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

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 zu senden, nachdem das letzte Paket der Anfrage empfangen wurde.
- **Unsichere LDAP-Anmeldeinformationen :** Gesamtzahl der Klartext-Bindungsanfragen. Wird als Liniendiagramm und Listendiagramm angezeigt.

Globaler Katalog

Sehen Sie sich die mit dem globalen Katalog verknüpften Transaktionsdaten in den folgenden Diagrammen an:

- **Transaktionen:** Gesamtzahl der Antworten und Fehler im globalen Katalog.
- **Transaktionen:** Gesamtzahl der Antworten und Fehler im globalen Katalog, zusätzlich zur Serververarbeitungszeit, die benötigt wurde, um das erste Paket als Antwort zu senden, nachdem das letzte Paket der globalen Kataloganforderung empfangen wurde.

DNS-Dienstaufzeichnungen

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

- **Transaktionen:** Gesamtzahl der Antworten und Fehler in Serviceaufzeichnungen.
- **Transaktionen:** Gesamtzahl der Antworten und Fehler von Servicedatensätzen, zusätzlich zur Serververarbeitungszeit, die benötigt wurde, um das erste Paket als Antwort zu senden, nachdem das letzte Paket der Anfrage empfangen wurde.

Systemintegritäts-Dashboard

Das Systemstatus-Dashboard bietet eine große Sammlung von Diagrammen, mit denen Sie sicherstellen können, dass Ihr ExtraHop-System wie erwartet läuft, Probleme beheben und Bereiche bewerten können, 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 von Systemleistungsdaten, die über die [ausgewähltes Zeitintervall](#), nach Region organisiert.

Das Systemintegritäts-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 System Health 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.



Hinweis Die Seite mit den Administrationseinstellungen bietet auch [Statusinformationen und Diagnosetools](#) für alle ExtraHop-Systeme.

Navigieren Sie im Systemstatus-Dashboard

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

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

Geräteerkennung

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

Datenfeed

Beurteilen Sie die Effizienz der Kabeldatenerfassung anhand von Diagrammen zu Durchsatz, Paketrate, Desynchronisierung und Erfassungsverlusten.

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

SSL Zertifikate

Überprüfen Sie die Statusinformationen für alle SSL-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 Arbeitssets und die Triggeraktivität im Systemdatenspeicher.

Geräteerkennung

Die Geräteerkennung Ein Abschnitt des Systemstatus-Dashboards bietet einen Überblick über die Gesamtzahl der Geräte in Ihrem Netzwerk. Sehen Sie, welche Arten von Geräten angeschlossen sind und wie viele dieser Geräte derzeit aktiv sind.

Die Geräteerkennung Dieser Abschnitt enthält die folgenden Diagramme:

- [Aktive Geräte](#)
- [Geräte insgesamt](#)

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.

Geräte insgesamt

Ein Liniendiagramm, das die Gesamtzahl der vom ExtraHop-System überwachten L3- und benutzerdefinierten Geräte anzeigt, unabhängig davon, ob sie aktiv oder inaktiv sind, im ausgewählten Zeitintervall. Neben dem Flächendiagramm wird in einem Wertdiagramm die Gesamtzahl der L3- und benutzerdefinierten Geräte angezeigt, die derzeit vom ExtraHop-System überwacht werden.

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 Netzwerks 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 Gesamtanzahl an Geräten enthält.

Datenfeed

Die Datenfeed In einem Bereich des Systemstatus-Dashboards können Sie die Effizienz der Kabeldatenerfassung anhand von Diagrammen zu Durchsatz, Paketrate, Desynchronisierung und Erfassungsausfällen beobachten.

Die Datenfeed Dieser Abschnitt enthält die folgenden Diagramme:

- [Durchsatz](#)
- [Paket-Rate](#)
- [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.

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.

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 Datensätze 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 Datenduplikation 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 auslösen](#) und [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

Verworfenen 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 Zielsystem 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 Zielsystem

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

Verworfenen Nachrichten in voller Warteschlange

Die Anzahl der an Datensatzspeicher und ODS-Ziele gesendeten Nachrichten, die gelöscht wurden, weil die Nachrichtenwarteschlange auf dem Zielsystem voll war. Eine hohe Anzahl verworfener Nachrichten kann darauf hindeuten, dass der Nachrichtendurchsatz zu hoch ist, um vom ExtraHop-System oder dem Zielsystem 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.

SSL Zertifikate

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

Die SSL Zertifikate Dieser Abschnitt enthält die folgende Tabelle:

- [Einzelheiten zum Zertifikat](#)

Einzelheiten 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 nicht entschlüsselt werden konnten, z. B. beim DHE-Schlüsselaustausch.

Getrennte Sitzungen

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. aufgrund von Fehlern, die durch Überschreitung der Spezifikationen der SSL-Beschleunigungshardware verursacht 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 SSL-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 Systemnutzungs-Dashboard können Sie überwachen, wie Benutzer mit dem ExtraHop-System interagieren.

Jedes Diagramm im Systemnutzungs-Dashboard enthält Visualisierungen von Benutzerinteraktionen mit dem ExtraHop-System und Erkennungen, die über das [ausgewählte Zeitintervall](#), nach Region organisiert.



Hinweis Das Systemnutzungs-Dashboard ist ein integriertes System-Dashboard, das Sie nicht bearbeiten, löschen oder zu 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-Benutzer

Beobachten Sie die Benutzeranmeldeaktivitäten und die aktuelle Anzahl der aktiven Benutzer auf dem ExtraHop-System.

- **Aktive Benutzer und Logins:** Die Häufigkeit, mit der sich Benutzer beim ExtraHop-System angemeldet haben, und aktuelle Schnappschüsse von aktiven Benutzern. Das Liniendiagramm zeigt die aktuell aktiven Benutzer und das Säulendiagramm zeigt die Anzahl der Benutzeranmeldungen im Laufe der Zeit. 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 Anmeldungen auf dem 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.

Armaturenbrett

Beobachten Sie, wie oft Benutzer sie ansehen [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 gemeinsam genutzte URL angezeigt wird.
- **Am häufigsten aufgerufene 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 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 ein [Detailseite zur Erkennung](#) erscheint nach einer Benutzeranmeldung, einem Klick oder einer direkten Navigation durch eine gemeinsam genutzte URL. Klicken Sie in der Legende auf einen der Metriknamen, um eine Aufschlüsselung nach Erkennungstyp vorzunehmen.
- **Am häufigsten aufgerufene Erkennungen:** Die Erkennungstypen, die im ausgewählten Zeitintervall am häufigsten angesehen wurden.
- **Gesamtzahl der Erkennungsansichten:** Die Gesamtwerte für Erkennungslistenansichten und Erkennungsdetailansichten über das ausgewählte Zeitintervall.
- **Erkennungsverfolgung (Liniendiagramm):** Die Anzahl der Entdeckungen, die mit und ohne ergriffene Maßnahmen abgeschlossen wurden, und die Anzahl der Untersuchungen, die im Laufe der Zeit eingeleitet wurden.
- **Erkennungsverfolgung (Listendiagramm):** Die Gesamtzahl der Entdeckungen, die mit und ohne ergriffene Maßnahmen geschlossen 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, die derzeit auf den Status In Bearbeitung gesetzt sind.
- **Gesamtzahl geschlossener Erkennungen:** Die Gesamtzahl der Erkennungen, die im ausgewählten Zeitintervall mit und ohne ergriffene Maßnahmen geschlossen wurden. Die Werte für „Gesamtzahl geschlossener Erkennungen“ schließen Erkennungen ein, die ausgeblendet wurden, nachdem der Erkennungsstatus festgelegt wurde.

Erkennungstypen

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

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

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 **Armaturenbrett**.
3. Führen Sie auf der Seite Dashboards einen der folgenden Schritte aus:
 - klicken **Armaturenbrett** 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-Ausgabertext wird dynamisch im rechten Vorschauenfenster 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](#)
 - [Bearbeiten Sie ein Diagramm mit dem Metric Explorer](#)

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 **Armaturenbrett**.
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 Quellenmenü in Ihrem Dashboard ausblenden möchten, fügen Sie den folgenden Parameter an das Ende der URL der Dashboard-Seite an: `&hideTemplatePanel=true`.

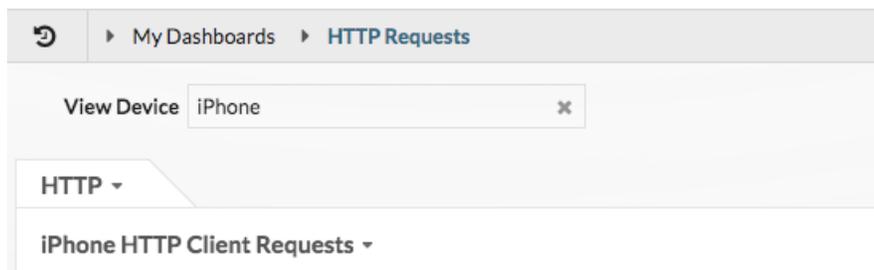


Abbildung 3: Vorher

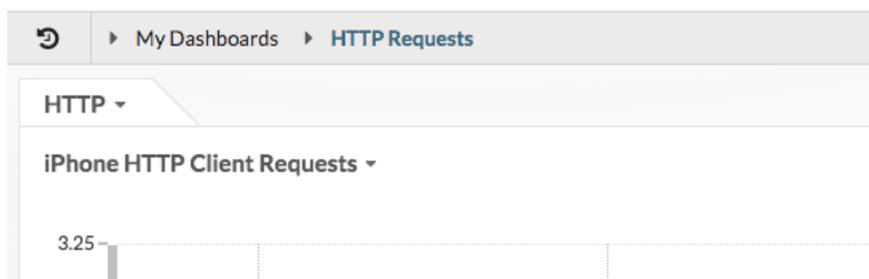


Abbildung 4: Nach

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 Anwendungs-, Gerät- oder Netzwerkdaten anzuzeigen. Sie können jeweils nur ein Dashboard kopieren.



Hinweis Wenn Sie nur ein Dashboard kopieren möchten, damit Sie die Quelle für das gesamte Dashboard ändern können, sollten Sie Folgendes in Betracht ziehen [ein Dashboard mit dynamischen Quellen erstellen](#) anstatt mehrere Kopien eines einzigen 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 auszuführen:
 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 modifizierten 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 **Eigenschaften des Dashboards**.
 - c) Geben Sie im Feld Titel einen neuen Namen ein.
 - d) klicken **Speichern**.



Hinweis Um ein Dashboard schnell zu kopieren, geben Sie die Tastenkombination ein `CD` und dann aktualisieren [Eigenschaften des Dashboards](#) oder ändern Sie Quellen.

Nächste Schritte

- [Eine Dashboard-Region bearbeiten](#)
- [Bearbeiten Sie ein Diagramm mit dem Metric Explorer](#)
- [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](#)

Bearbeiten Sie ein Diagramm mit dem Metric Explorer

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

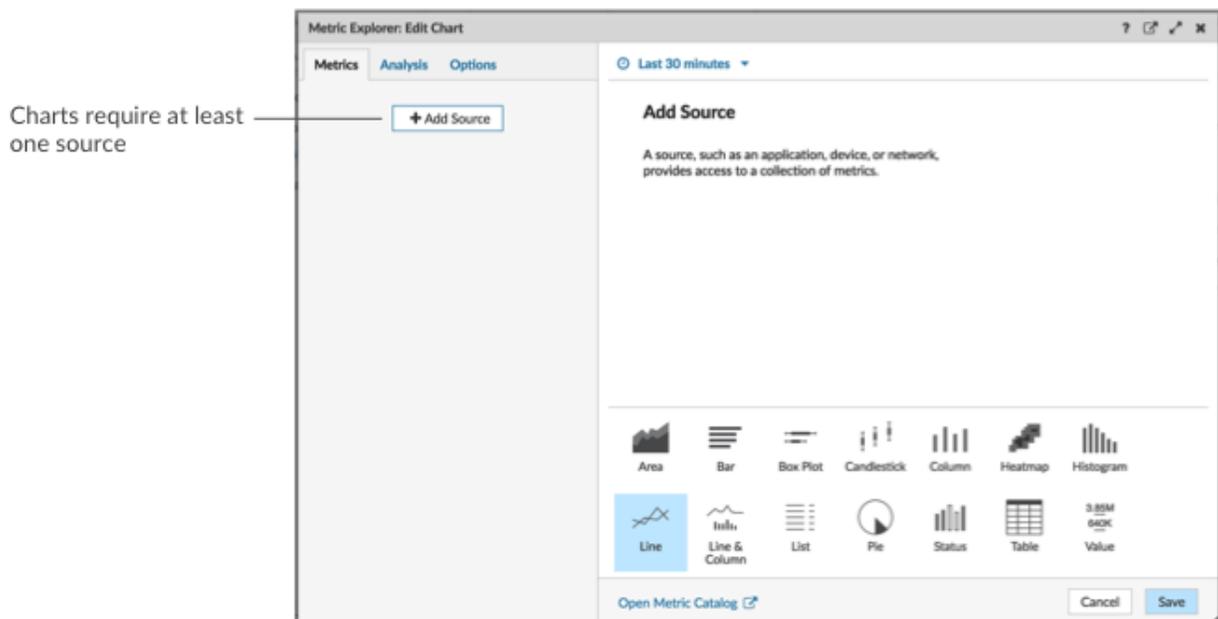
Sie müssen eine persönliche Schrift haben [Privilegien](#) oder höher und NPM-Modulzugriff zum Erstellen und Bearbeiten von Diagrammen in einem Dashboard.

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.

Type a protocol and metric name. Charts require at least one protocol metric.

If you are not sure about the name of a metric, you can search the Metric Catalog.

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

A single source type (such as an application) and at least one metric create a set. You can add more metrics to the set. To add another source type to your chart, click **Add Source** below the set.

Some chart types are only compatible with specific metric types. If a chart is not compatible with selected metrics, you cannot select it.

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

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

The screenshot shows the 'Metric Explorer: Edit Chart' window. On the left, there are three sections: 'Sources' with 'web1-sea' and 'web2-sea' listed, a 'Combine sources' checkbox, and an 'Add Device' button; 'Metrics' with 'HTTP Server - Requests' and 'Count' selected, and an 'Add Metric' button; and 'Details' with a 'Drill down by Client' dropdown set to 'Any IP Address' and a 'Top 5 results' display. The main area shows a line chart titled 'My web server chart' for the 'Last 30 minutes' period. The chart has a y-axis from 0 to 60 and an x-axis from 9:00 to 9:20. A dashed horizontal line is drawn at y=50. The legend on the right lists five request sources with corresponding colored lines. At the bottom, there is a chart type selector with icons for Area, Bar, Box Plot, Candlestick, Column, Heatmap, Histogram, Line (selected), Line & Column, List, Pie, Status, Table, and Value. Buttons for 'Open Metric Catalog', 'Cancel', and 'Save' are at the bottom right.

Sehen Sie sich Metrik Daten und Quellen genauer an, um Details anzuzeigen

Im Abschnitt „Details“ auf der Registerkarte „Metriken“ können Sie [Drilldown zur Anzeige detaillierter Metriken](#) oder [Drilldown zu einer Gerätegruppe](#) um einzelne Geräte innerhalb des Diagramms anzuzeigen. Sie können auch Detailmetriken nach exakten Übereinstimmungen filtern oder eine erstellen [Regex-Filter](#).

Fügen Sie auf der Registerkarte Analyse eine Basis- oder Schwellenwertlinie hinzu

Du [eine Dynamische Basislinie hinzufügen](#) oder [statische Schwellenwertlinie](#) zu deinem Diagramm.

Basislinien werden berechnet, nachdem das Diagramm gespeichert wurde. Um eine Linie anzuzeigen, die einen Schwellenwert darstellt, z. B. einen SLA-Wert (Service Level Agreement), fügen Sie Ihrem Diagramm eine statische Schwellenwertlinie hinzu.

Legendenbeschriftungen und den Diagrammtitel umbenennen

Bei Diagrammen, in denen eine Legende angezeigt wird, können Sie einen Metriknamen in der Diagrammlegende mit einem ändern [benutzerdefiniertes Etikett](#). Klicken Sie im Metric Explorer im Vorschauenfenster auf die Bezeichnung und wählen Sie dann **Umbenennen**. Um ein Diagramm umzubenennen, klicken Sie auf den Diagrammtitel und wählen **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:

- Metrik Daten von Byte in Bits umwandeln
- Metrik Daten von Basis 2 (Ki=1024) nach Basis 10 (K = 1000) konvertieren
- Ändern Sie die Y-Achse in einem Zeitreihendiagramm von einer linearen auf eine logarithmische Skala
- Metrikwerte in einem Diagramm abkürzen (z. B. 16.130.542 Byte auf 16,1 MB abkürzen)
- Sortieren von Metrikdaten in aufsteigender oder absteigender Reihenfolge in einem Balken-, Listen- oder Wertediagramm
- Ändern der Perzentilgenauigkeit in einem Tortendiagramm
- Eine Diagrammlegende ein- oder ausblenden
- Blenden Sie inaktive Metriken mit einem Wert von Null aus, sodass diese Metriken im Diagramm nicht sichtbar sind, einschließlich der Legende und der Bezeichnung
- Sparkline in eine Liste oder ein Wertediagramm einbeziehen
- Den Warnstatus für Daten anzeigen, die in Listen- oder Wertediagrammen angezeigt werden (weitere Informationen finden Sie unter [Alerts](#))
- Schalten Sie die Farbanzeige für Metrik Daten auf Graustufen um (mit Ausnahme von Diagrammen , die einen Warnstatus anzeigen)
- Zeigen Sie für IP-Adressbezeichnungen den Hostnamen (falls er anhand des DNS-Verkehrs in wire data erkannt wird) oder die Quell-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 SSL-Zertifikat abläuft.



Hinweis Einige Optionen sind nur für bestimmte Diagrammtypen verfügbar. Beispielsweise wird die Option, eine Sparkline einzubeziehen, nur auf der Registerkarte Optionen für Listen- und Wertediagramme angezeigt.

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 diese beiden 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](#) 

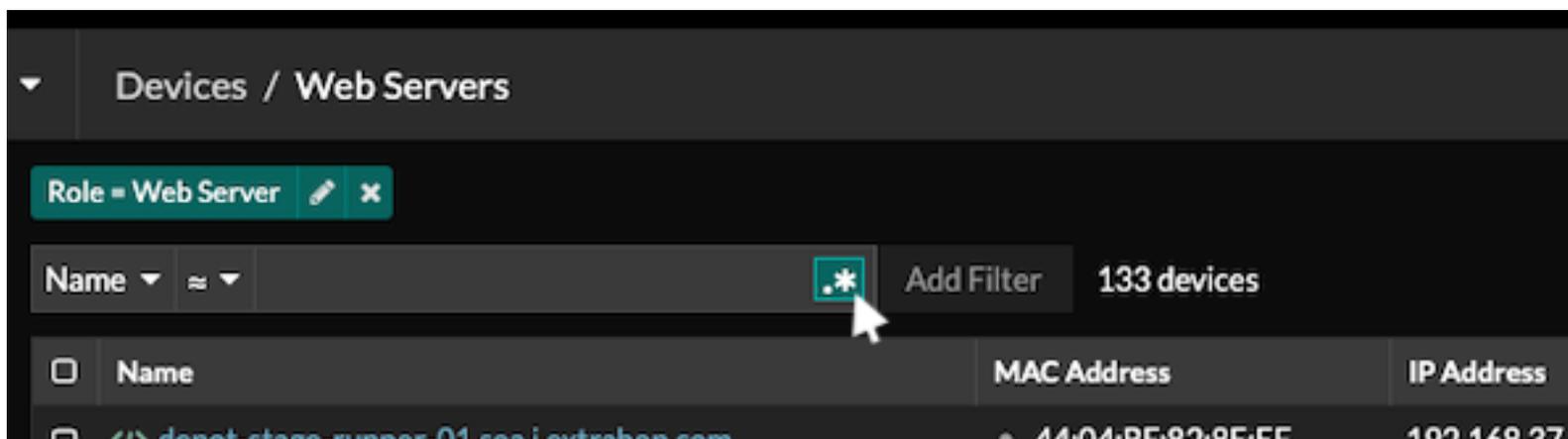
Filter für reguläre Ausdrücke

Filtern Sie Ihre Suchergebnisse, indem Sie reguläre Ausdrücke (Regex) in bestimmte Suchfelder im gesamten ExtraHop-System 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 im gesamten System über visuelle Indikatoren und akzeptieren die Standardsyntax.

Suchfelder mit einem Sternchen

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

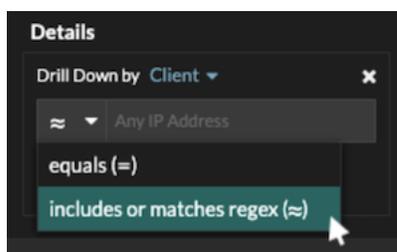


Dieser Feldtyp ist auf den folgenden Systemseiten verfügbar:

- 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.

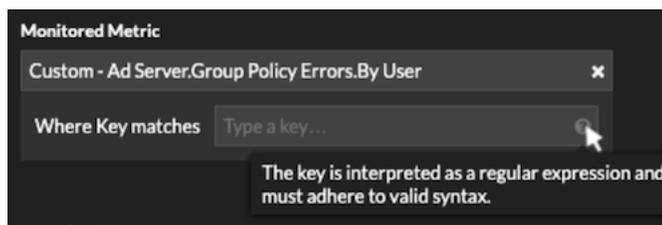


Dieser Feldtyp ist auf der folgenden Systemseite verfügbar:

- Bearbeiten eines Diagramms im Metric Explorer

Bestimmte Suchfelder mit einem Tooltip

Bewegen Sie den Mauszeiger über 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.

Chart-Szenario	Regex-Filter	So funktioniert
HTTP-Statuscodes vergleichen 200 zu 404.	(200 404)	Das vertikale Balkensymbol () ist der OR-Operator. Dieser Filter passt 200, oder 404, oder beide Statuscodes.

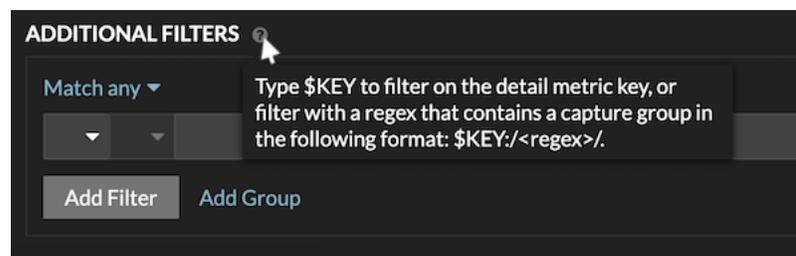
Chart-Szenario	Regex-Filter	So funktioniert
Zeigt einen beliebigen HTTP-Statuscode an, der eine enthält 4.	[41]	Eckige Klammern ([und]) kennzeichnen einen Zeichenbereich. Der Filter sucht nach jedem Zeichen innerhalb der Klammern, unabhängig von der Reihenfolge. Dieser Filter entspricht jedem Wert, der eine enthält 4 oder ein 1. Dieser Filter kann beispielsweise zurückgeben 204, 400, 101, oder 201 Statuscodes.
Alle anzeigen 500HTTP-Statuscodes auf -Ebene.	^ [5]	Das Caret-Zeichen (^) außerhalb der eckigen Klammern ([und]) bedeutet „beginnt mit“. Dieser Filter entspricht jedem Wert, der mit a beginnt 5. Dieser Filter kann beispielsweise zurückgeben 500 und 502 Statuscodes.
Alle anzeigen 400 und 500 HTTP-Statuscodes auf -Ebene.	^ [45]	Mehrere Werte in eckigen Klammern ([und]) werden einzeln gesucht, auch wenn ihnen das Caret-Symbol (^) vorangestellt ist. Dieser Filter sucht nicht nach Werten, die beginnen mit 45, entspricht aber allen Werten, die mit a beginnen 4 oder 5. Dieser Filter kann beispielsweise zurückgeben 400, 403, und 500 Statuscodes.
Zeigt alle HTTP-Statuscodes an, außer 200 Statuscodes auf -Ebene.	^ (?! 2)	Ein Fragezeichen (?) und Ausrufezeichen (!) in Klammern geben einen auszuschließenden Wert an. Dieser Filter entspricht allen Werten außer Werten, die mit a beginnen 2. Dieser Filter kann beispielsweise zurückgeben 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 Zeitraum angibt, dass hinter 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 187.18.	187\ ,18.	Spiele 187.18 und alles, was folgt. Der erste Punkt wird wörtlich behandelt, da ihm ein umgekehrter Schrägstrich (\)

Chart-Szenario	Regex-Filter	So funktioniert
		vorangestellt ist. 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.
Zeigen Sie eine beliebige IP-Adresse an, außer 187.18.197.150.	<code>^(?!187\.18\.197\.150)</code>	Passt zu allem außer 187.18.197.150, wo <code>^(?!)</code> gibt den auszuschließenden Wert an.
Schließt eine Liste bestimmter IP-Adressen aus.	<code>^(?!187\.18\.197\.15[012])</code>	Passt zu allem außer 187.18.197.150, 187.18.197.151, und 187.18.197.152, wo <code>^(?!)</code> gibt den auszuschließenden Wert an und die eckigen Klammern ([und]) geben mehrere Werte an.

Zusätzliche Filter

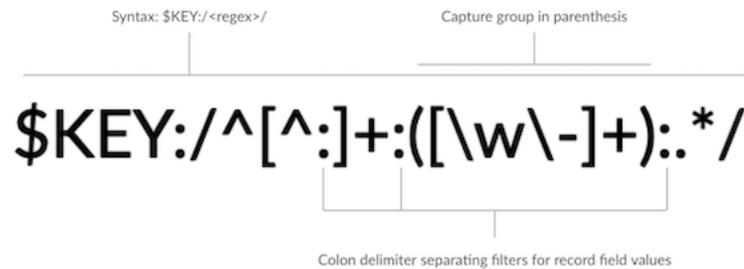
Wenn du [eine benutzerdefinierte Detail-Metrik erstellen](#) im Metrikkatalog können Sie dem Suchfeld **Zusätzliche Filter** im Bereich **Datensatzbeziehungen** erweiterte Regex-Syntax hinzufügen.

Der Tooltip wird angezeigt, nachdem Sie ausgewählt haben **Detail: Metrik** 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 Capture-Gruppe enthalten. Eine Capture-Gruppe wird durch Klammern gekennzeichnet. Ihre Erfassungsgruppe bestimmt den Filterwert.



- Wenn Sie einen bestimmten Wert aus einem Detail-Metrik Metrikschlüssel zurückgeben möchten, der mehrere Datensatzfeldwerte enthält, muss die Regex der folgenden Syntax folgen:

```
$SCHLÜSSEL: / <regex> /
```

Wenn Ihr Detail-Metrik Metrikschlüssel beispielsweise ipaddr:host:cipher lautet und Sie nur den IP-Adresswert zurückgeben möchten, würden Sie Folgendes eingeben:

```
$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 `$-SCHLÜSSEL`. Wenn Ihr Detail-Metrik Metrikschlüssel beispielsweise `ipaddr:host:cipher` lautet, geben Sie ein `$-SCHLÜSSEL` im Suchfeld, um alle drei dieser Felddatensatzwerte (IP-Adresse, Hostname und SSL-Verschlüsselungssuite) zurückzugeben.

Ein Textfeld-Widget bearbeiten

Wenn Sie erklärenden 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.

Das Textfeld-Widget unterstützt Markdown, eine einfache Formatierungssyntax, die einfachen Text mit nicht alphabetischen Zeichen wie „#“ oder „*“ in HTML konvertiert. Neue Textfeld-Widgets enthalten Markdown-Beispiele. Jedes Mal, wenn Sie [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 **Armaturenbrett**.
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. Text links eingeben und bearbeiten Herausgeber Fensterscheibe.

Der HTML-Ausgabebetext wird dynamisch auf der rechten Seite angezeigt. Vorschau Fensterscheibe. Mit Markdown können Sie die folgenden Inhaltstypen formatieren:

- [Text formatieren](#)

- [Bilder hinzufügen](#)
 - [Beispiele für Metrik hinzufügen](#)
7. klicken **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 in der [GitHub-Anleitungen: Markdown beherrschen](#). Allerdings werden nicht alle Formatierungsoptionen für die Markdown-Syntax im ExtraHop unterstützt [Textfeld-Widget](#).

Format	Beschreibung	Beispiel
Überschriften	Platzieren Sie ein Zahlenzeichen (#) 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.	* First example * Second example
Geordnete Listen	Platzieren Sie eine einzelne Zahl und einen Punkt (1.) vor Ihrem Text.	1. First example 2. Second example
Mutig	Platzieren Sie doppelte Sternchen vor und nach Ihrem Text.	**bold text**
Kursiv	Platzieren Sie vor und nach Ihrem Text einen Unterstrich.	<i>_italicized text_</i>
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
Zitate blockieren	Platzieren Sie eine rechtwinklige Klammer und ein Leerzeichen vor Ihrem Text.	On the ExtraHop website: > Access the live demo and review case studies.
Schrift Monospace	Platzieren Sie vor und nach Ihrem Text einen Backtick (`).	<code>`example code block`</code>
Emojis	Das Hinzufügen von Emojis in der Markdown-Syntax wird nicht unterstützt. Sie können jedoch ein Unicode-Emoji-Bild kopieren und in das Textfeld einfügen.	

Format	Beschreibung	Beispiel
	Sehen Sie die Unicode-Emoji-Diagramm Website für Bilder.	

Bilder in Markdown hinzufügen

Sie können dem Textfeld-Widget Bilder hinzufügen, indem Sie 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 mit Base64 codieren. Weitere Informationen finden Sie im folgenden Beitrag im ExtraHop-Forum: "[Bilder in Textfelder einfügen](#)".

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.

REST API Parameters

```
{
  "metric_category": "nfs_server_detail",
  "object_type": "device",
  "metric_specs": [
    {
      "name": "tcp"
    }
  ]
}
```

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

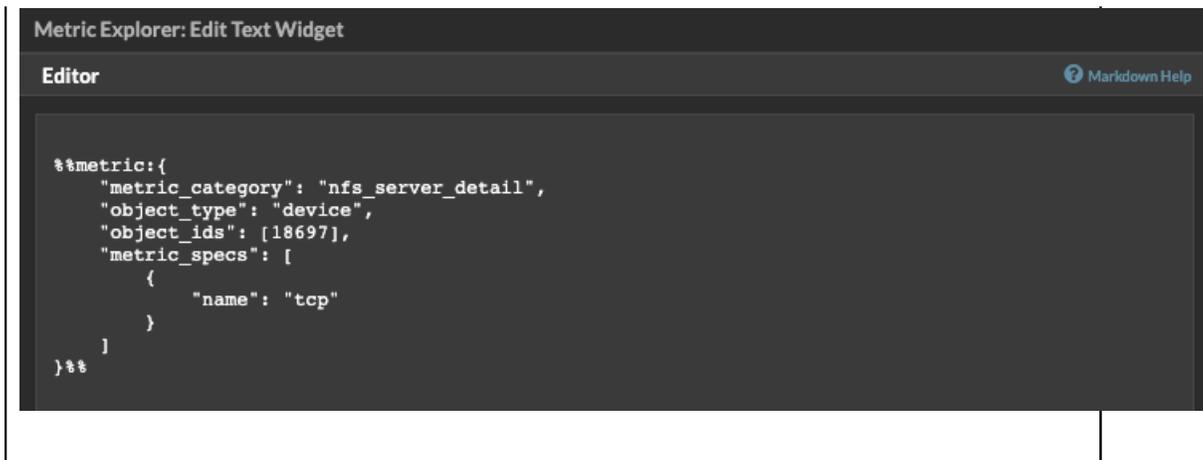
1. Klicken **Vermögenswerte**, und klicken Sie dann im linken Bereich auf einen Asset-Typ.
2. Klicken Sie auf den Namen des gewünschten Asset, und öffnen Sie dann das Eigenschaftenfenster.
3. Notieren Sie sich den Wert, der für die REST-API-ID angezeigt wird.

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

The screenshot shows the 'Device Properties' section of the ExtraHop interface. It includes fields for 'Display Name' (with options for custom or automatic), 'Device Role' (set to 'Auto (Other)'), and 'Device Description'. Under 'API Properties', the 'REST API ID' is highlighted in red and is '18697'. Other API properties shown include 'Discovery ID: 005056b26f100000' and 'URL: /devices/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 eine 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 **Armaturenbrett**.
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

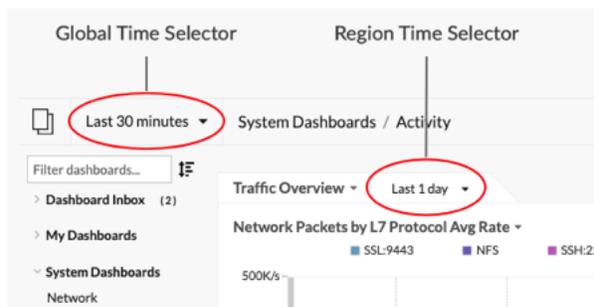
Erweitern Sie den Inhalt der Region zu einer Vollbildanzeige.

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 Time Selector 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 **Armaturenbrett**.
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.

- Um das Zeitintervall für die Region zu entfernen, klicken Sie auf die Überschrift der Region und wählen Sie **Verwenden Sie Global Zeitsелеktor**.
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.

- Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
- Klicken Sie oben auf der Seite auf **Dashboards**.
- Wählen Sie im Dashboard-Dock das Dashboard aus, das Sie bearbeiten möchten.
- Klicken Sie auf das Befehlsmenü  in der oberen rechten Ecke der Seite und wählen Sie dann **Eigenschaften des Dashboards**.
- 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**.

- 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 Anzeigoptionen:

- 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 **Armaturenbrett**.
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 (**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:

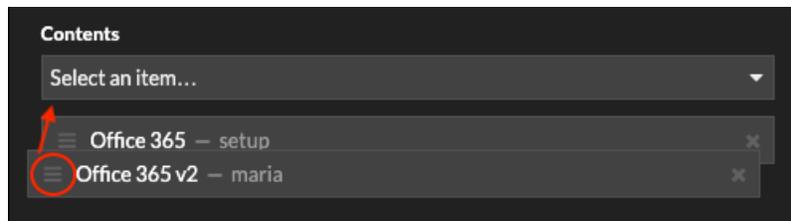
- Ihr **Benutzerrechte**  bestimmen Sie, ob Sie Sammlungen erstellen und teilen können.
 - Sie können einer Sammlung jedes Dashboard hinzufügen, das Ihnen gehört oder das Sie anzeigen oder bearbeiten dürfen.
 - Sie können ein Dashboard zu mehreren Sammlungen hinzufügen.
 - Sie können eine Sammlung teilen, 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.



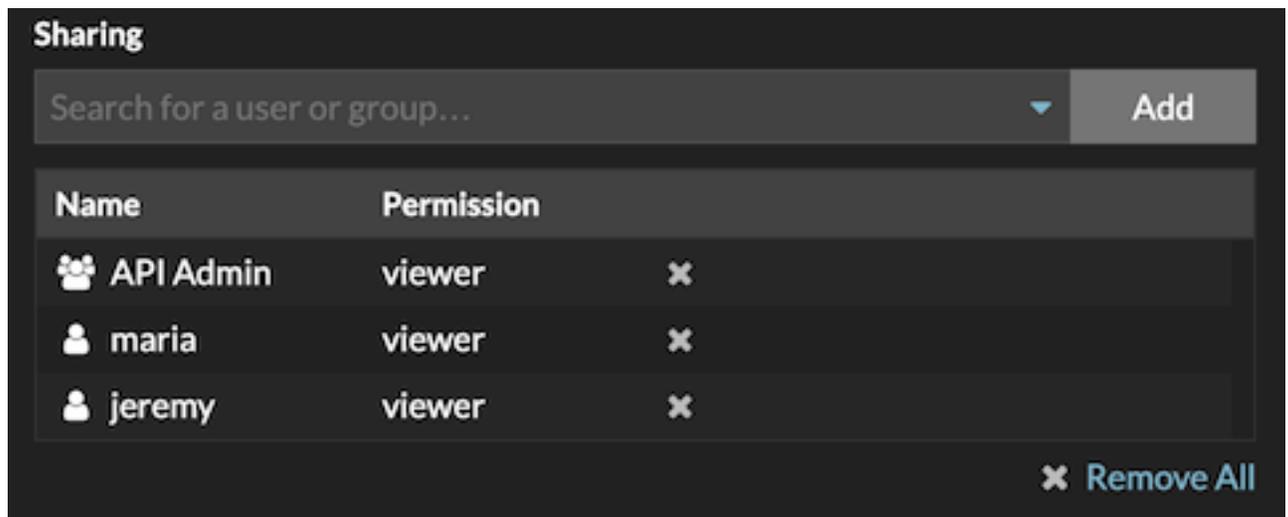
8. klicken **Speichern**.
Die Sammlung wird dem Dashboard-Dock hinzugefügt.

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 **Armaturenbrett**.
 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 **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 **Seite drucken** und wählen Sie dann **PDF** als Ziel aus den Druckeinstellungen in Ihrem Browser.
 - Klicken Sie von einem Sensor aus **Widget drucken** und wähle **PDF** als Ziel aus den Druckeinstellungen in Ihrem Browser.
 - Wählen Sie in einer Konsole [Anpassungen des PDF-Formats](#) und dann klicken **Als PDF exportieren**. Das Generieren einer PDF-Datei kann mehrere Sekunden dauern.



Hinweis über eine Tastenkombination auf die PDF-Druckoptionen zuzugreifen, geben Sie `pers..`

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 Diagrammdateien. 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 Diagrammdateien.

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.

Erstellen Sie einen geplanten Dashboard-Bericht

Sie können eine PDF-Datei mit ausgewählten Dashboards per E-Mail an einen oder mehrere Empfänger senden, indem Sie einen geplanten Dashboard-Bericht über ein Konsole.

Erstellen Sie einen Dashboard-Bericht (Reveal (x) Enterprise)

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

Bevor Sie beginnen

- Ihr Benutzerkonto muss Schreibbeschränkungen oder höher haben [Privilegien](#).
- Sie müssen sich bei einem Reveal (x) Enterprise anmelden Konsole das ist [für das Senden von E-Mails konfiguriert](#).
- Sie können nur einen Bericht für Dashboards erstellen, die Sie besitzen oder auf die Sie gemeinsam 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 dann klicken **Dashboard-Berichte**.
3. klicken **Erstellen**.
4. Geben Sie einen eindeutigen Namen für den Bericht in der **Name des Berichts** Feld.
5. Optional: In der **Beschreibung** Feld, geben Sie Informationen über den Bericht ein. Die Beschreibung erscheint nicht im Abschlussbericht, sondern nur in den Berichtseinstellungen.
6. Aus dem **Inhalt des Berichts** Drop-down-Liste, wählen Sie ein Dashboard aus.
 - Wenn Ihre Umgebung über mehrere Standorte verfügt, müssen Sie eine Standort auswählen.
 - Wenn das von Ihnen ausgewählte Dashboard über eine dynamische Quelle verfügt, müssen Sie eine Quelle auswählen.
7. Optional: Aus dem **Inhalt des Berichts** Wählen Sie in der Dropdownliste zusätzliche Dashboards aus, die Sie dem Bericht hinzufügen möchten.
8. Aus dem Zeitplan Führen Sie in diesem Abschnitt die folgenden Schritte aus, um einen Zeitplan für den Bericht zu konfigurieren:
 - a) Aus dem Zeitintervall Wählen Sie im Abschnitt den Zeitraum der Dashboard-Daten aus, die Sie in den Bericht aufnehmen möchten.
Das Zeitintervall bezieht sich auf die Zeit, zu der der Bericht gesendet wird.
 - b) Aus dem Häufigkeit melden In diesem Abschnitt legen Sie den Zeitplan für die E-Mail-Zustellung fest, indem Sie eine der folgenden Optionen auswählen:

Stündlich

Senden Sie den Bericht jede Stunde per E-Mail.

täglich	Geben Sie die Uhrzeit an, zu der der Bericht per E-Mail gesendet werden soll. klicken Zeitplan hinzufügen um den Bericht mehrmals täglich per E-Mail zu versenden.
Wöchentlich	Geben Sie einen oder mehrere Wochentage und die Uhrzeit an, zu der der Bericht per E-Mail gesendet werden soll. klicken Zeitplan hinzufügen um Berichts-E-Mails mehrmals am Tag oder zu unterschiedlichen Zeiten pro Woche zu versenden.

Die Häufigkeit der Berichte basiert auf [Standard-Systemzeit](#) von Ihrem ExtraHop-Administrator festgelegt.

9. Aus dem Format Führen Sie in diesem Abschnitt die folgenden Schritte aus, um das Berichtsformat zu konfigurieren:
- a) Legen Sie das Inhaltslayout fest, indem Sie aus der ersten eine der folgenden Optionen auswählen Stil Drop-down-Liste:

Schmal	Zeigt großen Text in Diagrammtiteln und Beschriftungen an, bietet jedoch weniger Platz für die Anzeige von Diagramm Daten. Lange Diagrammtitel und Beschriftungen werden möglicherweise gekürzt.
Mittel	(Standard) Zeigt eine Ansicht mit 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 Diagramm Daten.

- b) Legen Sie die Anzahl der Seitenumbrüche in der PDF-Datei fest, indem Sie aus der zweiten Option eine der folgenden Optionen auswählen Stil Drop-down-Liste:

Einzelne Seite	(Standard) 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. Wählen Sie diese Option, wenn Ihr Dashboard eine Tabelle oder Liste enthält, in der mehr als 20 detaillierte Metrikkwerte angezeigt werden.

- c) Stellen Sie das Anzeigethema 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.

10. Aus dem E-Mail senden Führen Sie im Abschnitt die folgenden Schritte aus , um E-Mail-Benachrichtigungen zu konfigurieren:

- a) Optional: Aus dem Benachrichtigungsgruppen Drop-down-Liste, wählen Sie eine Gruppe von Empfängern aus.

Wenn Sie die E-Mail-Gruppe, nach der Sie suchen, nicht sehen, können Sie E-Mail-Gruppen in den ExtraHop-Administrationseinstellungen oder über die REST-API konfigurieren. Wenden Sie sich an Ihren ExtraHop-Administrator, um eine hinzuzufügen [E-Mail-Benachrichtigungsgruppe](#).

- b) In der **Empfänger** 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 Hauptteil der Berichts-E-Mail ein. Die Namen der mit dem Bericht verknüpften Dashboards werden standardmäßig in der Nachricht angegeben.

11. 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 ist 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 Dashboard-Berichts zu beenden, löschen Sie das **Bericht aktivieren** kreuzen Sie den Bericht an oder löschen Sie ihn.

Erstellen Sie einen Dashboard-Bericht (Reveal (x) 360)

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

Bevor Sie beginnen

- Ihr Benutzerkonto muss Schreibbeschränkungen oder höher haben [Privilegien](#).
- Du musst dich bei Reveal (x) 360 anmelden Konsole.
- Sie können nur einen Bericht für Dashboards erstellen, die Sie besitzen oder auf die Sie gemeinsam 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 dann klicken **Dashboard-Berichte**.
3. klicken **Erstellen**.
4. Geben Sie einen eindeutigen Namen für den Bericht in der **Name des Berichts** Feld.
5. Optional: In der **Beschreibung** Feld, geben Sie Informationen über den Bericht ein. Die Beschreibung erscheint nicht im Abschlussbericht, sondern nur in den Berichtseinstellungen.
6. 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 von Ihnen ausgewählte Dashboard über eine dynamische Quelle verfügt, müssen Sie eine Quelle auswählen.
7. Optional: Aus dem **Inhalt des Berichts** Wählen Sie in der Dropdownliste zusätzliche Dashboards aus, die Sie dem Bericht hinzufügen möchten.
8. Aus dem Zeitplan Führen Sie in diesem Abschnitt die folgenden Schritte aus, um einen Zeitplan für den Bericht zu konfigurieren:
 - a) Aus dem Zeitintervall Wählen Sie im Abschnitt den Zeitraum der Dashboard-Daten aus, die Sie in den Bericht aufnehmen möchten.
Das Zeitintervall bezieht sich auf die Zeit, zu der der Bericht gesendet wird.

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

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

Die Häufigkeit der Berichte basiert auf [Standard-Systemzeit](#) von Ihrem ExtraHop-Administrator festgelegt.

9. Aus dem Format Führen Sie in diesem Abschnitt die folgenden Schritte aus, um das Berichtsformat zu konfigurieren:
- a) Legen Sie das Inhaltslayout fest, indem Sie aus der ersten eine der folgenden Optionen auswählen Stil Drop-down-Liste:

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 mit 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) Legen Sie die Anzahl der Seitenumbrüche in der PDF-Datei fest, indem Sie aus der zweiten Option eine der folgenden Optionen auswählen Stil Drop-down-Liste:

Einzelne Seite	(Standard) 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. Wählen Sie diese Option, wenn Ihr Dashboard eine Tabelle oder Liste enthält, in der mehr als 20 detaillierte Metrikwerte angezeigt werden.

- c) Stellen Sie das Anzeigethema 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.

10. Aus dem E-Mail senden Führen Sie im Abschnitt die folgenden Schritte aus , um E-Mail-Benachrichtigungen zu konfigurieren:

- a) In der **Empfänger** Feld, geben Sie die E-Mail-Adresse für jeden Empfänger ein, getrennt durch ein Komma.

- b) Aus dem Betreff Abschnitt, klicken **Benutzerdefiniert** um Ihre eigene Betreffzeile für die E-Mail zu schreiben. Die automatische Betreffzeile ist der Berichtsname.
- c) Optional: In der **Nachricht** Feld, geben Sie die Informationen, die Sie senden möchten, in den Hauptteil der Berichts-E-Mail ein. Die Namen der mit dem Bericht verknüpften Dashboards werden standardmäßig in der Nachricht angegeben.

11. 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 ist 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 Dashboard-Berichts zu beenden, löschen Sie das **Bericht aktivieren** kreuzen Sie den Bericht an oder löschen Sie ihn.

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.



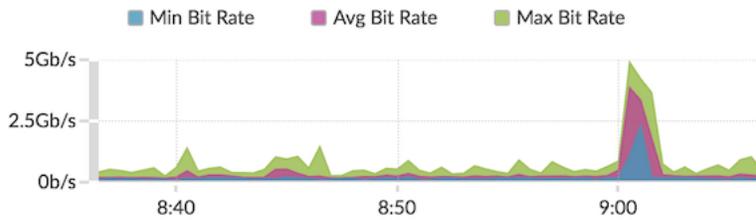
Hinweis: Dieses Diagramm unterstützt [Erkennungsmarker](#), die auf Erkennungen hinweisen, die mit Diagrammdaten verknüpft sind.



Hinweis: Erkennungen durch maschinelles Lernen erfordern eine [Verbindung zu ExtraHop Cloud Services](#).

Die folgende Abbildung zeigt ein Beispiel für ein Flächendiagramm.

Network Throughput ▾



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.

Latency by User ▾



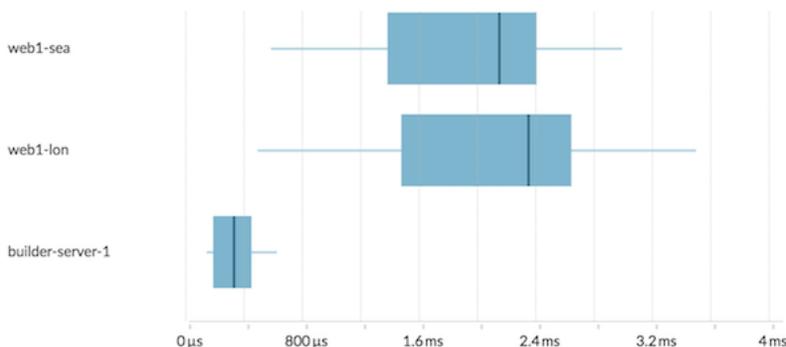
Boxplot-Diagramm

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.

HTTP Server Processing Time ▾



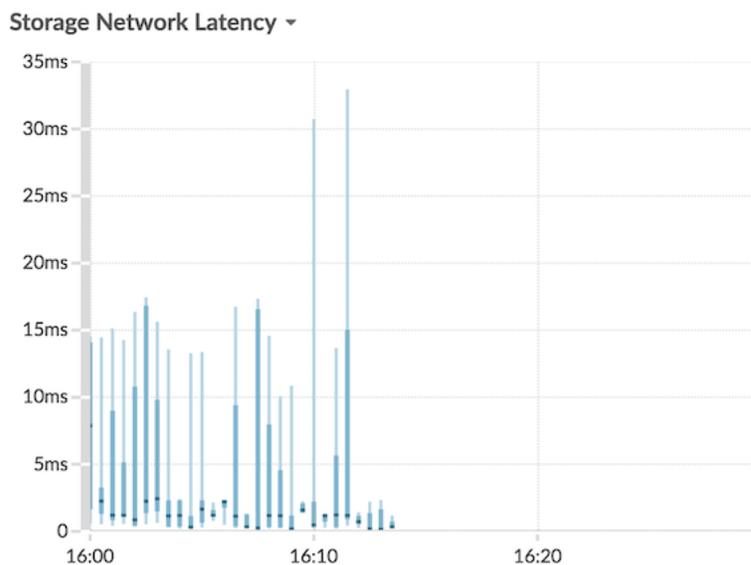
Kerzendiagramm

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

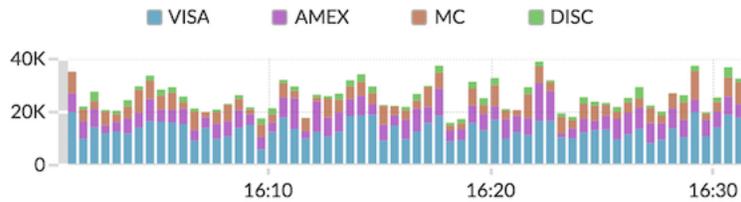
Metrische Daten werden im Zeitverlauf als vertikale Spalten angezeigt. Wenn Ihr Diagramm mehr als eine Metrik enthält, werden die Daten für jede Metrik als einzelne Spalte oder als Reihe angezeigt. Jede Reihe ist zusammengestapelt, um den kumulativen Wert der Daten zu veranschaulichen.

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.

Revenue per Second by Card Brand ▾



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.

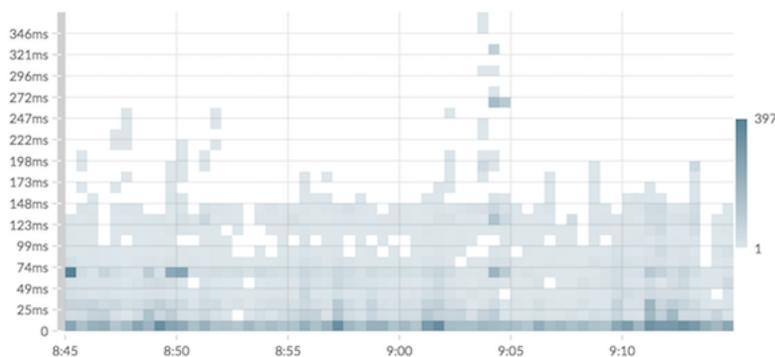
Wählen Sie die Heatmap aus, wenn Sie Muster in der Datenverteilung identifizieren möchten.

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.

HTTP Server Processing Time ▾



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:

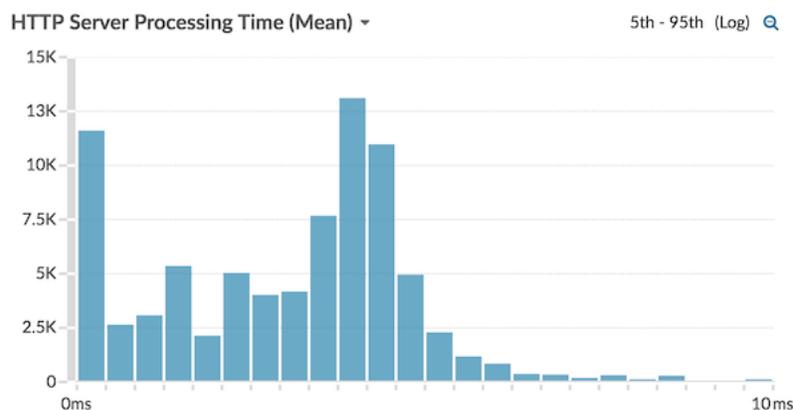
- Der Standarddatenbereich reicht vom 5. bis zum 95. Perzentil (5. bis 95), wodurch Ausreißer aus der Verteilung herausgefiltert werden. In der Ansicht Minimum bis Maximum (Min-Max) wird der gesamte Datenbereich angezeigt. Klicken Sie auf die Lupe in der oberen rechten Ecke des Diagramms, um zwischen 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.

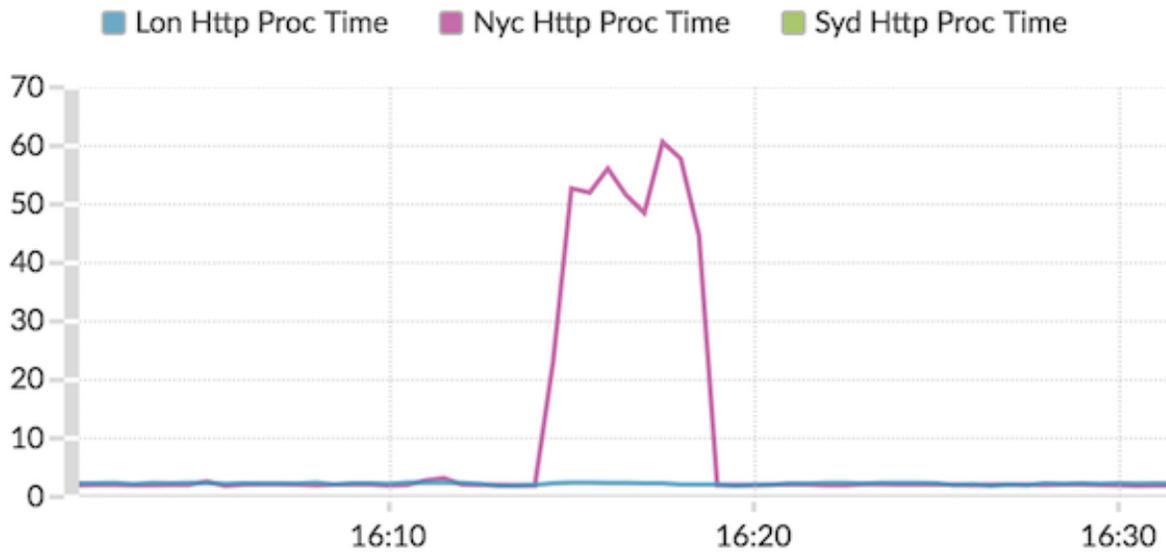
Wählen Sie das Liniendiagramm aus, um Änderungen im Laufe der Zeit zu vergleichen.



Hinweis Dieses Diagramm unterstützt [Erkennungsmarker](#), die auf Erkennungen hinweisen, die mit Diagrammdaten verknüpft sind.

Die folgende Abbildung zeigt ein Beispiel für ein Liniendiagramm.

HTTP Processing Time by Region ▾



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.

DNS errors over processing time ▾

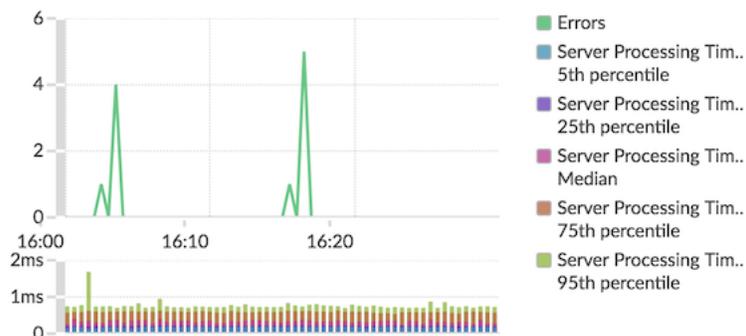


Diagramm auflisten

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

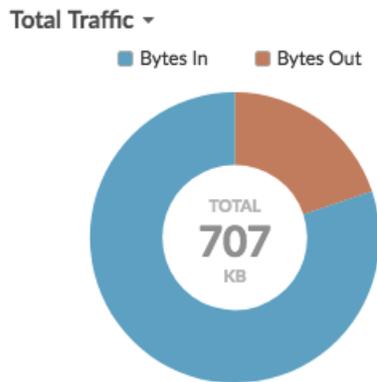
Metrische Daten werden als Teil oder Prozentsatz eines Ganzen angezeigt. Wenn Ihr Diagramm mehr als eine Metrik enthält, werden die Daten für jede Metrik im Kreisdiagramm als einzelnes Segment oder Reihe dargestellt.

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

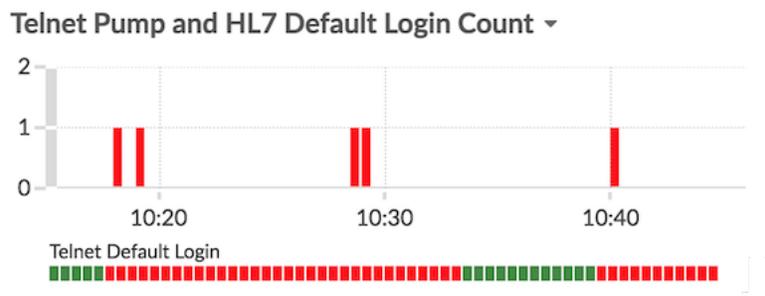
Metrische Daten werden in einem Säulendiagramm angezeigt. Die Farbe jeder Spalte steht für den schwerwiegendsten Warnstatus der konfigurierten Alarm für die Metrik. Sie können nur eine Quelle und Metrik für die Anzeige in diesem Diagramm auswählen.

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.

Web Server Transactions ▾

Device	↓ Responses	Errors	Requests
web1-lon	481,086	8	481,090
web1-sea	189,901	4	206,639
builder-server-1	14,295	0	14,295

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.

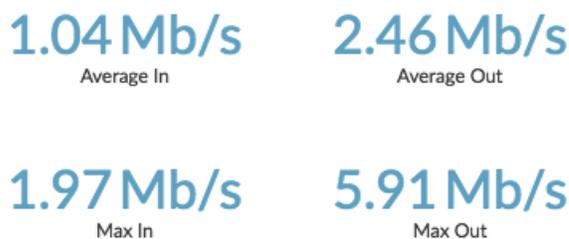
Dieses Diagramm enthält die folgenden Optionen:

- 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.

Throughput Summary ▾



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**.



Hinweise 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.



Hinweise 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](#)
- [Bearbeiten Sie ein Diagramm mit dem Metric Explorer](#)

Drilldown

Eine interessante Metrik führt natürlich zu Fragen zu den Faktoren, die mit diesem Metrikwert verbunden sind. Wenn Sie beispielsweise eine große Anzahl von DNS-Anforderungs-Timeouts in Ihrem Netzwerk feststellen, fragen Sie sich vielleicht, bei welchen DNS-Clients diese Timeouts auftreten. Im ExtraHop-System können Sie ganz einfach von einer Top-Level-Metrik aus einen Drilldown 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 detaillierte Metriken, um zu erfahren, welche Faktoren mit der interessanten Aktivität zusammenhängen.

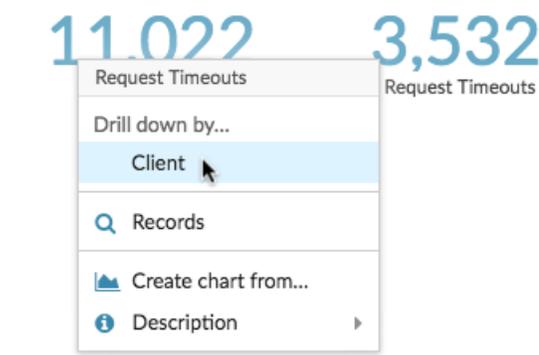
Drilldown von einem Dashboard oder einer Protokollseite aus

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.

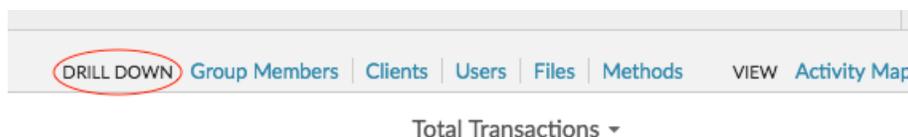
In den folgenden Schritten erfahren Sie, wie Sie eine Metrik finden und anschließend eine Aufgliederung vornehmen können:

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.

Total Requests and Timeouts ▾



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 Diagramm Daten, 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.

Dec 10 15:00
lasting 2 hours

37
RISK

LATERAL MOVEMENT

Potential DNS Brute Force Attacker Detected on sea.example.com

This device attempted an excessive number of reverse DNS lookups for several internal hostnames. Investigate to determine if this client is compromised and searching for valid hostnames through enumeration techniques.

This device scanned approximately 395 internal IP addresses.

sea.example.com
10.10.10.3

Activity Map Records

Anomalous DNS Client activity

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.

Dec 11 00:00
lasting 2 hours

NETWORK
INFRASTRUCTURE

DNS Server Errors on dns.example.com

This server sent an excessive number of the DNS NXDOMAIN/QUERY:A error, which indicates that domain name lookups failed.

Client linked to this detection

- client-01

dns.example.com
172.21.2.23

DNS Responses by Response Code

NXDOMAIN/QUERY:A

Drill down by...

- Client
- Records
- Create chart from...
- Description

Activity Map Records

6-hour Peak Value	Expected Range	Deviation
76.5 K	0-1.82 K	4,102%

- 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.

- Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
- 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“
- Klicken Sie auf den Namen einer Schwellenwarnung. Warndetails werden angezeigt.
 - Klicken Sie auf einen Metriknamen oder -schlüssel, wie in der folgenden Abbildung dargestellt.

Alert Details

Dec 12 10:46

● ERROR

Threshold Alert

Threshold alert on [All Activity](#)

The screenshot shows the 'All Activity' alert details. The 'HTTP Metrics' section is circled in red, and the 'Requests' metric is highlighted. A dropdown menu is open over the 'Requests' metric, showing the following options:

- Drill down by...
 - Client
 - Method
 - Referer
 - Server
 - URI
- Records
- Go to application...
 - All Activity - HTTP
- Create chart from...
- Description

- 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 Schlüssel aufgelistete Metriken untersuchen](#).

Untersuchen Sie detaillierte Metriken

Nachdem Sie eine Metrik von einem Dashboard, einer Protokollseite, einer Erkennung oder einer Alarm aus genauer betrachtet haben, können Sie Metrikergebnisse auf einer Detailseite der Metriken nach Schlüssel

untersuchen. Filtern Sie Metrikdaten oder wählen Sie verschiedene Schlüssel wie Statuscodes oder URIs aus, um Daten aus verschiedenen Perspektiven zu betrachten.

Die folgende Abbildung zeigt, wie Sie Daten auf einer Metrik-Detailseite filtern, pivotieren, sortieren oder exportieren.

The screenshot shows the 'Responses by Status Code' dashboard. A line chart at the top displays response counts over time, with a total of 193K responses. Below the chart is a table with columns for 'Records', 'Status Code', and 'Responses'. Annotations include: 'Filter results' pointing to the 'Add Filter' button; 'Click to sort by metric values' pointing to the 'Responses' column header; 'Click to access export options' pointing to the export icon; 'Change data calculations' pointing to the 'Count' dropdown; 'Pivot by key' pointing to the 'Drill Down by...' menu; and 'Click to create a record query for a device (if available)' pointing to the magnifying glass icon in the table.

Records	Status Code	Responses
Q	200	180,652
Q	302	4,690
Q	202	2,309
Q	206	1,330
Q	304	1,195
Q	204	1,108
Q	404	853
Total:		192,998

Wenn Sie eine Metrik nach IP, Client oder Server aufgeschlüsselt haben, werden IP-Adressen und Hostnamen (sofern sie anhand des DNS-Verkehrs beobachtet wurden) in der Tabelle angezeigt. Zusätzliche Optionen stehen Ihnen jetzt zur Verfügung. Sie können beispielsweise eine Geomap generieren oder direkt zu einer Client- oder Server-Protokollseite navigieren, wie in der folgenden Abbildung dargestellt.

The screenshot shows the 'Responses by Client' dashboard. A line chart at the top displays response counts over time, with a total of 193K responses. Below the chart is a table with columns for 'Records', 'Client IP', 'Host', 'Origin', 'Responses', and 'Server Processing Time Mean (ms)'. Annotations include: 'Generate a geomap to see the location of the IP address on a map' pointing to the 'View Geomap' button; and 'Click an IP address or hostname to go to a protocol page' pointing to the 'Client IP' column.

Records	Client IP	Host	Origin	Responses	Server Processing Time Mean (ms)
Q	192.168.0.103	192.168.0.103	-	207,113	1.055
Q	192.168.0.101	192.168.0.101	-	197,083	0.964
Q	192.168.0.1	192.168.0.1	192.168.0.103	137,578	0.287
Q	192.168.0.1	192.168.0.1	192.168.0.101	129,136	0.297
Q	192.168.0.102	192.168.0.102	-	69,163	0.784
Q	172.29.1.245	172.29.1.245	-	732	70.928
Q	172.21.1.1	172.21.1.1	-	731	0.54
Total:				783,917	

Ergebnisse filtern

Eine Detailseite kann bis zu 1.000 Schlüssel-Wert-Paare enthalten. Es gibt zwei Möglichkeiten, bestimmte Ergebnisse aus Daten zu finden: Ergebnisse filtern oder [klicken Sie auf eine Taste in der Tabelle, um einen weiteren Drilldown-Filter zu erstellen](#).

Um die Ergebnisse zu filtern, klicken Sie auf **Irgendein Feld**, und wählen Sie dann ein Feld aus, das je nach Schlüssel variiert. Sie können beispielsweise auswählen **Netzwerk-Lokalität** für Client- oder Serverschlüssel. Wählen Sie dann einen der folgenden Operatoren aus:

- Wählen = um eine exakte Zeichenkettenübereinstimmung durchzuführen.
- Wählen ≈ 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 # um eine ungefähre Zeichenkettenübereinstimmung aus Ihren Ergebnissen auszuschließen.
- Wählen > oder ≥ um einen Abgleich für Werte durchzuführen, die größer (oder gleich) einem bestimmten Wert sind.
- Wählen < oder ≤ um einen Abgleich für Werte durchzuführen, die kleiner (oder gleich) einem bestimmten Wert sind.
- klicken **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 ihn aus, und klicken Sie dann auf **Filter hinzufügen**.

Untersuchen Sie Bedrohungsdaten (Nur ExtraHop Reveal (x) Premium und Ultra)

Klicken Sie auf das rote Kamerasymbol  zum Ansehen [Bedrohungsinformationen](#) Details zu einem verdächtigen Host, einer verdächtigen IP-Adresse oder einem verdächtigen URI in Detail-Metrik Metrikdaten.

Markieren Sie einen Metrikwert im oberen Diagramm

Wählen Sie eine einzelne Zeile oder mehrere Zeilen aus, um die Diagramm Daten im obersten 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.

Je nach Schlüssel zu mehr Daten wechseln

Klicken Sie auf die Schlüsselnamen in der Einzelheiten Abschnitt, um detailliertere Metrikwerte zu sehen, aufgeschlüsselt nach anderen Schlüsseln. Für IP-Adresse oder Hostschlüssel klicken Sie in der Tabelle auf einen Gerätenamen, um zu einem Gerät Protokollseite, auf der der Datenverkehr und die Protokollaktivitäten im Zusammenhang mit diesem Gerät angezeigt werden.

Passen Sie das Zeitintervall an und vergleichen Sie Daten aus zwei Zeitintervallen

Durch Ändern des Zeitintervalls können Sie Metrikdaten aus 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 grauen Text, der angibt, wann die Drilldown-Metriken zuletzt abgerufen wurden. Um die Metriken für das angegebene Zeitintervall neu zu laden, klicken Sie in der Anzeige von Global Zeitselektor auf das Aktualisierungssymbol. 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 zu sehen, welche Schlüssel mit den größten oder kleinsten Metrikwerten verknüpft sind. Sortiere beispielsweise nach der Bearbeitungszeit, 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 Sie eine Zählmetrik in der Tabelle haben, klicken Sie auf **Zählen** 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 Sie eine Datensatz-Metrik in der Tabelle haben, 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 einsehen.

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

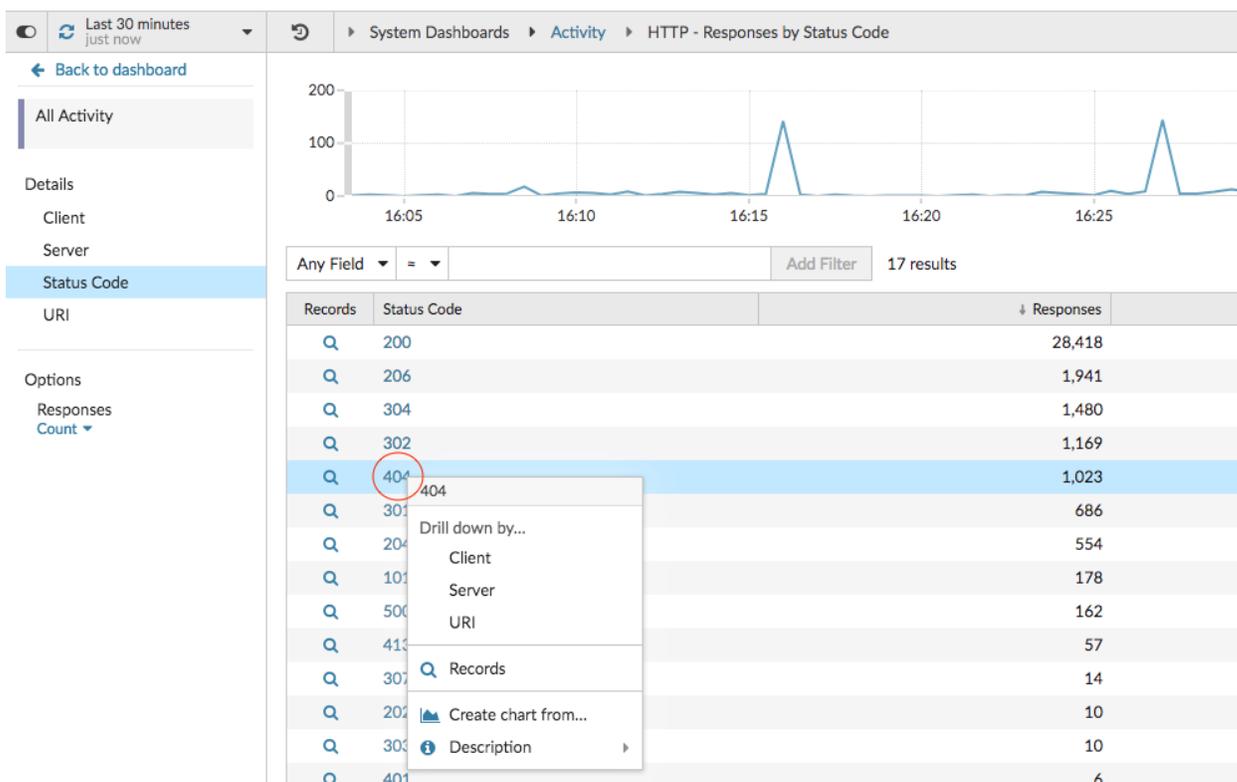
Nachdem Sie eine Top-Level-Metrik zunächst nach Schlüsseln aufgeschlüsselt haben, wird eine Detailseite mit einem Topset von Metrik Werten, aufgeschlüsselt nach diesem Schlüssel. Sie können dann einen Filter erstellen, um einen zweiten Drilldown mit einem anderen Schlüssel durchzuführen. Sie können beispielsweise 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 Topsets verfügbar.

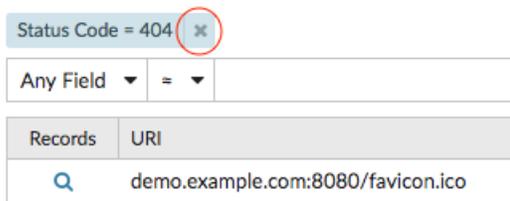
Die folgenden Schritte zeigen Ihnen, wie Sie von einem Diagramm aus einen Drilldown durchführen und dann von einer Detailseite mit Metriken aus erneut einen Drilldown durchführen:

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.

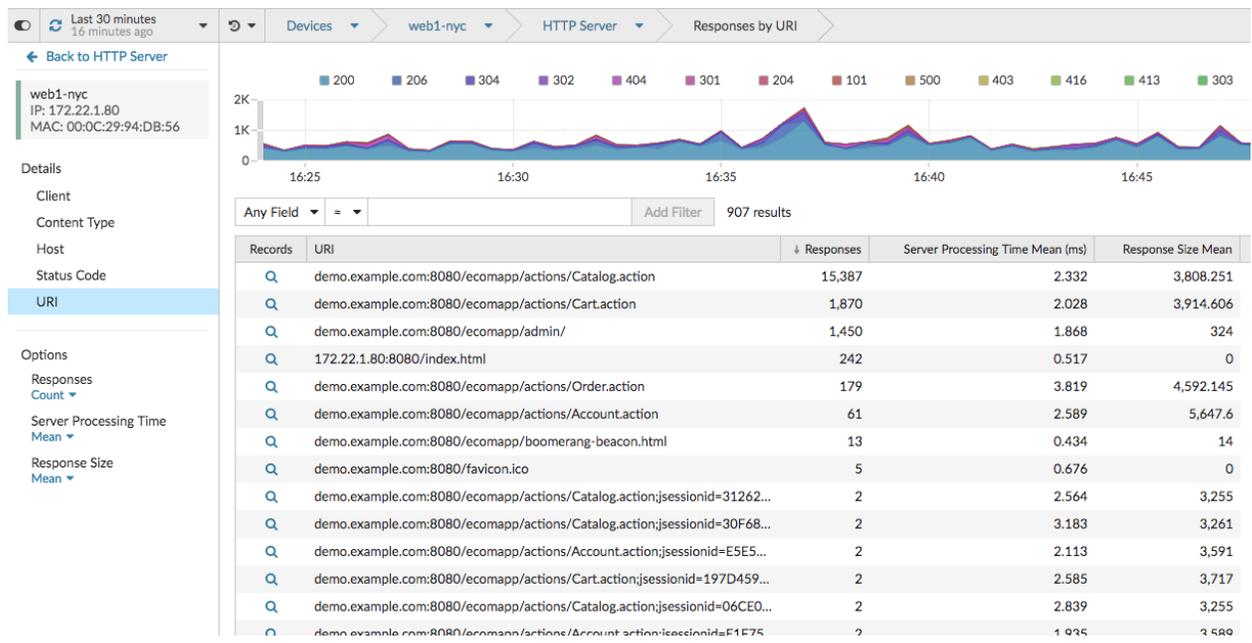


Der Schlüsselfilter wird über der Tabelle angezeigt. Sie können jetzt alle Detailmetriken anzeigen, die mit diesem einzelnen Schlüssel verknüpft sind.

- 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 Detailmetrikerwerte 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 Metrikerwerte 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:

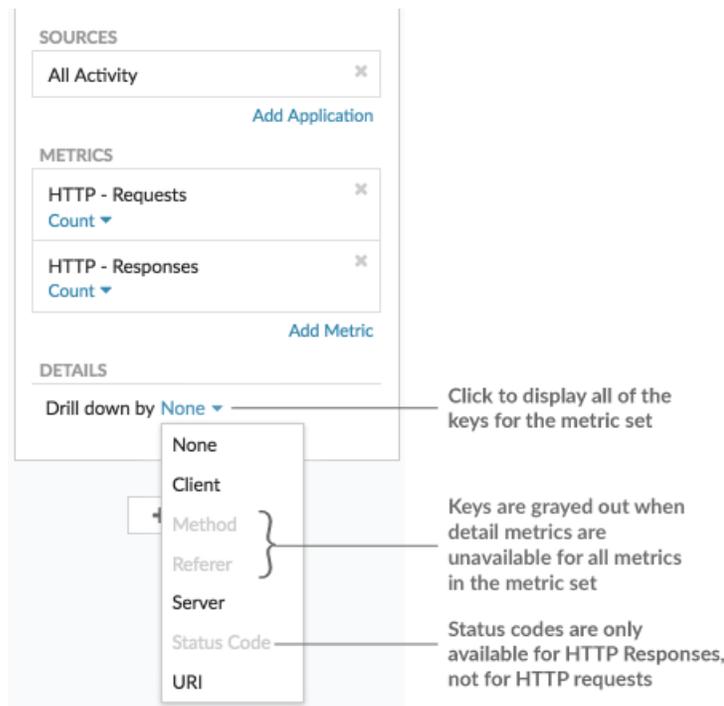
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Navigieren Sie zu einer Dashboard- oder Protokollseite.
3. Klicken Sie auf den Diagrammtitel und wählen Sie dann **Bearbeiten**.
4. In der Einzelheiten Abschnitt, klicken **Drilldown nach <None>**, wo <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 \approx Operator zur Anzeige von Schlüssel nach ungefähre Übereinstimmung oder mit Regex. Sie müssen Schrägstriche mit Regex im Filter für ungefähre Treffer weglassen.

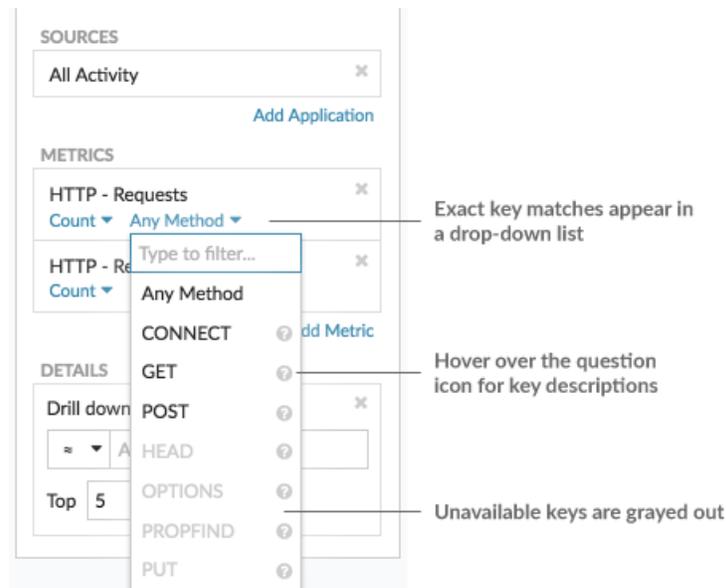
Hinweis Die # Die Filteroption zum Ausschließen von Ergebnissen ist nur verfügbar für [Detailseiten](#). Wenn Sie Ergebnisse in einem Dashboard-Diagramm ausschließen möchten, erstellen Sie ein [regulärer Ausdruck \(Regex\)](#).

- 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.

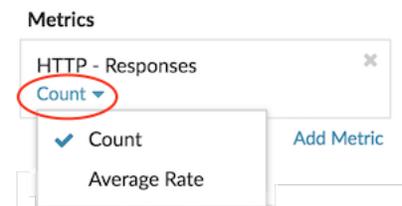
Hinweis Sie können eine exakte Schlüsselübereinstimmung pro Metrik anzeigen, wie in der folgenden Abbildung dargestellt. Klicken Sie auf den Namen der Drilldown-Metrik (z. B. **Alle Methoden**), um einen bestimmten Metrik Drilldown-Key auszuwählen (z. B. `GET`) aus der Drop-down-Liste. Wenn ein Schlüssel grau erscheint (z. B. `PROPFIND`), sind Drilldown-Metriksdaten 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.

Durchschnittsrates

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 [konfigurieren dein Diagramm mit einer Netzwerk- oder Gerätequelle](#).

Zeigen Sie den Durchschnittskurs in einem Diagramm an

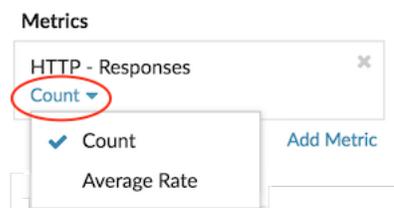
Wenn Sie ein Diagramm mit einer Fehler-, Antwort-, Anfrage- oder anderen Zählmetrik konfiguriert haben, wird automatisch die Gesamtzahl der Ereignisse im Laufe der Zeit angezeigt. Sie können das Diagramm weiter bearbeiten, um eine Durchschnittsrate pro Sekunde für Ihre Daten anzuzeigen.

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 **Armaturenbrett**.
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 **Armaturenbrett** 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)

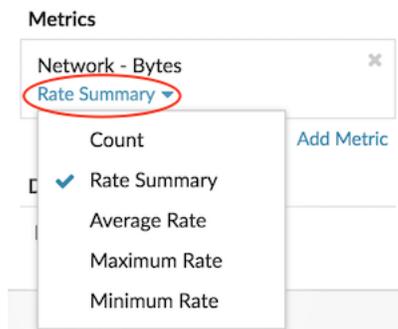
Für eine Gerätequelle

- 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.



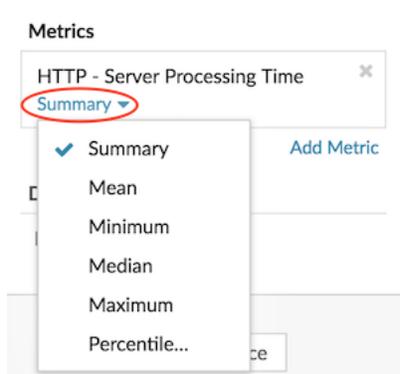
7. Wählen **Maximaler Tarif** aus dem Drop-down-Menü.
8. klicken **Speichern** um den Metric Explorer zu schließen.

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 Probenstet Metriken. Datensatzmetriken sind mit Timing und Latenz verknüpft, z. B. Metriken zur Serververarbeitungszeit und zur Roundtrip-Zeit. Samplest-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 Probenstet 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 **Armaturenbrett**.
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 Diagramm Daten zu unterscheiden. Basislinien werden nur in Flächen-, Kerzendigrammen, 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.

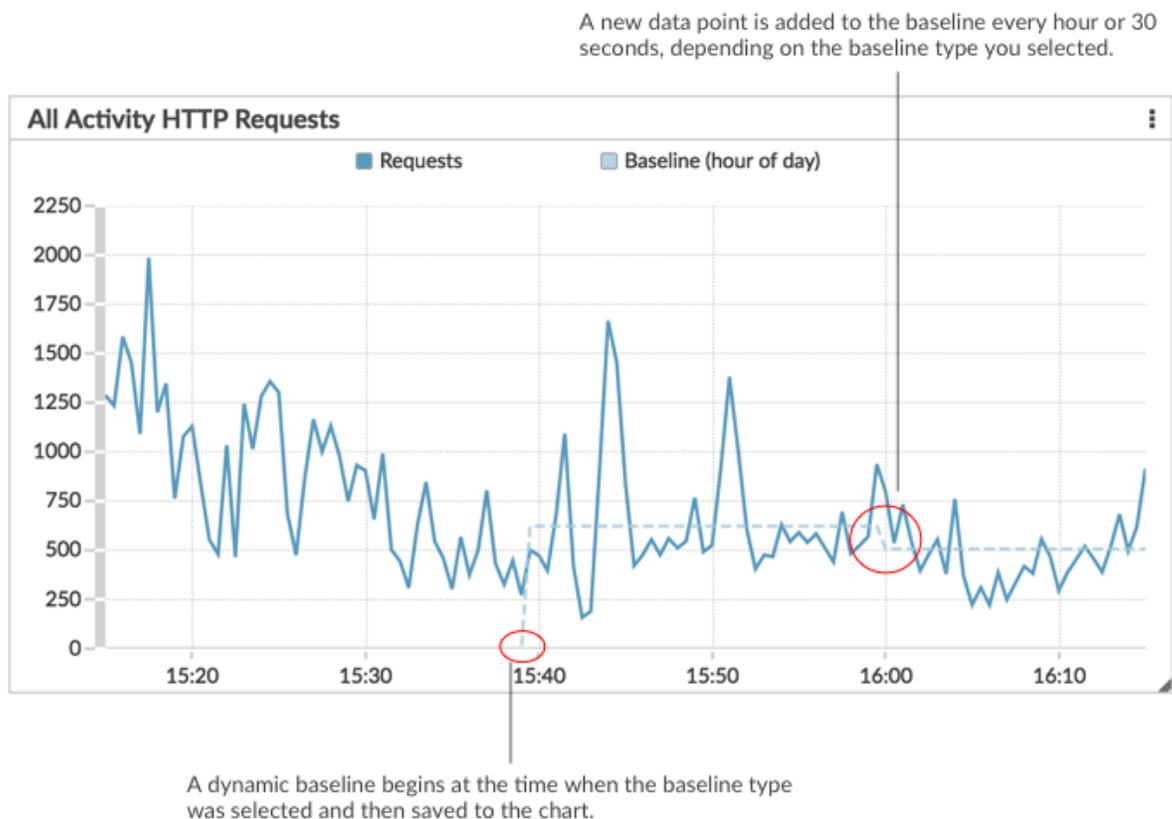
Die folgenden Schritte zeigen Ihnen, wie Sie einem vorhandenen Dashboard-Diagramm eine Dynamische Basislinie hinzufügen:

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

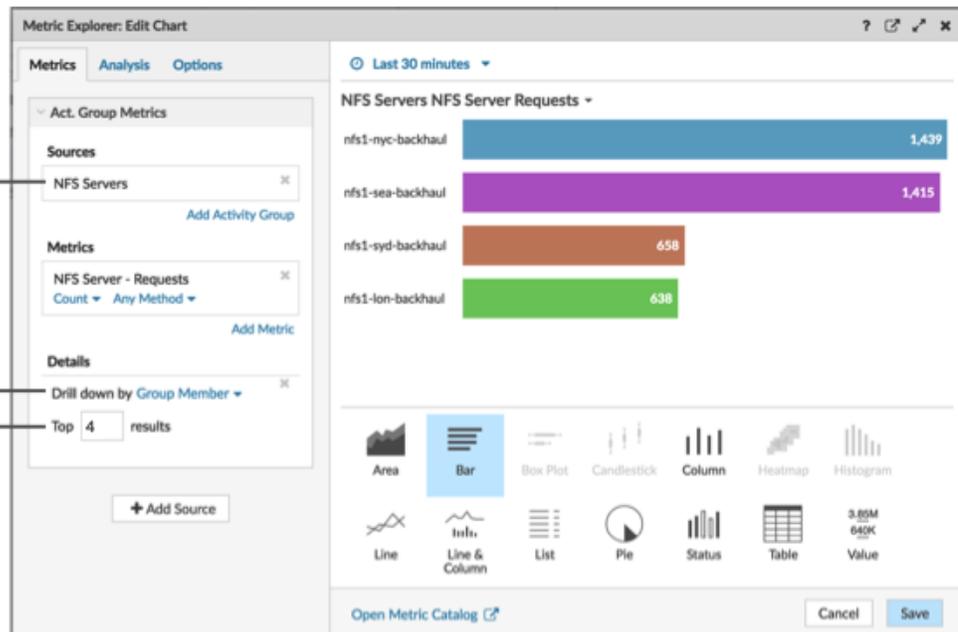
Gerätegruppenmitglieder in einem Diagramm anzeigen

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.

Select a device group as the source, such as the NFS Servers activity group.

Drill down by group member to see metrics by device.

Devices with the largest metric values are displayed. To view more devices, increase the number of results.



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 **Armaturenbrett**.
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.

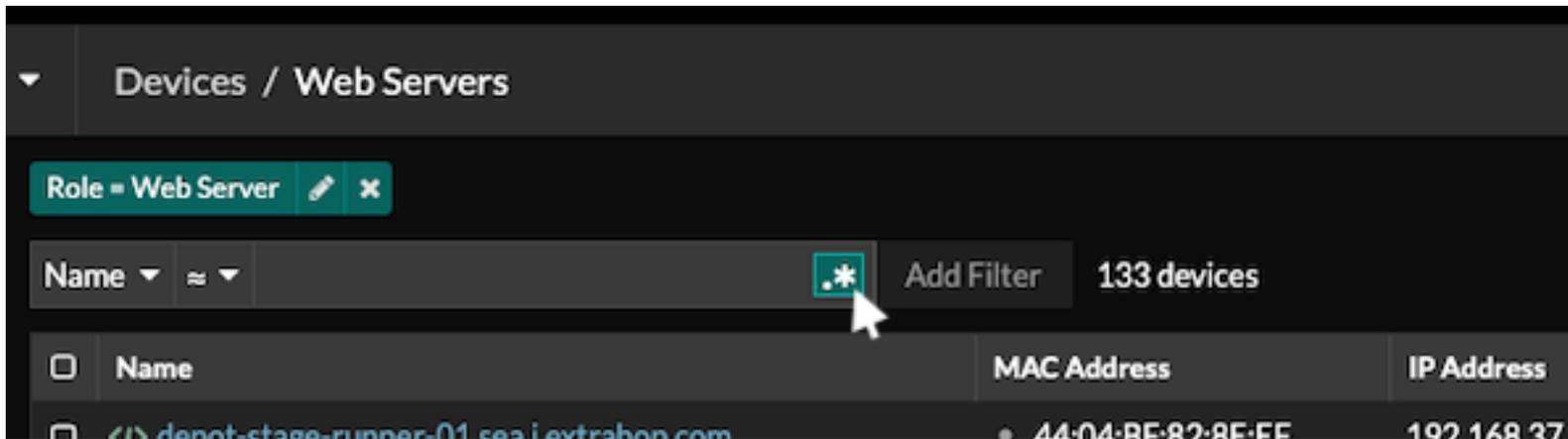
Filter für reguläre Ausdrücke

Filtern Sie Ihre Suchergebnisse, indem Sie reguläre Ausdrücke (Regex) in bestimmte Suchfelder im gesamten ExtraHop-System 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 im gesamten System über visuelle Indikatoren und akzeptieren die Standardsyntax.

Suchfelder mit einem Sternchen

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

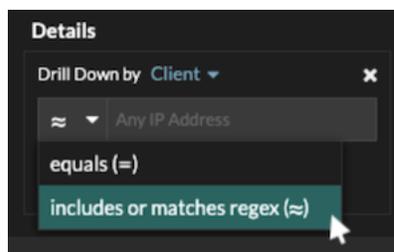


Dieser Feldtyp ist auf den folgenden Systemseiten verfügbar:

- 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.

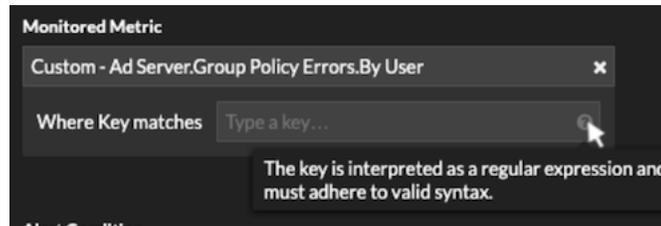


Dieser Feldtyp ist auf der folgenden Systemseite verfügbar:

- Bearbeiten eines Diagramms im Metric Explorer

Bestimmte Suchfelder mit einem Tooltip

Bewegen Sie den Mauszeiger über 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.

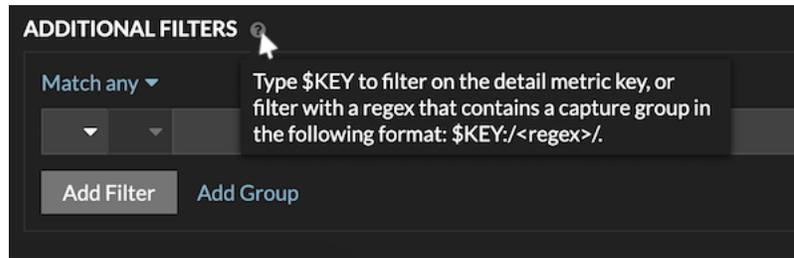
Chart-Szenario	Regex-Filter	So funktioniert
HTTP-Statuscodes vergleichen 200 zu 404.	(200 404)	Das vertikale Balkensymbol () ist der OR-Operator. Dieser Filter passt 200, oder 404, oder beide Statuscodes.
Zeigt einen beliebigen HTTP-Statuscode an, der eine enthält 4.	[4]	Eckige Klammern ([und]) kennzeichnen einen Zeichenbereich. Der Filter sucht nach jedem Zeichen innerhalb der Klammern, unabhängig von der Reihenfolge. Dieser Filter entspricht jedem Wert, der eine enthält 4 oder ein 1. Dieser Filter kann beispielsweise zurückgeben 204, 400, 101, oder 201 Statuscodes.
Alle anzeigen 500HTTP-Statuscodes auf -Ebene.	^ [5]	Das Caret-Zeichen (^) außerhalb der eckigen Klammern ([und]) bedeutet „beginnt mit“. Dieser Filter entspricht jedem Wert, der mit a beginnt 5. Dieser Filter kann beispielsweise zurückgeben 500 und 502 Statuscodes.
Alle anzeigen 400 und 500 HTTP-Statuscodes auf -Ebene.	^ [45]	Mehrere Werte in eckigen Klammern ([und]) werden einzeln gesucht, auch wenn ihnen das Caret-Symbol (^) vorangestellt ist. Dieser Filter sucht nicht nach Werten, die beginnen mit 45, entspricht aber allen Werten, die mit a beginnen 4 oder 5. Dieser Filter kann beispielsweise zurückgeben 400, 403, und 500 Statuscodes.
Zeigt alle HTTP-Statuscodes an, außer 200 Statuscodes auf -Ebene.	^ (?! 2)	Ein Fragezeichen (?) und Ausrufezeichen (!) in Klammern geben einen auszuschließenden Wert an. Dieser Filter entspricht allen Werten außer Werten, die mit a beginnen 2. Dieser Filter

Chart-Szenario	Regex-Filter	So funktioniert
		kann beispielsweise zurückgeben 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 Zeitraum angibt, dass hinter 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 187.18.	187\ ,18.	Spiele 187.18 und alles, was folgt. Der erste Punkt wird wörtlich behandelt, da ihm ein umgekehrter Schrägstrich (\) vorangestellt ist. 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.
Zeigen Sie eine beliebige IP-Adresse an, außer 187.18.197.150.	^(?!187\.18\.197\.150)	Passt zu allem außer 187.18.197.150, wo ^(?!) gibt den auszuschließenden Wert an.
Schließt eine Liste bestimmter IP-Adressen aus.	^(?!187\.18\.197\.15[012])	Passt zu allem 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

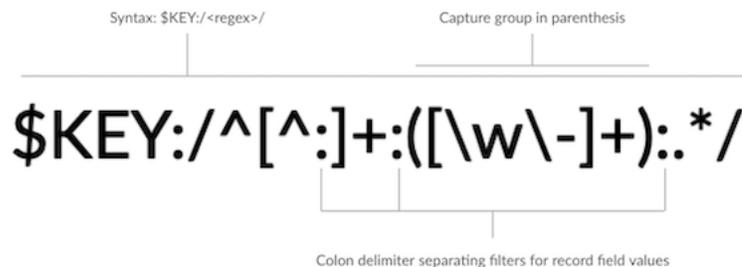
Wenn du [eine benutzerdefinierte Detail-Metrik erstellen](#) im Metrikkatalog können Sie dem Suchfeld Zusätzliche Filter im Bereich Datensatzbeziehungen erweiterte Regex-Syntax hinzufügen.

Der Tooltip wird angezeigt, nachdem Sie ausgewählt haben **Detail: Metrik** 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 Capture-Gruppe enthalten. Eine Capture-Gruppe wird durch Klammern gekennzeichnet. Ihre Erfassungsgruppe bestimmt den Filterwert.



- Wenn Sie einen bestimmten Wert aus einem Detail-Metrik Metrikschlüssel zurückgeben möchten, der mehrere Datensatzfeldwerte enthält, muss die Regex der folgenden Syntax folgen:

`$SCHLÜSSEL: / <regex> /`

Wenn Ihr Detail-Metrik Metrikschlüssel beispielsweise `ipaddr:host:cipher` lautet und Sie nur den IP-Adresswert zurückgeben möchten, würden Sie Folgendes eingeben:

`$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 `$-SCHLÜSSEL`. Wenn Ihr Detail-Metrik Metrikschlüssel beispielsweise `ipaddr:host:cipher` lautet, geben Sie ein `$-SCHLÜSSEL` im Suchfeld , um alle drei dieser Felddatensatzwerte (IP-Adresse, Hostname und SSL-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 Metrikerwert.
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

- [Suche nach Peer-Geräten](#)
- [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.

Metrics

TCP - Accepted Count ▾	✕
TCP - Connected Count ▾	✕
TCP - External Accepted Count ▾	✕
TCP - External Connected Count ▾	✕
TCP - Closed Count ▾	✕
TCP - Aborted Connections In Count ▾	✕
TCP - Aborted Connections Out Count ▾	✕

[Add Metric](#)

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.

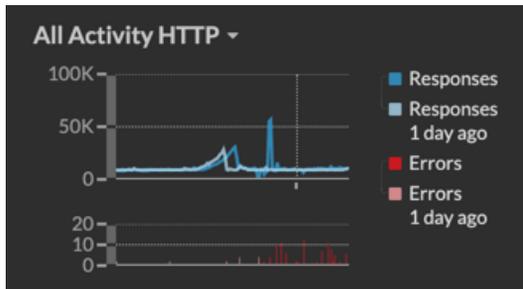
Nächste Schritte

[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 Metrik Aktivitäten sind auf der Seite Assets logisch in Abschnitte unterteilt, in denen Sie nach den benötigten Daten suchen können.

Geräte

Geräte, auch Assets und Endpoints genannt, sind Objekte in Ihrem Netzwerk mit einer MAC- oder IP-Adresse, die vom ExtraHop-System automatisch erkannt und klassifiziert wurden. Weisen Sie einem Diagramm, einer Alarm oder einem Auslöser ein beliebiges Gerät als Metrikquelle zu. [Erfahren Sie mehr über Geräte.](#)

Gerätegruppen

[Gerätegruppen](#) sind benutzerdefinierte Gerätesätze, die gemeinsam als Metrikquelle einem Diagramm, einer Alarm oder einem Auslöser 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 manuell Geräte hinzufügen oder entfernen. Das ExtraHop-System enthält auch integrierte dynamische Gerätegruppen nach Rolle und Protokollaktivität, die Sie als Metrik Quelle zuweisen können. Klicken Sie auf der Geräteseite auf einen Rollen- oder Protokoll-Link , um Metriken für eine integrierte Gerätegruppe anzuzeigen.

Nutzer

Auf der Seite Benutzer wird eine Liste aller aktiven Benutzer in Ihrem Netzwerk und der Geräte angezeigt, auf 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.

Bewerbungen

Anwendungen sind benutzerdefinierte Container, die verteilte Systeme in Ihrem Netzwerk darstellen. Erstellen Sie eine Anwendung, um alle Metrik Aktivitäten im Zusammenhang mit Ihrem Website-Traffic anzuzeigen – Webtransaktionen, DNS-Anfragen und -Antworten sowie Datenbanktransaktionen. Sehen Sie die [Häufig gestellte Fragen zu Anwendungen](#).

Basisanwendungen, die integrierte Metriken nach Protokollaktivität filtern, können sein [erstellt durch das ExtraHop-System](#). Komplexe Anwendungen, die benutzerdefinierte Metriken oder Metriken aus Nicht-L7-Verkehr sammeln, müssen [durch einen Auslöser erzeugt](#), was JavaScript-Code erfordert. Erfahre mehr über [Trigger bauen](#).

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 z. B. Clients, Server, Router, Load Balancer und Gateways. Jedes Gerät erhält die höchste verfügbare Analysestufe, die auf Ihrer Systemkonfiguration basiert.

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 Messwerte für ein Gerät auch dann verfolgt werden können, wenn die IP-Adresse über eine DHCP-Anfrage geändert oder neu zugewiesen wird. Wenn L3 Discovery aktiviert ist, ist es wichtig zu wissen, dass Geräte möglicherweise nicht eins zu eins mit den physischen Geräten in Ihrer Umgebung korrelieren. 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 von [Analyseebene](#) für dieses Gerät konfiguriert. Die Analyseebene bestimmt, welche Arten von Metriken generiert werden und welche Funktionen für die Organisation von Metrikdaten verfügbar sind.

Navigationsgeräte

Klicken **Vermögenswerte** aus dem oberen Menü und dann klicken **Geräte** um die folgenden Diagramme anzuzeigen, die Aufschluss über die aktiven Geräte geben, die während des ausgewählten Zeitintervalls in Ihrem Netzwerk erkannt wurden:

Aktive Geräte

Zeigt die Gesamtzahl der Geräte an, die vom ExtraHop-System erkannt wurden. Klicken Sie auf die Nummer, 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 dem [Seite „Geräteübersicht“](#).

Neue Geräte

Zeigt die Anzahl der Geräte an, die im letzten Monat entdeckt wurden, sowie die prozentuale Änderungsrate. Klicken Sie auf die Nummer, um eine Liste all dieser Geräte anzuzeigen.

Geräte nach Rolle

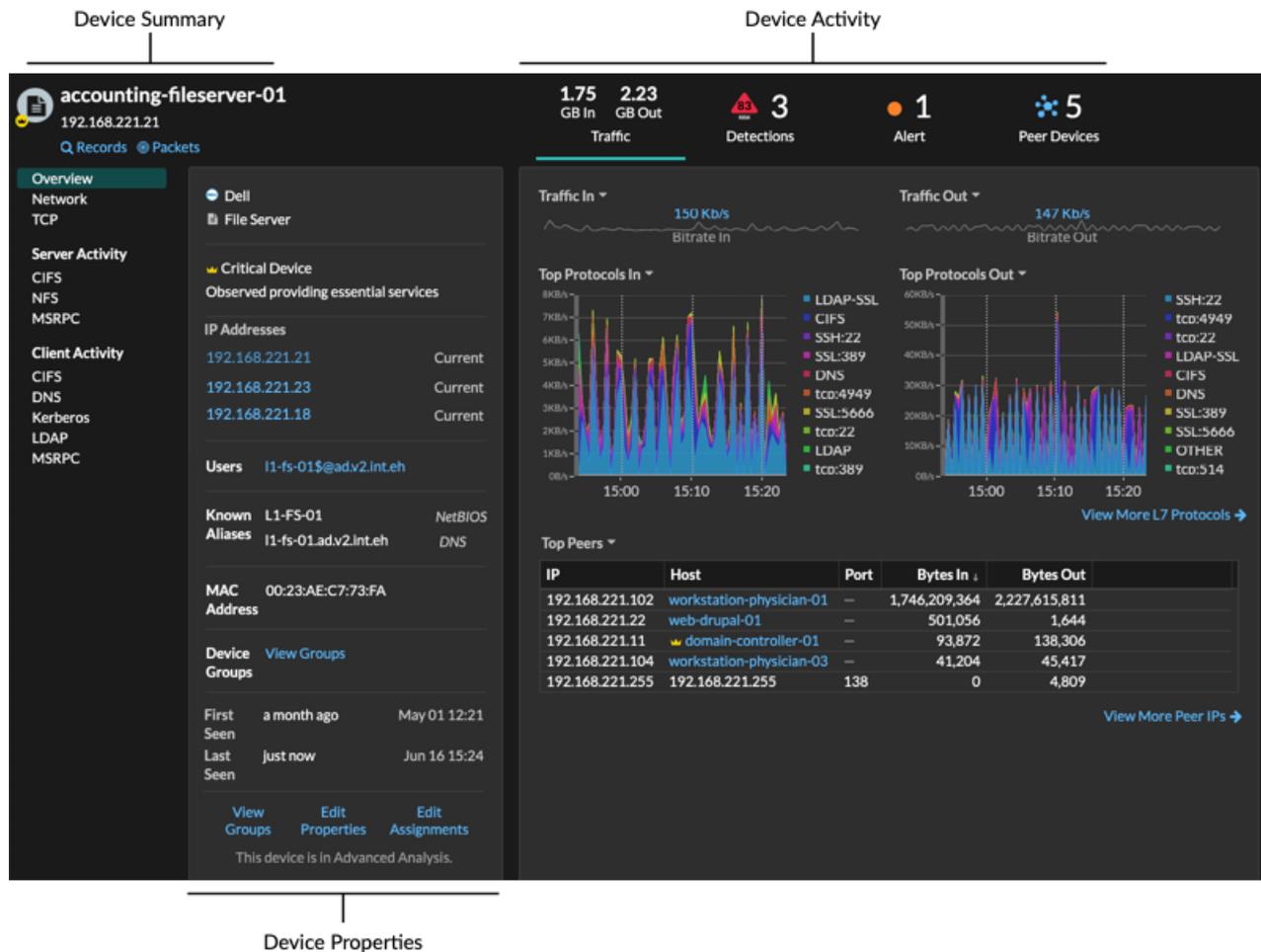
Zeigt jede Geräterolle und die Anzahl der Geräte an, die jeder Rolle zugewiesen sind, die während des angegebenen Zeitintervalls aktiv ist. Klicken Sie auf eine Geräterolle, um eine integrierte Seite mit der Übersicht über Gerätegruppen aufzurufen, die Metrikdaten, Peer-IPs und Protokollaktivitäten für 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 Gerätegruppenübersichtsseite mit spezifischen Metrikdiagrammen zu dieser Protokollaktivität aufzurufen. Klicken Sie auf eine Aktivitätsdiagramm, um alle Gerät-zu-Gerät-Verbindungen zu sehen. 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 ermittelt 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-Adresse oder MAC-Adresse und die dem Gerät zugewiesene Rolle. Wenn der Blick von einem Konsole, der Name der mit dem Gerät verknüpften Standort wird ebenfalls angezeigt.

- klicken **Aufzeichnungen** um eine zu starten **Datensatzabfrage** das wird von diesem Gerät gefiltert.
- klicken **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.

Hochwertiges Gerät

Eine hoher Wert Ikone erscheint, wenn das ExtraHop-System beobachtet hat, dass das Gerät Authentifizierung oder wichtige Dienste bereitstellt; Sie können auch **manuell ein Gerät als hohen Wert angeben**. Die Risikowerte für Erkennungen auf hoher Wert Geräten werden erhöht.

IP-Adressen

Eine Liste von IP-Adressen, die zu einem beliebigen Zeitpunkt während des ausgewählten Zeitintervalls auf dem Gerät beobachtet wurden. Wenn **L2-Entdeckung** aktiviert ist, zeigt die Liste möglicherweise sowohl IPv4- als auch IPv6-Adressen an, die gleichzeitig auf dem Gerät beobachtet werden, oder die Liste zeigt möglicherweise mehrere IP-Adressen an, 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 kann 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, mit denen die IP-Adresse verknüpft wurde, anzuzeigen.

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
- Name der Cloud-Instanz (wird in der Eigenschaft Known Alias angezeigt)
- Beschreibung der Cloud-Instanz (Instanz-Metadaten werden automatisch für Geräte in Flow Analysis angezeigt)

siehe [Fügen Sie Cloud-Instanzeigenschaften über den ExtraHop API Explorer hinzu](#)  für weitere Informationen.

Nutzer

Eine Liste der authentifizierten Benutzer, die am Gerät angemeldet sind. [Klicken Sie auf einen Nutzernamen](#) um auf die Seite Benutzer 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.

Hardware und Software

Die Hardware oder der Hersteller, die Marke und das Modell des Geräts sowie alle Betriebssysteme, die auf dem Gerät ausgeführt werden.

Das ExtraHop-System beobachtet den Netzwerkverkehr auf Geräten, um automatisch Hersteller, Marke und Modell zu ermitteln, oder Sie können [manuell eine neue Marke und ein neues Modell zuweisen](#).



Hinweis: [CrowdStrike-Integration](#)  nur auf Reveal (x) 360) Klicken Sie auf Links von CrowdStrike-Geräten, um Gerätedetails in CrowdStrike Falcon anzuzeigen, und [die Eindämmung von CrowdStrike-Geräten einleiten](#) die an einer Sicherheitserkennung Erkennung.

Schlagworte

Die [dem Gerät zugewiesene Tags](#). Klicken Sie auf einen Tagnamen, um die anderen Geräte anzuzeigen, denen das Tag zugewiesen ist.

Zuerst und zuletzt gesehen

Die Zeitstempel von der ersten Entdeckung des Geräts und der letzten Aktivität auf dem Gerät. NEU erscheint, wenn das Gerät innerhalb der letzten fünf Tage entdeckt wurde

Analyse

Die [Ebene der Analyse](#) die dieses Gerät empfängt.

Hier sind einige Möglichkeiten, wie Sie Geräteeigenschaften anzeigen und ändern können:

- klicken **Gruppen ansehen** um das anzusehen [Gerätegruppe](#) Mitgliedschaft für das Gerät.
- klicken **Eigenschaften bearbeiten** um Geräteeigenschaften anzuzeigen oder zu ändern , wie [Geräterolle](#), Gerätegruppenmitgliedschaften oder [Geräte-Tags](#).
- klicken **Aufgaben bearbeiten** um zu sehen oder zu ändern, welche [Warnungen](#) und [löst aus](#) sind dem Gerät zugewiesen.

Aktivität auf dem Gerät

Der Abschnitt Geräteaktivität enthält Informationen darüber, wie das Gerät mit anderen Geräten kommuniziert und welche Erkennungen und Warnungen mit dem Gerät verknüpft sind.

- klicken **Verkehr** um Diagramme für Protokoll- und Peer-Daten anzuzeigen, und dann [bohren](#) zu Metriken in Verkehrskarten.



Hinweis Verkehrsdigramme sind nicht verfügbar, wenn die Geräteanalyseebene auf Entdeckungsmodus ist. Um Verkehrskarten für das Gerät zu aktivieren, erhöhen Sie das Gerät auf [Fortgeschrittene Analyse](#) oder [Standardanalyse](#).

- klicken **Erkennungen** , um eine Liste der Entdeckungen anzuzeigen, und klicken Sie dann auf einen Erkennungsnamen, um [Erkennungsdetails anzeigen](#).
- klicken **Ähnliche Geräte** um eine Liste von Geräten mit ähnlichem Netzwerkverkehrsverhalten anzuzeigen, das bei einer Analyse des maschinellen Lernens beobachtet wurde. Mit ähnlichen Geräten können Sie bei der Bedrohungssuche Einblick in das normale Geräteverhalten gewinnen. Diese Registerkarte wird nur angezeigt, wenn dem Gerät ähnliche Geräte zugeordnet sind.
- (NPM-Modulzugriff erforderlich.) klicken **Alerts** , um eine Liste von Benachrichtigungen anzuzeigen, und klicken Sie dann auf einen Warnungsnamen, um [Warnungsdetails anzeigen](#). Diese Registerkarte wird nur angezeigt, wenn dem Gerät Warnmeldungen zugeordnet sind.
- klicken **Peer-Geräte** zu [Sehen Sie sich eine Aktivitätsdiagramm an](#), eine visuelle Darstellung der L4-L7-Protokollaktivität zwischen Geräten in Ihrem Netzwerk. Zu [Ändern Sie die Aktivitätsdiagramm](#) mit zusätzlichen Filtern und Schritten, klicken Sie **Activity Map öffnen**.



Hinweis Sie können die Seite „Geräteübersicht“ mit einem Lesezeichen für eine bestimmte Aktivitätsansicht versehen, indem Sie die `tab` URL-Parameter auf einen der folgenden Werte:

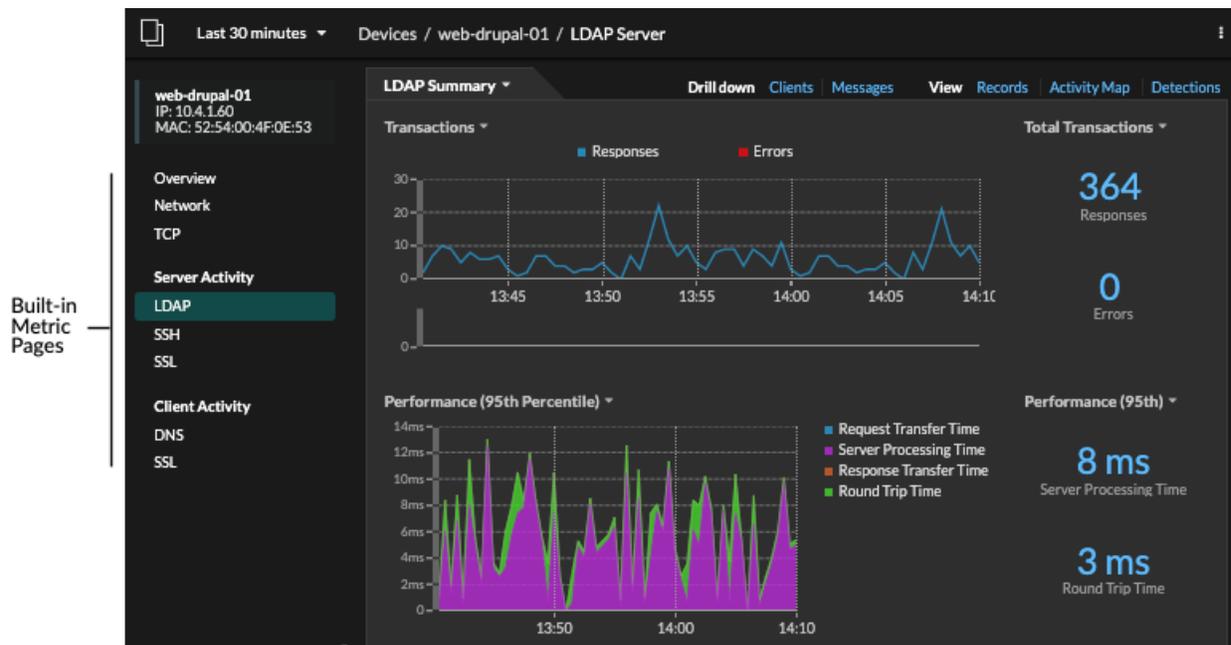
- `tab=traffic`
- `tab=detections`
- `tab=alerts`
- `tab=peers`

Die folgende URL zeigt beispielsweise immer Erkennungsaktivitäten 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 IP-Adress-Link, um Details zu einer IP-Adresse anzuzeigen.

Die folgenden Informationen werden für eine IP-Adresse angezeigt, die auf einem Gerät angezeigt wird:

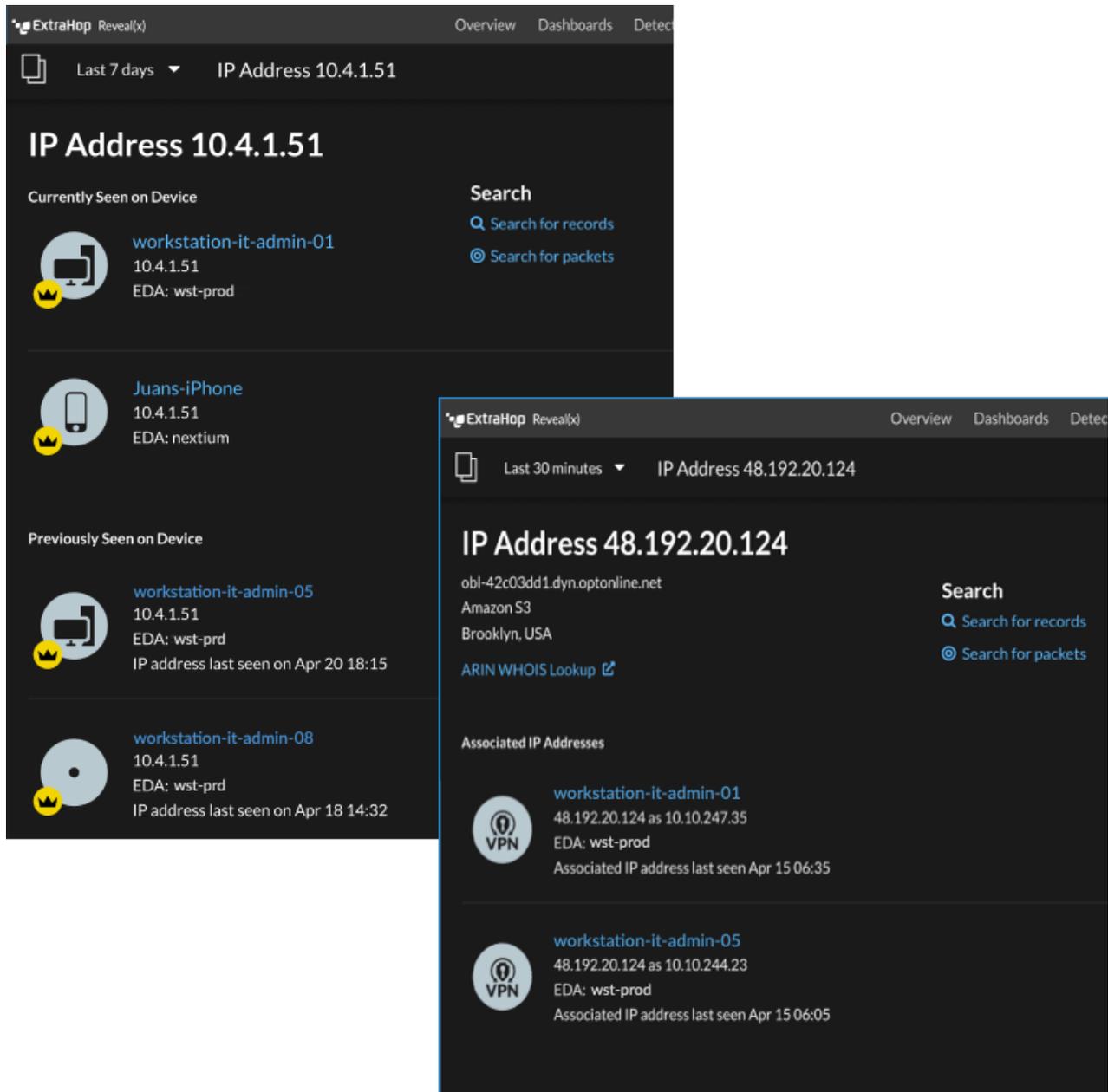
- Jedes Gerät, auf dem die IP-Adresse derzeit beobachtet wird, unabhängig vom ausgewählten Zeitintervall.
- Jedes Gerät, bei dem die IP-Adresse zuvor innerhalb des ausgewählten Zeitintervalls beobachtet wurde, einschließlich des Zeitstempel, ab dem die IP-Adresse zuletzt auf dem Gerät gesehen wurde.

Wenn [L2-Entdeckung](#) aktiviert ist, können sowohl IPv4- als auch IPv6-Adressen gleichzeitig auf dem Gerät beobachtet werden, oder es können dem Gerät im Laufe der Zeit unterschiedliche IP-Adressen von 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 kann 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 gesehen 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 [die Seite mit der Geräteübersicht anzuzeigen](#).
- klicken **Suche nach Datensätzen** um eine zu starten [Datensatzabfrage](#) das wird nach der IP gefiltert .
- klicken **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 zusammenfassen. 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. Mit Gerätegruppen können Sie weiterhin Metriken für jedes einzelne Gerät oder Gruppenmitglied anzeigen. Die Messwerte für ein benutzerdefiniertes Gerät werden wie für ein einzelnes Gerät gesammelt und angezeigt. Sie können keine einzelnen Gerätemetriken anzeigen.

Sowohl Gerätegruppen als auch benutzerdefinierte Geräte können Metriken auf der Grundlage Ihrer angegebenen Kriterien dynamisch aggregieren. Wir empfehlen, zuverlässige Kriterien wie die IP-Adresse des Gerät, die MAC-Adresse, das VLAN, das Tag oder den 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	<ul style="list-style-type: none"> • Gerätenamen und Aliase • IP-Adresse, MAC-Adresse, Subnetz • Quell- und Zielport • Entdeckungszeit • Kritikalität des Geräts • Rolle des Geräts • Protokollaktivität • Externe Verbindungen • Anbieter, Modell, Software • Eigenschaften der Cloud-Instanz • VLAN • Geräte-Tags 	<ul style="list-style-type: none"> • IP-Adresse • Bidirektionaler, eingehender oder ausgehender Datenverkehr • Peer-IP-Adresse • Quellport • Zielhafen • VLAN
Leistungskosten	Vergleichsweise niedrig. Da Gerätegruppen nur Metriken kombinieren, die bereits berechnet wurden, hat dies einen relativ geringen Effekt auf die Erfassung von Metrik. Bei einer hohen Anzahl von Gerätegruppen mit einer großen Anzahl von Geräten und komplexen Kriterien wird die Verarbeitung jedoch mehr Zeit in Anspruch nehmen.	Vergleichsweise hoch. Da die Metriken für benutzerdefinierte Geräte auf der Grundlage benutzerdefinierter Kriterien aggregiert werden, erfordert eine große Anzahl von benutzerdefinierten Geräten oder benutzerdefinierten Geräten mit extrem weit gefassten Kriterien mehr Verarbeitung. Benutzerdefinierte Geräte erhöhen auch die Anzahl der Systemobjekte, denen Metriken zugewiesen werden.
Metriken einzelner Gerät anzeigen	Ja	Nein
Bearbeitungssteuerung für Benutzer mit eingeschränktem Schreibzugriff	Ja Nutzer mit eingeschränkte Schreibrechte  kann Gerätegruppen erstellen und bearbeiten. Diese globale	Nein

	Gerätegruppen	Maßgeschneiderte Geräte
	Berechtigungsrichtlinie muss in den Administrationseinstellungen aktiviert werden.	
Bewährte Verfahren	Erstellen Sie für lokale Geräte, auf denen Sie die Metriken in einem einzigen Diagramm anzeigen und vergleichen möchten. Gerätegruppen können als Metrik-Quelle festgelegt werden.	Erstellen Sie es für Geräte, die sich außerhalb Ihres lokalen Netzwerk befinden, oder für Datenverkehrsarten, die 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 Messwerte 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 über eine Gruppe von Geräten verfügen, für die Sie Messwerte zu einem einzigen Gerät zusammenfassen möchten. Bei diesen Geräten kann es sich sogar um unterschiedliche physische Schnittstellen handeln, die sich auf demselben Gerät befinden. Wenn Sie die Messwerte für diese Schnittstellen zusammenfassen, können Sie leichter nachvollziehen, wie stark Ihre physischen Ressourcen insgesamt belastet sind, und nicht anhand der einzelnen 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 entfernten Standort oder Cloud-Dienst aus zu sammeln. Du kannst [Erfassen Sie Metriken von Remote-Standorten für benutzerdefinierte Geräte](#) um zu erfahren, wie Dienste an entfernten Standorten genutzt werden, und um 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 Messwerte zu einem einzigen Gerät zusammengefasst, das L2-L7-Metriken erfasst. Ein einzelnes benutzerdefiniertes Gerät zählt als ein Gerät auf Ihre lizenzierte Kapazität für [Erweiterte Analyse oder Standardanalyse](#), was es Ihnen ermöglicht [ein benutzerdefiniertes Gerät zur Beobachtungsliste hinzuzufügen](#). Alle Auslöser oder Warnungen werden dem benutzerdefinierten Gerät ebenfalls als einzelnes Gerät zugewiesen.

Benutzerdefinierte Geräte aggregieren zwar Metriken auf der Grundlage ihrer definierten Kriterien, aber die Metrikberechnungen werden nicht genauso behandelt wie für erkannte Geräte. Angenommen, Sie haben einem benutzerdefinierten Gerät einen Auslöser zugewiesen, das Datensätze in einen Recordstore überträgt. 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 der Leitung entspricht.

Benutzerdefinierte Geräte können sich auf die Gesamtleistung des Systems auswirken. 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 von benutzerdefinierten Geräten die Leistung Ihres Systems 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 für mehrere Geräte verfolgen können, die normalerweise nach gemeinsamen Attributen wie Protokollaktivitäten gruppiert sind.

Du kannst [eine statische Gerätegruppe erstellen](#) das erfordert, dass Sie manuell ein Gerät 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. Sie können zum Beispiel [Erstellen Sie eine dynamische Gerätegruppe basierend auf der Geräteerkennungszeit](#) das fügt Geräte hinzu, die während eines bestimmten Zeitintervalls entdeckt wurden.

Standardmäßig enthält die Gerätegruppenseite die folgenden dynamischen Gerätegruppen, die Sie überschreiben oder löschen können:

Neue Geräte (letzte 24 Stunden)

Beinhaltet Ressourcen und Endpunkte, die das ExtraHop-System in den letzten 24 Stunden zum ersten Mal erkannt hat.

Neue Geräte (letzte 7 Tage)

Beinhaltet Ressourcen und Endpunkte, die das ExtraHop-System in den letzten 7 Tagen zum ersten Mal erkannt hat.

Das ExtraHop-System umfasst auch integrierte dynamische Gerätegruppen nach Rolle und Protokoll. Sie können integrierte Gerätegruppen als Metrikquelle für Objekte wie Diagramme, Benachrichtigungen, 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 CIFS-Clients, um die Seite Gerätegruppenübersicht aufzurufen. 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.

Die Erfassung von Metriken mit Gerätegruppen hat keine Auswirkungen auf die Leistung. Wir empfehlen Ihnen jedoch, [priorisieren Sie diese Gruppen](#) durch ihre Bedeutung, sicherzustellen, dass die richtigen Geräte den höchsten Analysegrad erhalten.

Gerätegruppen sind eine gute Wahl, wenn Sie Geräte haben, die Sie gemeinsam als Quelle verwenden möchten. Sie könnten beispielsweise Messwerte für all Ihre Produktionswebserver mit hoher Priorität in einem Dashboard sammeln und anzeigen.

Durch das Erstellen einer Gerätegruppe können Sie all diese Geräte als eine einzige Metrik Quelle verwalten, anstatt sie als einzelne Quellen zu Ihren Diagrammen hinzuzufügen. Beachten Sie jedoch, dass alle zugewiesenen Auslöser oder Benachrichtigungen jedem Gruppenmitglied (oder 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 Gerätenamen 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

Je nach Art des Datenverkehrs, der dem Gerät oder dem Gerätemodell zugeordnet 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 beobachtete Traffic- und Verhaltensänderungen beobachtet werden. Wenn beispielsweise ein PC in einen Server umfunktionierte wurde, können Sie die Rolle sofort ändern, oder die Änderung wird im Laufe der Zeit beobachtet 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 . Die benutzerdefinierte Rolle kann einem Gerät nicht manuell zugewiesen werden.
	Angriffssimulator	Ein Gerät, auf dem 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-, CIFS- und MSRPC-Serveraktivitäten fungiert.
	Dateiserver	Ein Gerät, das auf Lese- und Schreibanforderungen für Dateien über NFS - und CIFS/SMB-Protokolle reagiert.
	Brandmauer	Ein Gerät, das den eingehenden und ausgehenden Netzwerkverkehr überwacht und den Datenverkehr gemäß den Sicherheitsregeln blockiert. Das ExtraHop-System weist Geräten diese Rolle nicht automatisch zu.
	Tor	Ein Gerät, das als Router oder Gateway fungiert. Das ExtraHop-System sucht bei der Identifizierung von Gateways nach Geräten, denen eine große Anzahl an eindeutigen IP-Adressen zugeordnet ist (ab einem bestimmten Schwellenwert). Gateway-Gerätenamen enthalten den Routernamen 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 Gesundheitsbedürfnisse und medizinische Umgebungen entwickelt wurde. Das ExtraHop-System weist diese Rolle möglicherweise zu, wenn es sich bei einem Gerät um eine bekannte medizinische Marke und ein bekanntes medizinisches Modell handelt oder wenn das Gerät DICOM-Verkehr verarbeitet.
	Mobilgerät	Ein Gerät, auf dem ein mobiles Betriebssystem installiert ist, z. B. iOS oder Android.
	NAT-Schnittstelle	Ein Gerät, das als Network Address Translation (NAT) -Gateway fungiert. Das ExtraHop-System weist diese Rolle möglicherweise zu, 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 Geräteeigenschaften für Software, Hardwaremarke und -modell sowie authentifizierte Benutzer nicht mehr für das Gerät angezeigt.

Ikone	Rolle	Beschreibung
	PC	Ein Gerät wie ein Laptop, ein Desktop, eine Windows-VM oder ein macOS-Gerät, das DNS-, HTTP- und SSL-Clientdatenverkehr verarbeitet.
	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 beobachteten Datenverkehrs (Multicast-DNS) 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  , weist das ExtraHop-System 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 von externen VPN-Peers zu, wenn die automatische Klassifizierung für diese Rolle in der laufenden Konfigurationsdatei aktiviert ist.
	Schwachstellen-Scanner	Ein Gerät, auf dem Programme zum Schwachstellenscanner ausgeführt werden.

Ikone	Rolle	Beschreibung
	Web-Proxyserver	Ein Gerät, das HTTP-Anfragen zwischen einem Gerät und einem anderen Server verarbeitet.
	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 in 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 Traffic- und Protokollmetriken auf einer Protokollseite anzeigen.

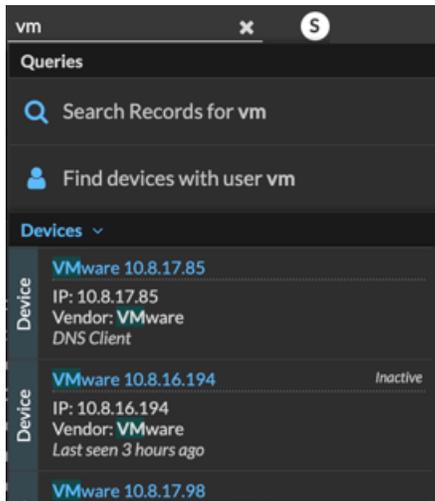
Es gibt mehrere Möglichkeiten, nach einem Gerät zu suchen:

- [Finden Sie ein Gerät über eine globale Suche](#)
- [Suchen Sie anhand von Details nach einem Gerät](#)
- [Suchen Sie nach Geräten anhand der Protokollaktivität](#)
- [Suchen Sie nach Geräten, auf die ein bestimmter Benutzer zugegriffen hat](#)
- [Suche nach Peer-Geräten](#)

Finden Sie ein Gerät 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, Hersteller, Tag, Beschreibung und Gerätegruppe. Wenn Sie beispielsweise nach dem Begriff suchen `vm`, in den Suchergebnissen werden möglicherweise Geräte angezeigt, die `vm` im Gerätenamen, Gerätehersteller oder Geräte-Tag.

1. Geben Sie einen Suchbegriff in das globale Suchfeld oben auf der Seite ein.
2. klicken **Beliebiger Typ** und wählen Sie dann **Geräte**.
Die Suchergebnisse werden in einer Liste unter dem Suchfeld angezeigt. klicken **Mehr Ergebnisse** um durch die Liste zu blättern.



Entsprechende Geräte, die während des angegebenen Zeitintervalls keine Aktivität hatten, haben die Bezeichnung Inaktiv.



Hinweis: Geräte, die länger als 90 Tage inaktiv waren, werden von den globalen Suchergebnissen ausgeschlossen. Sie können jedoch sofort [schließt alle Geräte aus, die weniger als 90 Tage inaktiv waren](#) über die Administrationseinstellungen.

3. Klicken Sie auf einen Gerätenamen, um das zu öffnen [Seite „Geräteübersicht“](#) und sehen Sie sich Geräteeigenschaften und Messwerte an.

Suchen Sie anhand von Details nach einem Gerät

Sie können anhand von Informationen, die über das Kabel beobachtet wurden, nach Geräten suchen, z. B. IP-Adresse, MAC-Adresse, Hostname oder Protokollaktivität. 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 Gerätenamen, IP-Adresse und Rolle hinzufügen, um Ergebnisse für Geräte anzuzeigen, die allen angegebenen Kriterien entsprechen.

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 **Geräte** im linken Bereich, und klicken Sie dann auf **Aktive Geräte** Diagramm.
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 entdeckter Gerätenamen kann beispielsweise die IP-Adresse oder den Hostnamen enthalten.
MAC-Adresse	Filtert Geräte nach der MAC-Adresse Gerät.
IP-Adresse	Filtert Geräte nach IP-Adresse in IPv4-, IPv6- oder CIDR-Blockformaten.
Standort	Filtert Geräte, die einer verbundenen Standort zugeordnet sind. Nur Konsole.
Entdeckungszeit	Filtert Geräte, die vom ExtraHop-System innerhalb des angegebenen Zeitintervalls

Option	Description
Analyseebene	<p>automatisch erkannt werden. Weitere Informationen finden Sie unter Erstellen Sie eine Gerätegruppe basierend auf der Erkennungszeit ↗.</p> <p>Filtert Geräte nach Analyseebene, wodurch festgelegt wird, welche Daten und Metriken für ein Gerät erfasst werden.</p> <p>Sie können keine dynamische Gerätegruppe für Geräte erstellen, die nach Analyseebene gefiltert sind.</p>
Modell	<p>Filtert Geräte nach Marke und Modellnamen. Die folgenden Tipps können Ihnen helfen, das gewünschte Gerätemodell zu finden:</p> <ul style="list-style-type: none"> • Wählen Sie den exakten Übereinstimmungsoperator (=) aus, um eine Dropdownliste vorhandener Modelle und Modellsätze anzuzeigen. • Wählen Sie den exakten Übereinstimmungsoperator (=) und wählen Sie dann Maßgeschneiderte Modelle um alle Geräte zu filtern, die einem benutzerdefinierten Modellsatz zugewiesen sind.
Aktivität	<p>Filtert Geräte nach der Protokollaktivität, die dem Gerät zugeordnet ist. Wenn Sie beispielsweise HTTP-Server auswählen, werden Geräte mit HTTP-Server-Metriken zurückgegeben, und jedes andere Gerät, dessen Geräterolle auf HTTP-Server festgelegt ist.</p> <p>Filtert auch Geräte, die eine externe Verbindung akzeptiert oder initiiert haben, sodass Sie feststellen können, ob Geräte verdächtige Aktivitäten ausführen.</p>
Cloud-Konto	<p>Filtert Geräte nach dem Cloud-Dienstkonto, das dem Gerät zugeordnet ist.</p>
Cloud-Instanz-ID	<p>Filtert Geräte nach der Cloud-Instanz-ID, die dem Gerät zugeordnet ist.</p>
Cloud-Instanztyp	<p>Filtert Geräte nach dem Cloud-Instanztyp, der dem Gerät zugeordnet ist.</p>
Hoher Wert	<p>Filtert Geräte, die als hoher Wert eingestuft werden, weil sie Authentifizierungsdienste bereitstellen, wichtige Dienste in Ihrem Netzwerk unterstützen oder vom Benutzer als wertvoll angegeben wurden.</p>
Derzeit aktiv	<p>Filtert Geräte nach Aktivitäten, die in den letzten 30 Minuten auf einem Gerät beobachtet wurden.</p>

Option	Description
Netzwerk-Lokalitätstyp	Filtert Geräte nach allen internen oder externen Netzwerkstandorten.
Name der Netzwerklokalität	Filtert Geräte nach dem Namen der Netzwerkadresse.
Rolle	Filtert Geräte nach der zugewiesenen Geräterolle, z. B. Gateway, Firewall, Load Balancer und DNS-Server.
Software	Filtert Geräte nach der auf dem Gerät erkannten Betriebssystemsoftware.
Subnetz	Filtert Geräte nach dem Subnetz, das dem Gerät zugeordnet ist.
Schlagwort	Filtert Geräte nach benutzerdefinierten Gerätekennzeichnungen.
Verkäufer	Filtert Geräte nach dem Namen des Geräteanbieters, der durch die OUI-Suche (Organizationally Unique Identifier) bestimmt wird.
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 sie bei der Datenverkehrsspiegelung auf dem Mirror-Port gespeichert werden. Nur verfügbar, wenn <code>devices_accross_vlans</code> Einstellung ist gesetzt auf <code>False</code> in der laufenden Konfigurationsdatei.
CDP-Name	Filtert Geräte nach dem CDP-Namen, der dem Gerät zugewiesen wurde.
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 wurde.
DNS-Name	Filtert Geräte nach jedem DNS-Namen, der dem Gerät zugewiesen wurde.
NetBIOS-Name	Filtert Geräte nach dem NetBIOS-Namen, der dem Gerät zugewiesen wurde.

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 der ausgewählten Kategorie entsprechen.

Option	Description
#	Filtert Geräte, die nicht exakt mit dem Suchfeld übereinstimmen.
≈	Filtert Geräte, die den Wert des Suchfeldes für die ausgewählte Kategorie enthalten.
≈/	Filtert Geräte, die den Wert des Suchfeldes 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 Suchfeldes für die ausgewählte Kategorie enthalten.

- Geben Sie im Suchfeld die Zeichenfolge ein, nach der gesucht 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, nach der gesucht werden soll, in das Suchfeld Feld. Wenn Sie Geräte anhand von Rollen suchen möchten, wählen Sie aus der Dropdownliste der Rollen aus.



Hinweis Abhängig von der ausgewählten Kategorie können Sie im Textfeld auf das Regex-Symbol klicken, um den Abgleich anhand eines regulären Ausdrucks zu aktivieren.



- klicken **Filter hinzufügen**.
Die Geräteliste wird nach den angegebenen Kriterien gefiltert.

Nächste Schritte

- Klicken Sie auf einen Gerätenamen, um Geräteeigenschaften und Messwerte auf dem [Seite „Geräteübersicht“](#).
- klicken **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.

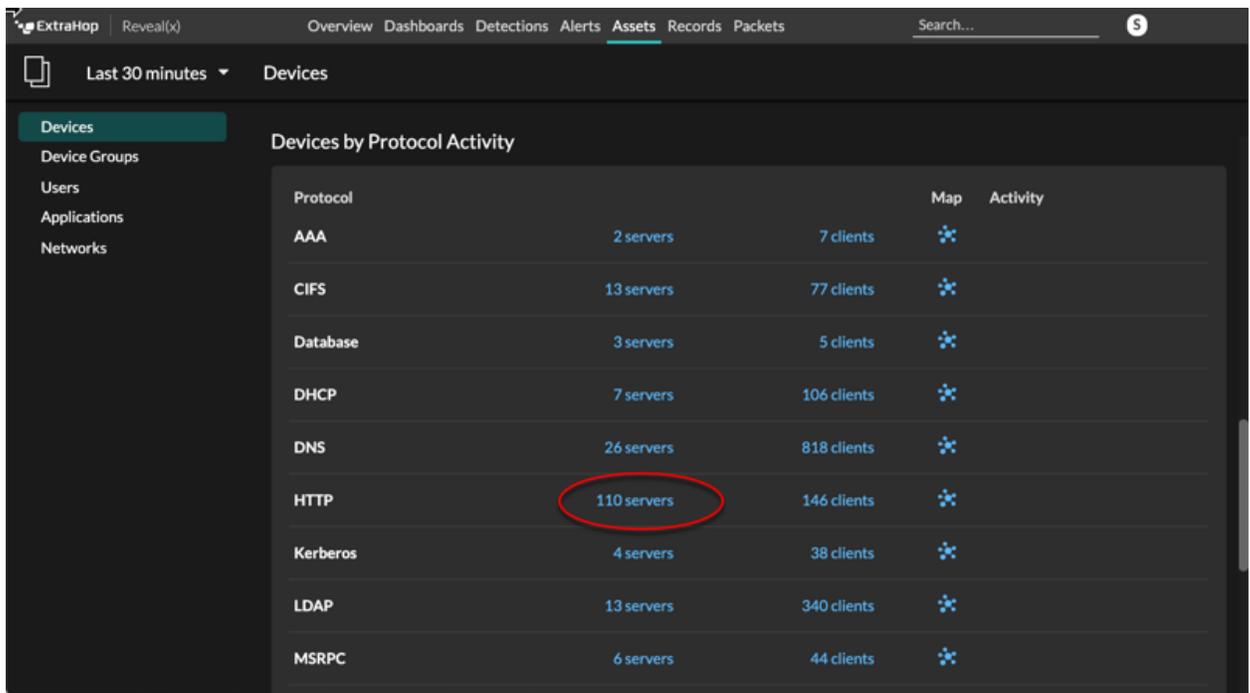
Suchen Sie nach Geräten anhand der Protokollaktivität

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 finden, 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.

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

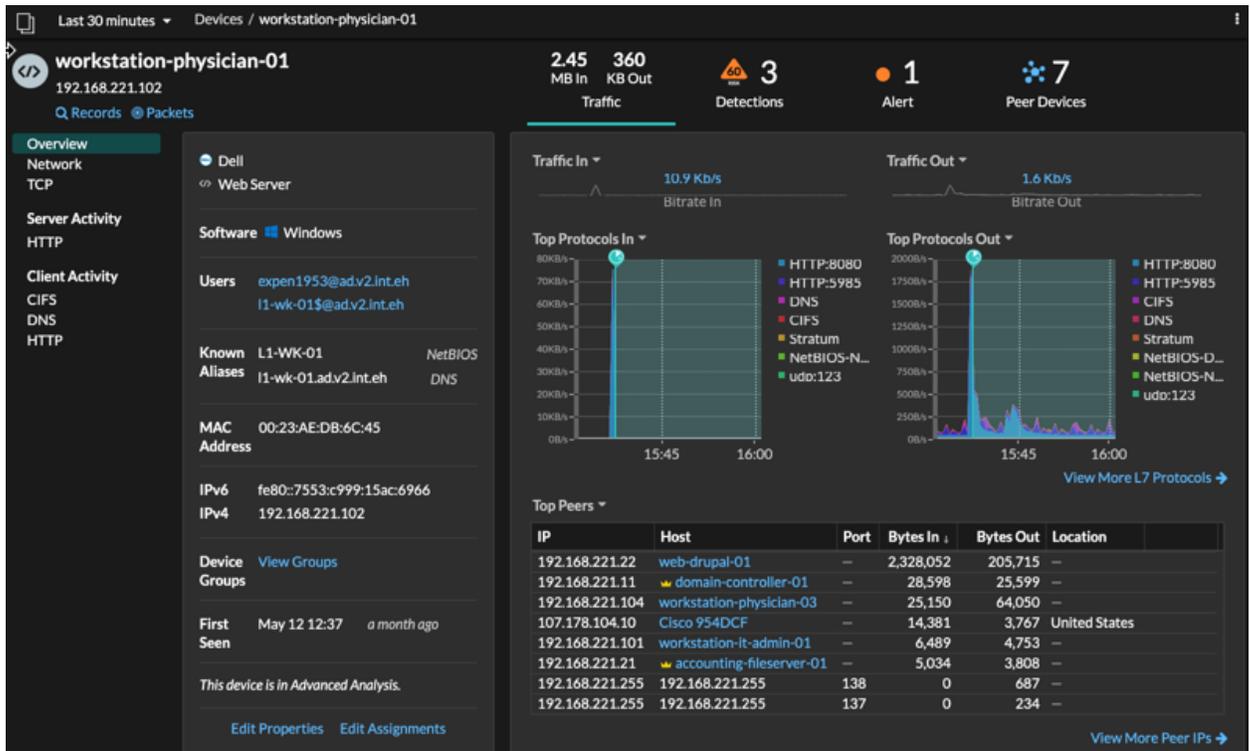
3. Klicken Sie im Diagramm Geräte nach Protokollaktivität auf die Anzahl der HTTP-Server, wie in der folgenden Abbildung dargestellt.



Hinweis: Wenn das gewünschte Protokoll nicht angezeigt wird, hat das ExtraHop-System diese Art von Protokollverkehr über die Leitung während des angegebenen Zeitintervalls möglicherweise nicht beobachtet, oder das Protokoll erfordert möglicherweise eine Modullizenz. Weitere Informationen finden Sie in der [Ich sehe den Protokollverkehr, den ich erwartet habe, nicht?](#) Abschnitt in den häufig gestellten Fragen zur Lizenz.

Auf der Seite werden Traffic- und Protokollmetriken angezeigt, die der Gruppe von HTTP-Servern zugeordnet sind.

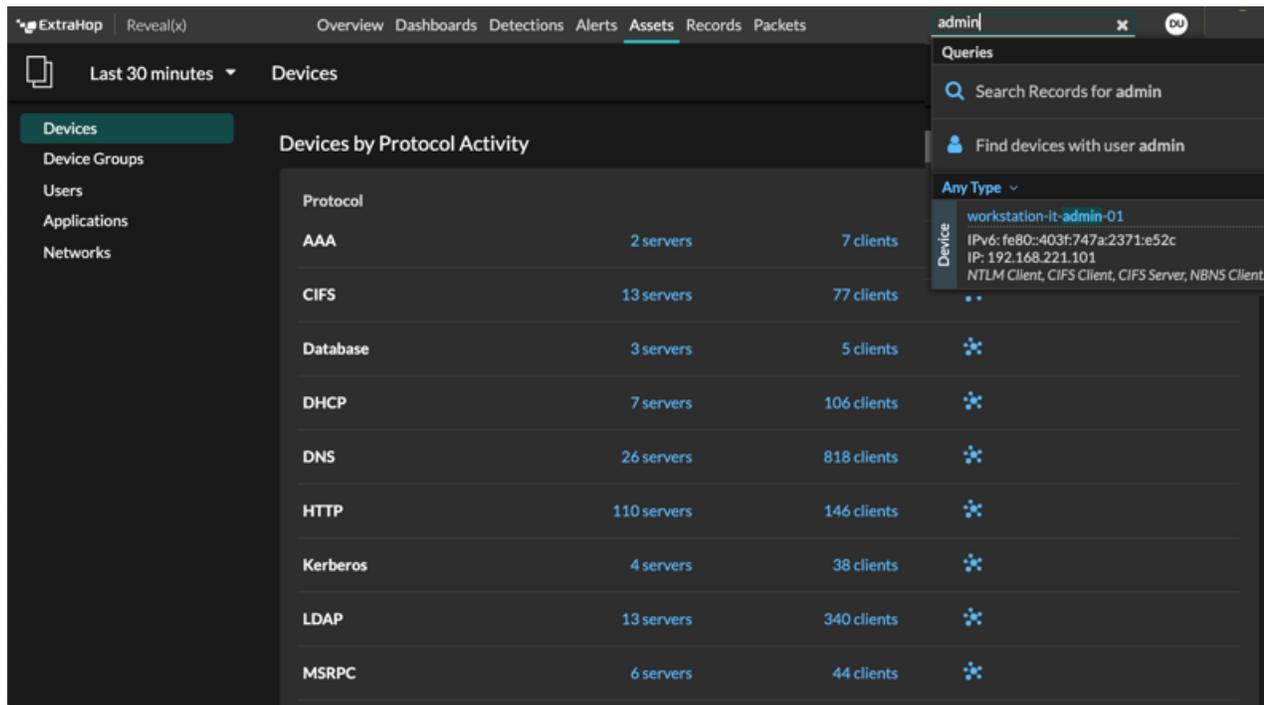
4. Klicken Sie oben auf der Seite auf **Mitglieder der Gruppe**.
Auf der Seite wird eine Tabelle mit allen Geräten angezeigt, die während des ausgewählten Zeitintervalls HTTP-Antworten über das Kabel gesendet haben.
5. Klicken Sie in der Tabelle auf einen Gerätenamen.
Auf der Seite werden Traffic- und Protokollmetriken angezeigt, die mit diesem Gerät verknüpft sind, ähnlich der folgenden Abbildung.



Suchen Sie nach Geräten, auf die ein bestimmter Benutzer zugegriffen hat

Auf der Seite Benutzer können Sie die aktiven Benutzer und die Geräte sehen, die sie während des angegebenen Zeitintervalls am ExtraHop-System angemeldet haben.

Hinweis: Sie können auch über das globale Suchfeld oben auf der Seite nach Benutzern suchen.



Dieses Verfahren zeigt Ihnen, wie Sie eine Suche von der Benutzerseite aus durchführen.

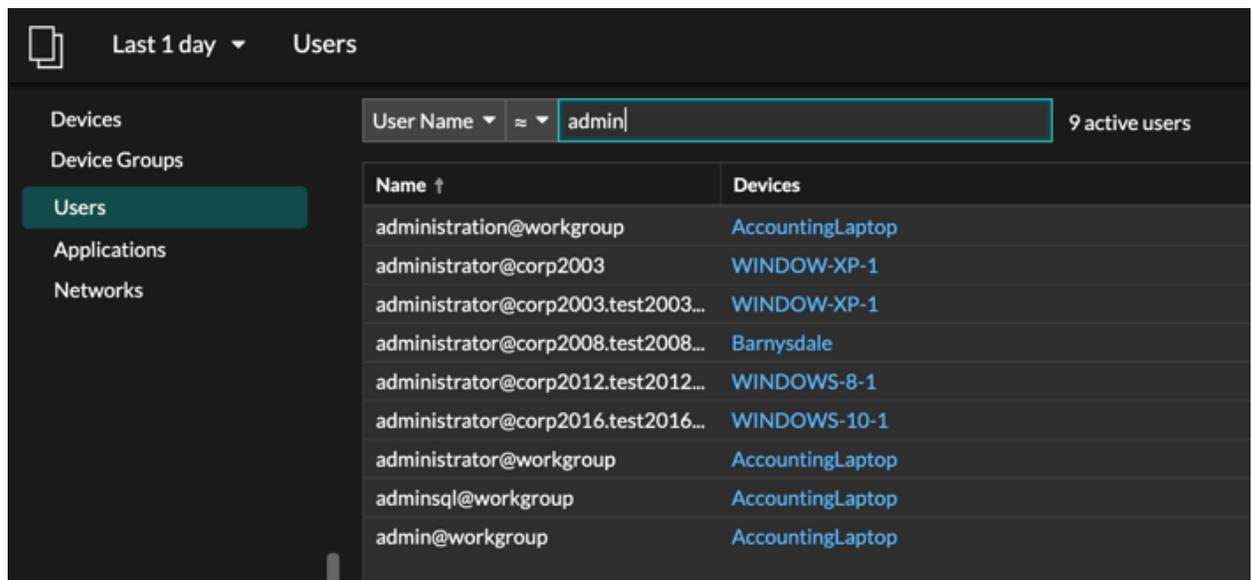
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Vermögenswerte**.
3. klicken **Nutzer** im linken Bereich.
4. Wählen Sie in der Suchleiste eine der folgenden Kategorien aus der Drop-down-Liste aus:

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 Protokoll, 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.

5. Wählen Sie einen der folgenden Operatoren aus der Dropdownliste aus:

Option	Description
=	Suchen Sie nach einem Namen oder Gerät, das exakt 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.

6. Geben Sie in das Textfeld den Namen des Benutzers oder Gerät ein, den Sie zuordnen oder ausschließen möchten.
Auf der Seite „Benutzer“ wird eine Ergebnisliste angezeigt, die der folgenden Abbildung ähnelt:



7. 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.

Suche nach Peer-Geräten

Wenn Sie wissen möchten, welche Geräte aktiv miteinander kommunizieren, können Sie von einer Protokollseite für Geräte oder Gerätegruppe aus nach Peer-IPs suchen.

Wenn du [bohren](#) Nach Peer-IP-Adresse können Sie eine Liste von Peer-Geräten untersuchen, Leistungs- oder Durchsatzmetriken für Peer-Geräte anzeigen und dann auf einen Peer-Gerätenamen klicken, um zusätzliche 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. [Suchen Sie 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

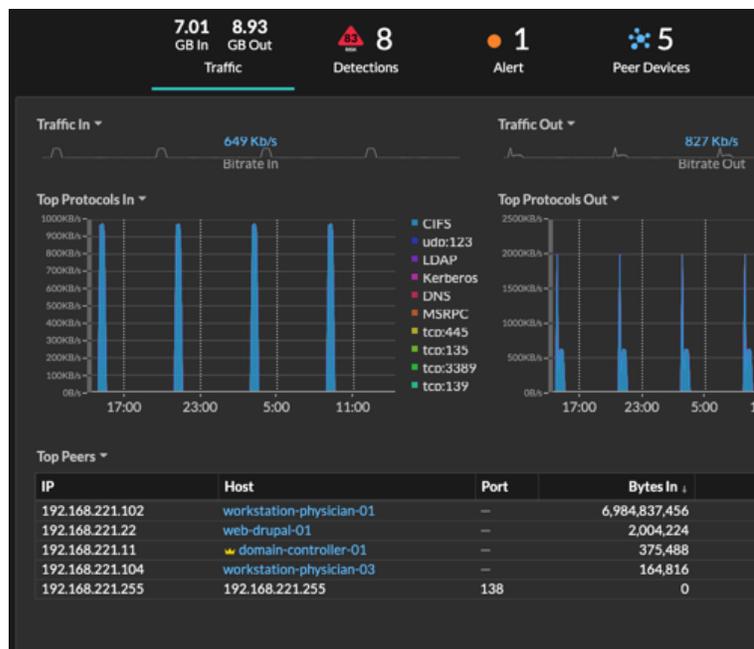
Für Geräte

Description

klicken **Weitere Peer-IPs anzeigen**, befindet sich am unteren Rand des Top-Peer-Charts.

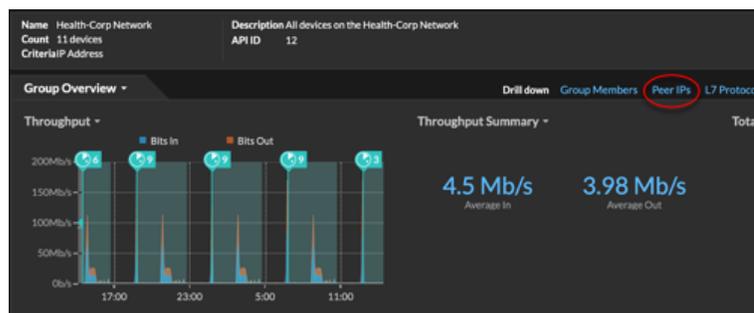
Option

Description

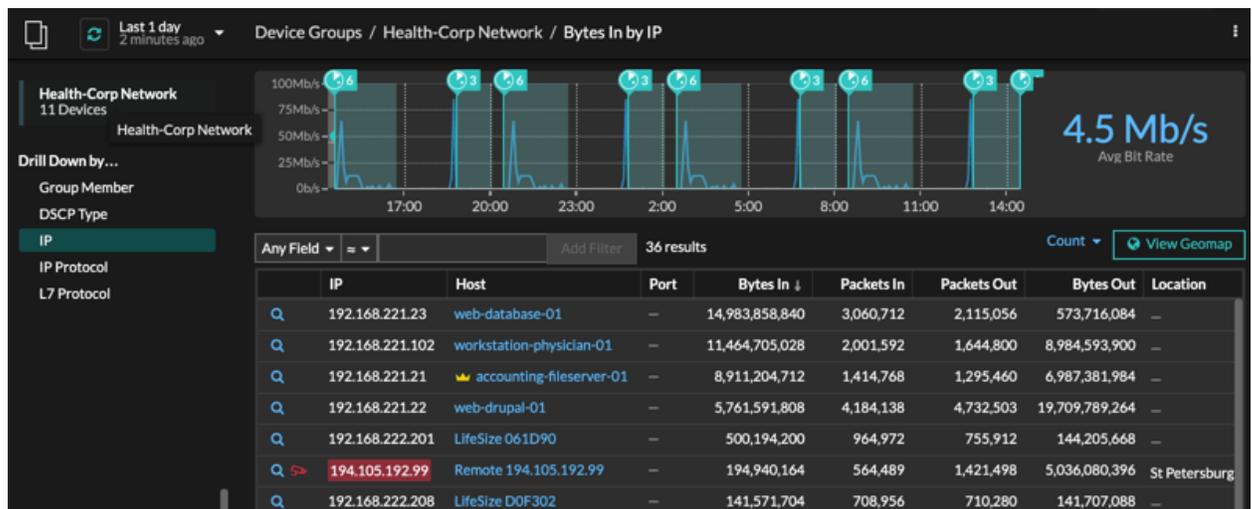


Für Gerätegruppen

klicken **Peer-IPs**, befindet sich im Bereich Details in der oberen rechten Ecke der Seite.



Es wird eine Liste von Peer-Geräten angezeigt, die nach IP-Adresse aufgeschlüsselt sind. Sie können Netzwerkbytes- und Paketinformationen für jedes Peer-Gerät untersuchen, wie in der folgenden Abbildung dargestellt.



View the peer device sending or receiving data from the source device. If available, click the hostname to learn about activity on that device.

View network throughput metrics for traffic associated with peer devices.

Einen Gerätenamen ändern

Das ExtraHop-System benennt Geräte automatisch, indem es den Verkehr mit den Namensprotokollen (DNS, DHCP, NETBIOS, CDP) passiv überwacht. Wenn für ein Gerät kein Verkehr mit dem Benennungsprotokoll beobachtet wird, zeigt der Gerätenamen 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 zur Änderung eines Gerätenamens:

- Benutzerdefinierte Namen werden nicht zwischen verbundenen ExtraHop-Systemen synchronisiert. Beispielsweise ist ein benutzerdefinierter Name, der für einen Sensor erstellt wurde, 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 drahtgebundene Daten 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**.
3. klicken **Geräte** im linken Bereich, und klicken Sie dann auf **Aktive Geräte** Diagramm.
4. 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.

5. klicken **Eigenschaften bearbeiten**.
6. klicken **Benutzerdefinierten Namen anzeigen**.
7. Geben Sie einen benutzerdefinierten Namen in das Feld ein.

8. klicken **Speichern**.

Eine Geräterolle ändern

Das ExtraHop-System erkennt und klassifiziert Geräte in Ihrem Netzwerk automatisch auf der Grundlage der Protokollaktivität oder des Gerätemodells und weist jedem Gerät eine Rolle zu, z. B. einem Gateway, Dateiserver, einer Datenbank oder einem Load Balancer. Sie können die einem Gerät zugewiesene Rolle jederzeit ändern.

Hier sind einige wichtige Überlegungen zum Ändern einer Geräterolle:

- Nachdem Sie das geändert haben **Geräterolle**, das Gerät wurde möglicherweise entfernt oder hinzugefügt **dynamische Gerätegruppen** die eine Gerät als Kriterien beinhalten.
- Änderungen der Geräterolle werden nicht zwischen verbundenen ExtraHop-Systemen synchronisiert. Wenn Sie beispielsweise eine Geräterolle auf einem ändern Sensor, die Rolle wird nicht von einer verbundenen 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**.

3. klicken **Geräte** im linken Bereich, und klicken Sie dann auf **Aktive Geräte** Diagramm.

4. 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.

5. klicken **Eigenschaften bearbeiten**.

6. In der Rolle des Geräts klicken Sie im Abschnitt auf die Dropdownliste, und klicken Sie dann auf eine der folgenden Rollen:

Rolle	Beschreibung
Automatisch	Weisen Sie die Rolle zu, die das ExtraHop-System für das Gerät identifiziert hat und die in Klammern steht.
Angriffssimulator	Weisen Sie es einem Gerät zu, auf dem Breach and Attack Simulation (BAS) -Software ausgeführt wird, um Angriffe in einem Netzwerk zu simulieren.
Datenbank	Weisen Sie es einem Gerät zu, das eine Datenbankinstanz hostet.
DHCP-Server	Weisen Sie es einem Gerät zu, dessen Hauptfunktion die Verarbeitung von DHCP-Serveraktivitäten ist.
DNS-Server	Weisen Sie es einem Gerät zu, dessen Hauptfunktion die Verarbeitung von DNS-Serveraktivitäten ist.
Domänencontroller	Weisen Sie es einem Gerät zu, das als Domänencontroller für Kerberos-, CIFS- und MSRPC-Serveraktivitäten fungiert.
Dateiserver	Weisen Sie es einem Gerät zu, das auf Lese- und Schreibanforderungen für Dateien über die Protokolle NFS und CIFS/SMB reagiert.

Rolle	Beschreibung
Brandmauer	Weisen Sie es einem Gerät zu, das den eingehenden und ausgehenden Netzwerkverkehr überwacht und den Datenverkehr gemäß den Sicherheitsregeln blockiert.
Tor	Weisen Sie es einem Gerät zu, das als Router oder Gateway fungiert.
IP-Kamera	Weisen Sie es einem Gerät zu, das Bild- und Videodaten über das Netzwerk sendet, z. B. Sicherheitskameras.
Load Balancer	Weisen Sie es einem Gerät zu, das als Reverse-Proxy für die Verteilung des Datenverkehrs auf mehrere Server fungiert.
Medizinisches Gerät	Weisen Sie es einem Gerät zu, das speziell für Gesundheitsbedürfnisse und medizinische Umgebungen entwickelt wurde.
Mobilgerät	Weisen Sie es einem Gerät zu, auf dem ein mobiles Betriebssystem wie iOS oder Android installiert ist.
NAT-Gateway	Weisen Sie es einem Gerät zu, 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 verbunden. Nachdem einem Gerät diese Rolle zugewiesen wurde, werden Geräteeigenschaften für Software, Hardwaremarke und -modell sowie authentifizierte Benutzer nicht mehr für das Gerät angezeigt.
PC	Weisen Sie es einem Gerät wie einem Laptop, Desktop, Windows-VM oder macOS-Gerät zu.
Drucker	Weisen Sie es einem Gerät zu, mit dem Benutzer Text und Grafiken von anderen verbundenen Geräten drucken können.
VoIP-Telefon	Weisen Sie es einem Gerät zu, das Voice over IP (VoIP) -Telefonanrufe verwaltet.
VPN-Gateway	Weisen Sie es einem Gerät zu, das zwei oder mehr VPN-Geräte oder -Netzwerke miteinander verbindet, um Remoteverbindungen zu überbrücken.
Schwachstellen-Scanner	Weisen Sie es einem Gerät zu, auf dem Schwachstellen-Scanner-Programme ausgeführt werden.
Web-Proxyserver	Weisen Sie es einem Gerät zu, das HTTP-Anfragen zwischen einem Gerät und einem anderen Server verarbeitet.

Rolle	Beschreibung
Webserver	Weisen Sie es einem Gerät zu, das Webressourcen hostet und auf HTTP-Anfragen reagiert.
Wi-Fi-Zugangspunkt	Weisen Sie es einem Gerät zu, das ein drahtloses lokales Netzwerk erstellt und ein drahtloses Netzwerksignal in einen bestimmten Bereich projiziert.
Andere	Einem Gerät zuweisen, wenn die Geräteaktivität nicht eindeutig eine einzelne Rolle identifiziert.

7. klicken **Speichern**.

Gerätemodell ändern

Das ExtraHop-System beobachtet den Netzwerkverkehr auf Geräten, um automatisch die Marke und das Modell des Anbieters zu ermitteln. Sie können das Gerätemodell jedoch manuell ändern.

Hier sind einige wichtige Überlegungen zum Ändern eines Gerätemodells:

- Geräte werden automatisch zu dynamischen Gerätegruppen hinzugefügt und daraus entfernt, wobei die Kriterien auf den Gerätemodellen basieren.
- Sie können ein Gerätemodell ändern von Sensoren und Konsolen. Wenn das Gerät aktualisiert wird auf einem Konsole, die Änderung wird mit dem verbundenen synchronisiert Sensoren. Die Änderung wird jedoch nicht von einer Person aus synchronisiert Sensoren zum 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**.
3. klicken **Geräte** im linken Bereich, und klicken Sie dann auf **Aktive Geräte** Diagramm.
4. Filtern Sie die Geräteliste, um das gewünschte Gerät zu finden, und klicken Sie dann auf den Gerätenamen.
Die Überblick über das Gerät Eine Seite wird angezeigt, auf der der Datenverkehr und die Protokollaktivität für das ausgewählte Gerät angezeigt werden.
5. klicken **Eigenschaften bearbeiten**.
6. In der Modell des Geräts Abschnitt, wählen Sie eine der folgenden Optionen aus:

Option	Description
Automatisch	<ul style="list-style-type: none"> • Wählen Sie diese Option, damit das ExtraHop-System automatisch die Marke und das Modell des Gerät ermitteln kann, die in Klammern angezeigt werden.
Benutzerdefiniert	<ol style="list-style-type: none"> 1. Wählen Sie diese Option, um Marke und Modell des Gerät manuell anzugeben. 2. klicken Geben Sie eine Gerätemarke an... und geben Sie den Namen der gewünschten Marke ein. In der Drop-down-Liste werden passende Marken angezeigt.

Option	Description
7. klicken Speichern .	<ol style="list-style-type: none"> 3. Wählen Sie eine Marke aus der Drop-down-Liste aus oder geben Sie einen benutzerdefinierten Markennamen ein. 4. klicken Geben Sie ein Gerätemodell an... und geben Sie den Namen des gewünschten Modells ein. Wenn Sie eine bestehende Marke ausgewählt haben, werden in der Drop-down-Liste passende Modelle für diese Marke angezeigt. 5. Wählen Sie ein Modell aus der Drop-down-Liste aus oder geben Sie einen benutzerdefinierten Modellnamen ein.

Manuelles Identifizieren eines Gerät hoher Wert

Das ExtraHop-System identifiziert Geräte, die Authentifizierung oder wichtige Dienste bereitstellen, automatisch als hoher Wert. Sie können jedoch auch manuell festlegen, ob ein Gerät von hoher Wert ist oder nicht.

Im Folgenden finden Sie einige wichtige Überlegungen zur Identifizierung eines Gerät hoher Wert:

- Die Risikowerte für Erkennungen auf hoher Wert Geräten werden erhöht.
- Geräte werden automatisch zu dynamischen Gerätegruppen hinzugefügt und daraus entfernt, wobei die Kriterien auf einem hoher Wert basieren.
- Sie können hoher Wert Geräte manuell identifizieren von Sensoren und Konsolen. Wenn das Gerät aktualisiert wird auf einem Konsole, die Änderung wird mit dem verbundenen synchronisiert Sensoren. Die Änderung wird jedoch nicht von einer Person aus synchronisiert Sensoren zum 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**.
3. klicken **Geräte** im linken Bereich, und klicken Sie dann auf **Aktive Geräte** Diagramm.
4. 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.
5. klicken **Eigenschaften bearbeiten**.
6. Wählen Sie im Abschnitt High Value eine der folgenden Optionen aus:
 - Wählen **Automatisch** damit das ExtraHop-System automatisch feststellen 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 es sich bei dem Gerät nicht um ein hoher Wert Gerät handelt.
7. klicken **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 Gerätenamen 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 sowohl dynamische als auch statische Gerätegruppen erstellen. Dynamische Gruppen fügen der Gruppe automatisch alle Geräte hinzu, die bestimmten Kriterien entsprechen, während bei statischen Gruppen jedes Gerät manuell hinzugefügt werden muss.

Erstellen Sie eine dynamische Gerätegruppe

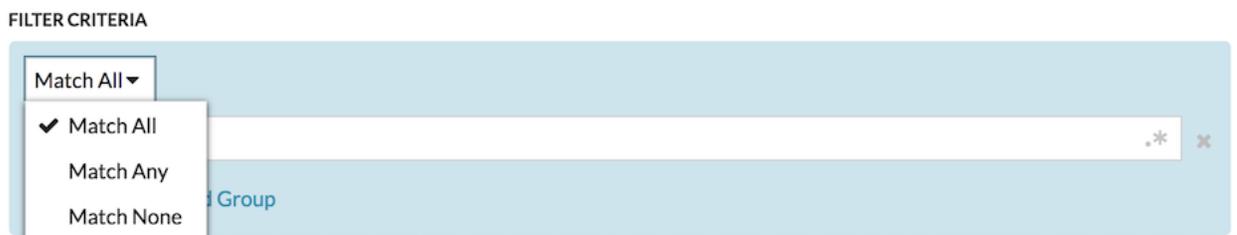
Sie können dynamische Gerätegruppen mit komplexen Filtern erstellen, mit denen Sie mehrere Kriterien angeben und verschachtelte Gruppen von Kriterien erstellen können.

 **Hinweis** Sie können schnell eine dynamische Gerätegruppe aus einer gefilterten Geräteliste auf der Geräteseite erstellen. klicken **Dynamische Gruppe erstellen** von der oberen rechten Ecke.

Sie können auch eine dynamische Gerätegruppe aus einer integrierten Gerätegruppe erstellen. Klicken Sie auf der Seite Geräte auf eine Rolle oder ein Protokoll, aktualisieren Sie die Filterkriterien und klicken Sie dann auf Speichern  Symbol von der oberen rechten Ecke.

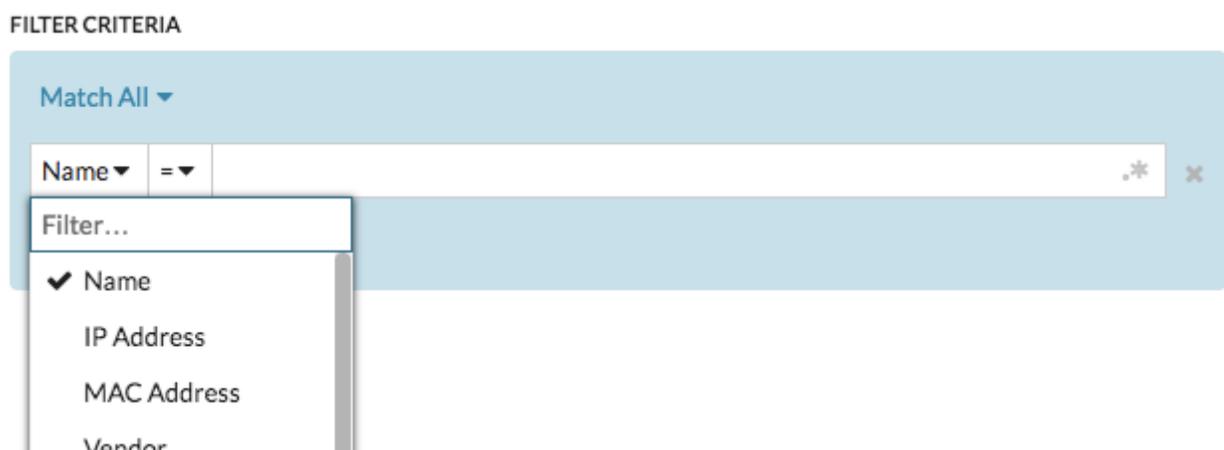
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.

2. Klicken Sie im oberen Menü auf **Vermögenswerte** und dann klicken **Gerätegruppen** im linken Bereich.
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 Recht muss in den Administrationseinstellungen aktiviert werden.
 - In der Liste werden nur eingeschränkte Schreibbenutzer mit aktiven Konten angezeigt.
 - Nur ein Benutzer mit Bearbeitungsberechtigungen für eine Gerätegruppe kann weitere Benutzer mit eingeschränkten Schreibberechtigungen hinzufügen.
6. Optional: In der **Beschreibung** Feld, fügen Sie Informationen zu dieser Gerätegruppe hinzu.
7. In der Art der Gruppe Abschnitt, klicken **Dynamisch**.
8. In der Kriterien filtern Abschnitt, klicken **Alle abgleichen** und wählen Sie dann einen der folgenden Vergleichsoperatoren aus der Dropdownliste aus:



Option	Description
Alle abgleichen	Filtert nur Geräte, die allen angegebenen Kriterien entsprechen.
Beliebiges abgleichen	Filtert Geräte, die einem der angegebenen Kriterien entsprechen.
Kein Spiel	Filtert Geräte, die keinem der angegebenen Kriterien entsprechen.

9. klicken **Name** und wählen Sie eine der folgenden Kategorien aus der Drop-down-Liste aus:



Option	Description
Name	Filtert Geräte nach dem erkannten Gerätenamen. Ein entdeckter Gerätenamen kann beispielsweise die IP-Adresse oder den Hostnamen enthalten.

Option	Description
MAC-Adresse	Filtert Geräte nach der MAC-Adresse Gerät.
IP-Adresse	Filtert Geräte nach IP-Adresse in IPv4-, IPv6- oder CIDR-Blockformaten.
Standort	Filtert Geräte, die einer verbundenen Standort zugeordnet sind. Nur Konsole.
Entdeckungszeit	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, wodurch festgelegt wird, 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 und Modellnamen. Die folgenden Tipps können Ihnen helfen, das gewünschte Gerätemodell zu finden: <ul style="list-style-type: none"> • Wählen Sie den exakten Übereinstimmungsoperator (=) aus, um eine Dropdownliste vorhandener Modelle und Modellsätze anzuzeigen. • Wählen Sie den exakten Übereinstimmungsoperator (=) und wählen Sie dann Maßgeschneiderte Modelle um alle Geräte zu filtern, die einem benutzerdefinierten Modellsatz zugewiesen sind.
Aktivität	Filtert Geräte nach der Protokollaktivität, die dem Gerät zugeordnet ist. Wenn Sie beispielsweise HTTP-Server auswählen, werden Geräte mit HTTP-Server-Metriken zurückgegeben, und jedes andere Gerät, 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.

Option	Description
Cloud-Instanztyp	Filtert Geräte nach dem Cloud-Instanztyp, der dem Gerät zugeordnet ist.
Hoher Wert	Filtert Geräte, die als hoher Wert eingestuft werden, weil sie Authentifizierungsdienste bereitstellen, wichtige Dienste in Ihrem Netzwerk unterstützen oder vom Benutzer als wertvoll angegeben 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 Netzwerkadresse.
Rolle	Filtert Geräte nach der zugewiesenen Geräterolle, z. B. Gateway, Firewall, Load Balancer und DNS-Server.
Software	Filtert Geräte nach der auf dem Gerät erkannten Betriebssystemsoftware.
Subnetz	Filtert Geräte nach dem Subnetz, das dem Gerät zugeordnet ist.
Schlagwort	Filtert Geräte nach benutzerdefinierten Gerätekennzeichnungen.
Verkäufer	Filtert Geräte nach dem Namen des Geräteanbieters, der durch die OUI-Suche (Organizationally Unique Identifier) bestimmt wird.
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 sie bei der Datenverkehrsspiegelung auf dem Mirror-Port gespeichert werden. Nur verfügbar, wenn <code>devices_accross_vlans</code> Einstellung ist gesetzt auf <code>False</code> in der laufenden Konfigurationsdatei.
CDP-Name	Filtert Geräte nach dem CDP-Namen, der dem Gerät zugewiesen wurde.
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 wurde.

Option	Description
DNS-Name	Filtert Geräte nach jedem DNS-Namen, der dem Gerät zugewiesen wurde.
NetBIOS-Name	Filtert Geräte nach dem NetBIOS-Namen, der dem Gerät zugewiesen wurde.

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 der ausgewählten Kategorie entsprechen.
#	Filtert Geräte, die nicht exakt mit dem Suchfeld übereinstimmen.
≈	Filtert Geräte, die den Wert des Suchfeldes für die ausgewählte Kategorie enthalten.
≈/	Filtert Geräte, die den Wert des Suchfeldes 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 Suchfeldes für die ausgewählte Kategorie enthalten.

11. Geben Sie im Suchfeld die Zeichenfolge ein, nach der gesucht werden soll, oder wählen Sie einen Wert aus der Dropdownliste aus. Der Eingabetyp wird durch die ausgewählte Kategorie bestimmt. Wenn Sie beispielsweise Geräte anhand des Namens suchen möchten, geben Sie die Zeichenfolge, nach der gesucht werden soll, in das Suchfeld ein. Wenn Sie Geräte anhand von Rollen suchen möchten, wählen Sie aus der Dropdownliste der Rollen aus.

FILTER CRITERIA

Match All ▾

Name ▾ ≈ ▾ accounting-.* ✕

Add Filter Add Filter Group

FILTER CRITERIA

Match All ▾

Role ▾ = ▾ Select an item... ✕

Add Filter Filter...

- Database
- DHCP Server
- DNS Server



Hinweis Abhängig von der ausgewählten Kategorie können Sie im Textfeld auf das Regex-Symbol klicken, um den Abgleich anhand eines regulären Ausdrucks zu aktivieren.

FILTER CRITERIA

Match All ▾

Name ▾ = ▾ ✕

Add Filter Add Filter Group

Type regular expression

- Optional: klicken **Filter hinzufügen** um weitere Filterkriterien hinzuzufügen.
- Optional: klicken **Filtergruppe hinzufügen** um den Ergebnissen des ursprünglichen Filters Filterkriterien hinzuzufügen.

Wenn Sie beispielsweise nach Gerätenamen filtern, die mit „acct“ 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 „acct“ beginnen.

- klicken **Speichern**.

Sie können die Kriterien ändern, indem Sie auf der Seite Gerätegruppen auf die Gruppe klicken, die Sie ändern möchten, und dann auf **Eigenschaften**.

Erstellen Sie eine statische Gerätegruppe

- Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
- klicken **Vermögenswerte** und dann klicken **Gerätegruppen**.
- klicken **Gerätegruppe erstellen**.
- 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 Recht muss in den Administrationseinstellungen aktiviert werden.
 - In der Liste werden nur Benutzer mit eingeschränkten Schreibzugriffen mit aktiven Konten angezeigt.
 - Nur ein Benutzer mit Bearbeitungsberechtigungen für eine Gerätegruppe kann weitere Benutzer mit eingeschränkten Schreibberechtigungen hinzufügen.
6. Optional: In der **Beschreibung** Feld, fügen Sie Informationen zu dieser Gerätegruppe hinzu.
7. In der Art der Gruppe Abschnitt, wählen **Statisch**.
8. klicken **Speichern**.
Ihre Gerätegruppe ist jetzt erstellt.
9. Fügen Sie Geräte zu Ihrer Gruppe hinzu.
 - a) klicken **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 **Einer Gruppe zuweisen**.
 - d) Wählen Sie eine Gerätegruppe aus der Gruppe Drop-down-Liste.
 - e) klicken **Zur Gruppe hinzufügen**.

Nächste Schritte

Entfernen Sie Geräte aus einer Gruppe, indem Sie das Kontrollkästchen neben dem Gerätenamen aktivieren und auf **Aus Gruppe entfernen** in der oberen rechten Ecke.

Benutzerdefiniertes Gerät erstellen

Erfassen Sie Metriken für ein Verkehrsegment 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 Kriterioptionen 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, Sensor und 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 Netzwerkstandorte und vertrauenswürdige Domänen an

Indem Sie Einzelheiten zu Ihren Netzwerkspezifikationen angeben, können Sie die von Ihrem ExtraHop-System generierten Messwerte und Erkennungen verbessern. Auf der Seite Netzwerkortschaften können Sie interne und externe IP-Adressen angeben und vertrauenswürdige Domänen hinzufügen, mit denen sich Ihre Geräte regelmäßig verbinden.

Hier sind einige wichtige Überlegungen zu diesen Einstellungen:

- Wenn Ihre ExtraHop-Bereitstellung eine Konsole umfasst, empfehlen wir Ihnen [Transfermanagement](#)  aller an die Konsole angeschlossenen Sensoren.
- Für ExtraHop Reveal (x) 360 werden diese Einstellungen für alle angeschlossenen Sensoren synchronisiert. Sie sollten diese Einstellungen nicht für einzelne Sensoren konfigurieren.
- Wenn Sie bei ExtraHop Reveal (x) Enterprise die Verwaltung auf eine verbundene Konsole übertragen, werden diese Einstellungen zwischen allen Sensoren synchronisiert. Andernfalls müssen die Einstellungen für die Netzwerklokalität auf allen Sensoren und Konsolen konfiguriert werden.
- Sie müssen vollständig geschrieben haben [Privilegien](#)  um diese Einstellungen zu ändern.

Geben Sie eine Netzwerklokalität an

Mithilfe von Netzwerklokalitäten können Sie den Datenverkehr von IP-Adressen und CIDR-Blöcken als intern oder extern in Ihrem Netzwerk klassifizieren. Sie können auch für jeden Standort einen Namen angeben, z. B. „DMZ“ oder „Gastnetzwerk“, und in Geräten und Datensätzen nach diesem Namen filtern.

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 **Netzwerk-Lokalitäten**.
3. klicken **Netzwerkstandort hinzufügen**.
4. Geben Sie im Feld Network Locality Name einen eindeutigen Namen ein.
5. Wählen Sie im Abschnitt Netzwerkortyp die Option Intern oder Extern aus, je nachdem, welche Klassifizierung Sie auf die IP-Adressen und CIDR-Blöcke anwenden möchten.
6. Geben Sie im 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.
7. Optional: In der Beschreibung Feld, geben Sie Informationen zur Netzwerklokalität ein.
8. klicken **Speichern**.
9. Um weitere Einträge hinzuzufügen, klicken Sie auf **Netzwerkstandort hinzufügen**.

Nächste Schritte

- Filtern Sie Geräte, indem Sie im Trifield-Filter Intern oder Extern als Netzwerk-Lokalitätstyp auswählen.
- Filtern Sie Geräte, indem Sie den Netzwerk-Lokalitätsnamen im Dreifeld-Filter angeben.
- Suchen Sie eine Metrik nach Client, Server oder IP-Adresse und wählen Sie im Dreifeld-Filter Intern oder Extern als Netzwerklokalität aus.
- Filtern Sie Datensätze, indem Sie einen der folgenden Filter angeben:
 - Name der Netzwerklokalität
 - Lokalitätsname des Client-Netzwerks

- Lokalitätsname des Servernetzwerks
- Lokalitätsname des Absendernetzwerks
- Name der Netzwerklokalität des Empfängers

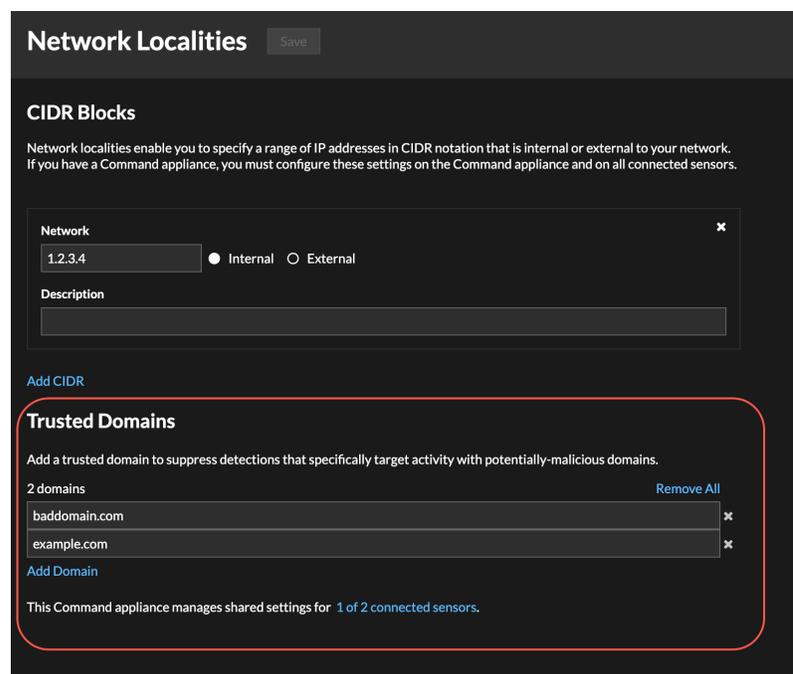
Eine vertrauenswürdige Domain hinzufügen

Bestimmte Erkennungen werden generiert, wenn ein Gerät eine Verbindung zu einer externen Domain herstellt. Wenn Sie wissen, dass eine Domain legitim ist, fügen Sie sie der Liste der vertrauenswürdigen Domains hinzu. Künftige Erkennungen, die auf bösartige Domainaktivitäten abzielen, werden für diese Domain unterdrückt.

Für Erkennungen, denen eine Domäne zugeordnet ist, können Sie auch [fügen Sie eine vertrauenswürdige Domain direkt von einer Erkennungskarte hinzu](#).



Hinweis Wenn Ihr ExtraHop-System über eine Konsole verfügt und dieses System für die Verwaltung von Tuning-Parametern konfiguriert ist, gelten diese vertrauenswürdigen Domänen für alle angeschlossenen Sensoren.



Network Localities Save

CIDR Blocks

Network localities enable you to specify a range of IP addresses in CIDR notation that is internal or external to your network. If you have a Command appliance, you must configure these settings on the Command appliance and on all connected sensors.

Network ×

1.2.3.4 Internal External

Description

[Add CIDR](#)

Trusted Domains

Add a trusted domain to suppress detections that specifically target activity with potentially-malicious domains.

2 domains Remove All

baddomain.com ×

example.com ×

[Add Domain](#)

This Command appliance manages shared settings for 1 of 2 connected sensors.

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 **Netzwerk-Landschaften**.
3. Unter Vertrauenswürdige Domains, klicken **Domain hinzufügen**.
4. Geben Sie einen vertrauenswürdigen Domänenname ein.
Der Domänenname muss exakt mit der Domain übereinstimmen, die Sie unterdrücken möchten. Wildcards und Regex werden nicht unterstützt. Um mehr als einen vertrauenswürdigen Domänenname hinzuzufügen, klicken Sie auf **Domain hinzufügen**. Geben Sie pro Feld einen einzelnen Domänenname ein.
5. klicken **Speichern**.

Prioritäten der Analyse

Das ExtraHop-System analysiert den Verkehr und sammelt Daten von allen erkannten Geräten auf einem einzigen Sensor. Jedes entdeckte Gerät erhält eine Analyseebene, die festlegt, welche Daten und Metriken für ein Gerät gesammelt werden. Analyseprioritäten bestimmen, welche Analysestufe ein Gerät erhält.

 **Wichtig:** Analyseprioritäten können sein [zentral verwaltet](#) von einer Konsole aus.

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 Gerätelistsenseite 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • L2-L3-Metriken • Karten mit Aktivitäten 	L2-Elterngeräte erhalten automatisch L2 Parent Analysis, mit Ausnahme von Gateways und Routern.
Strömungsanalyse	<ul style="list-style-type: none"> • 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 von Analyseprioritäten

Standardmäßig verwaltet jeder Paketsensor seine eigenen Analyseprioritäten, die bestimmen, welche Geräte empfangen Erweiterte Analyse oder Standardanalyse. Wenn Ihr Sensor mit einer Konsole verbunden ist, können Sie die Prioritätsverwaltung auf diese Konsole übertragen, um eine zentrale Ansicht dieser Einstellungen zu erhalten.

Hier sind einige wichtige Überlegungen zur Übertragung des Managements:

- Sie benötigen volle Schreibberechtigungen, um Analyseprioritäten bearbeiten zu können.
- Nach der Übertragung des Managements auf ein Konsole, alle weiteren Änderungen, die Sie an einzelnen Sensoren vornehmen, sind inaktiv. Sehen Sie, welche anderen [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 auf eine übertragene 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 dann klicken **Prioritäten der Analyse**.
3. Klicken Sie oben auf der Seite auf Konsole Dropdownliste und wählen Sie die Konsole aus, auf die Sie die Verwaltung übertragen möchten.
4. klicken **Übertragung**.



Hinweis Analyseunterbrechungen zu vermeiden, können Sie einen Entwurf der Einstellungen für die Analyseprioritäten für jeden Sensor speichern, bevor Sie die Verwaltung auf eine Konsole übertragen.

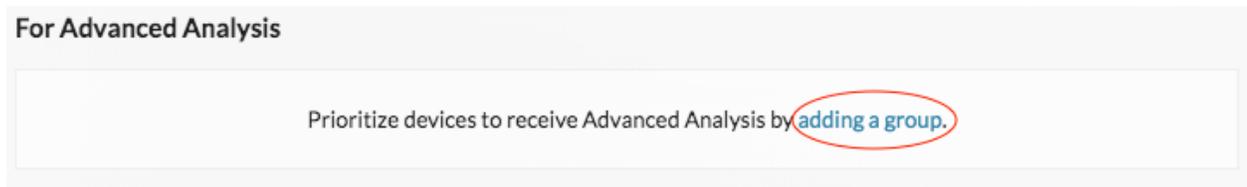
Priorisieren Sie Gruppen für Erweiterte Analyse

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.

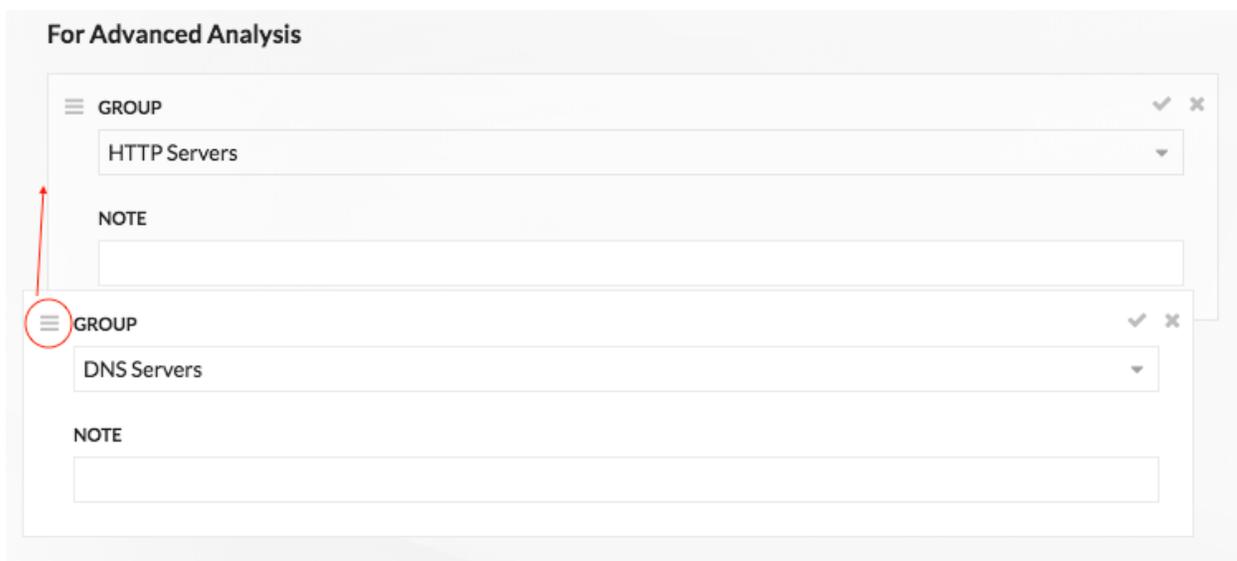
 **Hinweis** Wenn Ihr System Leistungsprobleme hat, klicken Sie auf **Aus**. Nur Geräte, die sich in priorisierten Gruppen oder auf der Beobachtungsliste befinden, erhalten die erweiterte Analyse.

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

For Advanced Analysis



dargestellt.

Priorisieren Sie Gruppen für die Standardanalyse

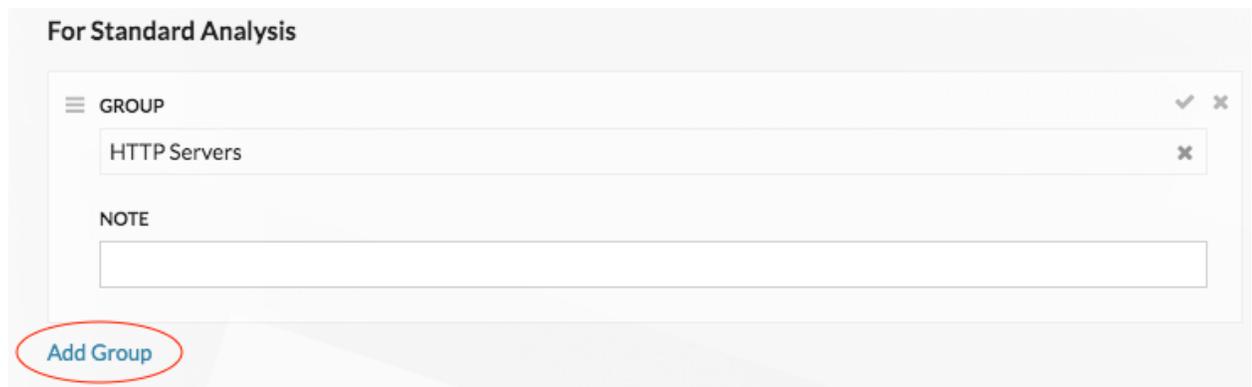
Sie können Gerätegruppen für die Standardanalyse auf der Grundlage ihrer Bedeutung für Ihr Netzwerk angeben. Die Gruppen werden in einer geordneten Liste geordnet.

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.

For Standard Analysis

Prioritize devices to receive Standard Analysis by [adding a group.](#)



- 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**.

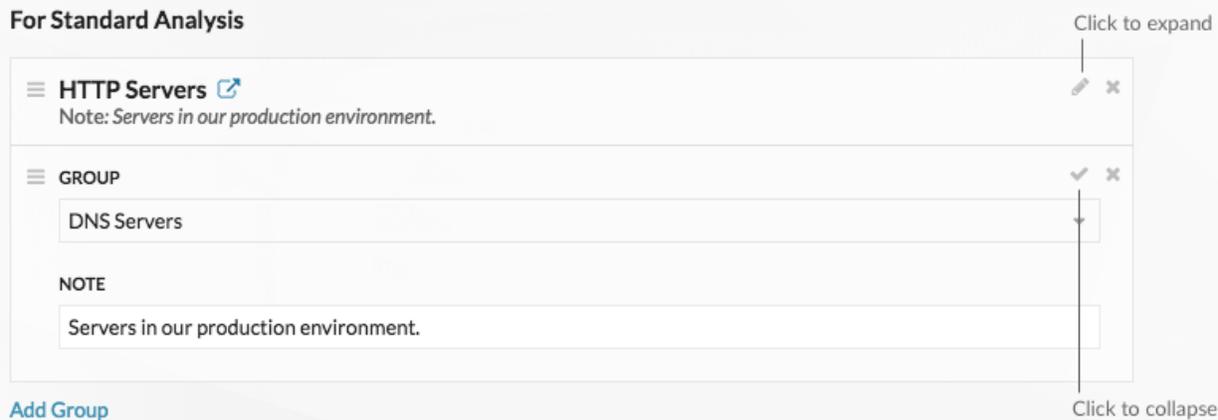
Nächste Schritte

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.

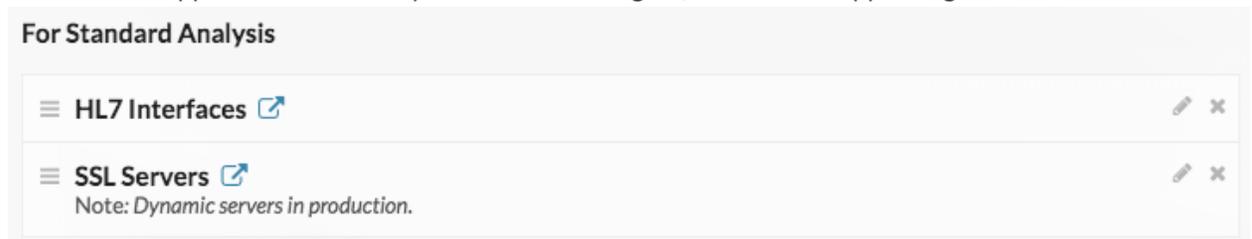


- Klicken Sie auf den Scheck ✓ Symbol, um die Gruppe zu reduzieren. Klicke auf den Stift ✎ Symbol, um die Gruppe erneut zu erweitern, wie in der folgenden Abbildung

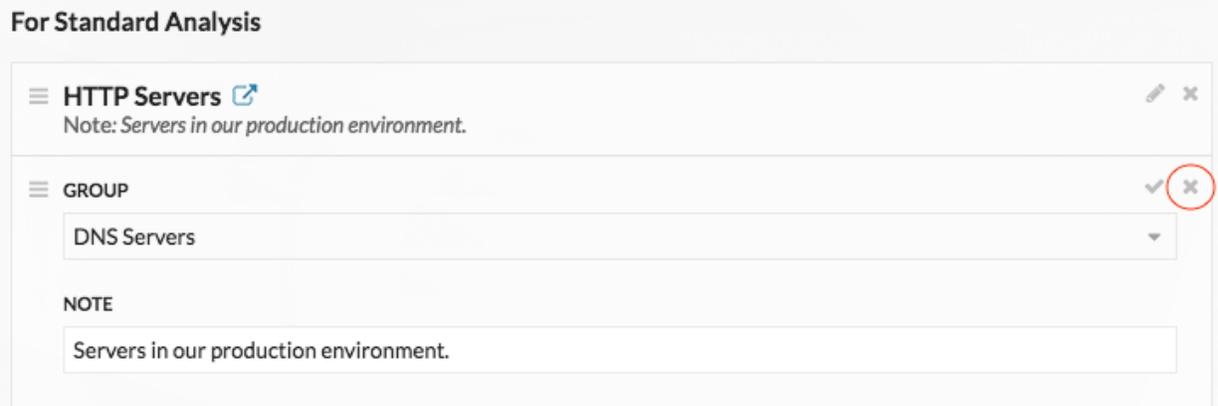


dargestellt. [Add Group](#)

- 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.

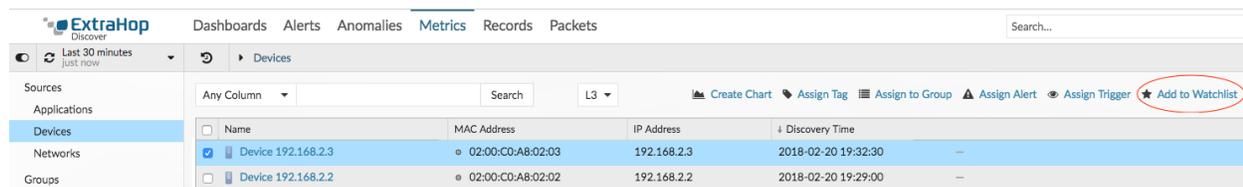
Ein Gerät zur Beobachtungsliste hinzufügen

Fügen Sie Geräte zur Beobachtungsliste hinzu, um Erweiterte Analyse sicherzustellen. Sie können der Überwachungsliste ein benutzerdefiniertes Gerät hinzufügen, aber Sie können der Beobachtungsliste kein übergeordnetes L2-Gerät hinzufügen, es sei denn, es handelt sich bei dem Gerät um ein Gateway oder einen Router, und Sie können kein Gerät in Flow Analysis hinzufügen. Geräte bleiben auf der Beobachtungsliste, unabhängig davon, ob sie inaktiv oder aktiv sind, aber ein Gerät muss aktiv sein, damit das ExtraHop-System Erweiterte Analyse Analysis-Metriken erfassen kann.



Hinweis: Statt mehrere Geräte zur Beobachtungsliste hinzuzufügen, [eine Gerätegruppe erstellen](#) und dann [priorisieren Sie diese Gruppe für Erweiterte Analyse](#). Oder fügen Sie über die Gerätelistsenseite mehrere Geräte zur Beobachtungsliste hinzu. Klicken Sie auf das Kästchen

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 **Vermögenswerte** oben auf der Seite und dann klicken **Geräte** im linken Bereich.
3. Suchen Sie nach dem gewünschten Gerät und klicken Sie dann auf den Gerätenamen. Die Seite „Geräteübersicht“ wird angezeigt, auf der der Datenverkehr und die Protokollmetriken für das Gerät angezeigt werden.
4. klicken **Eigenschaften bearbeiten**.

Groups [View Groups](#)

First Seen Dec 03 09:49 *8 days ago*

This device is in Advanced Analysis.
The L2 parent for this device is [App-14D6B4](#) (F0:18:98:14:D6:B4).

[Edit Properties](#) [Edit Assignments](#)

5. klicken **Dieses Gerät zur Beobachtungsliste hinzufügen**.
6. klicken **Erledigt**.

Ihr Gerät befindet sich 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 mit Aktivitäten

Eine Aktivitätsdiagramm ist eine dynamische visuelle Darstellung der L4-L7-Protokollaktivität zwischen Geräten in Ihrem Netzwerk. Sie können sich ein 2D- oder 3D-Layout der Geräteverbindungen in Echtzeit ansehen, um mehr über den Verkehrsfluss und die Beziehungen zwischen Geräten zu erfahren.

Activity Maps können Ihnen 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 Hauptursache für eine langsame Anwendung

Anwendungen hängen häufig von mehreren Dienstebenen innerhalb eines Netzwerk ab. Mithilfe einer Activity Map können Sie die Lieferkette des Datenverkehrs zu Ihrem langsamen Anwendungsserver identifizieren. Klicken Sie auf ein Gerät, um verwandte Kennzahlen 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 mit einem verdächtigen Gerät verbundenen Ost-West-Verkehr in Echtzeit verfolgt. Im Rahmen einer täglichen Sicherheitsüberwachungsstrategie können Sie eine Aktivitätsdiagramm erstellen, um sicherzustellen, dass Geräte keine unerwarteten Verbindungen mit anderen Geräten herstellen.

Hier sind einige wichtige Überlegungen zu Activity Maps:

- 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 Map ohne Daten angezeigt. Ändern Sie das Zeitintervall oder Ihre Herkunftsauswahl und versuchen Sie es erneut.
- Sie können eine Aktivitätsdiagramm aus einem erstellen Konsole um die Geräteverbindungen all Ihrer Sensoren zu sehen.
- Du kannst [Speichern und Teilen einer Aktivitätsdiagramm](#), gewährt anderen Systembenutzern oder Gruppen Ansichts- oder Bearbeitungszugriff. Du kannst auch [eine gespeicherte Aktivitätsdiagramm laden](#) um Karteneigenschaften zu ändern.

Weitere Informationen zu Aktivitätskarten finden Sie in der [Häufig gestellte Fragen zu Activity Maps](#) .

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

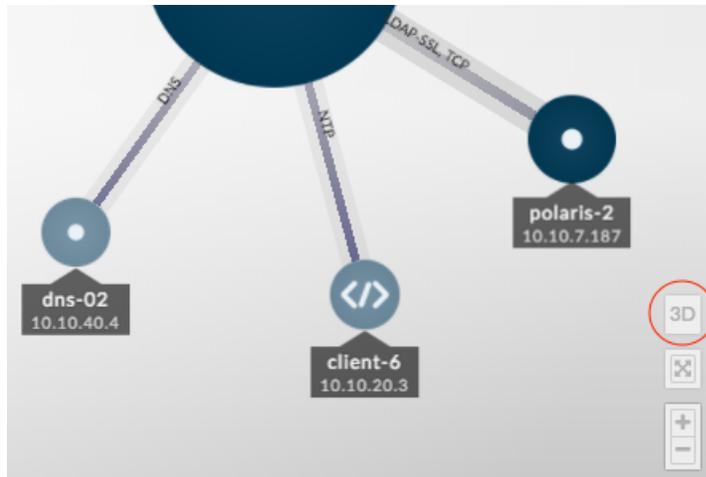
Geräte werden durch Kreise und Verbindungen durch Linien dargestellt.

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.

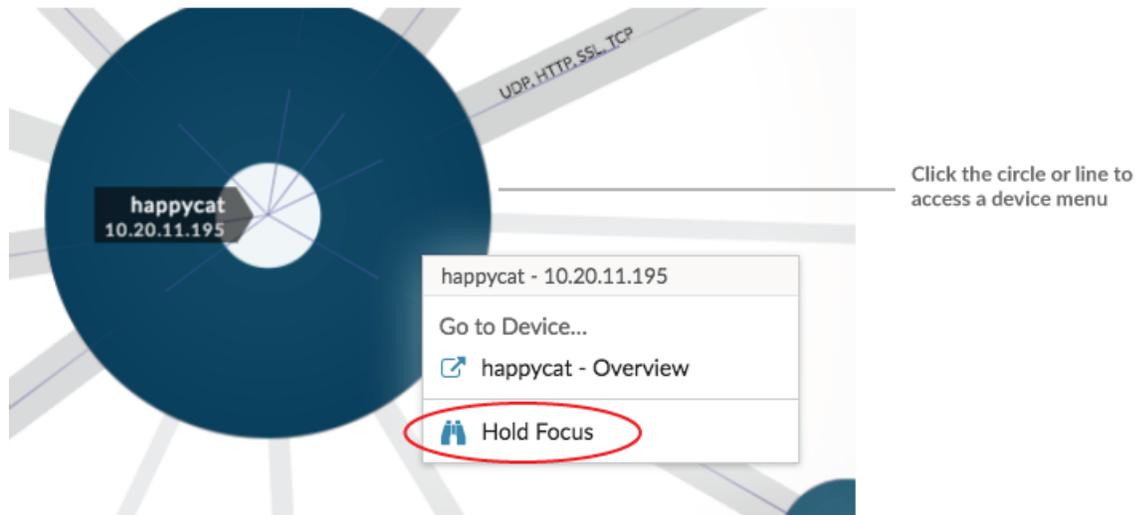


Neu positionieren, drehen und zoomen

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.

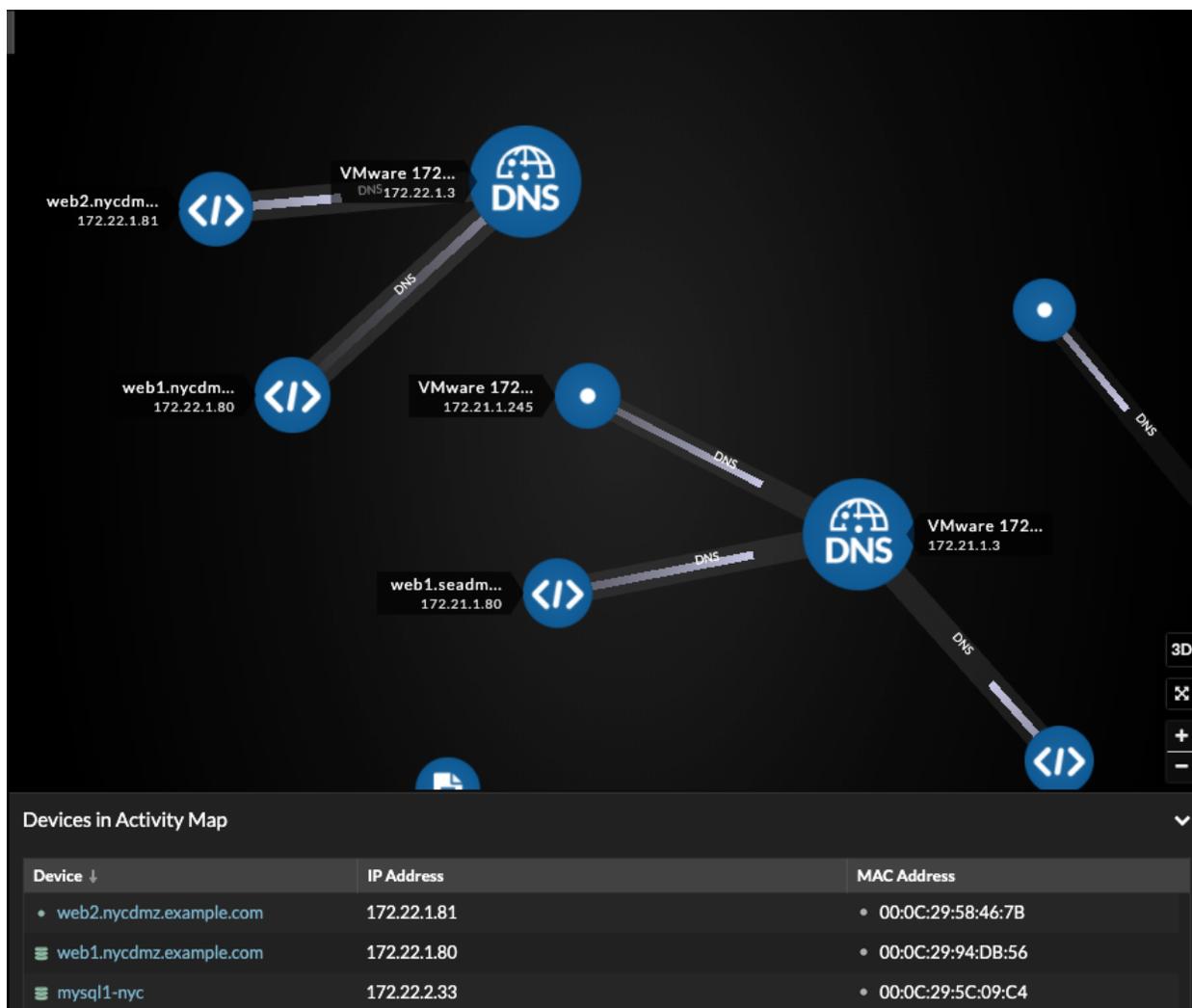
Fokus behalten

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.

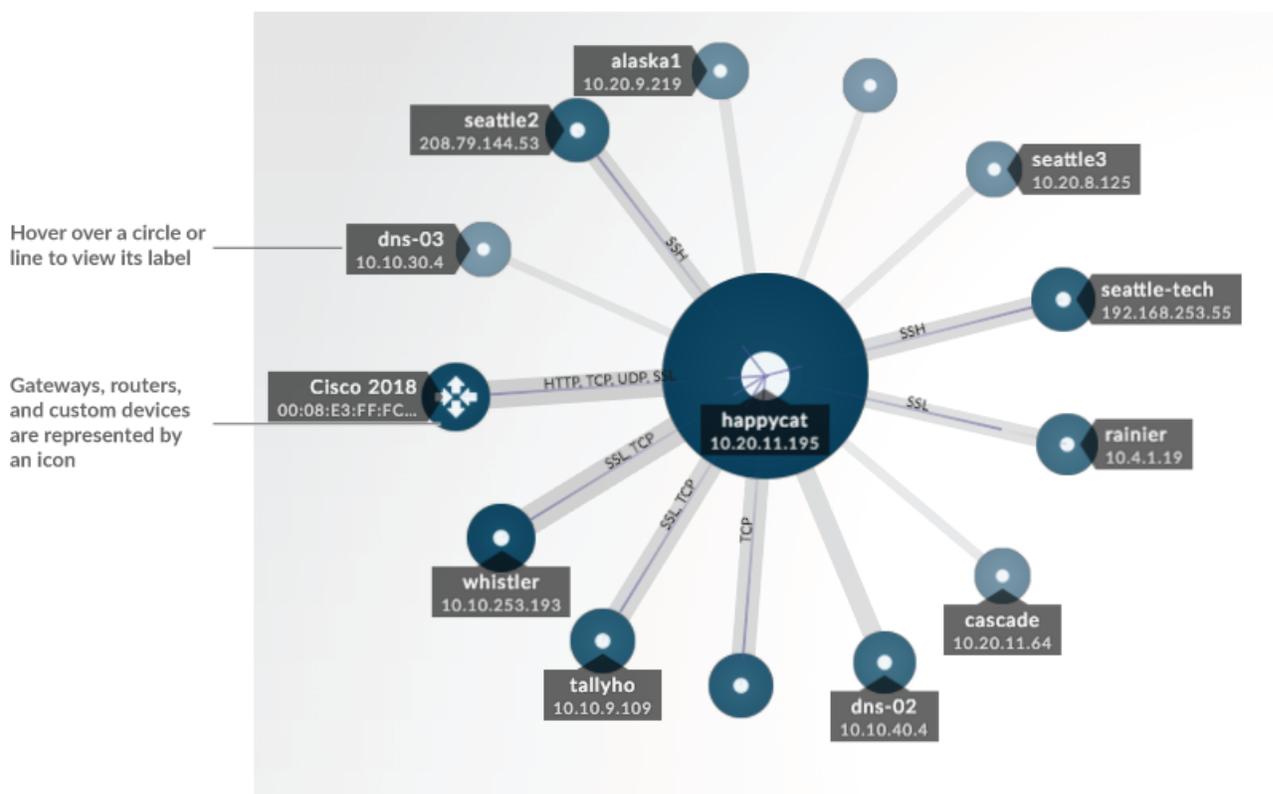


Beschriftungen und Icons

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.

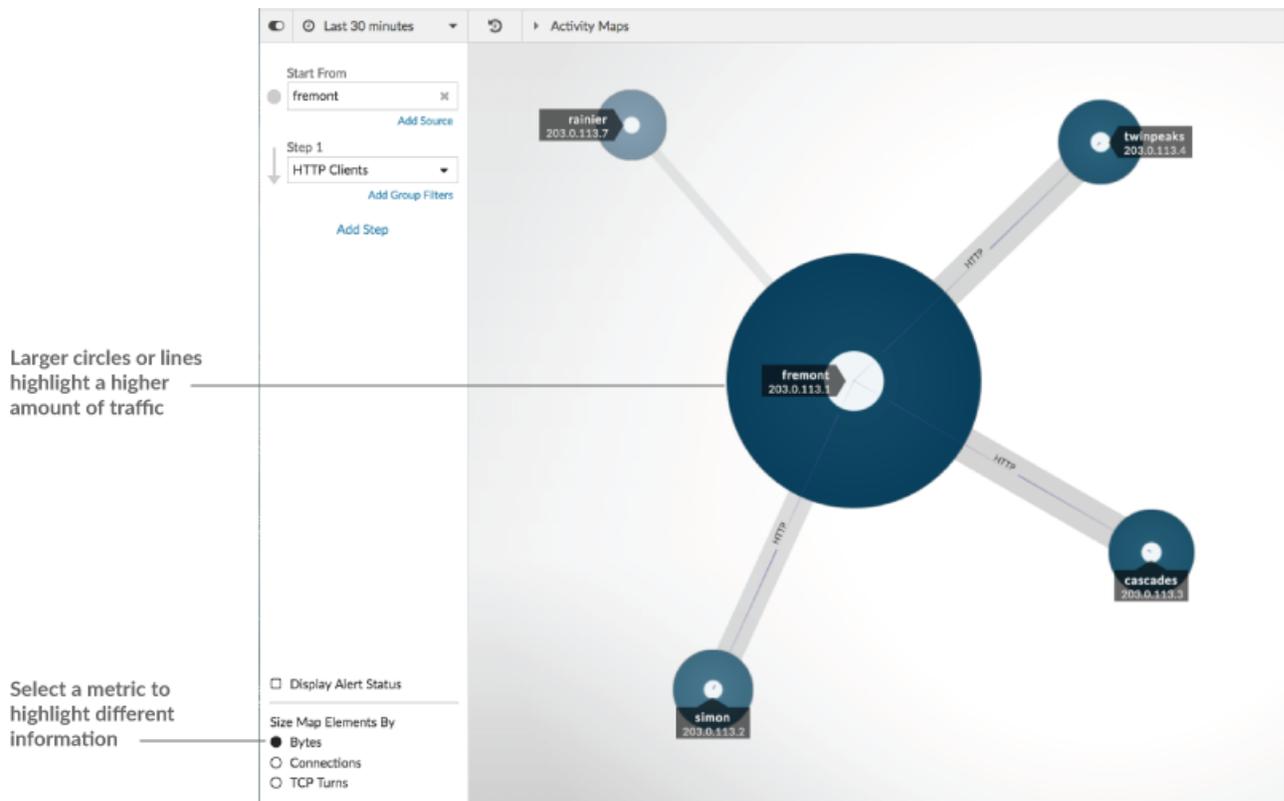
Um die Anzeige von Informationen zu optimieren, wird nicht jedes Etikett angezeigt. Bewegen Sie den Mauszeiger über einen Kreis oder eine Linie, um deren Bezeichnung anzuzeigen, wie in der folgenden Abbildung dargestellt.



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:

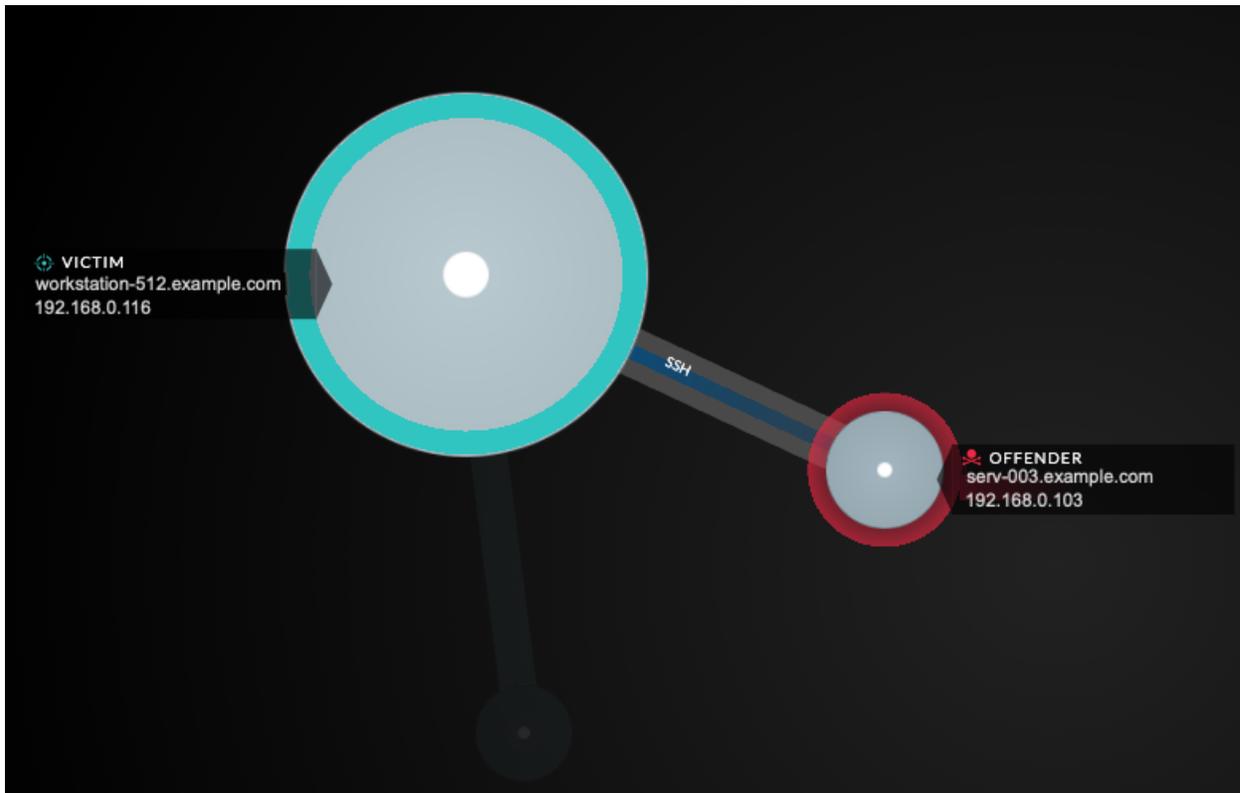
- **Byte:** Sehen Sie sich alle Geräte an, die während des Zeitintervalls Daten senden oder empfangen.
- **Verbindungen:** Es werden nur die Geräte angezeigt, die während des Zeitintervalls mindestens einmal eine neue Verbindung hergestellt haben.
- **TCP-Kurven:** Es werden nur die Geräte angezeigt, 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](#).

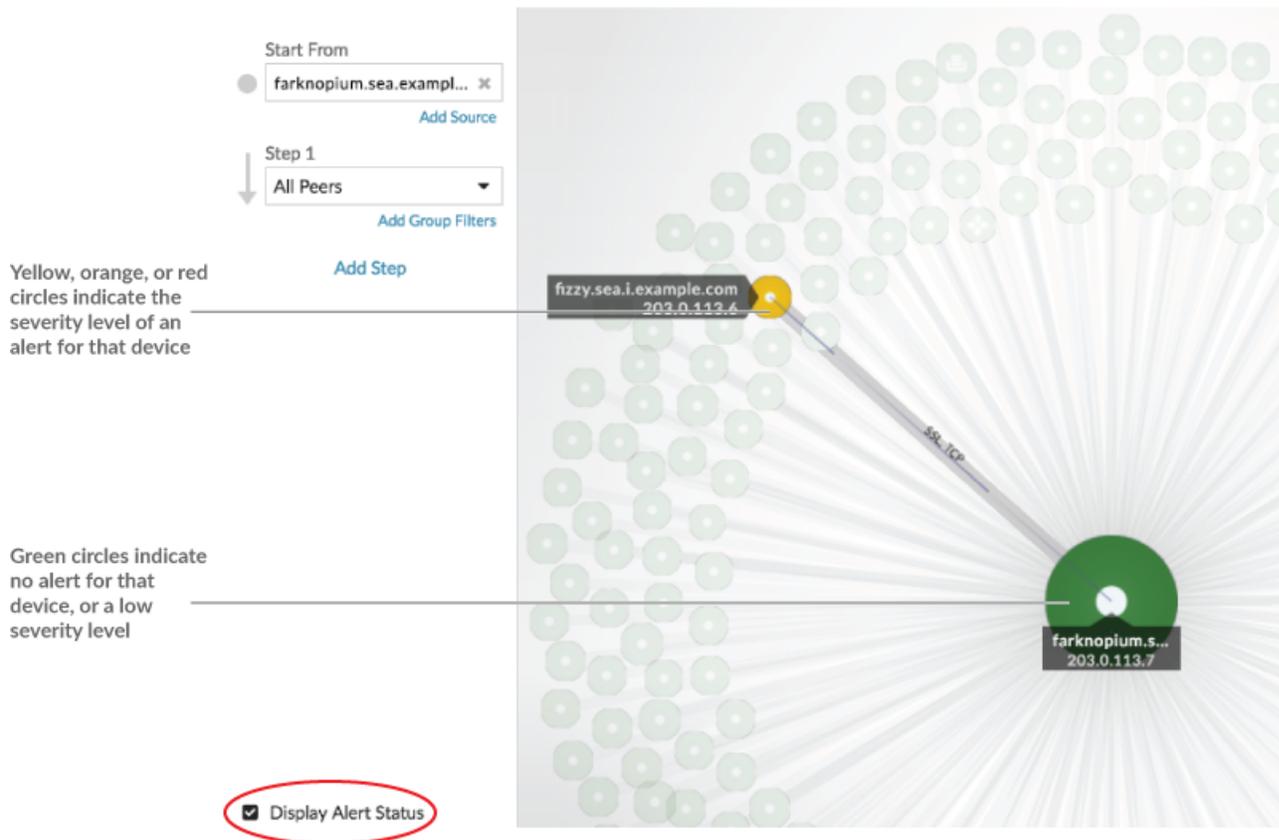
Klicken Sie auf einen Kreis mit einer Erkennungsmarkierung, um zugehörige Erkennungen anzuzeigen und zu ihnen zu navigieren, oder [Seite „Geräteübersicht“](#).

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)

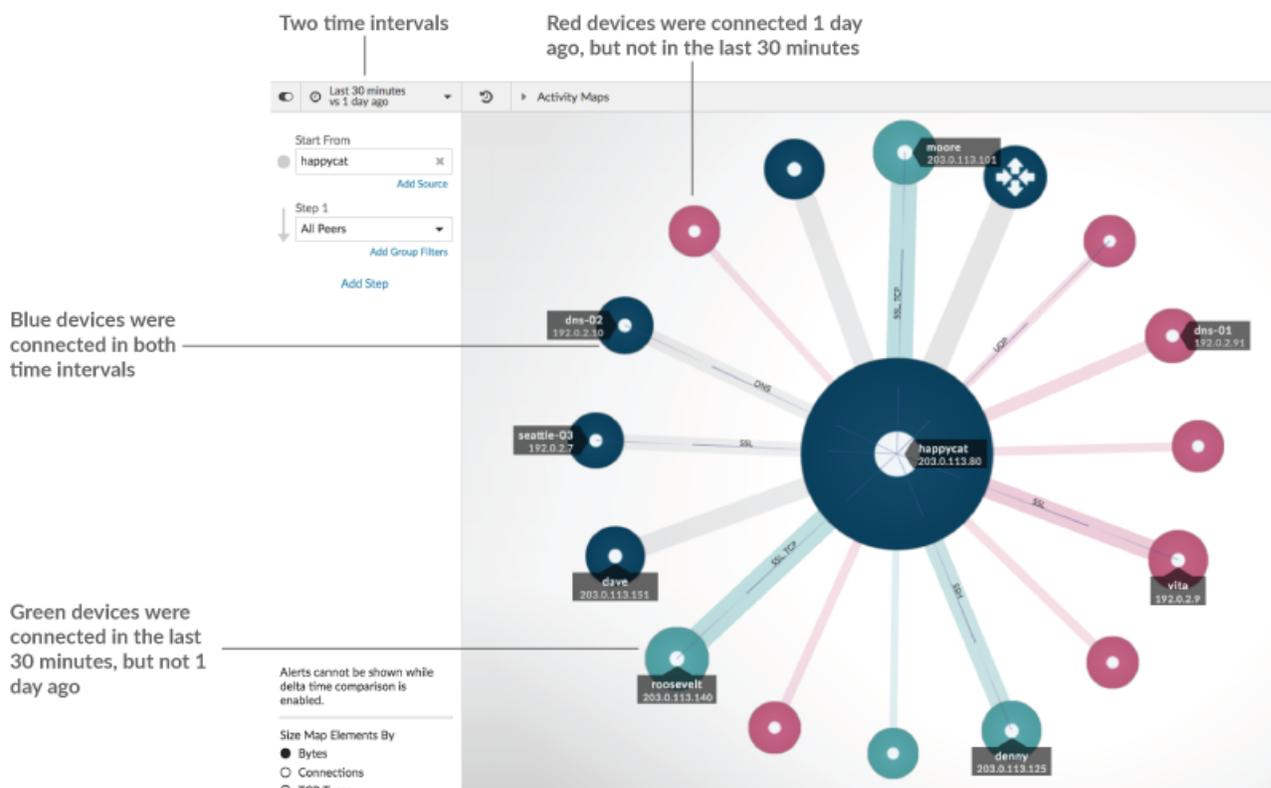
Um den Schweregrad einer Alarm für ein Gerät in Ihrer Karte anzuzeigen, wählen Sie **Warnstatus anzeigen** in der unteren linken Ecke oder auf der Seite, wie in der folgenden Abbildung dargestellt. Die Kreisfarbe entspricht dann dem schwerwiegendsten Status für alle Alarme, die einem Gerät während des 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

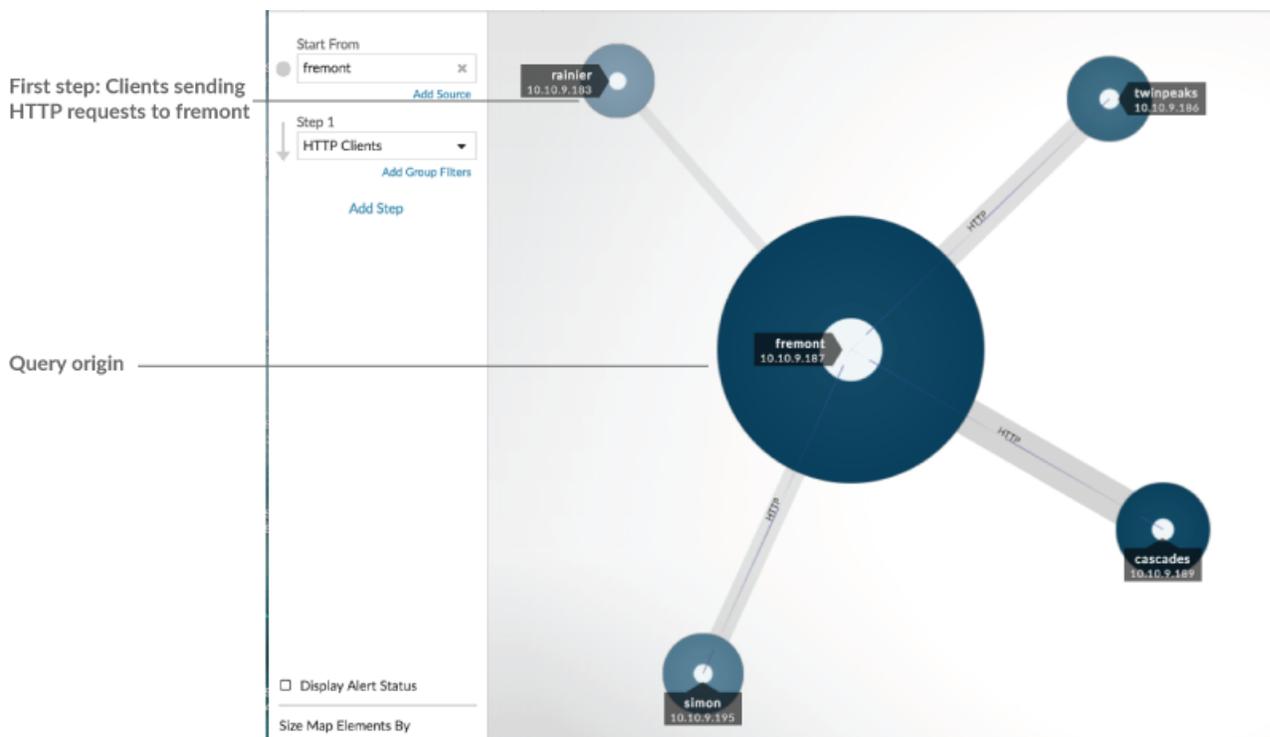
Wenn du [Vergleiche zwei Zeitintervalle, um Metrik Deltas zu finden](#), anhand verschiedener Farben in der Karte können Sie feststellen, wann Geräteverbindungen hergestellt wurden oder wann sich die Protokollaktivität für ein Gerät geändert hat. Zum Beispiel nach dem Erstellen eines Vergleichs zwischen **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.



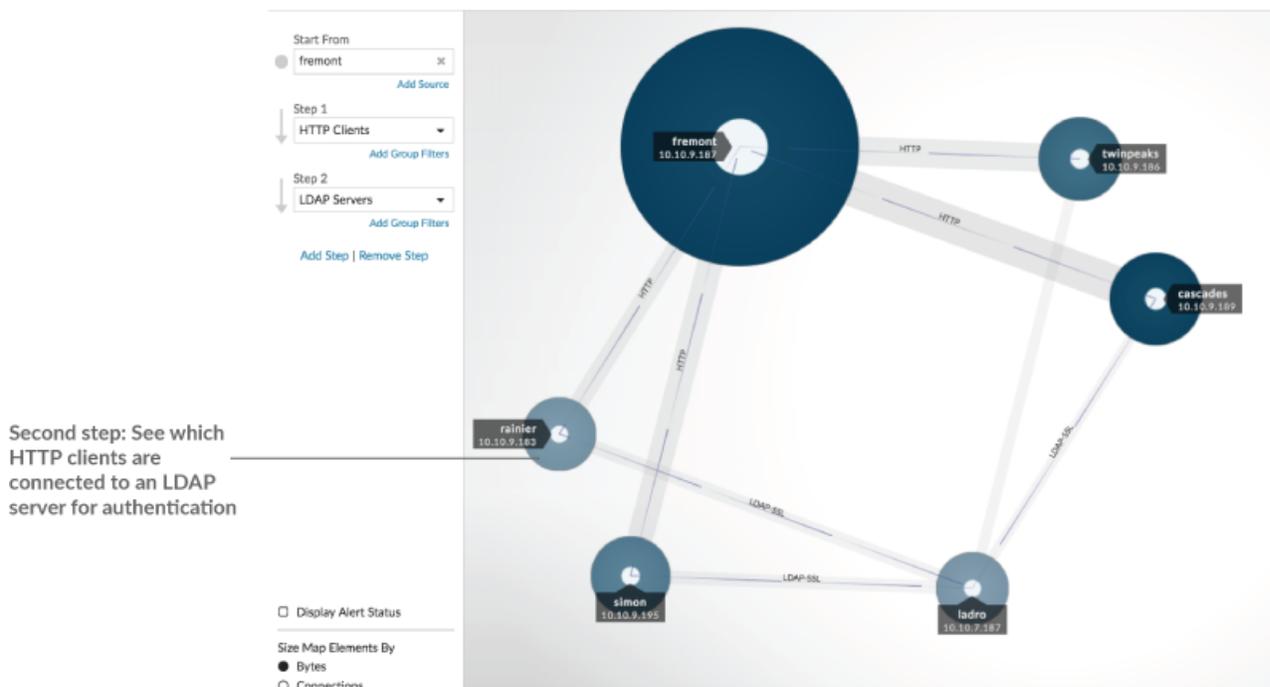
Hinweis Wenn alle Geräte eine einzige Farbe haben, z. B. grün, bedeutet dies, dass die Abfrage im früheren Zeitintervall keine Ergebnisse erbracht hat. Beispielsweise hatte das Ursprungsgerät im früheren Zeitintervall keine Protokollaktivität.

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.

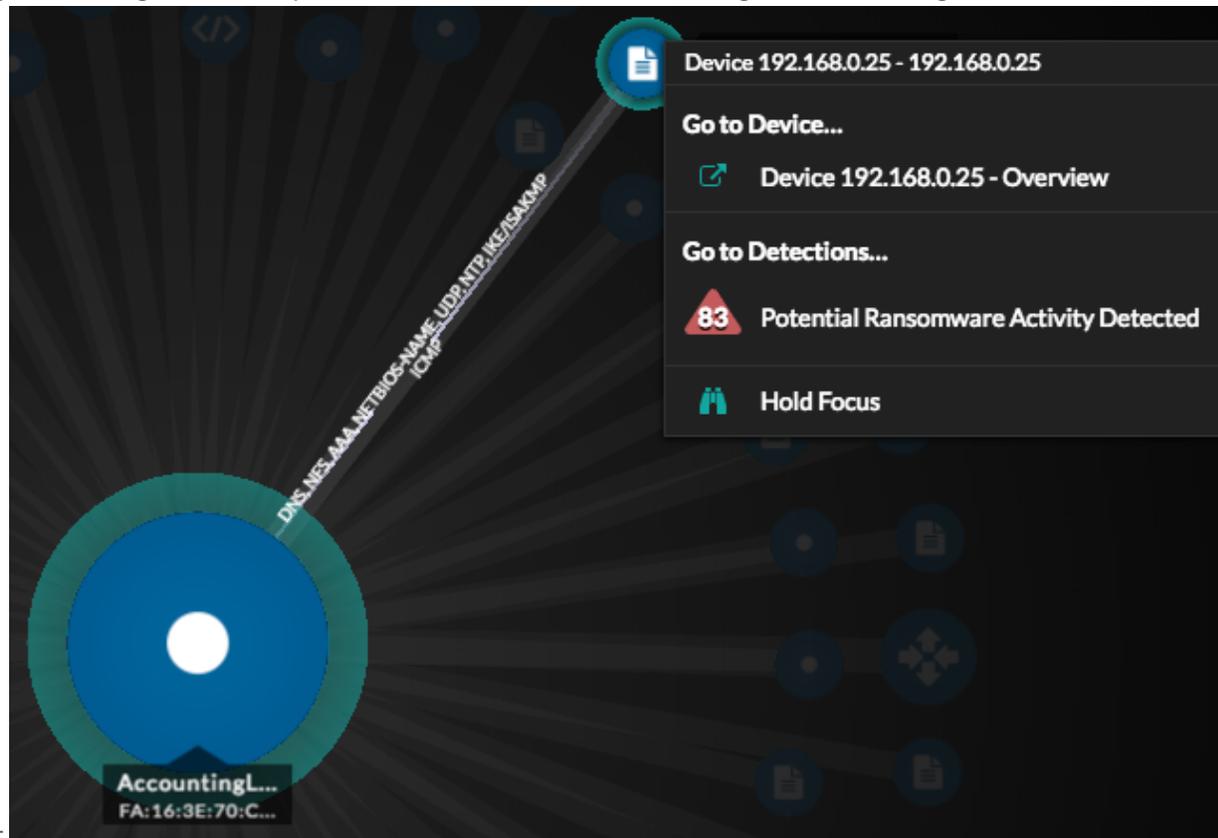


Wählen Sie den Gerätenamen aus dem Menü aus, um die Seite Geräteübersicht aufzurufen. Klicken Sie im linken Bereich auf einen Protokollnamen, um die Protokollseite aufzurufen, die eine Zusammenfassung wichtiger Protokollmetriken enthält, die beobachtet wurden und mit dem Gerät verknüpft wurden. Auf einer 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:

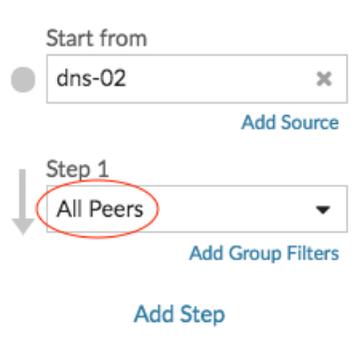
Option	Description
Für ein Gerät	klicken Geräte im linken Bereich und klicken Sie dann auf einen einzelnen Gerätenamen.
Für eine Gerätegruppe	klicken Gerätegruppen im linken Bereich und klicken Sie dann auf einen Gerätegruppennamen.
Für eine Gerätegruppe nach Protokollaktivität	klicken Aktivität im linken 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:

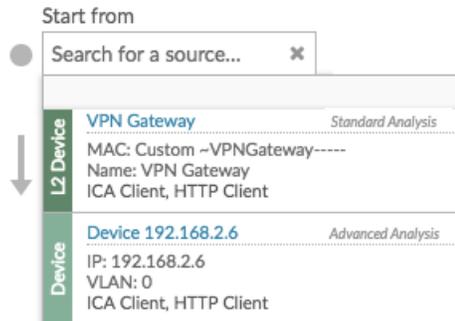
Option	Description
Für ein Gerät	klicken Peer-Geräte , befindet sich oben auf der Seite.
Für eine Gerätegruppe	klicken Karte der Aktivitäten , befindet sich in der Nähe der oberen rechten Ecke der Seite.

 **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.

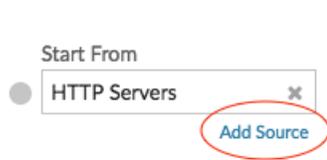
5. Filtern Sie in der Aktivitätsdiagramm Verbindungen nach Protokollaktivität, indem Sie die folgenden Schritte ausführen:
 - a) Klicken Sie auf die Drop-down-Liste in der Schritt 1 Abschnitt des linken Bereichs, wie in der folgenden Abbildung dargestellt.



- 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.

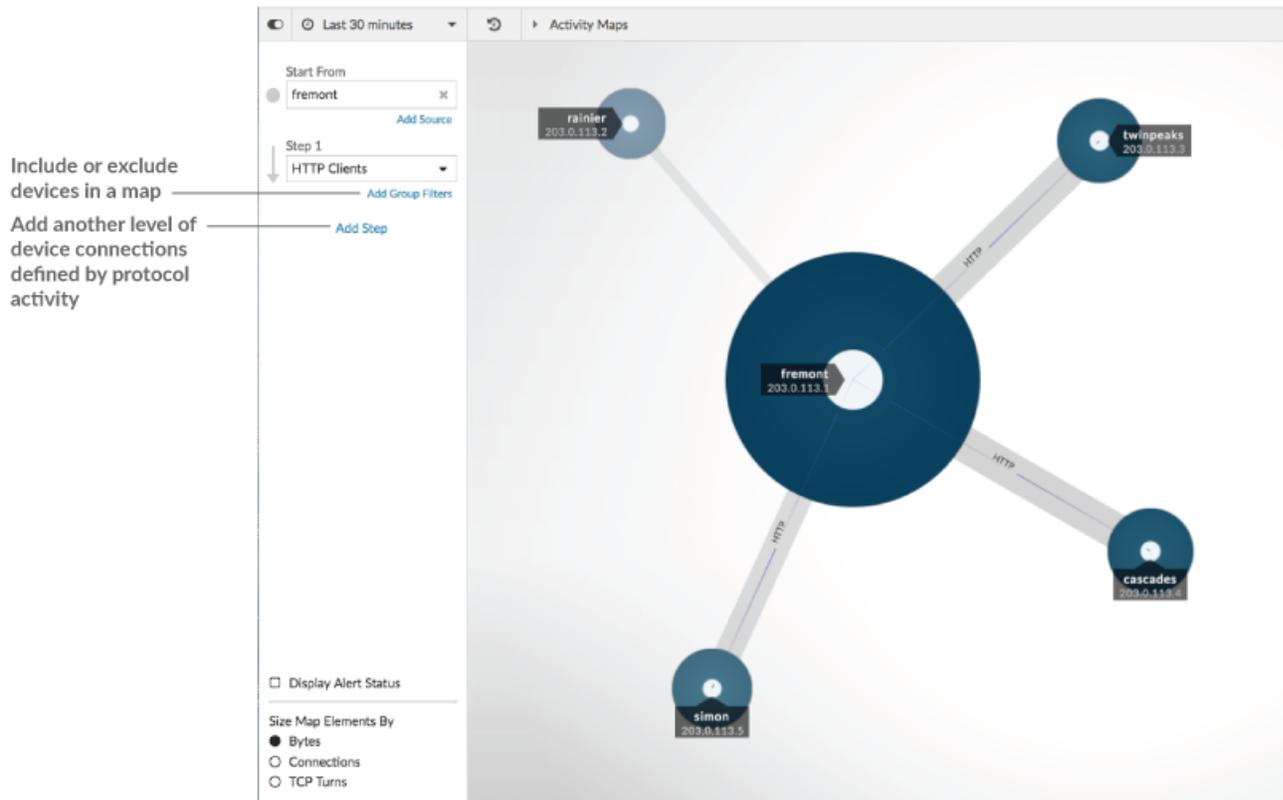


- b) Suchen Sie nach einem anderen Gerät oder einer anderen Gruppe und wählen Sie sie aus, um den Kartenursprung für die angezeigte Karte dynamisch zu aktualisieren.
- 7. Optional: Erstellen Sie eine Ad-hoc-Gruppe von Quellen, um schnell den Datenverkehr zu untersuchen, der von mehreren Geräten in derselben Map stammt. klicken **Quelle hinzufügen**.



Fügen Sie Verbindungen hinzu und filtern Sie Geräte zu Ihrer Karte

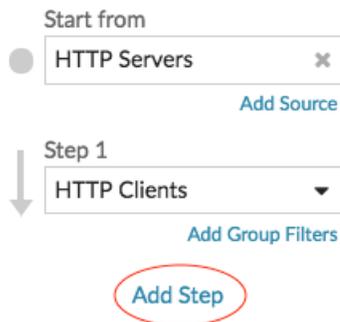
Um den Pfad des Datenverkehrs von den Ursprungsgeräten zu den nachgeschalteten Geräten besser zu verstehen, können Sie Ihrer Karte weitere Schritte hinzufügen. Sie können auch Filter erstellen, um Geräte in die Karte ein- oder auszuschließen. Die folgende Abbildung zeigt Ihnen, wie Sie Schritte hinzufügen und Filter erstellen.



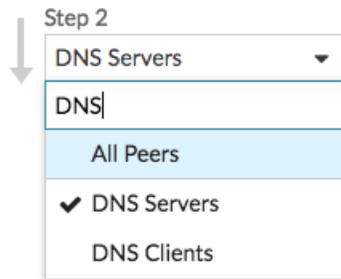
Fügen Sie eine weitere Ebene von Geräteverbindungen hinzu

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.

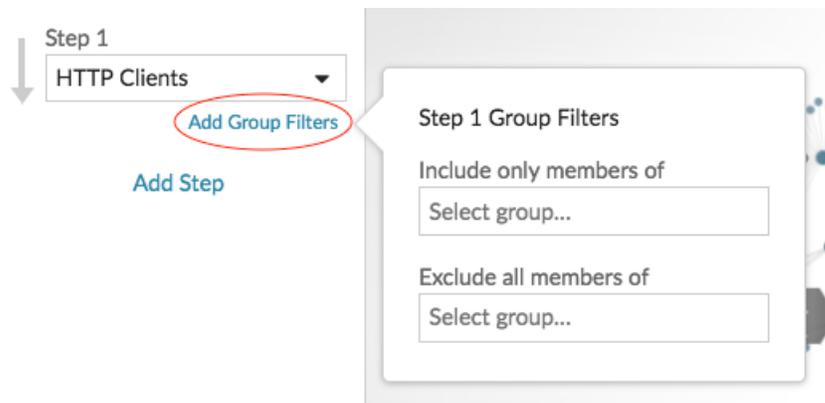


3. Klicken Sie auf eine beliebige Stelle außerhalb der Dropdownliste.

Geräte einbeziehen oder ausschließen

Sie können Geräte innerhalb eines Schritts nach ihren Filtern Gerätegruppe Mitgliedschaft.

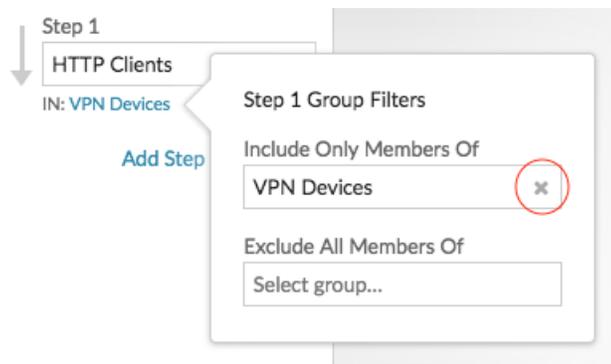
1. klicken **Gruppenfilter hinzufügen**.



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 klicken.  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 ungewöhnliches Verhalten und potenzielle Risiken für die Sicherheit und Leistung Ihres Netzwerk zu identifizieren.

Bevor Sie beginnen

Benutzern muss eine Genehmigung erteilt werden [Privilegien](#) um Erkennungen einzusehen.

Wenn ein ungewöhnliches Verhalten festgestellt wird, generiert das ExtraHop-System eine Erkennung und zeigt die verfügbaren Daten und Optionen an. Steuerelemente auf der Seite „Erkennungen“: Oberflächendetektionen, die [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 Sie auf folgende Weise bei der Wartung Ihres Netzwerk unterstützen:

- Sammeln Sie hochwertige, verwertbare Daten, um die Hauptursachen für Netzwerkprobleme zu ermitteln.
- Finden Sie unbekannte Probleme mit der 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.
- Kennzeichnet verdächtige IP-Adressen, Hostnamen und URIs, die durch Threat Intelligence identifiziert wurden.
- Heben Sie bewährte Methoden zur Stärkung der Sicherheit hervor.

Erfahre mehr über [Optimierung von Erkennungen](#).

-  **Wichtig:** Erkennungen können Sie zwar über Sicherheitsrisiken und Leistungsprobleme informieren, ersetzen jedoch 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.

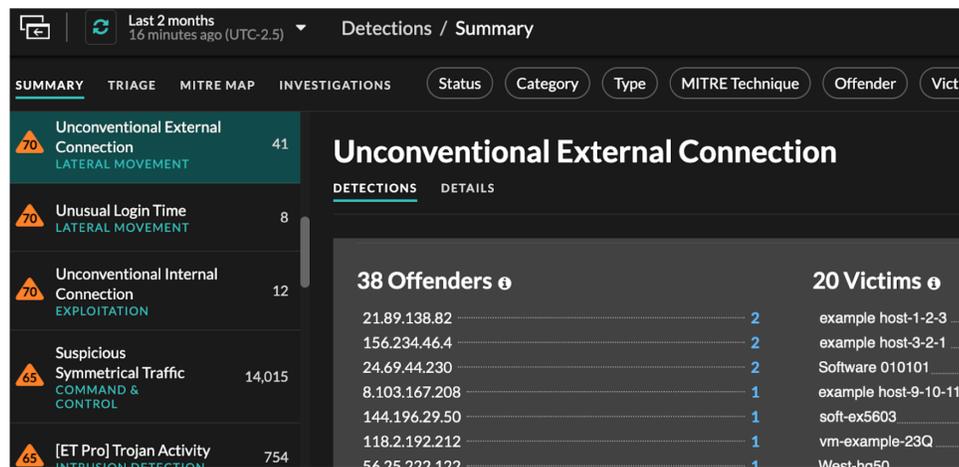
Erkennungen anzeigen

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

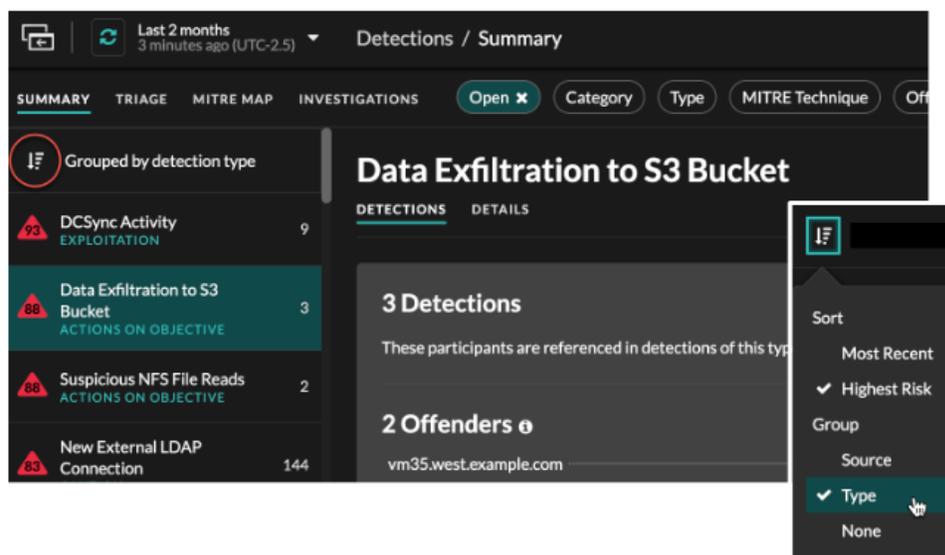
Sie können Erkennungen entweder nach der höchsten Risikoscore oder nach dem jüngsten Ereignis sortieren.

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.

The screenshot displays the 'Detections / Summary' page in the ExtraHop interface. On the left, a list of participants is shown, grouped by source device. The 'PCUser10' entry is highlighted, showing 7 detections. Annotations on the left side of the image point to the participant name, the number of detections, and the role (Offender/Victim). The main area shows a detailed view for 'PCUser10' with a 'DETECTIONS' tab selected. A specific detection is highlighted: 'SSL/TLS Connection to a Suspicious Host' with a risk level of 60 (CAUTION) and a timestamp of 'Aug 28 13:16'. Below this, a list of 'Suspicious hostname linked to this detection:' is shown, including 'hostname.com'. A 'PARTICIPANTS' section lists 'PCUser10' as an 'OFFENDER' with a link to 'west.example.com'. On the right, a 'DETECTIONS BY TYPE' panel is shown, listing various detection types such as '[ET Pro] Trojan Activity', '[ET Pro] Bad Unknown Traffic', 'Weak Cipher Suite', '[ET Pro] Attempted Admin', 'SSL/TLS Connection to a Suspicious Host', and 'DNS Request to a Suspicious Host'. Annotations on the right side of the image point to the 'DETAILS' link for the detection type and the list of detection types.

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) Die Triage-Ansicht zeigt Erkennungen, die ExtraHop auf der Grundlage einer kontextuellen Analyse von Faktoren in Ihrer Umgebung für die Triage empfiehlt.

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 stellt Authentifizierungs- oder grundlegende Dienste bereit, oder ein Asset, das **manuell als hoher Wert identifiziert**.

Es handelt sich um einen Haupttäter

Das Gerät oder die IP-Adresse war an zahlreichen Erkennungen und einer Vielzahl von Erkennungstypen beteiligt.

Beinhaltet einen seltenen Erkennungstyp

Der Erkennungstyp ist in letzter Zeit nicht in Ihrer Umgebung aufgetreten. Ungewöhnliche Erkennungstypen können auf einzigartiges, böses Verhalten hinweisen.

Erkennungen, die für die Triage empfohlen werden, werden in der Zusammenfassungsansicht priorisiert und unabhängig von der Sortierung ganz oben in Ihrer Entdeckungsliste angezeigt.

Du kannst **Erkennungen filtern** um nur Erkennungen anzuzeigen, die für die Triage empfohlen werden, und für die Triage empfohlen als Kriterien für eine **Benachrichtigungsregel**.

Hier sind einige Überlegungen zu den Empfehlungen für die Triage:

- Empfehlungen, die auf hochwertigen Vermögenswerten basieren, sind auf maximal fünf Erkennungen desselben Entdeckungstyps über einen Zeitraum von zwei Wochen beschränkt.
- Zwei Wochen an Sensordaten sind erforderlich, bevor Empfehlungen auf der Grundlage von Faktoren vom Typ „Haupttäter“ oder „Seltenheit“ ausgesprochen werden.

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.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
Drive-by Compromise T1189 215 Detections	Command and Scripting Interpreter T1059 1 Detection	Account Manipulation T1098	Boot or Logon Autostart Execution T1547	BITS Jobs T1197	Brute Force T1110 4 Detections	Account Discovery T1087 7 Detections	Exploitation of Remote Services T1210 3 Detections
Exploit Public-Facing Application T1190	Exploitation for Client Execution T1203	BITS Jobs T1197	Boot or Logon Initialization Scripts T1037	Build Image on Host T1612 7 Detections	Credentials from Password Stores T1555	Cloud Service Discovery T1526 11 Detections	Lateral Tool Transfer T1570
External Remote Services T1133	Inter-Process Communication T1559	Boot or Logon Autostart Execution T1547	Create or Modify System Process T1543	Exploitation for Defense Evasion T1211	Exploitation for Credential Access T1212	Domain Trust Discovery T1482	Remote Services T1021 5 Detections
Hardware Additions T1200	Native API T1106	Boot or Logon Initialization Scripts T1037	Event Triggered Execution T1546	Hijack Execution Flow T1574	Forced Authentication T1187	File and Directory Discovery T1083 3 Detections	Taint Shared Content T1080
Phishing T1566 2234 Detections	Scheduled Task/Job T1053 1847 Detections	Browser Extensions T1176 1 Detection	Exploitation for Privilege Escalation T1068	Impair Defenses T1562	Man-in-the-Middle T1557 3 Detections	Group Policy Discovery T1615	Use Alternate Authentication Material T1550
Supply Chain Compromise		Create Account	Hijack Execution Flow	Indicator Removal on Host T1070			

Tabelle „Untersuchungen“

In der Ansicht Untersuchungen werden alle erstellten Untersuchungen angezeigt.

Klicken Sie auf einen Namen für die Untersuchung, um die Untersuchung zu öffnen. Erfahre mehr über [Ermittlungen](#).

Erkennungen filtern

Sie können die Seite Erkennungen filtern, sodass nur die Erkennungen angezeigt werden, die Ihren angegebenen Kriterien entsprechen. Beispielsweise interessieren Sie sich möglicherweise nur für Exfiltrationserkennungen, die über HTTP erfolgen, oder für Erkennungen, die mit Teilnehmern verknüpft 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** filtern, 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 Operationserkennungen filtern oder eine spezifischere Kategorie auswählen, um Ihre Ansicht der Erkennungsseite weiter zu verfeinern. Wenn Sie auf den Kategoriefilter klicken, werden die meisten Kategorien unter dem **Alle Angriffskategorien** und **Alle Betriebskategorien** Die Optionen sind nach der Anzahl der Entdeckungen in der Kategorie sortiert. Härtungserkennungen werden immer am Ende der Liste angezeigt.

Zu den Erkennungen von Angriffen gehören die folgenden Kategorien, die den Phasen der Angriffskette entsprechen.

Steuerung 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 wertvollen Zielen und Schwächen, die er ausnutzen kann. Diese Erkennungen identifizieren Scans und Aufzählungstechniken.



Bei Erkennungen könnte 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 wurde. Informationen zum Ausblenden von Erkennungen im Zusammenhang mit diesen Geräten finden Sie unter [Erkennungen optimieren](#).

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 Ausbeutungstechniken.

Seitliche Bewegung

Ein Angreifer ist in Ihr Netzwerk eingedrungen und bewegt sich auf der Suche nach höherwertigen Zielen von Gerät zu Gerät. Diese Erkennungen identifizieren ungewöhnliches Geräteverhalten im Zusammenhang mit Datenübertragungen und Verbindungen in Ost-West-Korridoren.

Maßnahmen im Hinblick auf Zielsetzung

Der Angreifer ist kurz davor, sein Ziel zu erreichen, das vom Diebstahl sensibler Daten über die Verschlüsselung von Dateien bis hin zu Lösegeld reichen kann. Diese Erkennungen identifizieren, wenn ein Angreifer kurz davor ist, ein Kampagnenziel zu erreichen.

Vorsicht

Heben Sie Aktivitäten hervor, die keine unmittelbare Bedrohung für den Betrieb darstellen, die aber angegangen werden sollten, um ein gesundes Sicherheitsniveau aufrechtzuerhalten. Diese Erkennungen identifizieren auch Aktivitäten verdächtiger Teilnehmer, die mit Bedrohungsinformationen in Verbindung stehen.

Betrieb Erkennungen umfassen die folgenden Kategorien.

Authentifizierung und Zugriffskontrolle

Heben Sie erfolglose Versuche von Benutzern, Clients und Servern hervor, sich anzumelden oder auf Ressourcen zuzugreifen. Diese Erkennungen identifizieren potenzielle WLAN-Probleme im Zusammenhang mit Authentifizierungs-, 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 von schlechter Qualität für Endbenutzer hervor. Diese Erkennungen identifizieren Anwendungsprobleme, z. B. eine zu hohe 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 Clients daran hindern, eine IP-Adresse vom Server zu erhalten, oder sie 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), Dateiübertragung und E-Mail-Kommunikationsprotokollen hervor. Diese Erkennungen können

auf Dienstverschlechterungen hinweisen, bei denen VoIP-Anrufe fehlgeschlagen sind, und den entsprechenden SIP-Statuscode anzeigen oder darauf hinweisen, dass nicht autorisierte Anrufer versucht haben, mehrere Anruferanfragen zu stellen.

Aufbewahrung

Heben Sie Probleme beim 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/CIFS-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 schlechte Webserverleistung oder Probleme hervor, die bei der Analyse des Datenverkehrs über das HTTP-Protokoll beobachtet wurden. Diese Erkennungen könnten darauf hindeuten, dass interne Serverprobleme zu einer übermäßigen Anzahl von Fehlern der Stufe 500 führen, sodass Benutzer nicht auf die Anwendungen und Dienste zugreifen können, die sie benötigen.

Härten Erkennungen identifizieren Sicherheitsrisiken und Möglichkeiten zur Verbesserung Ihrer Sicherheitslage.

Härten

Heben Sie bewährte Methoden zur Stärkung der Sicherheit hervor, die durchgesetzt werden sollten, um das Risiko einer Ausnutzung zu verringern. Diese Erkennungen identifizieren Möglichkeiten, die Sicherheitslage Ihres Netzwerk zu verbessern, z. B. die Offenlegung von Anmeldeinformationen zu verhindern und abgelaufene SSL/TLS-Zertifikate von Servern zu entfernen. Nachdem Sie auf eine Härtungserkennung geklickt haben, können Sie zusätzliche Filter anwenden, um bestimmte Erkennungen innerhalb dieses Härtungserkennungstyps anzuzeigen. Erfahre mehr über [Filterung und Abstimmung von Härtungserkennungen](#).

Einbruchmeldesystem (Intrusion Detection System) Erkennungen identifizieren Sicherheitsrisiken und böses Verhalten.

Erkennung von Eindringlingen

Heben Sie Netzwerkverkehr hervor, der mit bekannten Signaturen unsicherer Praktiken, Exploit-Versuchen und Indikatoren für Sicherheitsbedrohungen im Zusammenhang mit Malware und Command-and-Control-Aktivitäten übereinstimmt.

 **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. Datenexfiltration oder abgelaufenen SSL-Serverzertifikaten. Sie können auch eine CVE-Identifikationsnummer in diesen Filter eingeben, um nur Erkennungen für eine bestimmte Sicherheitslücke im Bereich der öffentlichen Sicherheit anzuzeigen.

MITRE-Technik

Heben Sie Erkennungen hervor, die mit bestimmten MITRE-Technik-IDs übereinstimmen. Das MITRE-Framework ist eine weithin anerkannte Wissensdatenbank für Angriffe.

Täter und Opfer

Die mit einer Erkennung verbundenen Täter- und Opferendpunkte werden als Teilnehmer bezeichnet. Sie können Ihre Erkennungsliste so filtern, dass nur Erkennungen für einen bestimmten Teilnehmer angezeigt werden, z. B. für einen Täter mit einer unbekannt Remote-IP-Adresse oder für ein Opfer, bei dem es

sich um einen wichtigen Server handelt. Gateway- oder Load Balancer-Geräte, die Externer Endpunkt Endpunktteilnehmern zugeordnet sind, können in diesen Filtern ebenfalls angegeben werden.

Bevollmächtigter

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 ([Ticketsysteme von Drittanbietern](#) nur)
- Mindestrisikobewertung

Durch Erkennungen navigieren

Nachdem Sie ausgewählt haben, wie Ihre Erkennungsliste angezeigt, gruppiert und gefiltert werden soll, klicken Sie auf eine Erkennungskarte, um zur Erkennungsdetailseite zu gelangen.

Erkennungskarten

Jede Erkennungskarte identifiziert die Ursache der Erkennung, die Erkennungskategorie, den Zeitpunkt der Erkennung sowie die Opfer- und Täterbeteiligten. Sicherheitserkennungen beinhalten eine Risikoscore.

The screenshot shows a detection card with the following components:

- Risk score and attack chain phase:** A risk score of 70 (orange triangle) for 'VPN Client Data Exfiltration' (EXFILTRATION, ACTIONS ON OBJECTIVE). The timestamp is 'May 24 08:36' lasting an hour.
- Description and root cause of unusual behavior:** 'VPN Client 10 received an unusual amount of data from internal resources. This behavior indicates that the VPN client might be compromised and transferring unauthorized information out of the network. The VPN client received: 459.7GB from vpncenter.west10.example.com(192.168.72.198) over SSL:443. The risk score increased because of a highly privileged device.'
- Adjusted risk score:** The risk score increased because of a highly privileged device.
- Participant roles and device names:**
 - OFFENDER:** VPN Client 10 (192.168.237.50, Site: West 5)
 - VICTIM:** proxy.example.com (192.168.134.116, Site: West 5)
- Metric data:**

Network Metric	6h Snapshot	1hr Peak Value	Expected Range	Deviation
Bytes In		356 GB	0 B-623 MB	56,997%
- Detection tracking and tuning options:** 'Actions' dropdown and 'View Detection Details' link.

Risikobewertung

Misst die [Wahrscheinlichkeit, Komplexität und Auswirkungen auf das Geschäft](#) einer Sicherheitserkennung. Dieser Wert bietet eine Schätzung auf der Grundlage von Faktoren zur Häufigkeit und Verfügbarkeit bestimmter Angriffsvektoren im Vergleich zu den erforderlichen Fähigkeiten eines potenziellen Hackers und zu den Folgen eines erfolgreichen Angriffs. Das Symbol ist nach Schweregrad farblich gekennzeichnet: Rot (80-99), Orange (31-79) oder Gelb (1-30).

Teilnehmer

Identifiziert jeden Teilnehmer (Täter und Opfer), der an der Erkennung beteiligt war, anhand des Hostnamens oder der IP-Adresse. Klicken Sie auf einen Teilnehmer, um grundlegende Informationen und Zugangslinks anzuzeigen. Interne Endpunkte zeigen einen Link zur Seite „Geräteübersicht“ an; externe Endpunkte zeigen die Geolokalisierung der IP-Adresse an. [Links zur Endpunktsuche](#) 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 ursprüngliche Endpunkt wird als Teilnehmer betrachtet.



Hinweis Wenn HTTPS aktiviert ist, ist eine SSL/TLS-Entschlüsselung erforderlich, um Ursprungsendpunkte anzuzeigen. Erfahre mehr über [SSL/TLS-Entschlüsselung](#).

Bei der Gruppierung nach **Typ**, wird unter dem Erkennungstyp ein Übersichtsfenster angezeigt, das die Erkennungen nach Täter und Opfer aufschlüsselt und es Ihnen ermöglicht, schnell [Teilnehmerfilter anwenden](#).

Bei der Gruppierung nach **Quelle**, interne Geräterollensymbole sind rot hervorgehoben, wenn das Gerät bei einer Erkennung ein Täter war, und blaugrün, wenn es sich bei dem Gerät um ein Opfer handelte. Sie können klicken **Einzelheiten** unter dem Quellennamen, um eine Zusammenfassung der Erkennungen anzuzeigen, an denen diese Quelle Teilnehmer war. Diese Gerätedetails werden neben der Erkennungskarte auf Breitbildschirmen (1900 Pixel oder mehr) angezeigt.

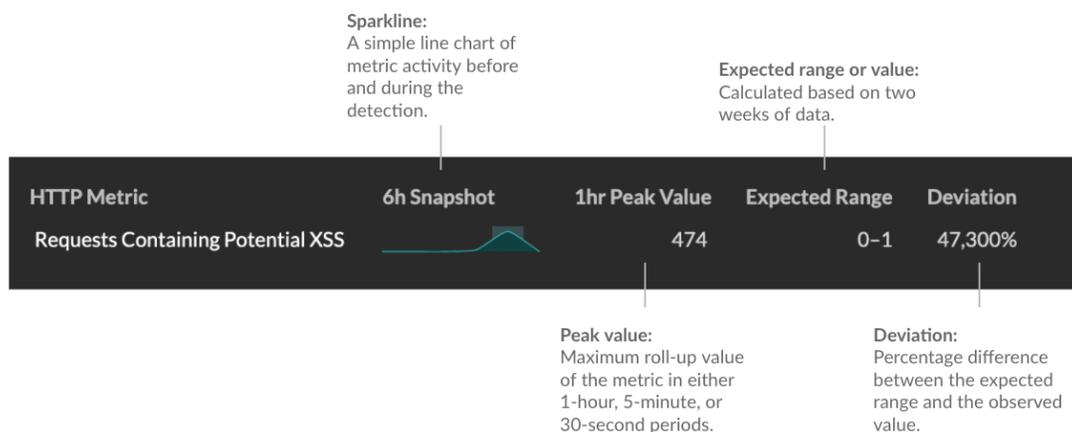
Dauer

Identifiziert, wie lange das ungewöhnliche Verhalten erkannt wurde, oder zeigt FORTLAUFEND an, wenn das Verhalten derzeit auftritt.

Bei Erkennungen, bei denen bewährte Methoden zur Erhöhung der Sicherheit hervorgehoben werden, werden zwei Daten angezeigt: das erste Mal und das Datum, an dem der Verstoß zuletzt festgestellt 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 der Typ 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, Datensatztransaktionen und Links zu Rohpaketen.

Auf die Erkennungskarteninformationen folgen alle verfügbaren Abschnitte für die Erkennung. Diese Abschnitte variieren je nach Art der Erkennung.

Erkennung von Spuren

Du kannst [Spur](#) oder [stimmen](#) die Erkennung, oder klicken **Zu einer Untersuchung hinzufügen** um die Erkennung in ein neues oder vorhandenes einzubeziehen [Untersuchung](#).

Wenn Sie eine konfiguriert haben [CrowdStrike-Integration](#) auf Ihrem ExtraHop-System können Sie [die Eindämmung von CrowdStrike-Geräten einleiten](#) die an der Erkennung beteiligt sind. (Nur Reveal (x) 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 Entschlüsselungs-Badge angezeigt.

Erfahre mehr über [SSL/TLS-Entschlüsselung](#) und [Entschlüsseln des Datenverkehrs mit einem Windows-Domänencontroller](#).

Erkennungseigenschaften

Stellt eine Liste von Eigenschaften bereit, die für die Erkennung relevant sind. Zu den Erkennungseigenschaften können beispielsweise eine Abfrage, ein URI oder ein Hacking-Tool gehören, das für die Erkennung von zentraler Bedeutung ist.

172.168.225.10

OFFENDER
 dns35.west.example.com
 192.168.46.64
 Site: West1

VICTIM
 workstation.example.com
 192.168.114.49
 Site: West1

Query Name: A.16.88.248.207.extime.192.168.187.25.east.network
 Client Port: 43673
 Server Port: 53

Related Detections

Current Detection

Karte der Aktivitäten

Bietet eine **Aktivitätsdiagramm** das hebt die an der Erkennung beteiligten Teilnehmer hervor. Auf der Aktivitätsdiagramm wird der Ost-West-Verkehr des Protokoll angezeigt, das mit der Erkennung verknüpft ist, sodass Sie den Umfang der bösertige Aktivität besser einschätzen können. Klicken Sie auf das Opfer oder den Täter, um ein Dropdownmenü mit Links zur Seite „Geräteübersicht“ und anderen Erkennungen aufzurufen, an denen das Gerät Teilnehmer ist.

Activity Map

VICTIM
 dns10.example.com
 192.168.241.112

Victim highlighted in teal

TCP, SSH, DNS, HTTP

OFFENDER
 client.example.com
 192.168.156.111

Offender highlighted in red

Navigate to Activity Map page

Go to Activity Map

Erkennungsdaten und Links

Stellt zusätzliche Daten im Zusammenhang mit der Erkennung bereit, die untersucht werden sollen. Die Datentypen können verwandte Metriken enthalten, Links zu [Datensatz](#) Transaktionsanfragen und ein Link zu einem allgemeinen [Pakete](#) abfragen. 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.

Metrische Daten 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.

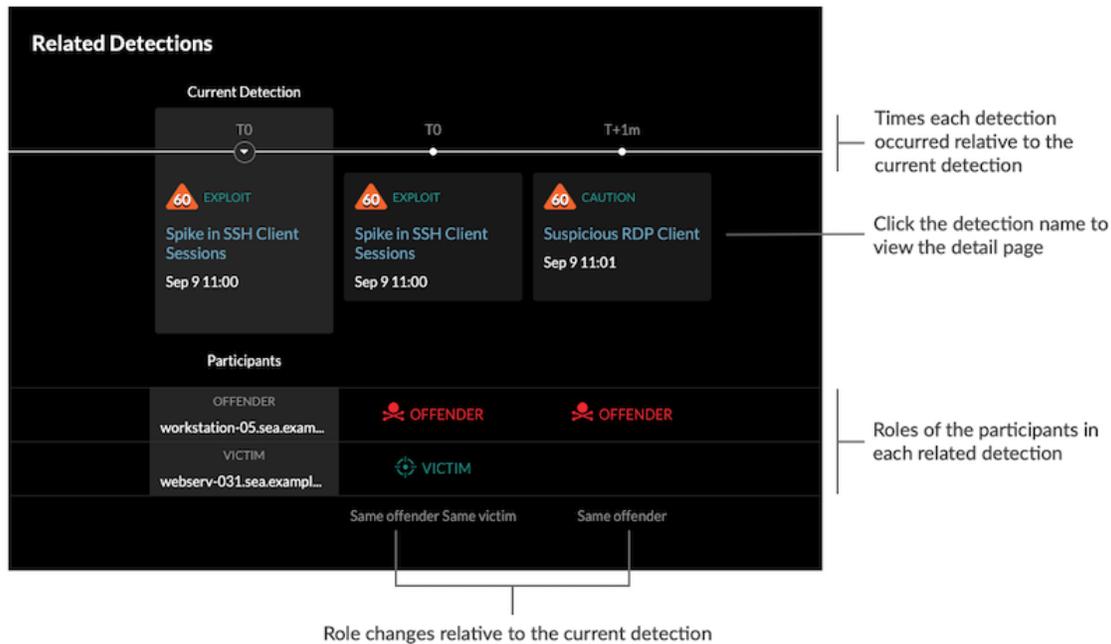
Verhalten vergleichen

Stellt ein Diagramm bereit, das die Aktivität des Täters neben der Aktivität ähnlicher Geräte in dem Zeitraum anzeigt, in dem die Erkennung erfolgte. Das Diagramm wird für Erkennungen angezeigt, die auf unkonventionelle Aktivitäten eines Gerät sind, und hebt unerwartetes Verhalten hervor, indem es neben dem Verhalten von Geräten im Netzwerk mit ähnlichen Eigenschaften angezeigt wird.



Verwandte Erkennungen

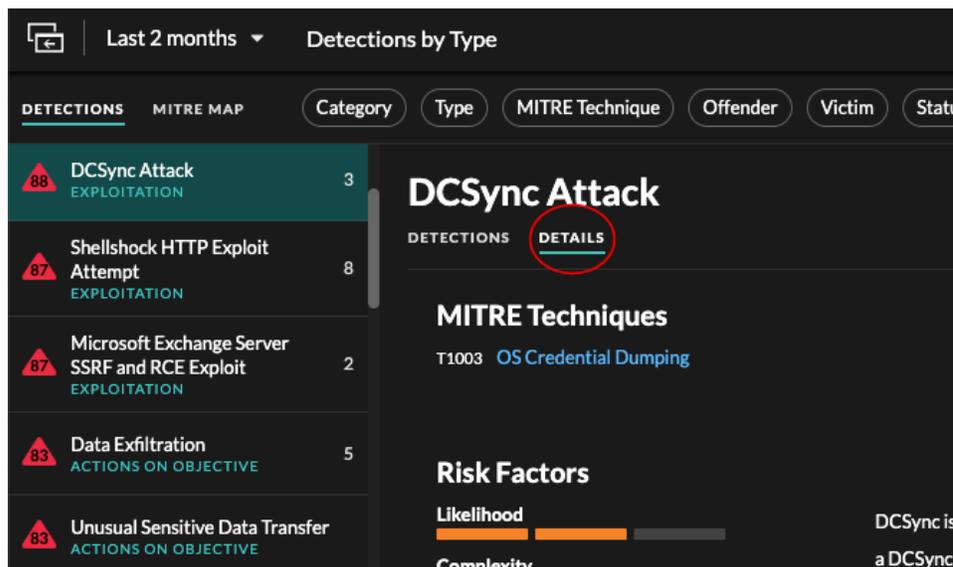
Bietet eine Zeitleiste mit Erkennungen im Zusammenhang mit der aktuellen Erkennung, anhand derer Sie eine größere Angriffskampagne identifizieren können. Zu den entsprechenden Erkennungen gehören die Rolle des Teilnehmer, die Dauer, der Zeitstempel und alle Rollenänderungen, wenn der Täter bei einer Erkennung zum Opfer einer anderen Erkennung wird. Klicken Sie in der Timeline auf eine zugehörige Erkennung, um die Detailseite für diese Erkennung aufzurufen.



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 (1900 Pixel oder mehr) angezeigt, oder Sie können darauf zugreifen, indem Sie darauf klicken **Einzelheiten** unter dem Erkennungstitel, wenn die Erkennungsseite gruppiert wird nach **Typen**.



Hinweis: Du kannst **Erkennung teilen** Detailseiten mit anderen ExtraHop-Benutzern.

Erkennungskatalog

Der Erkennungskatalog enthält eine vollständige Liste aller im ExtraHop-System verfügbaren Erkennungstypen. Sie können benutzerdefinierte Erkennungstypen auch auf der Seite Erkennungskatalog verwalten.

Sie können auf die Seite mit dem Erkennungskatalog zugreifen, indem Sie auf das Symbol Systemeinstellungen klicken.

Display Name	Author	Detection Type ID	Category	MITRE Technique
<input type="checkbox"/> Multiple SMB/CIFS Errors	ExtraHop	multiple_smb_cifs_errors	Storage	—
<input type="checkbox"/> NBT-NS Poisoning	ExtraHop	nbt_ns_poisoning	Exploitation	T1557: Man-in-the-Middle
<input type="checkbox"/> Network Privilege Escalation	ExtraHop	network_privilege_escalation	Lateral Movement	T1021: Remote Services
<input type="checkbox"/> Network Share Enumeration	ExtraHop	msrpc_network_share_enum	Reconnaissance	T1135: Network Share Discovery
<input type="checkbox"/> Network Segmentation Breach	garp	network_segmentation_breach	Lateral Movement	T1098: Account Manipulation

Zusätzlich zum Anzeigenamen und Autor können Sie die Liste der Erkennungstypen nach Erkennungstyp-ID, Erkennungskategorie, mit dem Erkennungstyp verknüpften MITRE-Techniken und Erkennungstypen, die Daten aus dem Fluss unterstützen, filtern Sensoren.

Klicken Sie auf eine integrierte Erkennung, um die Einstellungen für den Erkennungstyp Bereich, in dem der Name, der Typ und die zugehörigen Kategorien der Erkennung angezeigt werden. Um mehr über die Erkennung zu erfahren, klicken Sie auf **Details zum Erkennungstyp**.

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 [eine benutzerdefinierte Erkennung erstellen](#).
- 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 tafel. Integrierte Erkennungen, bei denen ExtraHop als Autor aufgeführt ist, können nicht bearbeitet werden.
- Um eine benutzerdefinierte Erkennung zu löschen, klicken Sie auf die Erkennung und dann auf **Löschen** von der Einstellungen für den Erkennungstyp Panel.

Ermittlungen

(nur NDR-Modul) Mithilfe von Untersuchungen können Sie mehrere Entdeckungen in einer einzigen Zeitleiste und Karte hinzufügen und anzeigen. Anhand einer Karte mit verbundenen Erkennungen können Sie feststellen, ob verdächtiges Verhalten eine gültige Bedrohung darstellt und ob eine Bedrohung von einem einzelnen Angriff oder Teil einer größeren Angriffskampagne stammt.

Investigation title

Authoring information

Updateable notes

Investigation timeline

Participants

Relative timestamps

Investigation map

Click detections to view detection cards

Sie können Untersuchungen auf einer Entdeckungsdetailseite oder über das Menü Aktionen auf jeder Entdeckungskarte erstellen und zu ihnen hinzufügen.

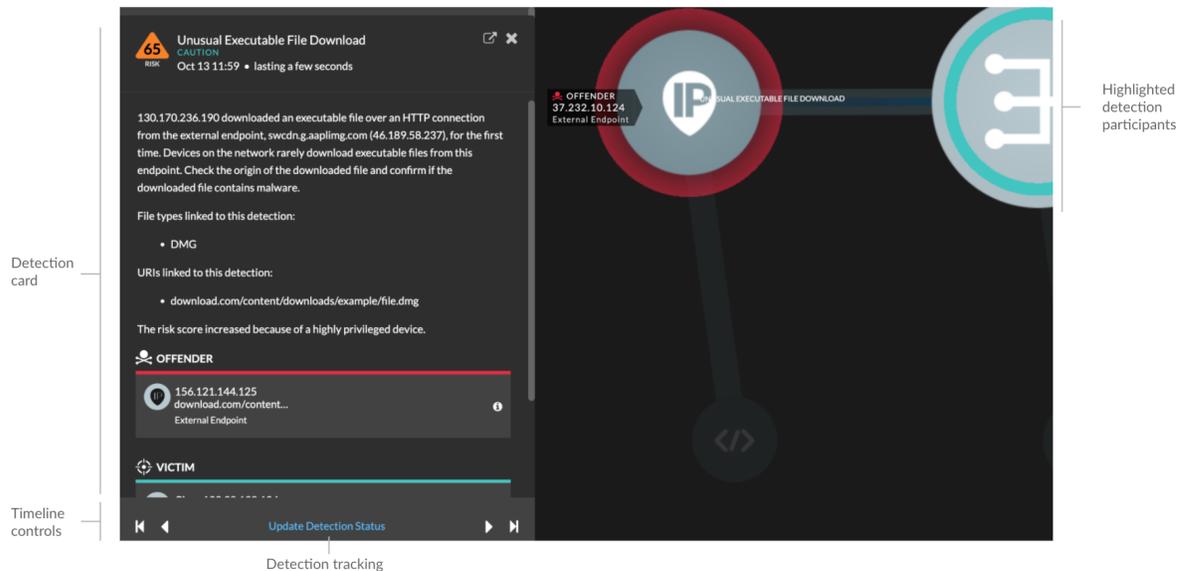
Jede Ermittlungsseite enthält die folgenden Tools:

Zeitplan für die Untersuchung

Die Zeitleiste wird links auf der Seite angezeigt und listet die hinzugefügten Erkennungen in chronologischer Reihenfolge auf. Neue Entdeckungen, die hinzugefügt werden, werden in der Zeitleiste entsprechend der Uhrzeit und dem Datum der Erkennung sowie relativ zur frühesten Erkennung, die mit T0 gekennzeichnet ist, angezeigt. Erkennungsteilnehmer werden unter dem Erkennungstitel angezeigt, und Informationen zur Erkennungsverfolgung, wie Beauftragter und Status, werden neben den Teilnehmern angezeigt.

Klicken Sie auf eine Erkennung in der Timeline, um die [Erkennungskarte](#) und markieren Sie die Erkennungsteilnehmer auf der Untersuchungskarte. Klicken Sie auf der Karte oder in der Ermittlungskarte auf einen Teilnehmer, um grundlegende Details und Links zur Seite mit der Geräteübersicht sowie zu anderen Erkennungen anzuzeigen, bei denen das Gerät ein Teilnehmer ist.

Klicken Sie in der oberen rechten Ecke der Erkennungskarte auf Gehe zu Symbol, um das zu sehen [Seite mit Erkennungsdetails](#), oder die Symbol, um die Erkennung zu schließen und zur Ermittlungszeitleiste zurückzukehren.



Klicken Sie unter der Erkennungskarte auf **Spurerkennung** zu bearbeiten [Erkennungsverfolgung](#) Informationen. Sie können auf die Timeline-Steuerelemente klicken, um andere Erkennungen in der Untersuchung anzuzeigen.

Ermittlungskarte

Die Ermittlungskarte zeigt den Täter und das Opfer jeder Erkennung im Rahmen der Untersuchung. Die Teilnehmer sind durch Linien verbunden, die mit dem Erkennungstyp gekennzeichnet sind, und Geräterollen werden durch ein Symbol dargestellt.

- Klicken Sie in der Untersuchungszeitleiste auf eine Erkennung, um die Teilnehmer hervorzuheben. Kreise sind rot hervorgehoben, wenn das Gerät der Täter ist, und blaugrün, wenn das Gerät das Opfer ist. Die Markierungen werden aktualisiert, wenn Sie auf eine andere Erkennung klicken, sodass Sie leichter erkennen können, wann ein Teilnehmer vom Opfer zum Täter wechselt.
- 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 zu navigieren oder [Seite „Geräteübersicht“](#).
- Zeigen Sie mit der Maus auf einen Kreis oder eine Linie, um die Bezeichnung anzuzeigen.

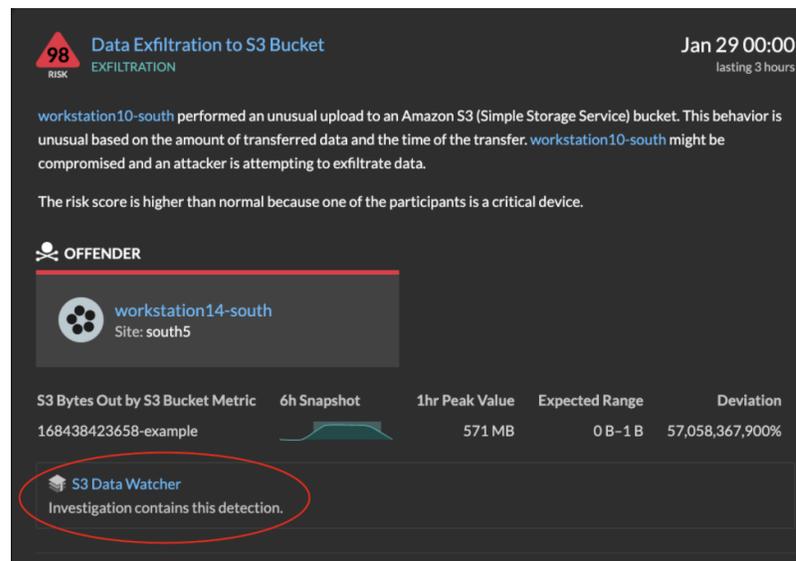
Hinweise

Klicken **Untersuchung bearbeiten** um Notizen hinzuzufügen oder den Namen der Untersuchung zu ändern. Du kannst weitermachen [einzelne Erkennungen verfolgen](#) nachdem Sie sie zu einer Untersuchung hinzugefügt haben.

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 Erkennungen im ExtraHop-System

Die Seite Erkennungen bietet zwar schnellen Zugriff auf alle Erkennungen, es gibt jedoch Indikatoren und Links zu Erkennungen im gesamten ExtraHop-System.



Hinweis: Erkennungen bleiben gemäß Ihrem [System-Lookback-Kapazität](#) für 1-Stunden-Metriken mit einer Mindestspeicherzeit von fünf Wochen. Erkennungen bleiben ohne unterstützende Metriken im System, 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 Gerätegruppenübersicht auf den Link Erkennungen, um zur Seite Erkennungen zu gelangen. Die Entdeckungsliste wird nach der Gerätegruppe als Quelle gefiltert.
- Klicken Sie auf der Protokollseite eines Gerät oder einer Gerätegruppe auf den Link Erkennungen, um zur Seite Erkennungen zu gelangen. Die Entdeckungsliste wird nach Quelle und Protokoll gefiltert.
- Klicken Sie auf einer Aktivitätsdiagramm auf ein Gerät, das animierte Impulse rund um die Kreisbeschriftung anzeigt, um [eine Liste der zugehörigen Erkennungen anzeigen](#). Klicken Sie auf den Link für eine einzelne Erkennung, um die Erkennungsdetails anzuzeigen.
- Zeigen Sie in einem Diagramm auf einem Dashboard oder einer Protokollseite mit der Maus auf ein [Erkennungsmarker](#) um den Titel der zugehörigen Erkennung anzuzeigen, oder klicken Sie auf die Markierung, um die Erkennungsdetails anzuzeigen.

Optimierung von Erkennungen

Hier sind einige bewährte Methoden, die Sie anwenden sollten, um Ihre Erkennungen zu verbessern: Fügen Sie Details zu Ihrem Netzwerk hinzu, aktivieren Sie das ExtraHop-System, um potenziell verdächtigen Datenverkehr 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 Datenverkehr normalerweise versteckt ist. Und wenn Ihr Netzwerk über Active Directory verfügt, verbergen sich eine Reihe von Erkennungen im verschlüsselten Datenverkehr in der gesamten Domäne.

Wir empfehlen dringend, die Entschlüsselung für zu aktivieren [SSL/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 einen 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 cloudbasierten 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 und Domänen, denen Sie vertrauen, z. B. eine vertrauenswürdige Domain, mit der Ihre Geräte regelmäßig eine Verbindung herstellen. Erkennungen durch maschinelles Lernen und Systemmetriken basieren auf Gerät- und Verkehrsklassifizierungen.

Wenn Ihre Geräte beispielsweise regelmäßig eine Verbindung zu einer unbekannt, aber vertrauenswürdigen Domain herstellen, die als externe IP-Adresse klassifiziert ist, werden Erkennungen für diese Domain unterdrückt.

Erkennungen optimieren

Mit diesen Einstellungen können Sie [Erkennungen ausblenden oder unterdrücken](#) nachdem das System sie generiert hat. Wenn Sie eine Erkennung sehen, die keinen Mehrwert bietet, können Sie das Rauschen in Ihrer Gesamtansicht reduzieren.

Wenn eine Erkennung beispielsweise anhand eines Täters, eines Opfers oder anderer Kriterien generiert wird, die für Ihr Netzwerk nicht von Belang sind, können Sie alle früheren und zukünftigen Erkennungen mit diesen Kriterien ausblenden.

Externe Klartext-Daten teilen

Mit dieser Option kann der Machine Learning Service [IP-Adressen, Hostnamen und Domains sammeln](#) die mit verdächtigen Aktivitäten verbunden sind.

Wenn Sie diese Option aktivieren, erweitern Sie einen kollektiven Datensatz potenzieller Bedrohungen, die Ihnen helfen und einen Beitrag zur Sicherheitsgemeinschaft leisten können.

Erkennungen nachverfolgen

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 Erkennungsseite filtern, um gelöste Probleme aus der Ansicht zu löschen oder um nach Erkennungen zu suchen.

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

- [Eine Regel für Erkennungsbenachrichtigungen erstellen](#) 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 Entdeckungen in einer einzigen Zeitleiste und Karte anzuzeigen.

Sie können auf die Liste der erstellten Untersuchungen zugreifen über **Ermittlungen** Symbol in der oberen rechten Ecke der Erkennungsseite.

Bevor Sie beginnen

- 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. 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 **Zu einer Untersuchung hinzufügen....**

5. Wählen **Erkennung zu einer neuen Untersuchung hinzufügen**.
6. klicken **Weiter**.
7. Geben Sie einen Namen ein und fügen Sie Notizen zur neuen Untersuchung hinzu.
8. klicken **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 Entdeckung aus einer Untersuchung zu löschen, klicken Sie in der Untersuchungszeitleiste auf das Löschsymboll (X) auf der Erkennung.

Eine Regel für Erkennungsbenachrichtigungen erstellen

Erstellen Sie eine Benachrichtigungsregel, wenn Sie eine Benachrichtigung über Entdeckungen erhalten möchten, die bestimmten Kriterien entsprechen.

Wenn eine Erkennung generiert wird, die Ihren Kriterien entspricht, wird eine Benachrichtigung mit Informationen aus dem [Erkennungskarte](#).

Sie können das System so konfigurieren, dass es eine E-Mail an eine Empfängerliste sendet oder einen bestimmten Webhook aufruft.

Bevor Sie beginnen

- Benutzern muss NDR- oder NPM-Modulzugriff gewährt werden und sie müssen über vollständigen Schreibzugriff verfügen [Privilegien](#) oder höher, um die Aufgaben in diesem Handbuch zu erledigen.
 - Reveal (x) 360 benötigt eine [Verbindung zu ExtraHop Cloud Services](#) um Benachrichtigungen per E-Mail und Webhooks zu senden. Reveal (x) Enterprise benötigt eine Verbindung zu ExtraHop Cloud Services, um Benachrichtigungen per E-Mail zu senden, kann aber auch ohne Verbindung eine Benachrichtigung über einen Webhook senden.
 - E-Mail-Benachrichtigungen werden über ExtraHop Cloud Services gesendet und können identifizierbare Informationen wie IP-Adressen, Benutzernamen, Hostnamen, Domainnamen, Gerätenamen oder Dateinamen enthalten. Reveal (x) Enterprise-Benutzer, deren gesetzliche Anforderungen externe Verbindungen verbieten, können Benachrichtigungen mit Webhook-Aufrufen so konfigurieren, dass Benachrichtigungen ohne externe Verbindung gesendet werden.
 - Reveal (x) 360 kann keine Webhook-Aufrufe an Endpunkte in Ihrem internen Netzwerk senden. Webhook-Ziele müssen für externen Datenverkehr geöffnet sein.
 - 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 Zertifizierungsstellen.
 - Reveal (x) Enterprise muss eine direkte Verbindung zu Webhook-Endpunkten herstellen, um Benachrichtigungen zu senden.
 - E-Mail-Benachrichtigungen werden von no-reply@notify.extrahop.com gesendet. Stellen Sie sicher, dass Sie diese Adresse zu Ihrer Liste der erlaubten 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 dann klicken **Regeln für Benachrichtigungen**.
 3. klicken **Erstellen**.
 4. In der Name Feld, geben Sie einen eindeutigen Namen für die Benachrichtigungsregel ein.
 5. In der Beschreibung Feld, fügen Sie Informationen über die Benachrichtigungsregel hinzu.
 6. In der Art der VeranstaltungAbschnitt, wählen **Sicherheitserkennung** oder **Leistungserkennung**.

7. In der Kriterien Abschnitt, klicken **Kriterien hinzufügen** um Kriterien festzulegen, nach denen eine Benachrichtigung generiert wird.
- **Mindestrisikobewertung**
 - **Typ**
 - **Kategorie**
 - **Technik**
 - **Täter**
 - **Opfer**
 - **Rolle des Geräts**
 - **Quelle**
 - **Seite**

Die Kriterienoptionen entsprechen den [Filteroptionen auf der Seite Erkennungen](#).

8. Klicken Sie im Abschnitt Aktionen auf **Aktion hinzufügen** um anzugeben, wie die Benachrichtigung gesendet werden soll.

- klicken **E-Mail senden** und geben Sie einzelne E-Mail-Adressen an, getrennt durch ein Komma.
- klicken **Rufen Sie Webhook an** und geben Sie die folgenden Einstellungen an:
 1. In der Nutzlast-URL Feld, geben Sie die URL des Webhooks ein.
 2. In der Nutzlast (JSON) Feld, geben Sie die JSON-Payload ein, die an die Payload-URL gesendet wird.

Sehen Sie die [Referenz zur Webhook-Benachrichtigung](#) zum Beispiel Payloads.

3. (Optional) Klicken Sie im Abschnitt Benutzerdefinierte Header auf **Kopfzeile hinzufügen** um benutzerdefinierte Schlüssel/Wert-Paare anzugeben.

Benutzerdefinierte Header werden dem Header der Webhook-HTTP-POST-Anforderung hinzugefügt.

4. klicken **Speichern**.
5. klicken **Verbindung testen**.

Eine Nachricht mit dem Titel Testbenachrichtigung wird an die Payload-URL gesendet, um die Verbindung zu bestätigen.



Hinweis Stellen Sie nach dem Testen der Verbindung sicher, dass Sie die Benachrichtigung in der Zielanwendung erhalten haben. Reveal (x) Enterprise zeigt eine Fehlermeldung an, wenn die Testbenachrichtigung nicht erfolgreich war.

6. 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.

9. In der Optionen Abschnitt, wählen Sie den **Benachrichtigungsregel aktivieren** Checkbox, um die Benachrichtigung zu aktivieren.

Wenn eine Erkennung den Kriterien entspricht, wird eine Benachrichtigung gesendet. Eine einzelne Erkennung generiert niemals mehr als eine Benachrichtigung pro Benachrichtigungsregel.

Referenz zur Webhook-Benachrichtigung

Dieses Handbuch enthält Referenzinformationen, die Ihnen beim Schreiben der JSON-Payload für Webhook-basierte Benachrichtigungen helfen sollen. Das Handbuch enthält einen Überblick über die

Payload-Schnittstelle (JSON), eine Liste von Erkennungsvariablen, die für Webhooks verfügbar sind, und Beispiele für die JSON-Struktur für gängige Webhook-Ziele wie Slack, Microsoft Teams und Google Chat.

Weitere Informationen zu Benachrichtigungsregeln finden Sie unter [Eine Regel für Erkennungsbenachrichtigungen erstellen](#).

Nutzlast JSON

ExtraHop-Webhooks sind in JSON formatiert und werden unterstützt von [Jinja2-Vorlagen-Engine](#). Wenn Sie eine Benachrichtigungsregel erstellen und die Webhook-Option auswählen, wird der Webhook-Editor auf der rechten Seite geöffnet, und Sie können die Payload bearbeiten.

Du kannst die Standard-Payload mit benutzerdefinierten Eigenschaften ändern oder eine JSON-Vorlage für Slack, Microsoft Teams oder Google Chat kopieren, und zwar aus dem [Beispiele](#) Abschnitt.

Standardmäßig enthält die Payload ein Beispiel `text` Eigentum. Das JSON-Beispiel in der Abbildung unten sendet eine Benachrichtigung mit dem Text „ExtraHop Erkennung“, gefolgt vom Erkennungstitel, der die Variable ersetzt.



Wir empfehlen, dass Sie Ihre Verbindung zur Webhook-URL testen, bevor Sie die Nutzlast ändern. 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 Feld Payload ein Fehler mit dem Fehler angezeigt.

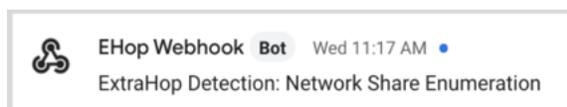
Variablen

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 Tätername 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.

Erkennung: *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.

risk_score: Zahl

Die Risikoscore der Erkennung.

Standort: Schnur

Die Standort, an der die Erkennung stattgefunden hat.

Startzeit_Text: Schnur

Der Zeitpunkt, zu dem die Erkennung begann.

Endzeit_Text: Schnur

Der Zeitpunkt, zu dem die Erkennung endete.

kategorien_array: Reihe von Zeichenketten

Eine Reihe von Kategorien, zu denen die Erkennung gehört.

Kategorien_Zeichenfolge: 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 MITRE-Taktik-IDs auflistet, die mit der Erkennung verknüpft sind.

Mitre_Techniken: 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 der Erkennung zugeordnet sind.

primärer Täter: Objekt

Ein Objekt, das den Haupttäter identifiziert und die folgenden Eigenschaften enthält:

extern: Boolescher Wert

Der Wert ist `true` wenn sich die IP-Adresse des primären Täters außerhalb Ihres Netzwerk befindet.

iPaddr: Schnur

Die IP-Adresse des Haupttäters.

name: Schnur

Der Name des Haupttäters.

Täter: Reihe von Objekten

Eine Reihe von Täterobjekten, die mit der Erkennung in Verbindung stehen. Jedes Objekt enthält die folgenden Eigenschaften:

extern: Boolescher Wert

Der Wert ist `true` wenn sich die IP-Adresse des Täters außerhalb Ihres Netzwerk befindet.

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

Ein Objekt, das das primäre Opfer identifiziert und die folgenden Eigenschaften enthält:

extern: Boolescher Wert

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 in Verbindung stehen. Jedes Objekt enthält die folgenden Eigenschaften:

extern: Boolescher Wert

Der Wert ist `true` wenn sich die IP-Adresse des Opfers außerhalb Ihres Netzwerk befindet.

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.

Schlaffe

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 eingeben musst.

Das folgende Beispiel zeigt die JSON-Payload für einen Slack-Webhook:

```
{
  "blocks": [
    {
      "type": "header",
      "text": {
        "type": "plain_text",
        "text": "Detection: {{ title }}"
      }
    },
    {
      "type": "section",
      "text": {
        "type": "mrkdn",
        "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

Sie können 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 können.

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 Reveal(x)",
                    "weight": "bolder"
                  }
                ]
              }
            ]
          }
        ],
        "text": ""
      },
      {
        "type": "TextBlock",
        "text": "**{{ title }}**"
      },
      {
        "type": "TextBlock",
        "spacing": "small",
        "isSubtle": true,
        "wrap": true,

```


Eine Erkennung verfolgen

Mit der Erkennungsverfolgung können Sie einer Erkennungskarte Benutzer zuweisen, einen Status festlegen und Notizen hinzufügen.

Sie können Ihre Erkennungsansicht auch nach einem bestimmten Status oder Beauftragten filtern.

Bevor Sie beginnen

Benutzer müssen über eingeschränkte Schreibberechtigungen verfügen [Privilegien](#) oder höher, um die Aufgaben in diesem Handbuch abzuschließen.

Sie können den Beauftragten auf einen beliebigen Benutzer im System ändern, Notizen hinzufügen und den Status einer Erkennung auf einen der folgenden Werte setzen:

Offen

Die Erkennung wurde nicht überprüft.

Bestätigen

Die Erkennung wurde beobachtet und sollte für die Nachsorge priorisiert werden.

In Bearbeitung

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 – Es wurden keine Maßnahmen ergriffen

Die Erkennung wurde überprüft und erforderte keine Maßnahmen.

The screenshot shows a detection card titled "Rare SSH Port" with a risk level of 60 and the category "COMMAND & CONTROL". The card indicates that data was sent on a non-standard SSH port (SSH:29418) on May 26 at 12:21, lasting for a minute. It identifies an offender (nat.west.example.com, 192.168.210.185) and a victim (workstation.west.example.com, 192.168.250.53). A table shows network bytes out by L7 protocol, with a peak value of 10.6 KB for SSH:29418. At the bottom, the status is "IN PROGRESS" (highlighted with a red circle), assigned to user "garyp", and last edited on Jun 02 12:05. An "Investigate This Detection" link is visible at the bottom right.

Hier sind wichtige Überlegungen zur Nachverfolgung von Erkennungen:

- Der Status Bestätigt oder Geschlossen verbirgt die Erkennung nicht.
- Der Erkennungsstatus kann von jedem privilegierten Benutzer aktualisiert werden.
- Wahlweise können Sie [Konfigurieren Sie das Erkennungs-Tracking mit einem Drittanbietersystem](#).
- Wenn Sie derzeit Erkennungen mit einem Drittanbietersystem verfolgen, wird die ExtraHop-Erkennungsverfolgung erst angezeigt, wenn Sie die Einstellung in der [Verwaltung](#) Einstellungen.

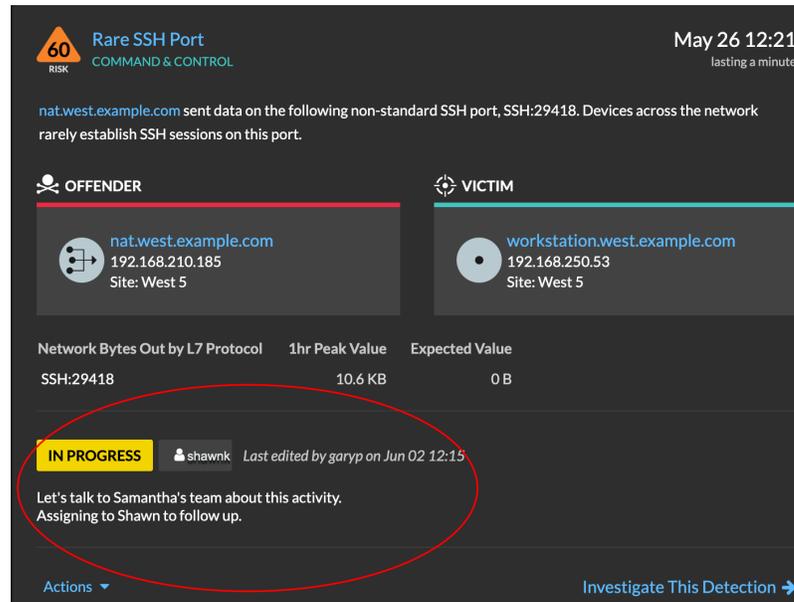
Gehen Sie wie folgt vor, um eine Erkennung zu verfolgen:

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 beobachtet und sollte für die Nachsorge priorisiert werden.
In Bearbeitung	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 – Es wurden keine Maßnahmen ergriffen	Die Erkennung wurde überprüft und erforderte keine Maßnahmen.

The screenshot shows a detection card titled "Rare SSH Port" with a risk level of 60 (RISK) and a category of "COMMAND & CONTROL". The card indicates that data was sent on a non-standard SSH port (SSH:29418) on May 26 at 12:21, lasting for a minute. It identifies an offender IP (192.168.210.185) and a victim IP (192.168.250.53). A table shows network bytes out by L7 protocol, with SSH:29418 having a 1hr peak value of 10.6 KB and an expected value of 0 B. At the bottom, the status is "IN PROGRESS" (highlighted with a red circle), assigned to user "garyp", and last edited on Jun 02 12:05. An "Investigate This Detection" link is also visible.

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.

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.

Track Detection

Status **Assignee**

No Status  Unassigned 

Integrations

 **CrowdStrike Falcon** 

4 participants are CrowdStrike devices

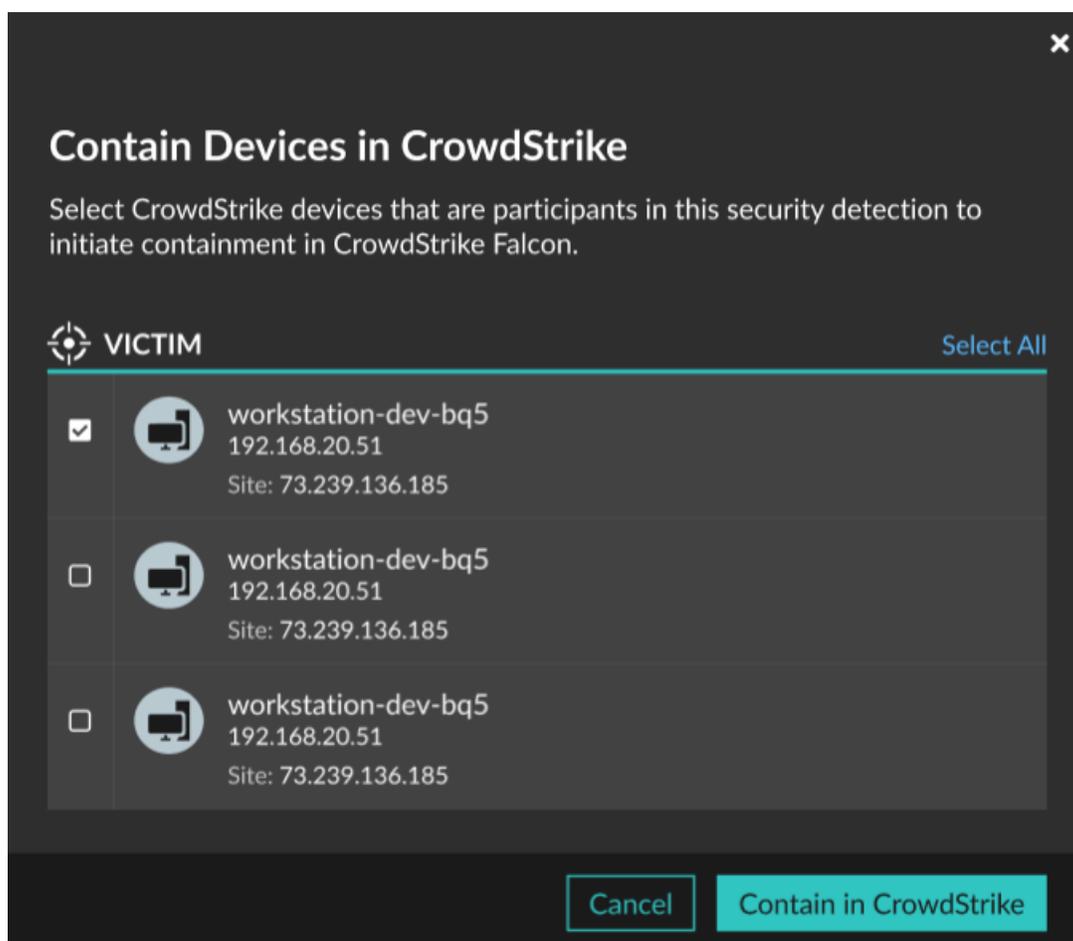
Contain Devices in CrowdStrike

Actions

[Add to an Investigation](#)

[Tune Detection](#)

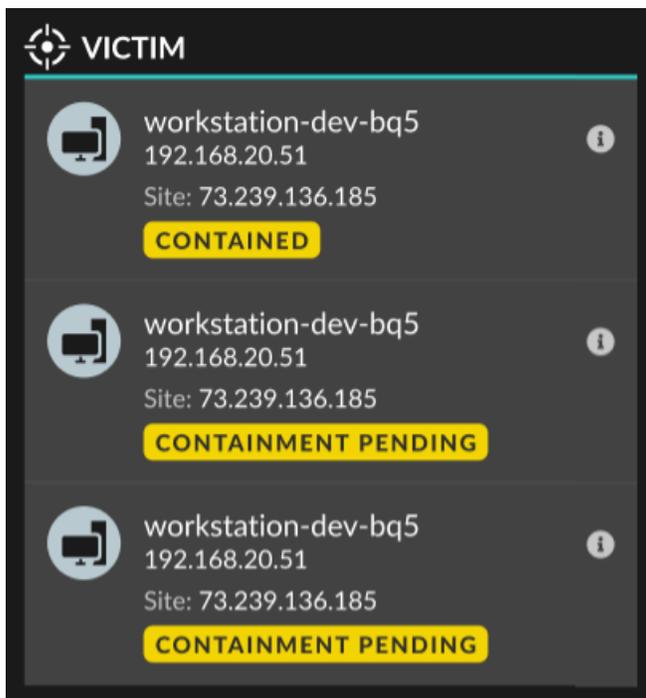
4. klicken **Geräte in CrowdStrike enthalten**.
Im Dialogfeld werden die CrowdStrike-Geräte angezeigt, die mit der Erkennung verknüpft sind.



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 [Auslöser](#). 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.

Erstellen Sie einen Auslöser, um benutzerdefinierte Erkennungen zu generieren

Trigger generieren benutzerdefinierte Erkennungen, indem sie den aufrufen `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 bezeichnet wird.

Der Auslöser identifiziert PowerShell-Verbindungen, indem er nach JA3-Hashes für SSL-Clients sucht, die zu bekannten PowerShell-Clients gehören.

Wenn die SSL-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 dann klicken **Auslöser**.
2. klicken **Erstellen**.
3. Geben Sie die folgenden Einstellungen für die Trigger-Konfiguration 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 zu verdächtiger 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 Github erstellt. PowerShell-Clients werden durch JA3-Hashes identifiziert.

Ereignisse

Wählen Sie das Ereignis aus, für das der Auslöser ausgeführt wird.

In unserem Beispiel wählen wir das Ereignis `SSL_OPEN` aus. Dieses Ereignis tritt auf, wenn eine SSL-Verbindung zum ersten Mal 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 sich vergewissert haben, dass die benutzerdefinierte Erkennung ordnungsgemäß funktioniert, ändern Sie die Zuweisung zu einer Gerätegruppe, die all Ihre wichtigen Microsoft-Server enthält. Weitere Informationen zum Erstellen von Gerätegruppen finden Sie unter [Eine Gerätegruppe erstellen](#).

4. Geben Sie im rechten Bereich den Code ein, der bestimmt, wann Ihre benutzerdefinierte Erkennung generiert wird.

In unserem Beispiel identifiziert der folgende Triggercode, wann ein Client eine Verbindung zu Pastebin, githubusercontent oder Github initiiert:

```
if(SSL.host.match(/pastebin/i) || SSL.host.match(/raw.githubusercontent.com/i) || SSL.host.match(/github.com/i)) {
```

```
}

```

5. Geben Sie als Nächstes den Code ein, der Ihre benutzerdefinierte Erkennung festlegt. Die `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 <code>[benutzerdefiniert]</code> .
Beschreibung der Erkennung	Text, der auf einer Erkennungskarte unter dem Titel und der Kategorie angezeigt wird. 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 <code>\$(Flow.client.ipaddr)</code> und <code>\$(Flow.server.ipaddr)</code> die IP-Adresse des Client- und Servergeräts im Fluss anzeigen und <code>\$(Flow.l7proto)</code> zeigt das L7-Protokoll an. Einschließen <code>\n</code> am Ende jeder Textzeile, um sicherzustellen, dass die Beschreibung korrekt angezeigt wird.
Risikoscore	Eine Zahl, die die Wahrscheinlichkeit, Komplexität und die geschäftlichen Auswirkungen einer Sicherheitserkennung misst. Das

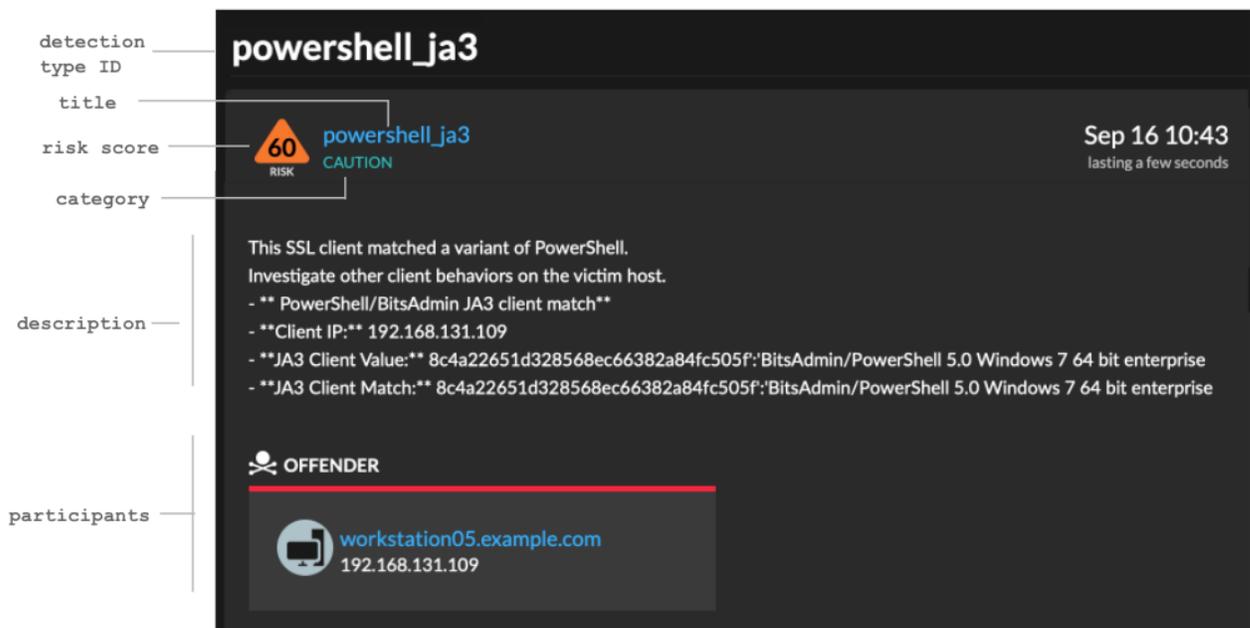
Wert	Beschreibung
	<p>Risikoeinstufungssymbol wird oben auf der Erkennungskarte angezeigt und ist nach Schweregrad farblich gekennzeichnet: Rot (80-99), Orange (31-79) oder Gelb (1-30). Du kannst Erkennungen nach Risiko sortieren.</p>
<p>Täter, Teilnehmer Teilnehmer des Opfers</p>	<p>Eine Reihe von Objekten, die die Teilnehmer an der Erkennung identifizieren. 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.</p> <p>Das folgende Array identifiziert beispielsweise den Server als Täter und den Client als Opfer in einem Fluss:</p> <pre data-bbox="876 703 1453 934"> participants: [{ role: 'offender', object: Flow.server.device}, { role: 'victim', object: Flow.client.device }] </pre> <p>Weitere Informationen zu Gerät, IP-Adresse und Anwendungsobjekten finden Sie in der Trigger-API-Referenz.</p>
<p>Identitätsschlüssel</p>	<p>Eine Zeichenfolge, die die Identifizierung laufender Erkennungen ermöglicht. Wenn mehrere Erkennungen mit demselben Identitätsschlüssel und demselben Erkennungstyp innerhalb des angegebenen Zeitraums generiert werden <code>identityTtl</code> Parameter, die Erkennungen werden zu einer einzigen laufenden Erkennung zusammengefasst.</p> <p>Erstellen Sie eine eindeutige Identitätsschlüsselzeichenfolge, indem Sie Merkmale der Erkennung kombinieren.</p> <p>Der folgende Identitätsschlüssel wird beispielsweise durch die Kombination der Server-IP-Adresse und der Client-IP-Adresse erstellt:</p> <pre data-bbox="876 1564 1453 1669"> identityKey: [Flow.server.ipaddr, Flow.client.ipaddr].join('!!!') </pre>
<p>Zeitraum</p>	<p>Die Zeitspanne nach der Generierung einer Erkennung, in der doppelte Erkennungen zu einer fortlaufenden Erkennung zusammengefasst werden. Der Zeitraum wird zurückgesetzt und die Erkennung endet erst, wenn der Zeitraum abgelaufen ist.</p> <p>Die folgenden Zeiträume sind gültig:</p>

Wert	Beschreibung
	<ul style="list-style-type: none"> hour day week
	Der Standardzeitraum ist hour.

Das folgende Beispiel zeigt den fertigen Skriptabschnitt.

```
commitDetection('powershell_ja3', {
  title:
'PowerShell / BitsAdmin Suspicious Connection',
  description:
"This SSL 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 erscheinen auf der Erkennungskarte ähnlich der folgenden Abbildung:



6. klicken **Speichern** und dann klicken **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 wurde. [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.

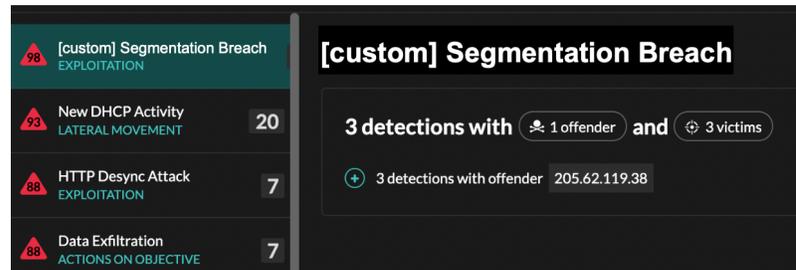
5. klicken **Speichern**.

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

[Eine Regel für Erkennungsbenachrichtigungen erstellen](#). 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 SSL host name is not set, exit
if(SSL.host === null) { return; }

// Continue only if the SSL 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',
        '05af1f5calb87cc9cc9b25185115607d': '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 SSL 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'
            });
        }
    }
}

```

Erkennungen optimieren

Mit der Erkennungsoptimierung können Sie das Rauschen reduzieren und kritische Erkennungen, die sofortige Aufmerksamkeit erfordern, sichtbar machen.

Es gibt zwei Möglichkeiten, Erkennungen zu optimieren: Sie können Optimierungsparameter hinzufügen, die verhindern, dass Erkennungen jemals generiert werden, oder Sie können Optimierungsregeln erstellen, die bestehende Erkennungen basierend auf Erkennungstyp, Teilnehmern oder Erkennungseigenschaften verbergen.

Parameter abstimmen

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 im Zusammenhang mit Gateway-Geräten und Tor-Knoten unterdrücken.

Die Tuning-Parameter werden über das verwaltete [Parameter abstimmen](#) Seite und [vertrauenswürdige Domänen](#) werden von der Seite Network Locations aus verwaltet.

Tuning-Regeln

Mit Optimierungsregeln können Sie Kriterien angeben, die generierte Erkennungen verbergen, die jedoch nur einen geringen Wert haben 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.

Optimierungsregeln verbergen alle vergangenen, aktuellen und zukünftigen Erkennungen und Teilnehmer, die den angegebenen Kriterien entsprechen, und betreffen die folgenden Systembereiche:

- Versteckte Erkennungen führen nicht dazu, dass entsprechende Auslöser und Warnungen ausgeführt werden, solange die Regel aktiviert ist.
- Versteckte Entdeckungen werden in Diagrammen nicht als Erkennungsmarkierungen angezeigt.
- Versteckte Entdeckungen werden nicht auf Aktivitätskarten angezeigt, aber versteckte Teilnehmer werden auf Ermittlungskarten angezeigt.
- Versteckte Erkennungen werden nicht in der Anzahl der Entdeckungen auf verwandten Seiten angezeigt, z. B. auf der Seite „Geräteübersicht“ oder der Seite „Aktivität“.
- Versteckte Entdeckungen und Teilnehmer erscheinen nicht im Executive Report.
- Versteckte Erkennungen sind nicht in E-Mail- und Webhook-Benachrichtigungen enthalten.

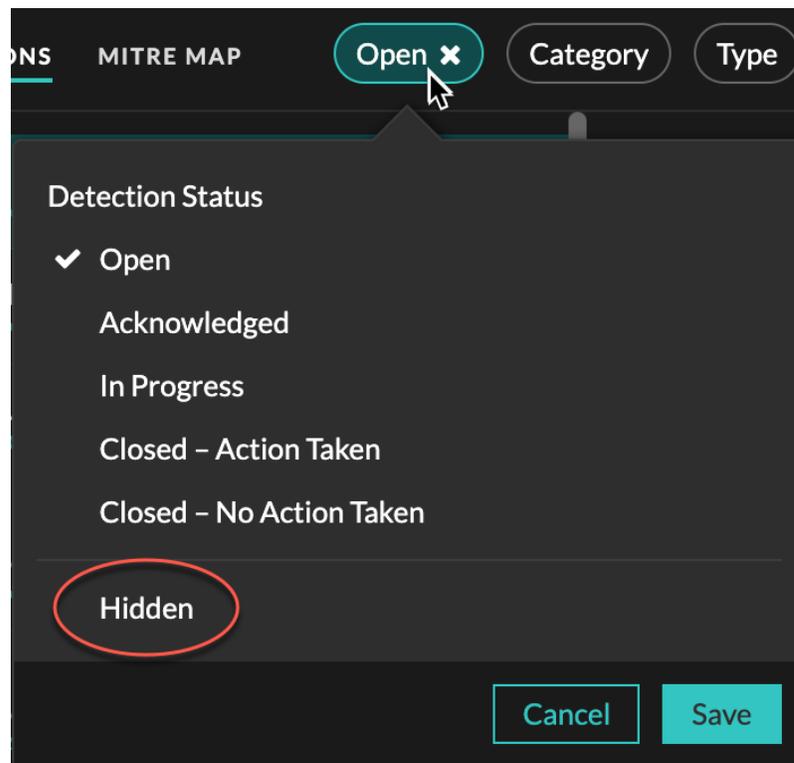


Hinweis Wenn Sie keine Erkennungsmarkierungen für Erkennungen sehen, bestätigen Sie, dass [Erkennungsmarker](#) wurden nicht deaktiviert.

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 Netzwerke 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 Vorgehensweisen

Es ist besser, einen einzelnen Parameter oder eine Regel zu erstellen, die umfassender ist, als mehrere sich überschneidende Parameter und Regeln zu erstellen.

Im Folgenden finden Sie einige Empfehlungen zur Optimierung Ihrer Erkennungseinstellungen:

- Fügen Sie zunächst Optimierungsparameter hinzu, um Erkennungen zu vermeiden, an denen bekannte oder vertrauenswürdige Agenten beteiligt sind. Lesen Sie unbedingt die [Tuning-Parameter](#) und [Netzwerkstandorte](#) Seiten für bestehende Parameter, um Redundanz zu vermeiden.
- Stellen Sie fest, ob Sie alle Erkennungen für einen bestimmten Teilnehmer, z. B. einen Schwachstellenscanner, verbergen möchten, und wählen Sie **Alle Erkennungsarten**. Wenn Sie sich nach Geräterolle verstecken möchten, erhöhen Sie den Bereich auf Gerätegruppe.
- Wenn ein **IP-Adresse oder CIDR-Block** ist in der Dropdownliste Täter oder Opfer ausgewählt. Fügen Sie Einträge zur Liste im Feld IP-Adressen hinzu oder entfernen Sie sie, um den Geltungsbereich der Optimierungsregel zu erweitern oder zu reduzieren.
- Standardmäßig laufen Optimierungsregeln nach 8 Stunden ab. Sie können eine andere Ablaufzeit aus der Dropdownliste auswählen oder eine neue Ablaufzeit auswählen, nachdem Sie eine abgelaufene Regel erneut aktiviert haben, aus der [Tuning-Regeln](#) Seite.
- 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.
- Wenn Sie beim Hinzufügen einer Optimierungsregel ein Gerät identifizieren, das nicht korrekt klassifiziert ist, können Sie [Ändern Sie die Geräterolle](#).
- 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 einen regulären Ausdruck anzugeben und Kriterien für eine gezielte Optimierungsregel hinzuzufügen.
- Wenden Sie das an **Versteckt** Statusfilter für Erkennungen Seite zum Anzeigen von Erkennungen, die [derzeit versteckt](#) durch Tuning-Regeln.

Erfahren Sie, wie [Unterdrücken Sie Erkennungen mit Optimierungsparametern](#) und [Erkennungen mit Optimierungsregeln ausblenden](#).

Unterdrücken Sie Erkennungen mit Optimierungsparametern

Stellen Sie Informationen über Ihre Netzwerkumgebung bereit, damit das ExtraHop-System verhindern kann, dass geringwertige oder redundante Erkennungen jemals generiert werden.

Sie können Tuning-Parameter aus dem hinzufügen [Tuning-Parameter](#) oder [Netzwerk-Lortschaften](#) Seiten, oder Sie können sie direkt von einer Erkennungskarte hinzufügen. Darüber hinaus können Sie IP-Adressbereiche als interne oder externe Bereiche Ihres Netzwerk klassifizieren.

Erfahre mehr über [Erkennungen optimieren](#).

Geben Sie Optimierungsparameter für Erkennungen und Metriken an

Geben Sie Optimierungsparameter an, um die Metriken zu verbessern und zu verhindern, dass Erkennungen mit geringem Wert jemals 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 dann klicken **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 bei regelbasierten Erkennungen ignoriert, da sie zu

Option	Description
Ausgehende Tor-Knoten	<p>redundanten oder häufigen Erkennungen führen können.</p> <p>Wählen Sie diese Option, um potenzielle Probleme mit Gateway-Geräten wie Firewalls, Routern und NAT-Gateways zu identifizieren.</p> <p>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.</p> <p>Wählen Sie diese Option, um Erkennungen bei ausgehenden Verbindungen zu bekannten Tor-Knoten zu identifizieren, wenn Ihre Umgebung erheblichen ausgehenden Tor-Traffic beobachtet.</p>
Eingehende Tor-Knoten	<p>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.</p> <p>Wählen Sie diese Option, um Erkennungen bei eingehenden Verbindungen von bekannten Tor-Knoten zu identifizieren, wenn Ihre Umgebung erheblichen eingehenden Tor-Traffic beobachtet.</p>
Beschleunigte Beaconsing-Erkennung	<p>Standardmäßig erkennt das ExtraHop-System potenzielle Beaconsing-Ereignisse über HTTP und SSL.</p> <p>Wählen Sie diese Option, um Beaconsing-Ereignisse schneller als die Standarderkennung zu erkennen.</p> <p>Beachten Sie, dass die Aktivierung dieser Option die Erkennung von Beaconsing-Ereignissen verbessern kann, die nicht böswillig sind.</p>
IDS-Erkennungen	<p>Standardmäßig sind ExtraHop-Systeme mit verbundenen Sensoren des Intrusion Detection Systems (Intrusion Detection System)  generieren Sie nur Erkennungen für den Datenverkehr innerhalb Ihres Netzwerk. Wählen Sie diese Option, um IDS-Erkennungen für Datenverkehr zu generieren, der von einem Externer Endpunkt eingeht.</p> <p>Beachten Sie, dass die Aktivierung dieser Option die Anzahl der IDS-Erkennungen erheblich erhöhen kann.</p>
Privilegierte Active Directory Directory-Konten	<p>Geben Sie reguläre Ausdrücke (Regex) an, die privilegierten Active Directory-Konten in Ihrer Umgebung entsprechen. Die Parameterliste enthält eine Standardliste regulärer Ausdrücke für</p>

Option	Description
	<p>häufig verwendete privilegierte Konten, die Sie bearbeiten können.</p> <p>Das ExtraHop-System identifiziert privilegierte Konten und verfolgt die Kontoaktivitäten in Kerberos-Datensätzen und -Metriken.</p>
Zulässige öffentliche DNS-Server	<p>Geben Sie öffentliche DNS-Server an, die in Ihrer Umgebung zulässig sind und die von regelbasierten Erkennungen ignoriert werden sollen.</p> <p>Geben Sie eine gültige IP-Adresse oder einen gültigen CIDR-Block an.</p>
Zulässige HTTP CONNECT-Ziele	<p>Geben Sie URIs an, auf die Ihre Umgebung über die HTTP CONNECT-Methode zugreifen kann.</p> <p>URIs müssen formatiert sein als <code><hostname>:<port number></code>. Wildcards und Regex werden nicht unterstützt.</p> <p>Wenn Sie keinen Wert angeben, werden Erkennungen, die auf diesem Parameter basieren, nicht generiert.</p>

4. klicken **Speichern**.

Nächste Schritte

klicken **Erkennungen** vom oberen Navigationsmenü zu [Erkennungen anzeigen](#).

Fügen Sie einen Tuning-Parameter oder eine vertrauenswürdige Domain von einer Erkennungskarte hinzu

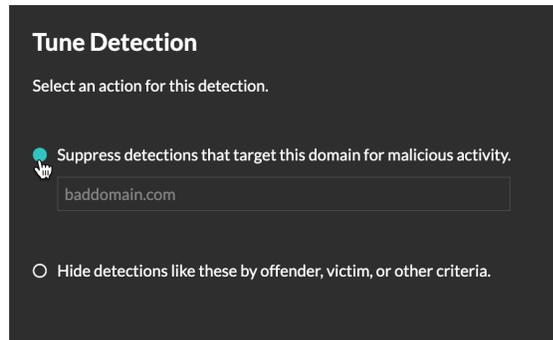
Wenn Sie auf eine Erkennung mit geringem Wert stoßen, können Sie Optimierungsparameter und vertrauenswürdige Domänen direkt von einer Erkennungskarte hinzufügen, um zu verhindern, dass ähnliche Erkennungen generiert werden.

Bevor Sie beginnen

Benutzer müssen über Vollschreibzugriff oder höher verfügen [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 **Aktionen** aus der unteren linken Ecke der Erkennungskarte.
4. klicken **Erkennung abstimmen....**

Wenn der Erkennungstyp mit einem Optimierungsparameter verknüpft ist, wird die Option angezeigt, die Erkennung durch Hinzufügen eines Optimierungsparameters oder einer vertrauenswürdigen Domäne zu unterdrücken. Wenn der Erkennung kein Tuning-Parameter zugeordnet ist, können Sie [die Erkennung mit einer Tuning-Regel ausblenden](#).



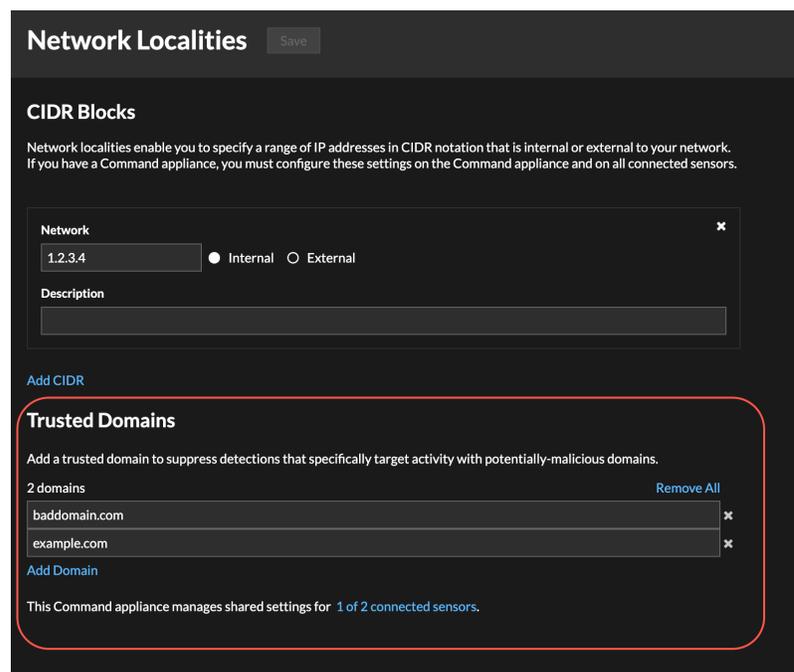
5. Klicken Sie auf **Erkennungen unterdrücken...** Option und klicken **Speichern**. Die Bestätigung „Tuning-Parameter hinzugefügt“ wird angezeigt und der neue Parameter wird dem **Tuning-Parameter** Seite. Für vertrauenswürdige Domänen wird die Domain hinzugefügt unter **Vertrauenswürdige Domains** auf der Seite Network Localities.

Eine vertrauenswürdige Domain hinzufügen

Bestimmte Erkennungen werden generiert, wenn ein Gerät eine Verbindung zu einer externen Domain herstellt. Wenn Sie wissen, dass eine Domain legitim ist, fügen Sie sie der Liste der vertrauenswürdigen Domains hinzu. Künftige Erkennungen, die auf böartige Domainaktivitäten abzielen, werden für diese Domain unterdrückt.

Für Erkennungen, denen eine Domäne zugeordnet ist, können Sie auch [fügen Sie eine vertrauenswürdige Domain direkt von einer Erkennungskarte hinzu](#).

 **Hinweis** Wenn Ihr ExtraHop-System über eine Konsole verfügt und dieses System für die Verwaltung von Tuning-Parametern konfiguriert ist, gelten diese vertrauenswürdigen Domänen für alle angeschlossenen 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 dann klicken **Netzwerk-Landschaften**.
3. Unter Vertrauenswürdige Domains, klicken **Domain hinzufügen**.
4. Geben Sie einen vertrauenswürdigen Domänenname ein.
Der Domänenname muss exakt mit der Domain übereinstimmen, die Sie unterdrücken möchten. Wildcards und Regex werden nicht unterstützt. Um mehr als einen vertrauenswürdigen Domänenname hinzuzufügen, klicken Sie auf **Domain hinzufügen**. Geben Sie pro Feld einen einzelnen Domänenname ein.
5. klicken **Speichern**.

Erkennungen mit Optimierungsregeln ausblenden

Mit Optimierungsregeln können Sie Erkennungen ausblenden, die bestimmten Kriterien entsprechen.

Um die Erstellung redundanter Regeln zu vermeiden, stellen Sie sicher, dass Sie dem ExtraHop-System zunächst Informationen über Ihre Netzwerkumgebung hinzufügen, indem Sie [Angaben von Tuning-Parametern](#).

Erfahre mehr über [Erkennungen optimieren](#).

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.

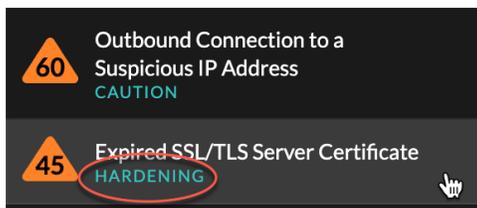
Bevor Sie beginnen

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](#).

Fügen Sie auf der Seite „Tuning-Regeln“ eine Tuning-Regel hinzu

Erstellen Sie Optimierungsregeln, um Erkennungen nach Erkennungstyp, Teilnehmer oder bestimmten Erkennungseigenschaften 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 auf das Symbol Systemeinstellungen  und dann klicken **Tuning-Regeln**.
3. klicken **Erstellen**.
4. Spezifizieren [Kriterien Abstimmung Optimierungsregeln](#) und klicken **Speichern**.

Die Regel wird der Tabelle Tuning-Regeln hinzugefügt. Erfahre mehr über [Tuning-Regeln](#).

- Spezifizieren Sie die [Kriterien Abstimmung Optimierungsregeln](#) und klicken **Erstellen**.

Die Regel wird der Seite Tuning-Regeln hinzugefügt. Erfahre mehr über [Verwaltung von Tuning-Regeln](#).

Kriterien für Optimierungsregeln

Wählen Sie eines der folgenden Kriterien aus, um zu bestimmen, welche Erkennungen durch eine Optimierungsregel ausgeblendet werden.

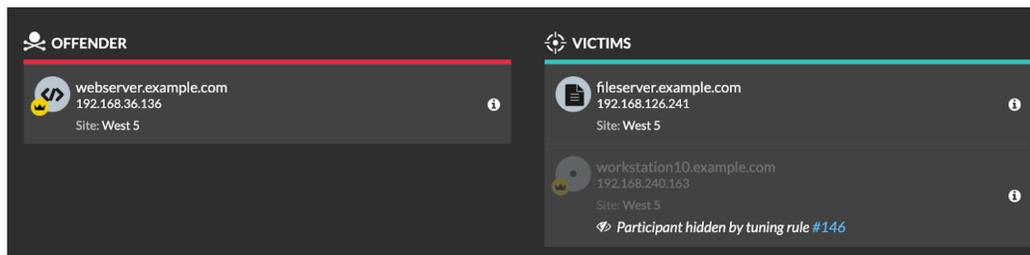
Art der Erkennung

Sie können je nach Systemmodul eine Optimierungsregel erstellen, die für einen einzelnen Erkennungstyp gilt, oder festlegen, dass die Regel für alle Sicherheits- oder Leistungserkennungstypen gilt. Regeln, die alle Arten von Sicherheitserkennung umfassen, sind in der Regel Aktivitäten im Zusammenhang mit Schwachstellenscannern vorbehalten.

Teilnehmer

Identifizieren Sie die Teilnehmer an einer Optimierungsregel anhand der IP-Adresse, Gerät Gerätenamens oder [Netzwerklokalität](#). Sie können Teilnehmer auch anhand der vom ExtraHop-System identifizierten Rollen ausblenden. Wenn das ExtraHop-System beispielsweise einen externen Scandienst identifiziert, können Sie Erkennungen für diesen bestimmten Dienst ausblenden oder eine Optimierungsregel erstellen, die alle externen Scandienste ausblendet.

Bei Erkennungen mit mehreren Tätern können Sie eine Liste mit IP-Adressen oder CIDR-Blöcken hinzufügen oder auf eine Gerätegruppe verweisen. Sie können auch Optimierungsregeln erstellen, die einen einzelnen Teilnehmer verbergen, ohne eine gesamte Erkennung auszublenden.



Sie können wählen, ob Sie alle Täter oder alle Opfer verstecken möchten. So können Sie beispielsweise den Täter bei einer Noisy-Scan-Erkennung verstecken, unabhängig davon, wer am Opfer beteiligt ist.

Erkennungseigenschaften

Erstellen Sie eine Optimierungsregel, die Erkennungen durch eine bestimmte Eigenschaft verbirgt. Sie können beispielsweise seltene SSH-Port-Erkennungen für eine einzelne Portnummer oder Datenexfiltration in S3-Bucket-Erkennungen für einen bestimmten S3-Bucket ausblenden.

Criteria

Detection Type

Data Exfiltration to S3 Bucket

All security detection types

Offender

Device group: Accepted External Connections ▼

Property

S3 Bucket

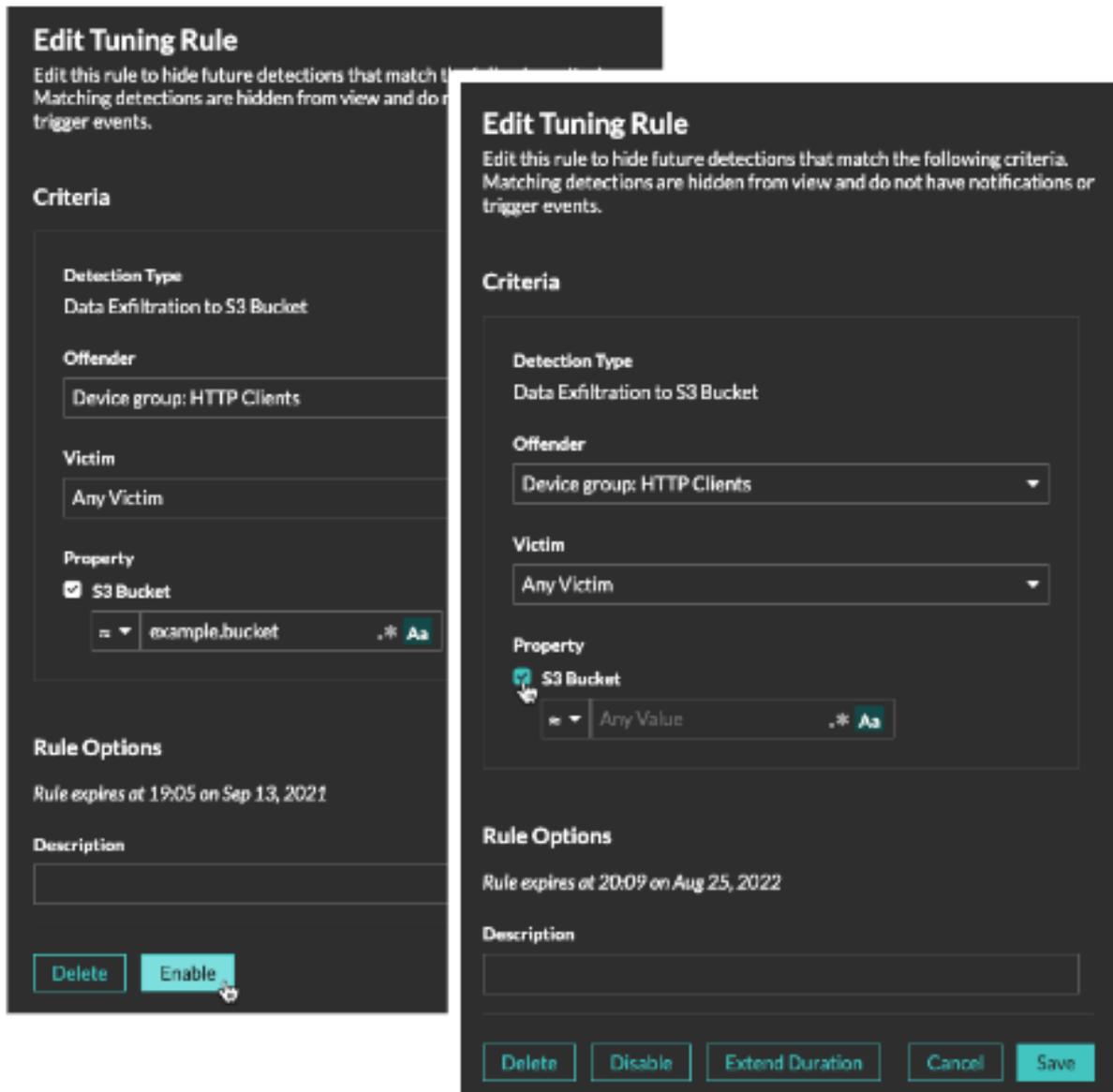
≈ ▼ example-S3bucket .* Aa

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**.

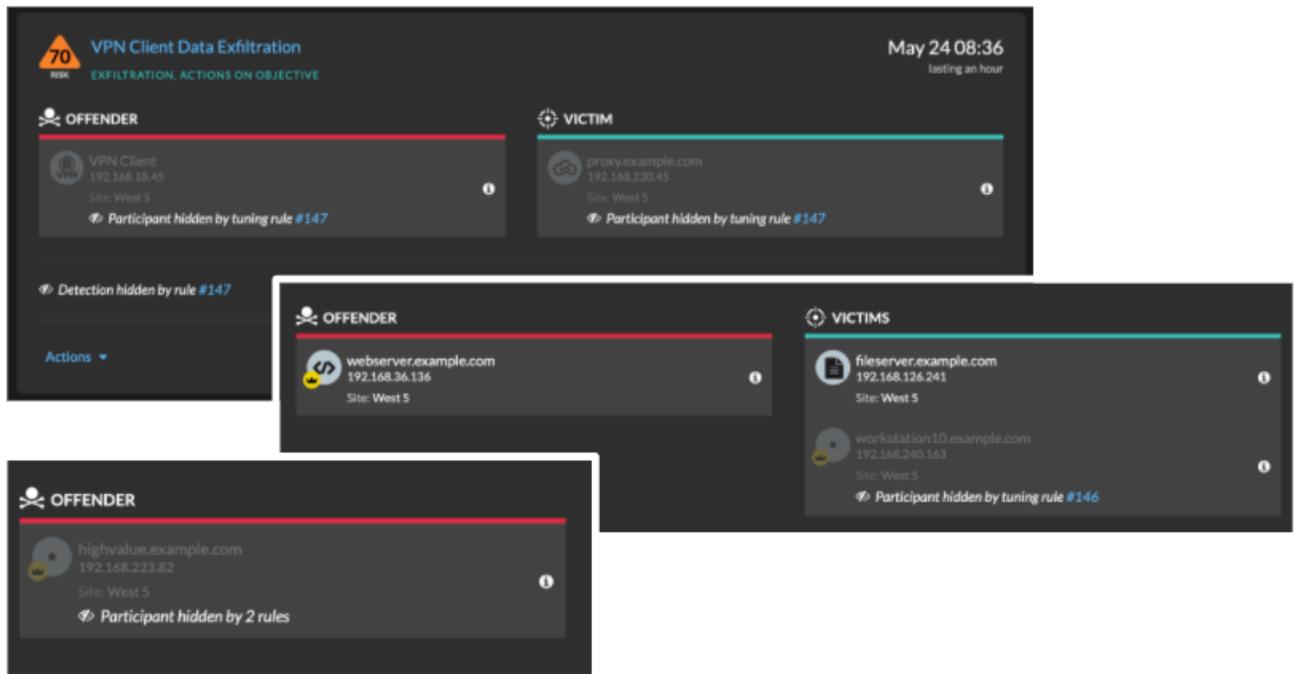
Klicken Sie auf eine Tuning-Regel in der Tuning-Regeln Tabelle zum Öffnen der Optimierungsregel bearbeiten tafel. Aktualisieren Sie Teilnehmer, Regelkriterien oder Eigenschaften, um den Geltungsbereich der Regel anzupassen. Klicken Sie auf die Schaltflächen am unteren Rand des Fensters, um eine Regel 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.



Härtungserkennungen filtern und optimieren

Erkennungen in der Kategorie Härtung tragen dazu bei, das Risiko einer Ausnutzung zu verringern. Sie können eine große Anzahl von Hardening-Erkennungen auswählen, indem Sie die Erkennungsseite filtern und Abstimmung.

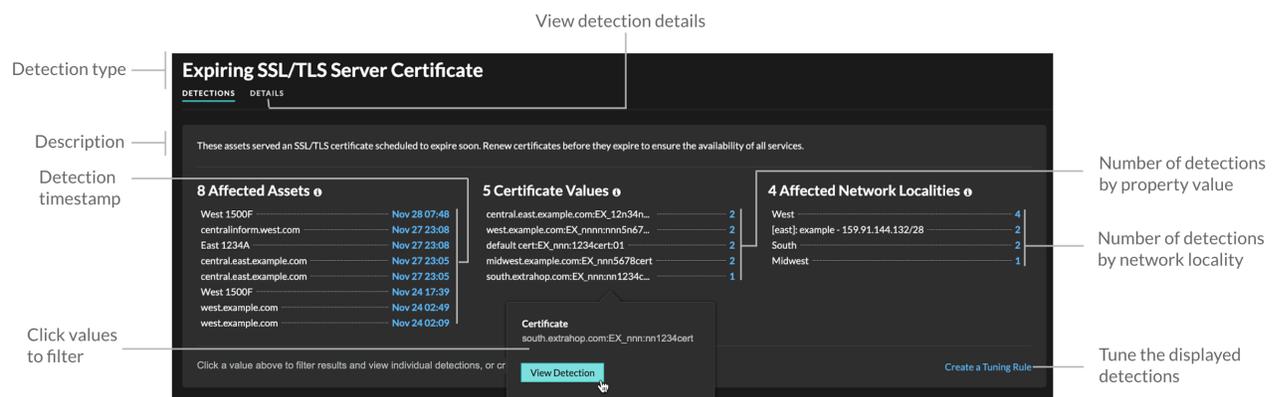
Bevor Sie beginnen

Benutzern muss eine Genehmigung erteilt werden [Privilegien](#) um Erkennungen anzuzeigen, und Sie müssen über vollständige Schreibrechte oder höhere Rechte verfügen, um eine Optimierungsregel zu erstellen.

Erfahre mehr über [Erkennungen optimieren](#).

Erfahre mehr über [Abstimmung von Best Practices](#).

Klicken Sie auf eine Härtungserkennung aus dem [Erkennungen](#) Seite, um die Zusammenfassung zu sehen. Zusammenfassungen der Hardening-Erkennung identifizieren den Erkennungstyp, die Ressourcen, die an Erkennungen dieses Typs beteiligt sind, die Erkennungseigenschaften und die Netzwerkstandorte, die die betroffenen Ressourcen enthalten.



Klicken Sie auf einen beliebigen Asset-, Objekt- oder Netzwerk-Lokalitätswert, um einzelne Erkennungen anzuzeigen, die mit diesem Wert verknüpft sind.

Betroffene Vermögenswerte

Eine Liste von Assets, die an Hardening-Erkennungen des ausgewählten Typs beteiligt sind. Die Liste der betroffenen Vermögenswerte ist nach dem Zeitpunkt sortiert, zu dem die Erkennung zuletzt stattgefunden hat.

Immobilienwerte

Eine Liste der wichtigsten Eigenschaftswerte, die dem Erkennungstyp zugeordnet sind. Beispielsweise listet der Erkennungstyp Weak Cipher Suite die Cipher Suites auf, auf die bei Erkennungen verwiesen wird, und der Erkennungstyp Ablaufendes SSL/TLS-Serverzertifikat listet Zertifikate auf, deren Ablauf geplant ist. Die Liste der Eigenschaftswerte ist nach der Anzahl der Erkennungen sortiert, die den Eigenschaftswert enthalten.

Betroffene Netzwerkstandorte

Eine Liste von Netzwerklokalitäten, die Hardening-Erkennungen des ausgewählten Typs enthalten. Die Liste der betroffenen Netzwerke ist nach der Anzahl der Entdeckungen in der Netzwerklokalität sortiert.

Indem Sie die Ergebnisse nach einer einzelnen Asset, Immobilie oder Lokalität filtern, können Sie Erkennungen identifizieren, die sich auf kritische Systeme auswirken oder [eine Optimierungsregel erstellen](#). Dadurch werden Erkennungen mit geringem Wert ausgeblendet, die den gefilterten Ergebnissen ähneln.

Ticket-Tracking für Erkennungen konfigurieren

Mit der Ticketverfolgung können Sie Tickets, Alarme oder Fälle in Ihrem Work-Tracking-System mit ExtraHop-Erkennungen verbinden. Jedes Ticketsystem von Drittanbietern, das Open Data Stream (ODS) -Anfragen akzeptieren kann, wie Jira oder Salesforce, kann mit ExtraHop-Erkennungen verknüpft werden.

Bevor Sie beginnen

- Sie benötigen Zugriff auf ein ExtraHop-System mit einem Benutzerkonto, das [Rechte für die System- und Zugriffsadministration](#).
- Sie müssen mit dem Schreiben von ExtraHop-Triggern vertraut sein. siehe [Auslöser](#) 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-Skripts vertraut sein und über einen gültigen API-Schlüssel verfügen, um die folgenden Verfahren ausführen zu können. siehe [Generieren Sie einen API-Schlüssel](#).

Aktivieren Sie die Ticketverfolgung und geben Sie eine URL-Vorlage an

Sie müssen die Ticketverfolgung aktivieren, bevor REST-API-Skripts Ticketinformationen auf dem ExtraHop-System aktualisieren können. Geben Sie optional eine URL-Vorlage an, die dem Ticket in Ihrem Ticketsystem einen HTML-Link auf der Erkennungskarte hinzufügt.

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. Wählen **Verfolgen Sie Erkennungen von einem externen Ticketsystem**.
4. Optional: Geben Sie im Feld URL 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`. Die `$ticket_id` Die Variable wird durch die der Erkennung zugeordnete Ticket-ID ersetzt.

Today 14:00
lasting an hour

83
RISK

LATERAL MOVEMENT

Status: **CLOSED**

Ticket ID: **EX-4437**

Assignee: **hopuser**

Suspicious CIFS Client File Share Access on AccountingLaptop

This device sent an excessive number of read requests over the Common Internet File System (CIFS) protocol. This anomaly indicates that the device might be compromised and is preparing files for data exfiltration.

Server linked to this anomaly:

- corpshare.example.com (192.168.6.179)

AccountingLaptop Activity Map

CIFS Metric	6-hour Snapshot	Peak Value	Expected Range	Deviation
Reads		1.13 K	0-1	112,500%

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
  }
};

```

- 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](#).

- 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);
```

Senden Sie Ticketinformationen über die REST-API an Erkennungen

Nachdem Sie in Ihrem Ticket-Tracking-System einen Auslöser zum Erstellen von Tickets für Erkennungen konfiguriert haben, können Sie die Ticketinformationen auf Ihrem ExtraHop-System über die REST-API aktualisieren.

Ticketinformationen werden unter Erkennungen auf der Seite Erkennungen im ExtraHop-System angezeigt. Weitere Informationen finden Sie in der [Erkennungen](#) Thema.

Das folgende Python-Beispielskript verwendet 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 Überprüfung des SSL-Zertifikats 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:

The screenshot displays a security alert titled "Suspicious CIFS Client File Share Access on AccountingLaptop". It indicates that the device sent an excessive number of read requests over the CIFS protocol, suggesting a potential compromise for data exfiltration. The alert is linked to the server `corpshare.example.com (192.168.6.179)`. On the left, the ticket status is "CLOSED", the ID is "EX-4437", and the assignee is "hopuser". A table below provides a 6-hour snapshot of CIFS Reads, showing a peak value of 1.13 K, an expected range of 0-1, and a significant deviation of 112,500%.

CIFS Metric	6-hour Snapshot	Peak Value	Expected Range	Deviation
Reads		1.13 K	0-1	112,500%

Status

Der Status des Tickets, das mit der Erkennung verknüpft ist. Die Ticketverfolgung unterstützt die folgenden Status:

- Neu
- In Bearbeitung
- 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.

Bevollmächtigter

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.

The screenshot shows a detection alert with the following details:

- Risk Level:** 65 EXPLOITATION
- Time:** Today 09:00 (lasting an hour)
- Buttons:** Acknowledge, Hide Detections Like This
- Title:** Spike in SSH Server Sessions
- Description:** webserv-031.sea.example.com received an unusually large number of short SSH sessions, which could be caused by planned maintenance, or could indicate a potential brute force attack. The risk score increased because of device importance.
- Offender:** workstation-05.sea.example.com (192.168.123.113)
- Victim:** webserv-031.sea.example.com (192.168.80.9)
- SSH Metric:** Short Sessions
- 6h Snapshot:** A line graph showing a spike in short sessions.
- 1hr Peak Value:** 248
- Expected Range:** 0-1
- Deviation:** 24,700%

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.

Investigate Servers

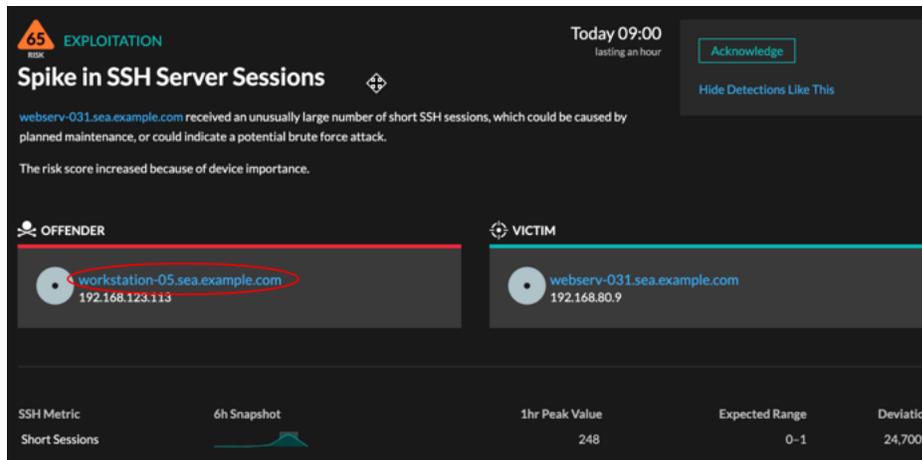
View the targeted servers

	Server IP	Host	Requests ↓
	192.168.136...	Citrix	7,947
	192.168.133...	Example-05	7,817
	192.168.254...	exds1	7,231
	192.168.227...	Citrix-55	6,195

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 einen Erkennungsscan erhalten, können Sie herausfinden, ob dem mit dem Scan verknüpften Gerät 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

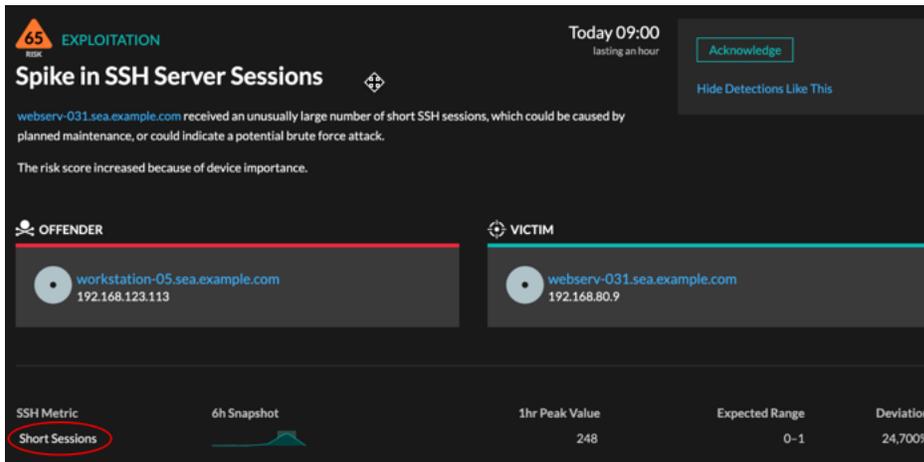
Klicken Sie auf das Activity Map-Symbol neben einem Gerätenamen, um die Geräteverbindungen nach Protokoll während der Erkennung anzuzeigen. Wenn Sie beispielsweise eine laterale Bewegung Bewegungserkennung erhalten, können Sie herausfinden, ob das verdächtige Gerät über ein Fernsteuerungsprotokoll Verbindungen mit 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 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 Erkennung durch einen Aufklärungsscan erhalten, können Sie im Detail herausfinden, welche Client-IP-Adressen während der Erkennung mit der ungewöhnlich hohen Anzahl von 404-Statuscodes verknüpft wurden.

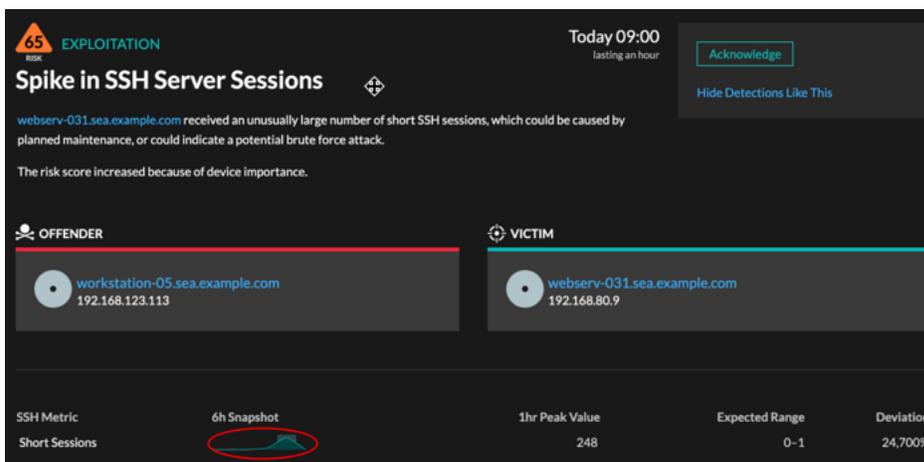


Verfügbarkeit

Die Drilldown-Option ist für Erkennungen verfügbar, die mit Topset 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, das Sie dann zu einem Dashboard zur Überwachung hinzufügen können. 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.

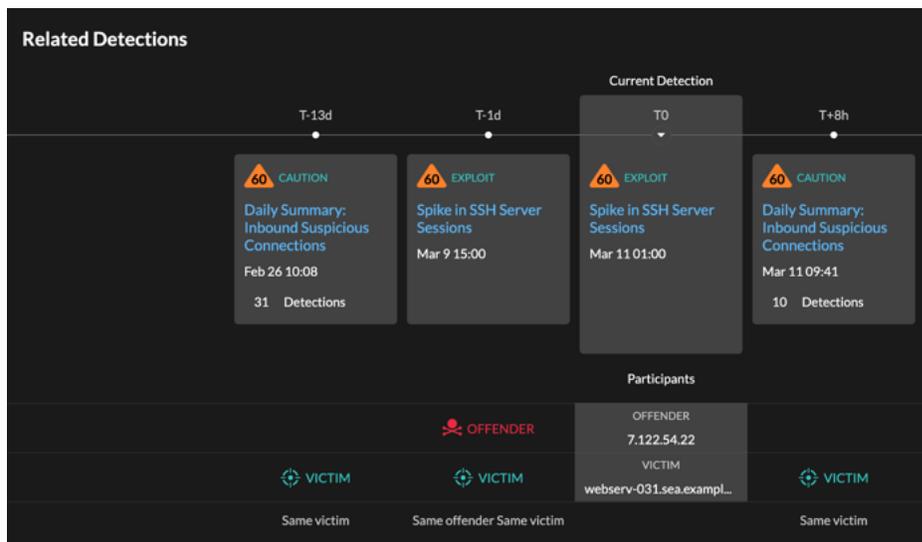


Verfügbarkeit

Die Sparkline-Option ist für Erkennungen verfügbar, die mit Metriken verknüpft waren und eine Dauer von mehr als einer Stunde hatten. Für 1-Sekunden-Metriken ist eine Sparkline verfügbar, wenn die Dauer mehr als 30 Sekunden betrug.

Verwandte Erkennungen

Klicken Sie auf verwandte Erkennungen, um Einblicke in verdächtiges Verhalten und neue Angriffe bei mehreren Erkennungen mit gemeinsamen Teilnehmern zu erhalten. Beispielsweise könnte ein Opfer bei der aktuellen Erkennung, das als Täter an einer späteren Erkennung beteiligt ist, darauf hinweisen, dass das Gerät kompromittiert wurde. Sie können zugehörige Erkennungsdetails anzeigen, um festzustellen, ob die Erkennungsereignisse ähnlich sind, und um zu sehen, welche anderen Geräte beteiligt sind.



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

Klicken Sie auf ein rotes Kamerasymbol um auf detaillierte Bedrohungsinformationen über einen Bedrohungsindikator zuzugreifen.

Threat Intelligence liefert bekannte Daten über verdächtige IP-Adressen, Hostnamen und URIs, anhand derer Risiken für Ihr Unternehmen identifiziert werden können. Diese Datensätze, die als Bedrohungssammlungen bezeichnet werden, sind standardmäßig in Ihrem Reveal (x) -System und in der Sicherheits-Community aus kostenlosen und kommerziellen Quellen verfügbar.

Verfügbarkeit

Threat Intelligence muss auf Ihrem Reveal (x) -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.

NETWORK INFRASTRUCTURE Mar 18 00:00
lasting 6 hours [Acknowledge](#)

DNS Server Errors

[Hide Detections Like This](#)

What caused this detection?
dns-07.sea.example.com sent an excessive number of the DNS NXDOMAIN/QUERY:PTR error, which indicates that domain name lookups failed.

What should I investigate?

OFFENDER

ntp-01.sea.example.com
192.168.128.109
EDA: eda.sea.l.example.com

VICTIM

dns-07.sea.example.com
192.168.5.253
EDA: eda.sea.l.example.com

DNS Responses by Response Code	12h Snapshot	1hr Peak Value	Expected Range	Deviation
NXDOMAIN/QUERY:PTR		3.23 K	0-143	2,159%

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.

Investigate Servers

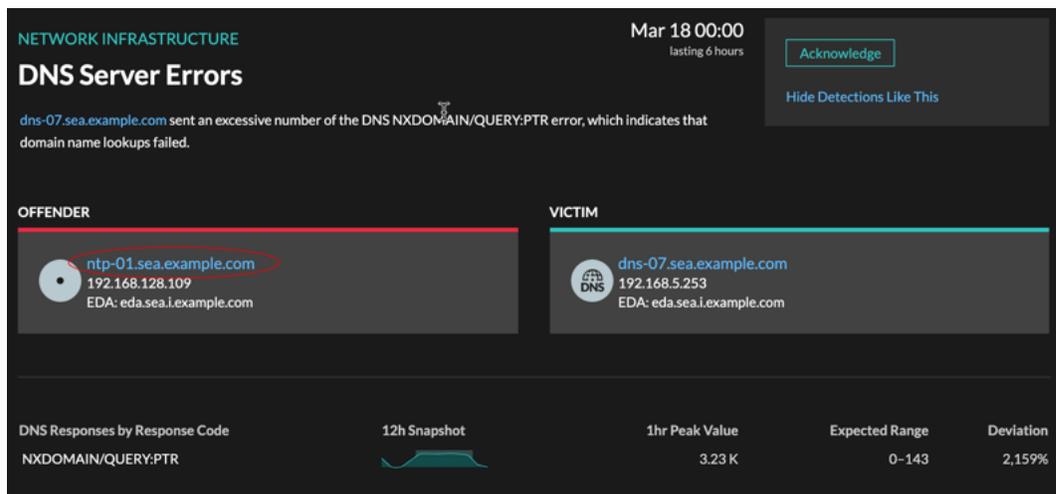
View the targeted servers

	Server IP	Host	Requests ↓
	192.168.136...	Citrix	7,947
	192.168.133...	Example-05	7,817
	192.168.254...	exds1	7,231
	192.168.227...	Citrix-55	5,495

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

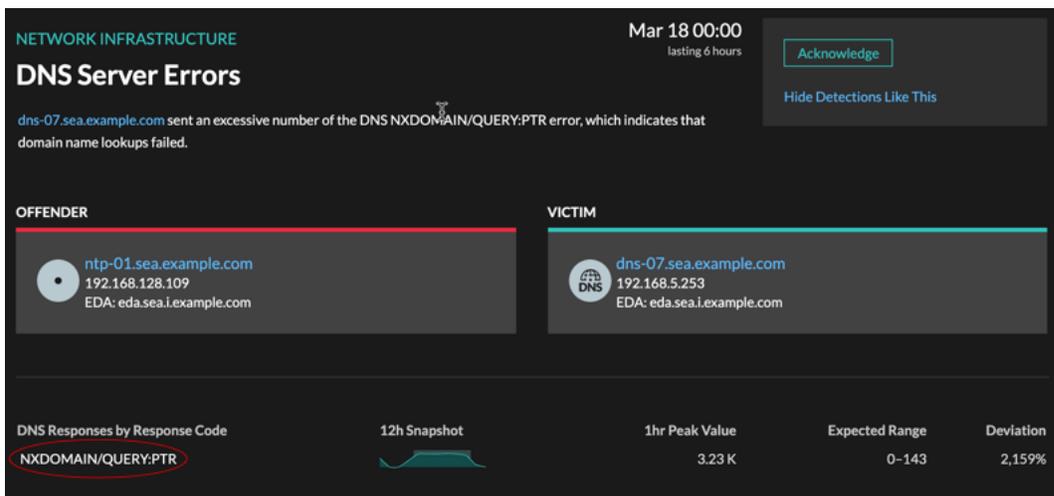
Klicken Sie auf das Activity Map-Symbol neben einem Gerätenamen, um die Geräteverbindungen nach Protokoll während der Erkennung anzuzeigen. Wenn Sie beispielsweise eine Erkennung von LDAP-Authentifizierungsfehlern erhalten, können Sie eine Aktivitätsdiagramm erstellen, um zu erfahren, welche Geräte während 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.

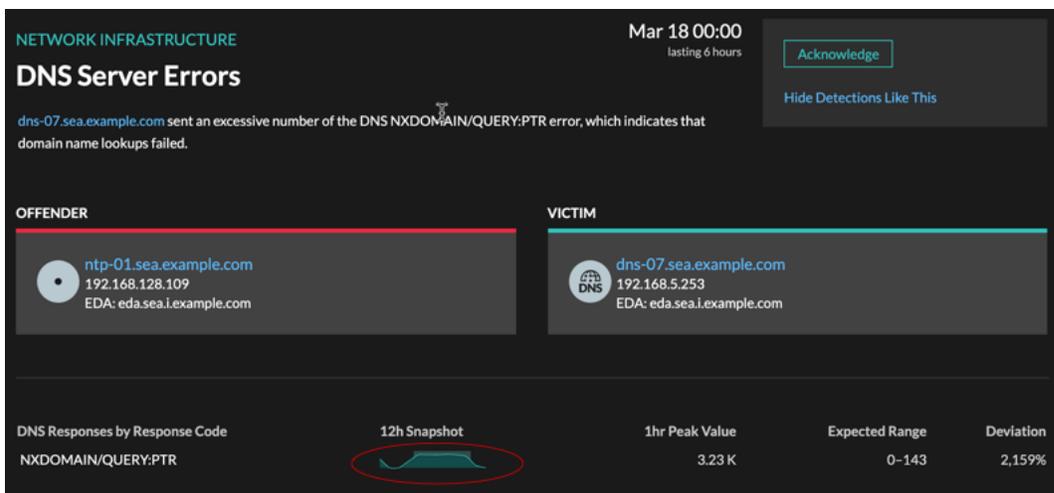


Verfügbarkeit

Die Drilldown-Option ist für Erkennungen verfügbar, die mit Topset 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.



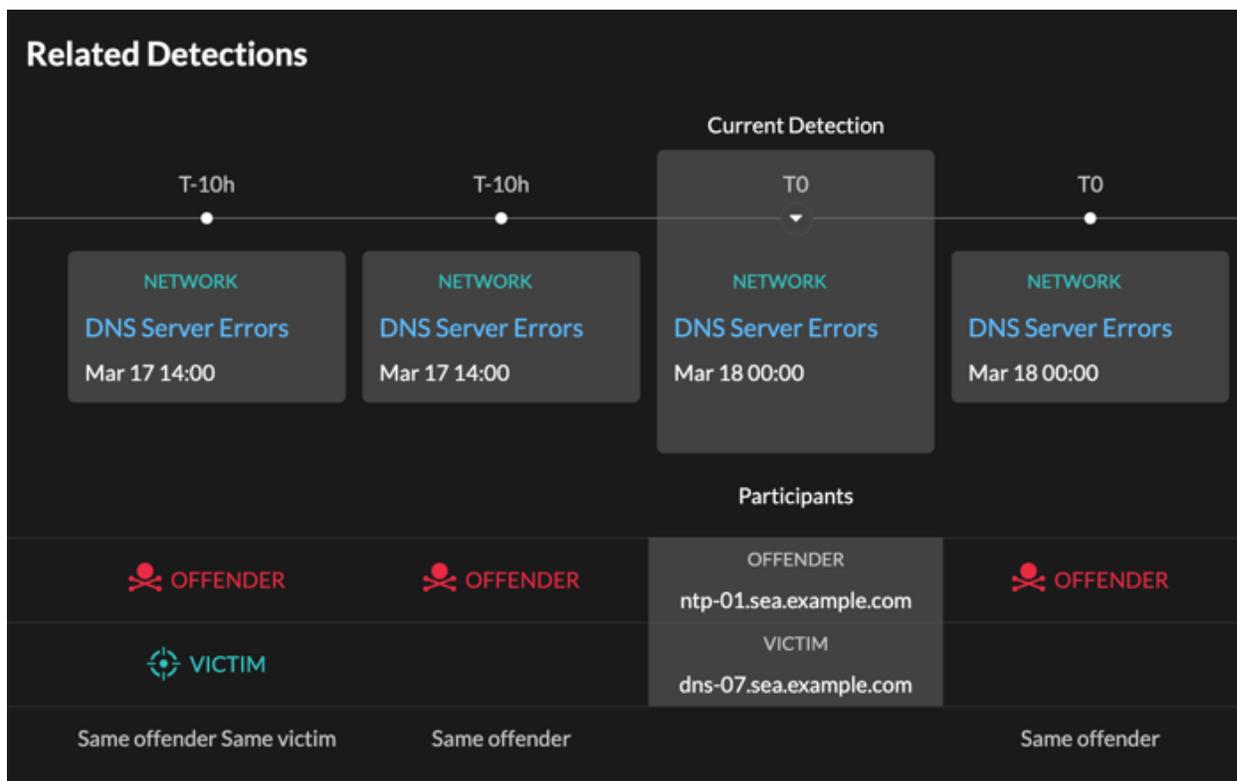
Verfügbarkeit

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

Threat Briefings bieten Hinweise zu potenziellen Bedrohungen für Ihr Netzwerk.

In den Bedrohungsinformationen werden die folgenden Ereignisse behandelt:

- Branchenweite Sicherheitsereignisse, bei denen das ExtraHop-System Erkennungen im Zusammenhang mit bekannten Sicherheitslücken aufdeckt.
- Sicherheitsanalyse-Briefings, die maschinelle Lernanalysen anbieten, die speziell auf Ihr Netzwerk zugeschnitten sind.
- (Nur Reveal (x) 360.) Retrospektive Threat Analysis Briefings, in denen neue Bedrohungsindikatoren in aktualisierten, von ExtraHOP kuratierten Bedrohungsinformationen erkannt werden.

Threat Briefings enthalten Erkennungen von Scans, Exploits und Indicators of Compromise (Kompromittierungsindikatoren), die im Zusammenhang mit der Bedrohung stehen. Die Informationen in den einzelnen Briefings variieren je nach Art der Bedrohung. Die Informationen im Zusammenhang mit dem Briefing werden in der Cloud aktualisiert, sobald Details über das Kompromittierungsindikatoren, mögliche Angriffsvektoren und bekannte Risiken bekannt werden.

Bedrohungsinformationen sind 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:

- [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 es wird eine Benachrichtigungs-E-Mail gesendet, wenn das Briefing aktualisiert wird. Ältere Briefings finden Sie im Bereich Archiviert auf der Seite Threat Briefing. klicken **Briefing wiederherstellen** auf der Detailseite, um das Briefing wieder in den Bereich Aktiv der Seite Threat Briefing zu verschieben.

Benachrichtigungsregel Bedrohungsübersicht Bedrohungsinformationen erstellen

Sie können eine Benachrichtigungsregel erstellen, die eine Empfängerliste per E-Mail benachrichtigt, 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 Zugriff auf das NDR-Modul gewährt werden und sie müssen Vollschreibzugriff haben [Privilegien](#)  oder höher, um die Aufgaben in diesem Handbuch zu erledigen.
 - 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 erlaubten 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 dann klicken **Regeln für Benachrichtigungen**.
 3. klicken **Erstellen**.

4. Geben Sie im Feld Name einen eindeutigen Namen für die Benachrichtigungsregel ein.
5. Fügen Sie im Feld Beschreibung Informationen zur Benachrichtigungsregel hinzu.
6. Wählen Sie im Abschnitt Ereignistyp **Bedrohungsinformation**.
7. Geben Sie einzelne E-Mail-Adressen an, getrennt durch ein Komma.
8. Klicken Sie im Bereich Optionen auf **Kontrollkästchen „Benachrichtigungsregel aktivieren“** um die Benachrichtigung zu aktivieren.
9. klicken **Speichern**.

Bedrohungsinformationen

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

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

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

Sammlungen von Bedrohungen

Das ExtraHop-System unterstützt Bedrohungssammlungen aus verschiedenen Quellen.

Da Cyber-Bedrohungsinformationen von der Community gesteuert werden, gibt es viele externe Quellen für die Erfassung von Bedrohungen. Daten aus diesen Sammlungen können in ihrer Qualität oder Relevanz für Ihre Umgebung variieren. Um die Genauigkeit zu wahren und das Rauschen zu reduzieren, empfehlen wir Ihnen, Ihre Uploads auf hochwertige Threat-Intelligence-Daten zu beschränken, die sich auf eine bestimmte Art von Eindringversuchen konzentrieren, z. B. eine Sammlung für Malware und eine andere Sammlung für Botnetze.

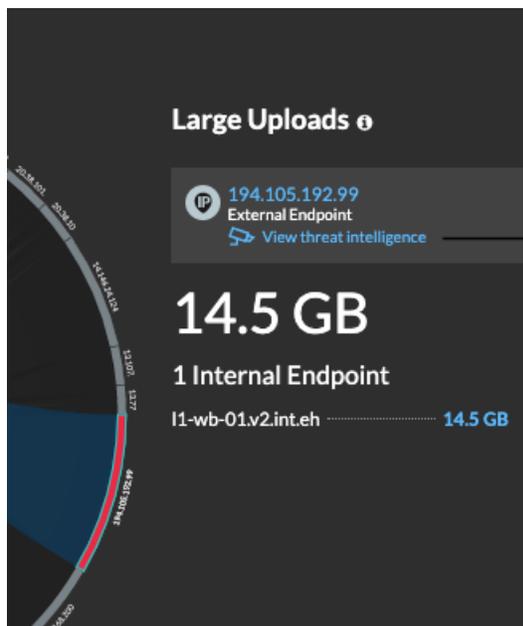
Von ExtraHop kuratierte Bedrohungssammlungen werden alle 12 Stunden aktualisiert. Verdächtige IP-Adressen, Domains, Hostnamen und URIs werden in Systemdiagrammen und Aufzeichnungen angezeigt.

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

Bedrohungssammlungen von [Partnerintegrationen müssen in ExtraHop Reveal \(x\) 360 importiert werden](#).

Untersuchung von Bedrohungen

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



Click links or camera icons to view details.

Threat Intelligence

Suspicious Endpoint 194.105.192.99

Address:
Address: 194.105.192.99 | Danger Assessment: 99 | False Positives: 0 | owner: Demons

Type	IP Malware Watchlist
Confidence	85
Collection	KnownThreats
Producer	Demonstration List of Known Malware IP addresses
Added	May 21, 2018 6:50 PM PDT

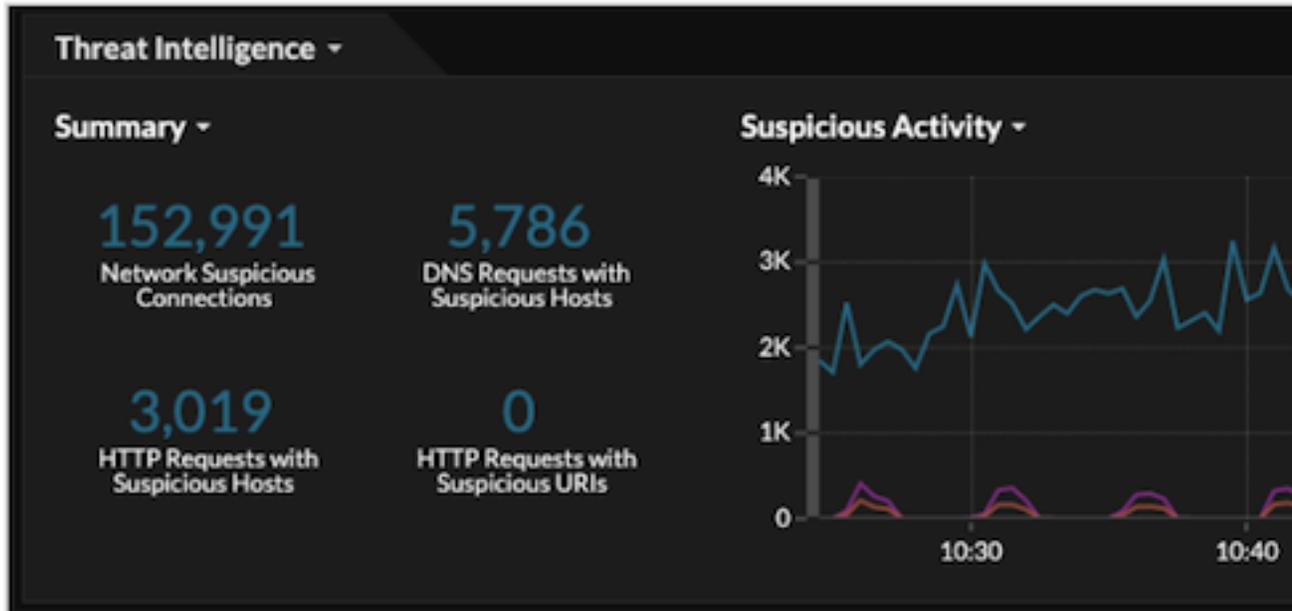
- Wenn die Bedrohungssammlung hinzugefügt oder aktualisiert wird, nachdem das System die verdächtige Aktivität beobachtet hat, werden Bedrohungsinformationen erst dann auf diese IP-Adresse, diesen Hostnamen oder diese URI angewendet, wenn die verdächtige Aktivität erneut auftritt.
- Wenn eine von ExtraHop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

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

Dashboard zur Erhöhung der Sicherheit

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

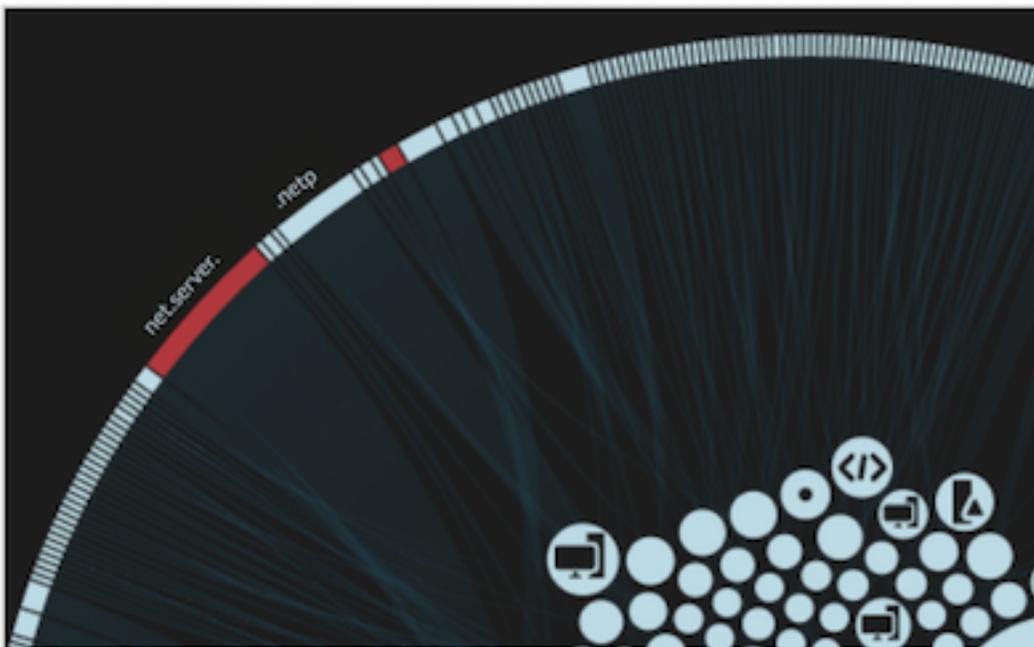
Sie Details zu der Metrik aufrufen oder Datensätze für zugehörige Transaktionen



abfragen.

Perimeter im Überblick

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



Erkennungen

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

60
RISK CAUTION

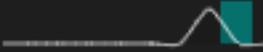
Outbound Suspicious Connection

This client connected to a device with a suspicious IP address. This IP address is considered found in your Reveal(x) system. Investigate to determine if this client is the victim of a malw

OFFENDER

 **work-031.sea.example.com**
192.168.6.120

TCP Metric 5m Snapshot 30s

Suspicious Connections 

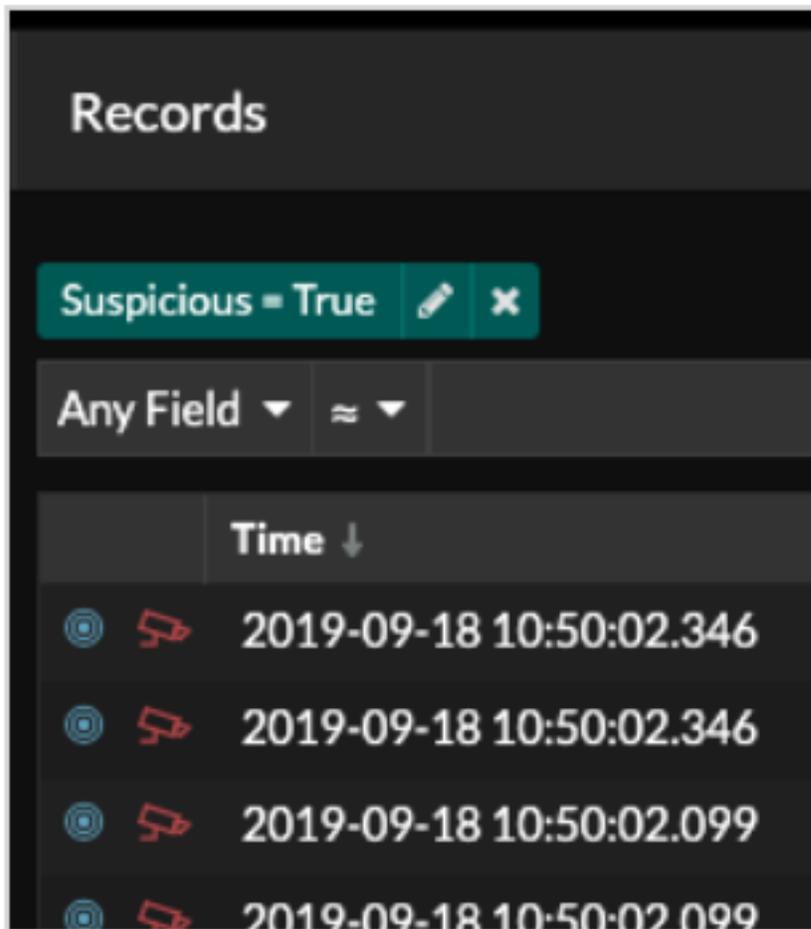
INVESTIGATION STEPS

→ [View the suspicious IP address](#)

Rekorde

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

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



Bedrohungssammlungen verwalten

ExtraHop Reveal (x) kann sich bewerben [Bedrohungsinformationen](#) zu Ihren Netzwerkaktivitäten auf der Grundlage von Bedrohungssammlungen, die von ExtraHop, Partnerintegrationen oder anderen kostenlosen und kommerziellen Quellen bereitgestellt werden.

Informationen zum Hinzufügen von Bedrohungsinformationen von CrowdStrike finden Sie unter [Integrieren Sie Reveal \(x\) 360 mit CrowdStrike](#).

Bevor Sie beginnen

- Erfahre mehr über [Bedrohungsinformationen](#).
- Du musst haben [Rechte für die System- und Zugriffsadministration](#) auf jeder Konsole und jedem Sensor, um Bedrohungssammlungen zu verwalten.

Von ExtraHop kuratierte Bedrohungssammlungen aktivieren oder deaktivieren

Die Bedrohungssammlungen von ExtraHop identifizieren Hinweise auf Sicherheitslücken im gesamten System.

Bedrohungssammlungen von ExtraHop aktualisieren automatisch Systeme, die mit den ExtraHop Cloud Services verbunden sind. Sie können die Konnektivität auf dem [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 dann klicken **Bedrohungsinformationen**.
3. Wählen oder deaktivieren Sie in der ExtraHop Threat Intelligence-Tabelle die **Aktiviert** Checkbox in der Spalte Status.

Das System sucht automatisch alle 12 Stunden nach Aktualisierungen der von ExtraHOP kuratierten Bedrohungssammlungen. Die Spalte Letzte Aktualisierung gibt das Datum und die Uhrzeit der letzten Aktualisierung an.

ExtraHop Threat Collections			
ExtraHop-curated threat intelligence collections are available by default on your Reveal(x) system.			
Name	Last Updated	Status	
Malicious Host Names and URIs	2021-02-27 14:30:26	<input checked="" type="checkbox"/> Enabled	
Malicious Botnet IP Addresses	2021-10-25 14:54:36	<input checked="" type="checkbox"/> Enabled	
Malicious Botnet Host Names and URIs	2021-10-25 14:54:36	<input checked="" type="checkbox"/> Enabled	
Malicious Brute Force IP Addresses	2021-10-25 14:54:37	<input checked="" type="checkbox"/> Enabled	
Malicious IP Addresses from Machine Learning Service	2021-07-08 14:53:11	<input checked="" type="checkbox"/> Enabled	
Malicious Cobalt Strike C2 IP Addresses	2021-10-25 14:54:37	<input checked="" type="checkbox"/> Enabled	
Malicious IP Addresses	2021-10-25 14:54:36	<input checked="" type="checkbox"/> Enabled	
Malicious Host Names and URIs from Machine Learning Service	2021-07-23 15:25:01	<input checked="" type="checkbox"/> Enabled	
Malicious C2 IP Addresses	2021-10-25 14:54:37	<input checked="" type="checkbox"/> Enabled	

Laden Sie eine Bedrohungssammlung hoch

Laden Sie Bedrohungssammlungen aus kostenlosen und kommerziellen Quellen hoch, um Hinweise auf eine Gefährdung im gesamten ExtraHop-System 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.

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 TAR.GZ -Dateien formatiert werden. Reveal (x) unterstützt derzeit STIX Version 1.0 – 1.2.
- Sie können Bedrohungssammlungen zur Selbstverwaltung direkt auf Reveal (x) 360 hochladen Sensoren. Wenden Sie sich an den ExtraHop-Support, um eine Bedrohungssammlung auf ExtraHop-Managed hochzuladen Sensoren.
- Die maximale Anzahl von Observables, die eine Bedrohungssammlung enthalten kann, hängt von Ihrer Plattform und Lizenz ab. Weitere Informationen 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 dann klicken **Bedrohungsinformationen**.
3. klicken **Benutzerdefinierte Sammlungen verwalten**.
4. klicken **Neue Kollektion hochladen**.
5. Geben Sie im Feld Sammlungs-ID eine eindeutige Sammlungs-ID ein. Die ID darf nur alphanumerische Zeichen enthalten und Leerzeichen sind nicht zulässig.
6. klicken **Datei wählen** und wähle eine `.tgz` Datei, die eine STIX enthält.
7. Geben Sie einen Anzeigenamen in das Feld Anzeigename ein.
8. klicken **Sammlung hochladen**.
9. Wiederholen Sie diese Schritte für jedes verbundene Sensor und auf allen Konsolen.

Alerts

Mithilfe von Benachrichtigungen können Sie leicht erkennen, wenn wichtige Ereignisse in Ihrem Netzwerk auftreten oder wenn sich Bereiche nicht wie erwartet verhalten, z. B. Verstöße gegen die Softwarelizenzvereinbarung (SLA) oder langsame Datenbank-Antwortzeiten.

Konfigurierte Warnbedingungen bestimmen, wann eine Alarm generiert wird. Warnbedingungen sind eine Kombination von Einstellungen, z. B. ein Zeitintervall, ein Metrikwert und Metrikberechnungen, 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 Benachrichtigungen](#)

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 Benachrichtigungen](#).

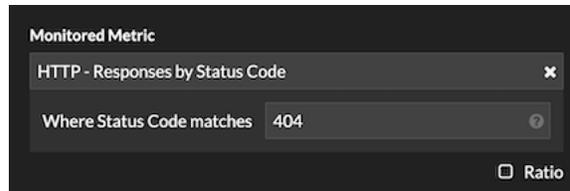
6. In der **Art der Warnung** Abschnitt, klicken **Schwellenwertalarm**.
7. In der **Zugewiesene Quellen** Feld, geben Sie den Namen eines Gerät, einer Gerätegruppe oder einer Anwendung ein und wählen Sie dann aus den Suchergebnissen aus.
Um nach einer Standort, einem Flussnetz oder einer Flussschnittstelle 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.

- 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.

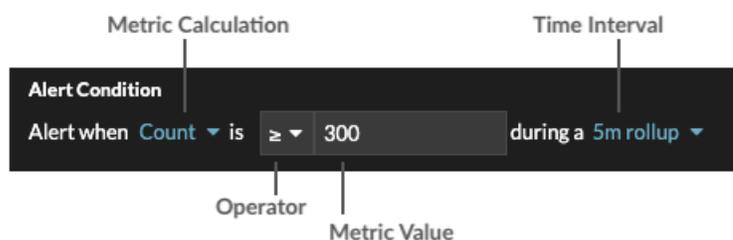
Hinweis Wenn Sie eine auswählen [Detailmetrik](#), Sie können einen Schlüsselwert angeben. Sie könnten beispielsweise HTTP – Antworten nach Statuscode auswählen und dann 404 als Schlüsselwert angeben. Eine Alarm wird nur generiert, wenn HTTP-Antworten mit 404-Statuscodes auftreten.



- 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.



- Geben Sie im Abschnitt Warnbedingung die Bedingungen für die Generierung einer Warnung an.



- Wählen Sie eine Metrikberechnung aus, um anzugeben, wie der Metrikwert innerhalb des Zeitintervalls berechnet werden soll. Die verfügbaren Optionen hängen vom Datentyp ab.

Zählen	<ul style="list-style-type: none"> • Zählen • Rate pro Sekunde • Rate pro Minute • Preis pro Stunde
Datensatz	<ul style="list-style-type: none"> • Minimum • 25. Perzentil • Median

	<ul style="list-style-type: none"> • 75. Perzentil • Maximal
Probenset	<ul style="list-style-type: none"> • Gemein • +1 bis +7 Standardabweichungen • -1 bis -7 Standardabweichungen
Maximum, Snapshot	Keine Messung; der Prüfer vergleicht den tatsächlichen Metrik Wert.

- Wählen Sie einen Operator aus, um anzugeben, wie die Metrikberechnung mit dem Metrikwert verglichen werden soll.
- Geben Sie den Metrikwert an, der mit der Metrikberechnung verglichen werden soll.
- 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
- 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.
 - Klicken Sie im Abschnitt Status auf eine Option, um die Alarm zu aktivieren oder zu deaktivieren.
 - Optional: [Ein Ausschlussintervall hinzufügen](#) um Warnmeldungen zu bestimmten Zeiten zu unterdrücken.
 - 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.

- Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
- Klicken Sie auf das Symbol Systemeinstellungen  und dann klicken **Warnmeldungen**.
- klicken **Erstellen**.
- Geben Sie einen eindeutigen Namen für die Alert-Konfiguration in der **Name** Feld.
- 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 Benachrichtigungen](#).

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	<p>Berechnen Sie einen Trend, indem Sie die Standardabweichung als konstanten Wert mit dem aktuellen Trend vergleichen.</p> <p>Aus dem Art der Abweichung Drop-down-Liste, wählen Sie einen Typ aus:</p> <ul style="list-style-type: none"> • Stichprobenbasiert • Bevölkerungsbezogen
Relative Standardabweichung	<p>Berechnen Sie einen Trend, indem Sie die Standardabweichung als Wert relativ zum Mittelwert des aktuellen Trends vergleichen.</p> <p>Aus dem Art der Abweichung Drop-down-Liste, wählen Sie einen Typ aus:</p> <ul style="list-style-type: none"> • 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	<p>Berechnet einen Trend, indem der Durchschnitt gewichtsbasierter Metrikwerte gebildet wird.</p> <p>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.</p>
Doppelter exponentieller Mittelwert	<p>Berechnet einen Trend, indem der Durchschnitt gewichtsbasierter Metrikwerte gebildet wird.</p> <p>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</p>

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	<p>Berechnet einen Trend auf der Grundlage eines statischen Metrikwerts im Vergleich zu einer Metrikberechnung.</p> <p>Geben Sie einen statischen Wert an und wählen Sie eine Metrikberechnung aus:</p> <ul style="list-style-type: none"> • Preis pro Stunde • Rate pro Minute • Zählen <p>Dieses Modell ist nützlich, um konstante Linien für SLAs zu zeichnen.</p>
Trimean	<p>Berechnet einen Trend auf der Grundlage des gewichteten Durchschnitts der Metrikwerte 25., 50. und 75. Perzentil.</p>
Time Delta	<p>Berechnen Sie einen Trend, indem Sie aktuelle Metrikwerte mit historischen Daten vergleichen.</p>
Gewonnener Mittelwert	<p>Berechnen Sie einen Trend, indem Sie Metrikwerte mit bestimmten niedrigen und hohen Prozentwerten abrufen und sie durch die niedrigsten und höchsten verbleibenden Werte ersetzen.</p> <p>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.</p> <p>Aus dem Winsorisierung Drop-down-Liste, wählen Sie ein Prozentpaar aus:</p> <ul style="list-style-type: none"> • 5/95. Perzentil • 10/90. Perzentil • 25/75. Perzentil

b) Aus dem **Trendfenster** Dropdownliste, wählen Sie ein Berechnungsfenster aus.

Gleiche Stunde der Woche	<p>Berechnen Sie einen Trend, indem Sie die Kennzahlen vergleichen, die jede Woche aus demselben einstündigen Fenster stammen.</p>
Gleiche Stunde des Tages	<p>Berechnen Sie einen Trend, indem Sie die Messwerte vergleichen, die jeden Tag aus demselben einstündigen Fenster stammen.</p>
Gleitender Minutendurchschnitt	<p>Berechnen Sie einen Trend, indem Sie den Durchschnitt der Metrikwerte ermitteln, die jede Minute innerhalb eines bestimmten</p>

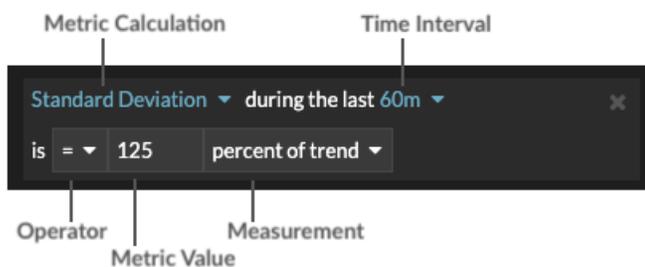
Zeitraums ab dem aktuellen Zeitpunkt erfasst wurden.

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

- 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.
- Klicken Sie im Abschnitt Status auf eine Option, um die Alarm zu aktivieren oder zu deaktivieren.
- Optional: [Ein Ausschlussintervall hinzufügen](#) um Warnmeldungen zu bestimmten Zeiten zu unterdrücken.
- 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 (Reveal (x) 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

- Du musst haben [volle Schreibrechte](#) oder höher.
 - Ihr ExtraHop-System muss [konfiguriert für das Senden von Benachrichtigungen](#).
 - 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](#).
- Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
 - Klicken Sie auf das Symbol Systemeinstellungen  und dann klicken **Alerts**.
 - Klicken Sie in der Tabelle Benachrichtigungen auf die gewünschte Alarm.
 - Geben Sie im Abschnitt Benachrichtigungen die E-Mail-Gruppen und Adressen an, die benachrichtigt werden sollen, wenn die Alarm auftritt.
 - 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.
 - Optional: klicken **SNMP-Trap senden** um Benachrichtigungen an einen SNMP-Listener zu senden.

6. Optional: Fügen Sie der E-Mail-Benachrichtigung zusätzliche Metriken hinzu.
Die E-Mail enthält den Wert dieser Metriken, als die Alarm aufgetreten ist.
 - a) klicken **Erweiterte Optionen anzeigen**.
 - b) Aus dem Zusätzliche Metriken in E-Mail-Benachrichtigungen Abschnitt, klicken **Metrik hinzufügen**.
 - c) Geben Sie im 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 (Reveal (x) 360)

Sie können einer Warnungskonfiguration eine Benachrichtigung hinzufügen, die beim Auftreten der Alarm eine E-Mail an eine oder mehrere angegebene E-Mail-Adressen sendet. Die E-Mail enthält Warnungsdetails und einen Link zum Anzeigen der Warnquelle.

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 **Alerts**.
3. Klicken Sie in der Tabelle Benachrichtigungen 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, als die Alarm aufgetreten ist.
 - a) klicken **Erweiterte Optionen anzeigen**.
 - b) Klicken Sie im Abschnitt Zusätzliche Metriken in E-Mail-Benachrichtigungen auf **Metrik hinzufügen**.
 - c) Geben Sie im 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 **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.

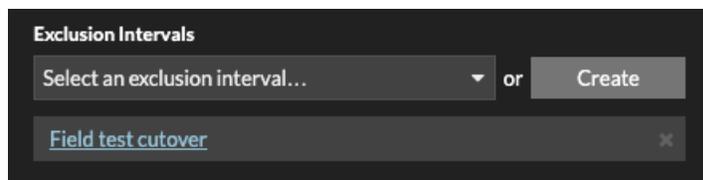
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen  und dann klicken **Warnmeldungen**.
3. Klicken Sie in der Tabelle Benachrichtigungen auf die gewünschte Alarm.

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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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. 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**.

Rekorde

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), transaktionell (wie HTTP, CIFS und NFS) und sitzungsbasiert (wie SSL und ICA) sind.

Wenn Sie beispielsweise fünfzig HTTP 503-Fehler hatten, 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.

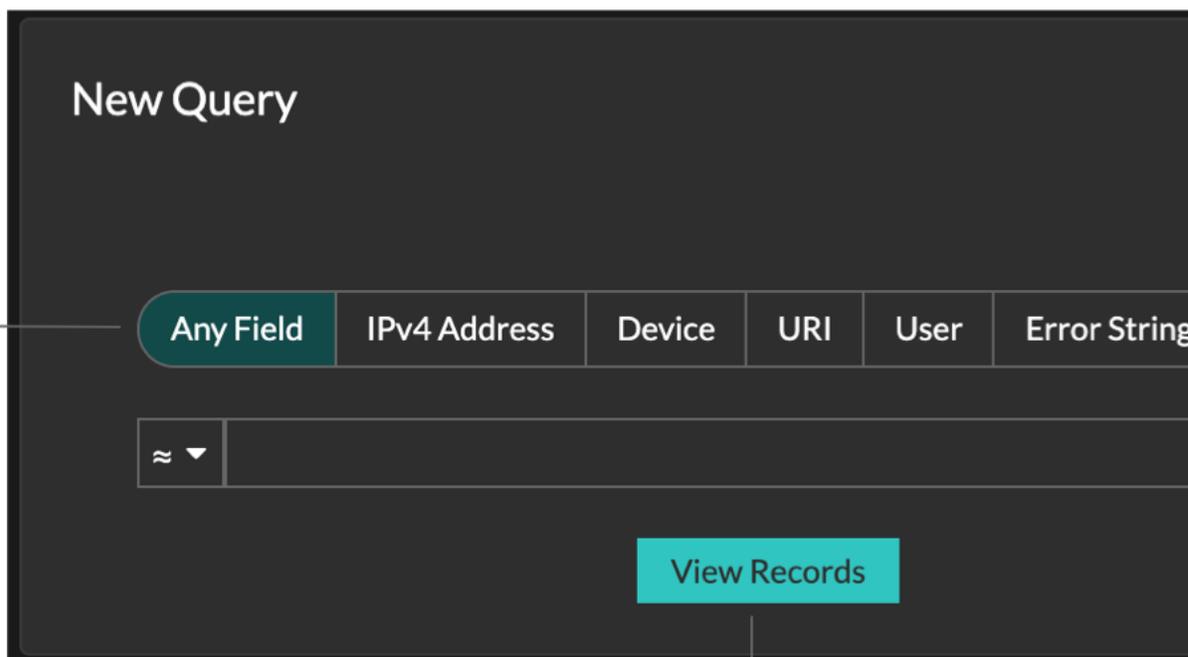
Bevor du anfängst

- Sie müssen über einen konfigurierten Recordstore verfügen, z. B. einen [ExtraHop Recordstore](#), [Splunk](#), oder [Google BigQuery](#).
- Sie können nur einen Recordstore für das ExtraHop-System konfigurieren.
- Ihr ExtraHop-System muss für das Sammeln und Speichern konfiguriert sein [Flow-Aufzeichnungen](#) oder [L7-Aufzeichnungen](#).

In Datensätzen navigieren

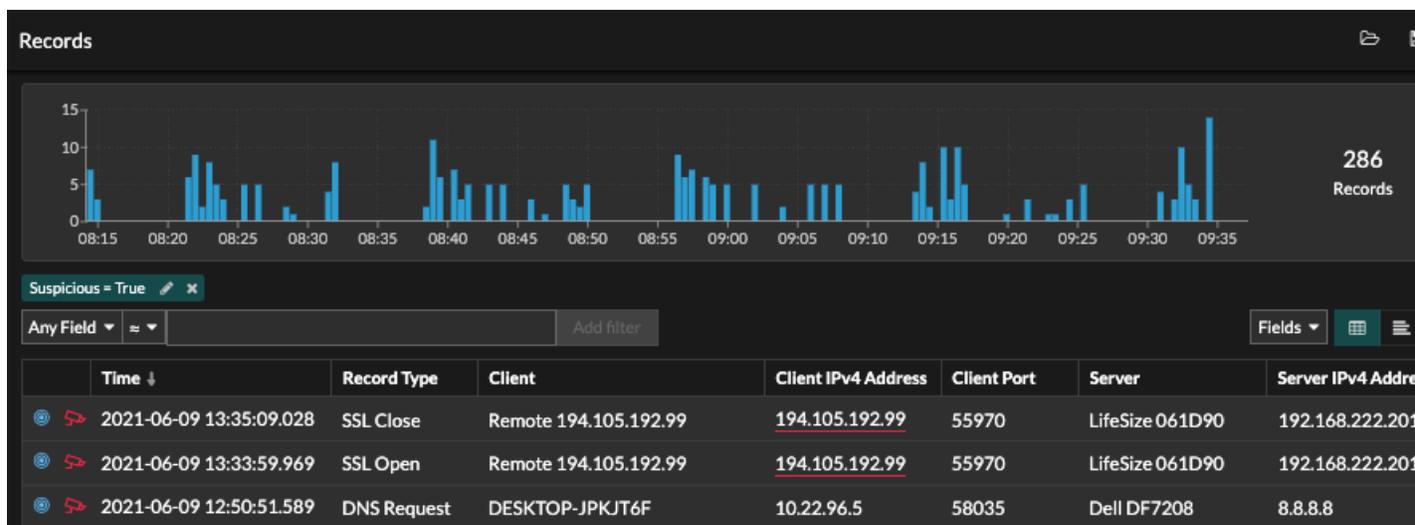
Klicken **Rekorde** aus dem oberen Menü, um eine neue Datensatzabfrage zu erstellen. Auf der Seite Neue Abfrage können Sie einen Filter und einen Datensatztyp angeben.

Select a field to search on



Click to start a record query

Die Ergebnisse werden auf der Hauptseite „Datensätze“ angezeigt.



Hinweis: Eine Abfrage kann auf der Grundlage des Zeitintervalls und der Filterkriterien zu Millionen von Datensätzen führen. Wenn eine Abfrage die maximale Anzahl von Abfrageergebnissen überschreitet, wird eine verkürzte Anzahl von Datensätzen angezeigt. (Nur im ExtraHop-Plattenladen.)

Im Folgenden finden Sie einige Möglichkeiten, wie Sie die Ergebnisse von Datensatzabfragen genauer untersuchen können:

- Zeigen Sie im Datensatzdiagramm mit der Maus auf ein Zeitintervall, um die Anzahl der Datensätze anzuzeigen, oder klicken Sie und ziehen Sie mit der Maus über das Diagramm, um die Ergebnisse der Datensatzabfrage auf ein Zeitintervall einzuzugrenzen.

- Klicken Sie auf einen Hostnamen oder eine IP-Adresse, um Details zu 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 anzusehen [Bedrohungsinformationen](#) für's Datensatz.
- Klicken Sie auf ein Paketsymbol, um ein zu starten [Paketabfrage](#) das wird durch diesen Datensatz gefiltert.
- Aufzeichnungsergebnisse werden standardmäßig in einer Tabelle angezeigt. Klicken Sie auf die Tabellenansicht oder Ausführliche Ansicht  Symbole zum Umschalten der Datensatzansicht.
- 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 **Anfrage fortsetzen** um die Suche fortzusetzen.
- Klicken Sie auf **Felder** Dropdownliste, um zusätzliche Datensatzinformationen zur Datensatzansicht hinzuzufügen.
- Klicken und ziehen Sie in der Tabellenansicht die Spaltenüberschriften, um die Datensatzinformationen anzuordnen.
- Bewerben [einfach](#) oder [erweiterte Filter](#) um potenzielle Probleme zu finden, wie z. B. zu lange Bearbeitungszeiten oder ungewöhnliche Antwortgrößen.



Hinweis Um eine Datensatzabfrage für eine benutzerdefinierte Metrik zu erstellen, müssen Sie zunächst die Datensatzbeziehung definieren, indem Sie [Verknüpfen der benutzerdefinierten Metrik mit einem Datensatztyp](#).

Filtern Sie Ihre Datensätze mit einer einfachen Abfrage

Es gibt eine Reihe von Möglichkeiten, wie Sie die Ergebnisse Ihrer Datensatzabfrage filtern können, um genau die Transaktion zu finden, nach der Sie suchen. In den folgenden Abschnitten werden die einzelnen Methoden beschrieben und es werden Beispiele gezeigt, mit denen Sie beginnen können, um sich damit vertraut zu machen.

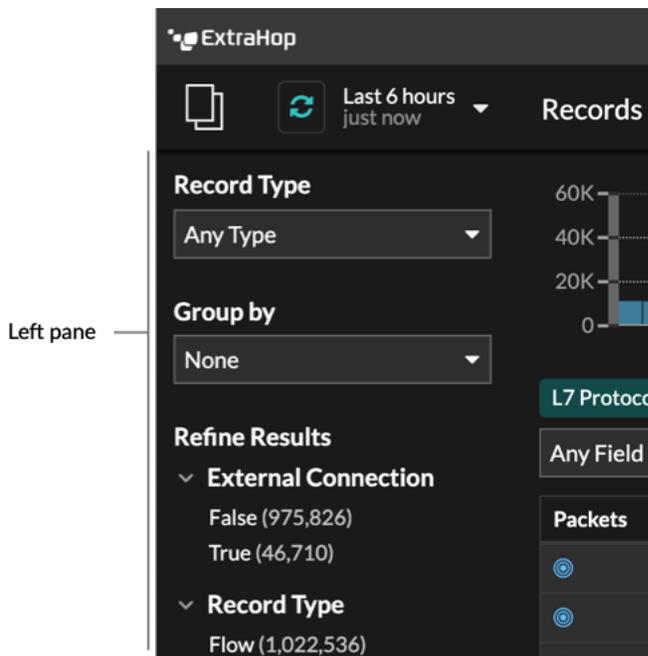
Wenn Sie versuchen, Datensätze nach einfachen Kriterien zu filtern (wenn Sie beispielsweise alle HTTP-Transaktionen von einem einzigen Server haben möchten, der 404-Dateien generiert hat), können Sie eine einfache Abfrage auf eine der folgenden Arten erstellen:

- Fügen Sie im linken Bereich einen Filter hinzu oder verfeinern Sie die Ergebnisse
- Einen Filter aus dem Trifield hinzufügen
- Fügen Sie einen Filter direkt aus den Datensatzergebnissen hinzu

Informationen zu komplexen Filtern finden Sie unter [Datensätze mit einem erweiterten Filter abfragen](#).

Filtern von Datensatzergebnissen aus dem linken Bereich

Wenn du klickst **Rekorde** im oberen Menü werden alle verfügbaren Datensätze für das gewählte Zeitintervall angezeigt. Sie können dann im linken Bereich filtern, um Ihre Ergebnisse zu verfeinern.



Die **Art des Datensatzes** Das Dropdownmenü 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.

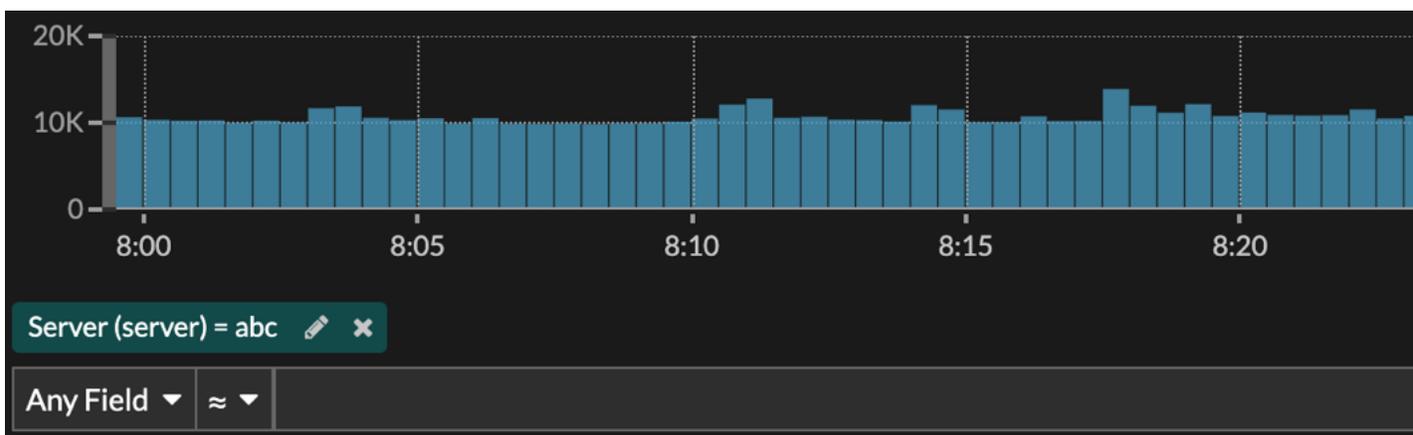
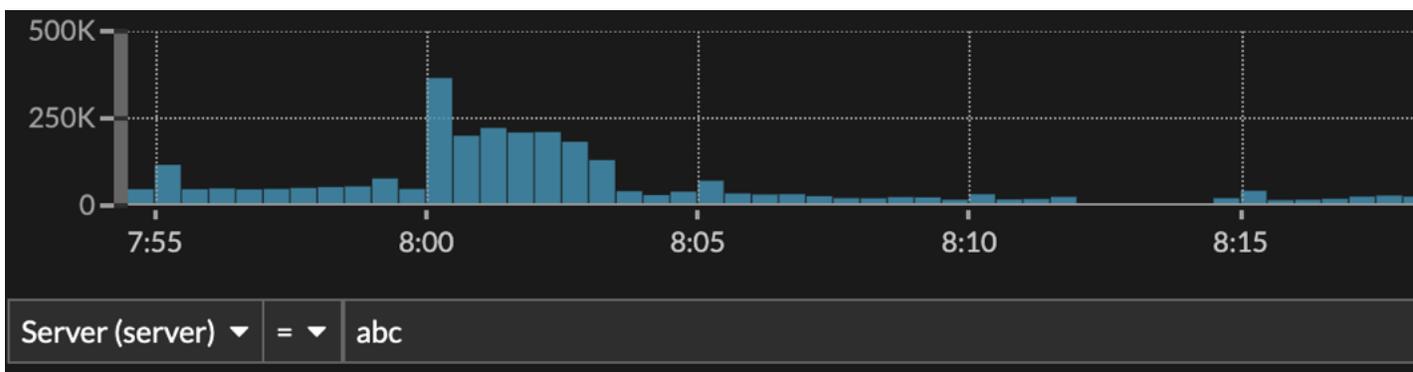
 **Hinweis** Da Sie zum Sammeln von Datensätzen einen Auslöser schreiben müssen, benötigen Sie eine Möglichkeit, die Art der Daten zu identifizieren, die Sie sammeln werden. Es gibt integrierte Datensatztypen, die alle verfügbaren bekannten Felder für ein Protokoll sammeln. Sie können mit einem integrierten Datensatztyp (wie HTTP) beginnen und einen Auslöser schreiben, um nur die Felder für dieses Protokoll zu sammeln, die für Sie wichtig 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.

Die **Gruppieren nach** In der Dropdownliste finden Sie eine Liste mit Feldern, nach denen Sie den Datensatztyp weiter filtern können.

Die **Ergebnisse verfeinern** Dieser Abschnitt zeigt Ihnen eine Liste gängiger Datensatzfilter für den ausgewählten Datensatztyp mit der Anzahl der Datensätze, die dem Filter entsprechen, in Klammern.

Filterung von Rekordergebnissen durch das Trifield

Wählen Sie ein Feld aus der **Irgendein Feld** Dropdownmenü (z. B. Server), wählen Sie einen Operator aus (z. B. das Gleichheitszeichen (=)), und geben Sie dann einen Hostnamen ein. klicken **Filter hinzufügen**, und der Filter wird über der Filterleiste hinzugefügt.



Ihre Ergebnisse zeigen nur Datensätze, die dem Filter entsprechen. In unserem Beispiel bedeutet dies, dass wir nur Ergebnisse für Transaktionen sehen, die für den Server mit dem Namen abc bestimmt sind.

Die folgenden Operatoren können basierend auf dem ausgewählten Feldnamen ausgewählt werden:

Betreiber	Beschreibung
=	Gleichwertig
≠	Entspricht nicht
≈	Beinhaltet

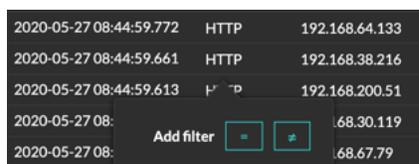
Wenn Datensätze in einem ExtraHop-Recordstore gespeichert sind, entspricht der Include-Operator ganzen Wörtern, die durch Leerzeichen und Satzzeichen getrennt sind. Eine Suche nach „www.extra“ würde beispielsweise mit „www.extra.com“ übereinstimmen, aber nicht mit „www.extrahop.com“.

Für alle anderen Recordstores 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.

Betreiber	Beschreibung
	Regex- und Platzhalterzeichen werden nicht unterstützt.
≈/	Schließt aus Wenn Datensätze in einem ExtraHop-Recordstore gespeichert sind, entspricht der Ausschluss-Operator ganzen Wörtern, die durch Leerzeichen und Satzzeichen getrennt sind. Eine Suche nach „extra“ würde beispielsweise „www.extra.com“ ausschließen, aber nicht „www.extrahop.com“. Für alle anderen Recordstores entspricht der Excludes-Operator 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
existiert nicht	Existiert nicht

Direkt aus den Datensatzergebnissen filtern

Sie können einen beliebigen Feldeintrag auswählen, der entweder in der Tabellenansicht oder in der ausführlichen Ansicht in Ihren Datensatzergebnissen 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 wird).

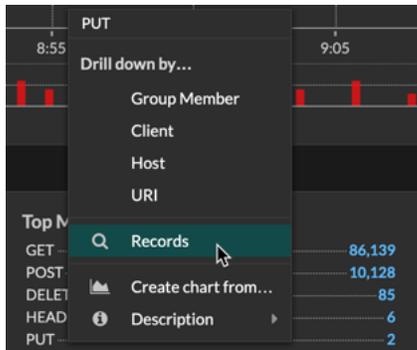


2020-05-27 08:44:59.772	HTTP	192.168.64.133
2020-05-27 08:44:59.661	HTTP	192.168.38.216
2020-05-27 08:44:59.613	HTTP	192.168.200.51
2020-05-27 08:		68.30.119
2020-05-27 08:		68.67.79

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.

Aufzeichnungen sammeln

Bestimmte Arten von Datensätzen sind standardmäßig für die Erfassung aktiviert. Sie können die Arten von Datensätzen, die gesammelt und an Ihren Recordstore gesendet werden, hinzufügen oder daraus entfernen Einstellungen//Aufzeichnungen Seite. Diese Datensätze enthalten hauptsächlich Informationen über Nachrichten, Transaktionen und Sitzungen, die über gängige L7-Protokolle wie DNS, HTTP und SSL gesendet werden.

Wenn Sie nur bestimmte Details aus Transaktionen sammeln möchten, können Sie benutzerdefinierte Datensätze über die [ExtraHop-Trigger-API](#).

Hinweis Du kannst [verwalte diese Einstellungen](#) zentral von einer Konsole aus.

Erfahre mehr über [ExtraHop Records](#).

Bevor Sie beginnen

Sie müssen über einen konfigurierten Recordstore verfügen, z. B. [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 dann klicken **Plattensammlung**.
3. Auf dem Rekorde Seite, aktivieren Sie das Kontrollkästchen neben den Transaktionstypen, die Sie erfassen und im Recordstore speichern möchten, und klicken Sie dann auf **Aktivieren**.
4. klicken **Rekorde** aus dem oberen Menü, und klicken Sie dann auf **Aufzeichnungen ansehen** um eine Abfrage zu starten.

Wenn Sie keine Datensätze 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 sammeln und speichern. Dabei handelt es sich um Kommunikationsdaten auf Netzwerkebene zwischen zwei Geräten über ein IP-Protokoll. Wenn Sie diese Einstellung aktivieren, aber keine IP-Adressen oder Portbereiche hinzufügen, werden alle erkannten Flow-Datensätze 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 benötigen Zugriff auf ein ExtraHop-System mit [Rechte für die System- und Zugriffsadministration](#).

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
 2. In der Aufzeichnungen Abschnitt, klicken **Automatische Flussaufzeichnungen**.
 3. Wählen Sie den **Aktiviert** Checkbox.
 4. In der Intervall für Veröffentlichungen 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. Klicken Sie dann auf das grüne Plus (+) Symbol. (Sie können einen Eintrag entfernen, indem Sie auf das rote Löschen klicken (X) Symbol.)
 6. In der Portbereiche Feld, geben Sie einen einzelnen Port oder Portbereich ein. Klicken Sie dann auf das grüne Plus (+) Symbol.
 7. klicken **Speichern**.
- Flow-Datensätze, die Ihren Kriterien entsprechen, werden jetzt automatisch an Ihren konfigurierten Recordstore gesendet. Warten Sie einige Minuten, bis die Aufzeichnungen gesammelt wurden.
8. Klicken Sie im ExtraHop-System auf **Rekorde** aus dem oberen Menü, und klicken Sie dann auf **Aufzeichnungen ansehen** um eine Abfrage zu starten.

Wenn Sie keine Datensätze 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](#).

Sammeln Sie L7-Datensätze mit einem Auslöser

L7-Protokolle können über eine globale Triggerfunktion als Datensatz festgeschrieben (gesammelt und gespeichert) werden. L7-Datensätze umfassen Nachrichten, Transaktionen und Sitzungen, die über gängige L7-Protokolle wie DNS, HTTP und SSL 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](#).

Zunächst schreiben wir einen Auslöser, um Informationen aus dem integrierten HTTP-Datensatztyp mit der Methode `commitRecord()` zu sammeln, die für alle 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 über einen konfigurierten Recordstore verfügen, z. B. [ExtraHop Recordstore](#), [Splunk](#), oder [Google BigQuery](#)
- Diese Anweisungen setzen eine gewisse Vertrautheit voraus mit [ExtraHop-Trigger](#), für die Erfahrung mit JavaScript erforderlich ist. 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 **Auslöser**.
3. klicken **Erstellen**.
4. In der Trigger erstellen Fenster, vervollständigen Sie Ihre Informationen, ähnlich dem folgenden Beispiel:
 - **Name:** HTTP-Antworten
 - **Beschreibung:** Dieser Auslöser sammelt HTTP-Antworten.
5. Markieren Sie das Kästchen neben **Debug-Log aktivieren**.
6. Wählen Sie in 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 **Speichern**.

Nächste Schritte

Warten Sie einige Minuten, bis die Datensätze erfasst wurden, und überprüfen Sie dann im nächsten Schritt, ob Ihre Datensätze erfasst werden, indem Sie auf **Rekorde** aus dem oberen Menü und dann klicken **Aufzeichnungen ansehen** um eine Abfrage zu starten.

Wenn Sie nach 5 Minuten keine HTTP-Einträge sehen, klicken Sie auf **Debug-Protokoll**. Klicken Sie unten auf der Seite im Trigger-Editor auf einen Tab, um zu sehen, ob es Fehler gibt, die Sie beheben können. Wenn der Auslöser ausgeführt wird, wird die Meldung „HTTP-Antworten übergeben“ angezeigt. Wenn nach der Ausführung 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.

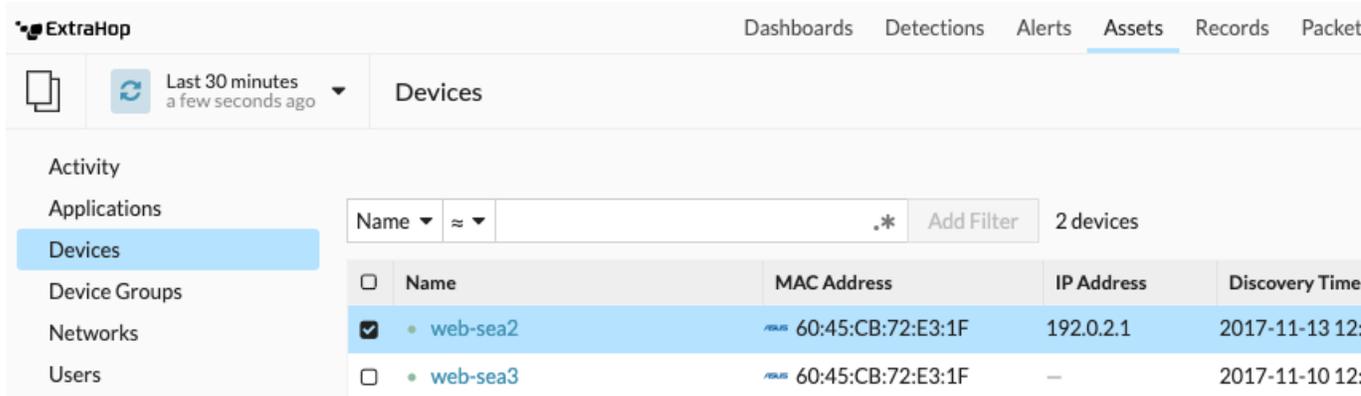
```

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`.



The screenshot shows the ExtraHop interface with the 'Assets' tab selected. Under 'Devices', there is a search bar and a table of devices. The table has columns for Name, MAC Address, IP Address, and Discovery Time. Two devices are listed: 'web-sea2' and 'web-sea3'. The 'web-sea2' device is selected with a checked checkbox.

<input type="checkbox"/>	Name	MAC Address	IP Address	Discovery Time
<input checked="" type="checkbox"/>	web-sea2	60:45:CB:72:E3:1F	192.0.2.1	2017-11-13 12:...
<input type="checkbox"/>	web-sea3	60:45:CB:72:E3:1F	—	2017-11-10 12:...

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.

PROBLEMS   DEBUG LOG

```
[Tue Jun 18 13:36:01] committing web404 HTTP record
[Tue Jun 18 13:36:14] committing web404 HTTP record
[Tue Jun 18 13:36:14] committing web404 HTTP record
[Tue Jun 18 13:36:19] committing web404 HTTP record
```

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.

Create Record Format

Display Name

HTTP 404

Author

ExtraHop

Record Type

web404

Schema on Read

```

1  [
2    {
3      "display_name": "Status Code",
4      "name": "statusCode",
5      "data_type": "n",
6      "facet": true,
7      "default_visible": true
8    },
9    {
10     "display_name": "URI",
11     "name": "uri",
12     "data_type": "s",
13     "meta_type": "uri",
14     "default_visible": true
15   },
16   {
17     "display_name": "User Agent",
18     "name": "userAgent",
19     "data_type": "s"
20   },

```

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 Aufzeichnungsformat

Die Einstellungen für das Aufzeichnungsformat Auf dieser Seite wird eine Liste aller integrierten und benutzerdefinierten Aufzeichnungsformate angezeigt, die auf Ihren ExtraHop-Sensoren oder Ihrer Konsole verfügbar sind. Wenn Sie ein benutzerdefiniertes Datensatzformat erstellen müssen, empfehlen wir Ihnen, das Schema zu kopieren und in gelesene Informationen aus einem integrierten Datensatzformat einzufügen. 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 es kein Datensatzformat für den Datensatz gibt, wird der Datensatztyp angezeigt.

Autor

(Optional) Der Autor des Datensatzformat. Alle integrierten Aufzeichnungsformate werden angezeigt `ExtraHop` als Autor.

Art 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 Aufzeichnungsformate 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 Array im JSON-Format mit mindestens einem Objekt, das aus einem Feldnamen- und 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 Einstellungen für das Datensatzformat beschränkt und wird in keiner Datensatzabfrage angezeigt.

default_visible

(Optional) Wenn gesetzt auf `true`, wird dieses Feld 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 Sie klicken können, um einen Filter hinzuzufügen.

Datentyp

Die Abkürzung, die den Typ der in diesem Feld gespeicherten Daten identifiziert. Die folgenden Datentypen werden unterstützt:

Art der Daten	Abkürzung	Beschreibung
Anwendung	<code>app</code>	ExtraHop-Anwendungs-ID (Zeichenfolge)
boolesch	<code>b</code>	Boolescher Wert
Gerät	<code>dev</code>	ExtraHop-Geräte-ID (Zeichenfolge)
Flussschnittstelle	<code>fint</code>	Flow-Schnittstellen-ID
Flussnetz	<code>fnet</code>	Flow-Netzwerk-ID
IPv4	<code>addr4</code>	Eine IPv4-Adresse im Dotted-Quad-Format. Filter, die größer oder kleiner als sind, werden unterstützt.

Art der Daten	Abkürzung	Beschreibung
IPv6	addr6	Eine IPv6-Adresse. Es werden nur string-orientierte Filter unterstützt.
Nummer	n	Zahl (Ganzzahl oder Fließkomma)
Schnur	s	Generische Zeichenfolge

metatyp

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:

Art der Daten	Metatyp
Schnur	<ul style="list-style-type: none"> • domain • uri • user
Zahl	<ul style="list-style-type: none"> • bytes • count • expiration • milliseconds • packets • timestamp

Datensätze mit einem erweiterten Filter abfragen

Sie können Datensätze, die im Recordstore gespeichert sind, mit einem erweiterten Filter abfragen.



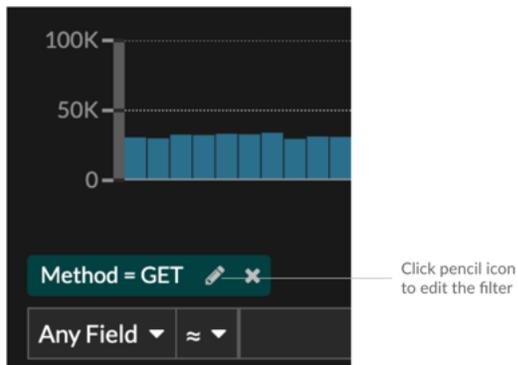
Hinweis Um eine Datensatzabfrage für eine benutzerdefinierte Metrik zu erstellen, müssen Sie zunächst die Datensatzbeziehung definieren, indem Sie [Verknüpfen der benutzerdefinierten Metrik mit einem Datentyp](#).

Nächste Schritte

- Informationen zum Abfragen eines bestimmten Datensatz finden Sie in unserer exemplarischen Vorgehensweise für [Fehlende Webressourcen entdecken](#).
- Du kannst auch [Automatisieren Sie diese Aufgabe über die REST-API](#).

Filtern Sie Ihre Datensätze mit erweiterten Abfragerregeln

Für erweiterte Abfragen können Sie komplexe Filter erstellen und ändern, indem Sie auf die Schaltfläche Erweiterter Filter hinzufügen klicken.  oder indem Sie auf das Stiftsymbol klicken  neben jedem Filter, den Sie hinzugefügt haben.



Hier sind einige wichtige Dinge, die Sie über erweiterte Abfragen wissen sollten:

- Sie können mehrere Kriterien mit den Operatoren OR (Match Any), AND (Match All) und NONE angeben
- Sie können Filter gruppieren und sie innerhalb jeder Gruppe auf vier Ebenen verschachteln.
- Sie können eine Filtergruppe bearbeiten, nachdem Sie sie erstellt haben.
- Sie können einen beschreibenden Namen erstellen, um den allgemeinen Zweck der Abfrage zu identifizieren.

Erstellen Sie einen komplexen Filter mit AND- und OR-Operatoren

Das folgende Beispiel zeigt, wie Sie eine erweiterte Abfrage erstellen können, um Ihre Datensätze nach komplexen Kriterien zu filtern. Wir werden einen Filter erstellen, um Ergebnisse für alle HTTP-Datensätze zurückzugeben, die zwei URIs plus einen Statuscode größer oder gleich 400 oder eine Verarbeitungszeit von mehr als 750 Millisekunden enthalten.

Wichtig: Um dieses Beispiel auszuprobieren, müssen Sie HTTP-Verkehr in Ihrem Netzwerk haben.

Advanced Filter

Filter Criteria

Match All ▾

Status Code ▾ ≥ ▾ 400 ✕

Processing Time ▾ > ▾ 750 ✕

Add Filter Add Filter Group

Custom Display Name

Slow and Broken Web Assets

1. klicken **Rekorde** aus dem oberen Menü.
2. klicken **Aufzeichnungen ansehen**.
3. Wählen Sie im linken Bereich **HTTP** aus dem Bereich Ergebnisse verfeinern. Im Bereich Ergebnisse verfeinern werden nur verfügbare Datensätze angezeigt. Dieser Schritt stellt sicher, dass Sie über verfügbare Datensätze für diese Abfrage verfügen.

Hinweis: Datensatztypen werden nicht als Filter angezeigt, sondern im linken Bereich.

4. Klicken Sie auf die Schaltfläche „Erweiterten Filter hinzufügen“ . Die Schaltfläche befindet sich auf der rechten Seite der Seite über den Suchergebnissen der Datensätze.

5. Unter Kriterien filtern, wählen **Alle abgleichen** aus der Drop-down-Liste. Match All ist ein UND-Operator, mit dem wir nach Kriterien suchen können, die dem Statuscode und den Kriterien für die Bearbeitungszeit entsprechen.
6. Wählen **Statuscode**, je größer oder gleich dem Vorzeichen (\geq), und geben Sie dann ein 400 im Zahlenfeld.
7. klicken **Filter hinzufügen** um einen Filter für die Verarbeitungszeit hinzuzufügen.
8. Wählen **Bearbeitungszeit**, das Größer-Als-Zeichen ($>$), und geben Sie dann ein 750 im Zahlenfeld. In den nächsten Schritten werden wir eine Gruppe von Kriterien hinzuzufügen, die speziell für die von uns hinzugefügten Felder gelten.
9. klicken **Filtergruppe hinzufügen**.
Wir behalten **Beliebiges abgleichen** für diese Gruppe. Match Any ist ein OR-Operator und ermöglicht es uns, nach Kriterien zu suchen, die einer unserer URIs entsprechen.
10. klicken **Filter hinzufügen** um der Gruppe einen Filter hinzuzufügen.
11. Klicken Sie auf **Irgendein Feld** Drop-down-Menü und Auswahl **URI**.
12. Wählen Sie die Inklusivleistungen aus (\approx) Symbol.
13. Geben Sie eine URI für einen Ihrer Webserver in das Textfeld Feld. Wir werden hinzufügen `assets.example.com`.
14. klicken **Filter hinzufügen** um der Gruppe einen zweiten URI-Filter hinzuzufügen.
15. Klicken Sie auf **Irgendein Feld** Drop-down-Menü und Auswahl **URI**.
16. Wählen Sie die Inklusivleistungen aus (\approx) Symbol.
17. Geben Sie eine URI für einen Ihrer Webserver in das Textfeld Feld. Wir werden hinzufügen `media.example.com`.
18. In der Benutzerdefinierter Anzeigename Feld, geben Sie einen aussagekräftigen Namen ein, damit der Filter auf der Ergebnisseite leicht zu identifizieren ist, andernfalls zeigt der Anzeigename den ersten Filter und die Anzahl der anderen angewendeten Regeln an:



Wir werden „Slow and Broken Web Assets“ in das Feld eingeben.

19. klicken **Speichern**.

Nachdem du geklickt hast **Speichern**, wird die Abfrage automatisch ausgeführt und gibt Datensätze zurück, die einem der URI entsprechen und entweder einen Statuscode größer oder gleich 400 oder eine Verarbeitungszeit von mehr als 750 Millisekunden haben.

Nächste Schritte

Sie können auf das Symbol Speichern klicken  von oben rechts auf der Seite, um Ihre Kriterien für ein anderes Mal zu speichern.

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.

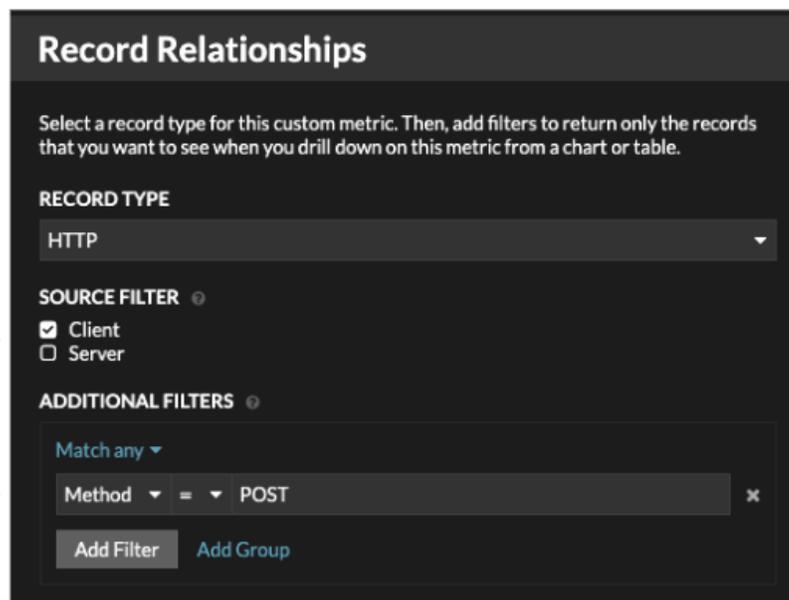
Bevor Sie beginnen

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.

Specify the source filter for this custom metric. Source filters are updated based on record type.

Add advanced query rules or a regular expression (regex).



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 mit einer Trace-Appliance kontinuierlich zu sammeln, zu suchen und herunterzuladen. Dies kann nützlich sein, um Netzwerkeinbrüche und andere verdächtige Aktivitäten zu erkennen.

Sie können auf der Paketseite im ExtraHop-System nach Paketen suchen und diese herunterladen. [Paketssuche](#) 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 dennoch Pakete sammeln über [löst aus](#) . siehe [Initiieren Sie präzise Paketerfassungen, um Bedingungen ohne Fenster zu analysieren](#) für ein Beispiel.

Pakete abfragen

Starten Sie eine schnelle Paketabfrage, indem Sie auf **Pakete** aus dem oberen Menü. Das ExtraHop-System fragt nach allen Paketen ab und zeigt die Seite Paketabfrage an. Wenn Sie das Zeitintervall ändern, wird die Abfrage erneut gestartet. 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 und die Uhrzeit auf der linken Seite zeigt den Endpunkt der Abfrage an. Der blaue Balken zeigt 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.

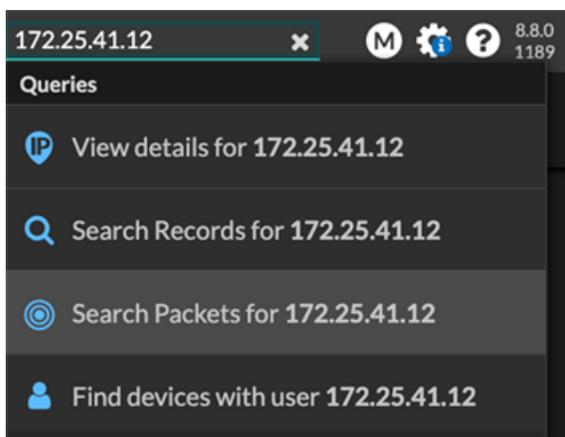
Die folgende Abbildung 23 bietet einen Überblick über die Seite „Paketabfrage“ und ihre Funktionen:

The screenshot shows the 'Packets' page in the ExtraHop interface. At the top, there are navigation tabs: Overview, Dashboards, Detections, Alerts, Assets, Records, and **Packets**. A search bar is located in the top right corner. Below the navigation, there's a 'Packet Query Results' section. On the left, there's a 'Refine Results' sidebar with a list of IP addresses and their associated data sizes. The main area features a 'Packet Query' section with a time range selector (From Feb 23, 1:51:02 pm to Until Feb 23, 1:56:02 pm) and a 'Download PCAP' button. Below this is a table of packet details. The table has columns for Time, Src IP, Dst IP, IP Proto, Src Port, Dst Port, Flags, Bytes, Src MAC, Dst MAC, EtherType, and VLAN ID. The table shows several rows of network traffic data. At the bottom, there's a '100 packet preview' section with navigation arrows.

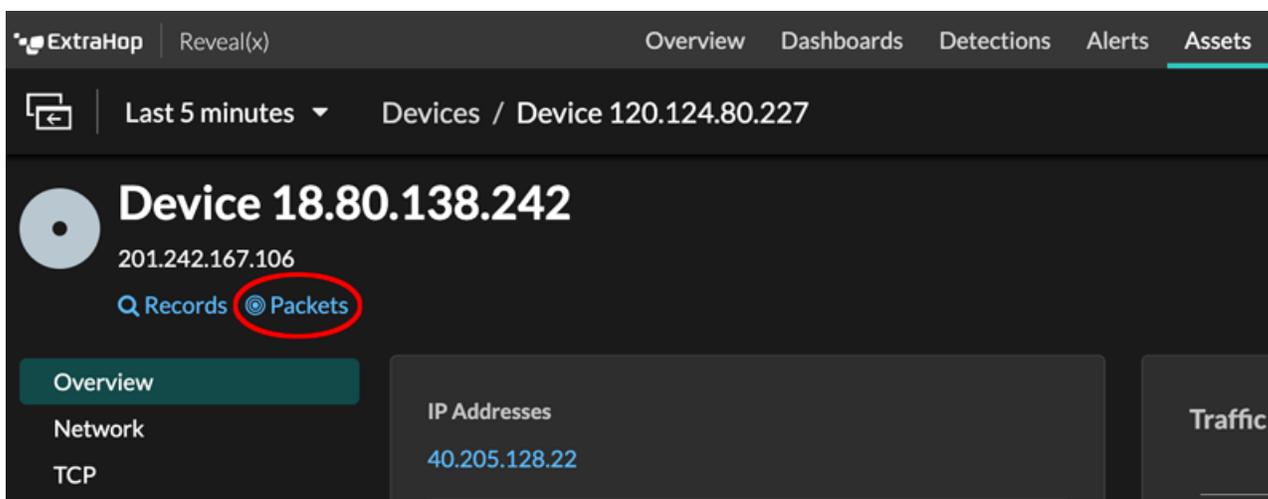
Hinweis: Pakete mit der Berkeley-Paketfilter-Syntax filtern.

Es gibt mehrere Stellen im ExtraHop-System, von denen aus Sie eine Paketabfrage starten können:

- Geben Sie eine IP-Adresse in das globale Suchfeld ein und wählen Sie dann das Symbol Pakete suchen .



- klicken **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 beliebigen Diagramm mit Messwerten für Netzwerkbytes oder Pakete nach IP-Adresse auf eine IP-Adresse oder einen Hostnamen, um ein Kontextmenü zu sehen. Klicken Sie dann auf das Paketsymbol (📄) um das Gerät und das Zeitintervall abzufragen.

The screenshot shows the ExtraHop Threat Hunting interface. At the top, there are navigation tabs: Overview, Dashboards, Detections, Alerts, and Assets. The main heading is 'Threat Hunting / HTTP'. Below this is a line graph showing data over time from 15:36:00 to 15:36:30. A search bar contains 'Any Field ≈'. Below the search bar is a table with columns for search criteria and results. The first row shows 'Client IP' with a search icon and the value '100.152.8.59'. The second row shows '192.168.23.82'. A context menu is open over the IP '100.152.8.59', displaying the following information: '100.152.8.59', 'External Endpoint', 'Las Vegas, Nevada, United States', and 'myip.opendns.com'. Below this information are options: 'Go To', 'ARIN Whois Lookup', 'Records', and 'Packets' (which is circled in red). At the bottom of the menu is a button labeled 'Go to IP Address Details'.

Konfigurieren Sie eine globale PCAP

Eine globale PCAP sammelt 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. Klicken Sie im Abschnitt Paketerfassungen auf **Globale Paketerfassung**.
3. In der Starten Sie die globale Paketerfassung Abschnitt, füllen Sie die folgenden Felder aus. Sie müssen nur die gewünschten Kriterien für die Paketerfassung angeben:
 - **Name:** Ein Name zur Identifizierung der PCAP.
 - **Max. Anzahl Pakete:** Die maximale Anzahl von Paketen, die erfasst werden sollen.
 - **Max. Byte:** Die maximale Anzahl von Byte, die erfasst werden sollen.
 - **Max. Dauer (Millisekunden):** Die maximale Dauer der PCAP in Millisekunden. Wir empfehlen den Standardwert 1000 (1 Sekunde) oder eine Konfiguration von bis zu 60000 Millisekunden (1 Minute).
 - **Snaplen:** Die maximale Anzahl von Byte, die pro Frame kopiert werden. Der Standardwert ist 96 Byte, aber Sie können diesen Wert auf eine Zahl zwischen 1 und 65535 setzen.
4. klicken **Start**.
 - 💡 **Hinweis:** Notieren Sie sich die Uhrzeit, zu der Sie mit der Erfassung beginnen, damit Sie die Pakete leichter finden können.
5. klicken **Stopp** um die Paketerfassung zu beenden, bevor eine der Höchstgrenzen erreicht ist.

Laden Sie Ihre PCAP herunter.

- Klicken Sie auf Reveal (x) Enterprise systems auf **Pakete** aus dem oberen Menü und dann klicken **PCAP herunterladen**.

Um Ihre PCAP zu finden, 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 Packet Capture.

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 pcapng 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.

The screenshot shows the ExtraHop interface with a BPF filter query: `BPF = src portrange 80-443 and net 10.10`. The results show 45,483 packets. A table of 20 packets is displayed, with columns for Time, Src IP, Dst IP, IP Proto, Src Port, Dst Port, Flags, Bytes, Src MAC, Dst MAC, EtherType, and VLAN ID.

Time	Src IP	Dst IP	IP Proto	Src Port	Dst Port	Flags	Bytes	Src MAC	Dst MAC	EtherType	VLAN ID
2018-02-14 15:10:54...	10.10.11.249	10.10.9.69	TCP	443	4429...	ACK	66	44:A8:42:34:16...	00:50:56:94:72...	IPv4	--
2018-02-14 15:10:54...	10.10.11.249	10.10.9.69	TCP	443	4429...	ACK	66	44:A8:42:34:16...	00:50:56:94:72...	IPv4	--
2018-02-14 15:10:54...	10.4.1.49	10.10.252...	TCP	443	4995...	PSH A...	27...	52:54:00:D8:2E...	00:00:0C:07:AC...	IPv4	--

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 192.168.1.10 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: <ul style="list-style-type: none"> • Gepunktetes Viereck (x.x.x.x)

Primitiv	Beispiele	Beschreibung
		<ul style="list-style-type: none"> • Dreifach gepunktet (x.x.x) • Gepunktetes Paar (x.x) • Einzelne Zahl (x)
<code>[ip ip6] tcp tcpflags & (tcp-[ack fin syn rst push urg])</code>	<code>tcp[tcpflags] & (tcp-ack) !=0</code> <code>tcp[13] & 16 !=0</code> <code>ip6 and (ip6[40+13] & (tcp-syn) != 0)</code>	Entspricht allen Paketen mit dem angegebenen TCP-Flag
Fragmentierte IPv4-Pakete (ip_offset! = 0)	<code>ip[6:2] & 0x3fff != 0x0000</code>	Stimmt mit allen Paketen mit Fragmenten überein.

Speichern Sie SSL-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 [Pakete mit gespeicherten Schlüsseln entschlüsseln](#).

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie im Abschnitt Systemkonfiguration auf **Erfassen**.
3. klicken **Speicherung von SSL-Sitzungsschlüsseln**.
4. Wählen **SSL-Sitzungsschlüsselspeicher aktivieren**.
5. klicken **Speichern**.

Nächste Schritte

Weitere Hinweise zum Herunterladen von Sitzungsschlüsseln finden Sie unter [Laden Sie Sitzungsschlüssel mit Paketerfassungen herunter](#).

Laden Sie Sitzungsschlüssel mit Paketerfassungen herunter

Sie können die Datei PCAP Next Generation (pcapng) herunterladen, die alle erfassten SSL-Sitzungsschlüssel für SSL-Paketerfassungen enthält. Anschließend können Sie die zugehörige Paketerfassungsdatei mit einem Paketanalyse-Tool wie Wireshark herunterladen und öffnen, das die entschlüsselte Nutzlast anzeigen kann.

Bevor Sie beginnen

- Sie müssen über einen konfigurierten Packetstore verfügen, bevor Sie Pakete und Sitzungsschlüssel von einem heruntergeladenen Sensor oder einer Konsole. Sehen Sie unsere [Leitfäden zur Bereitstellung](#) um loszulegen.
- Die Konsole muss für SSL Shared Secrets lizenziert sein.
- Die [Speicherung von SSL-Sitzungsschlüsseln](#) Die Einstellung muss am Sensor aktiviert sein.
- Reveal (x) Enterprise-Benutzer müssen entweder Systemzugriff und Administration haben [Privilegien](#) oder eingeschränkte Rechte mit Zugriff auf Pakete und Sitzungsschlüssel. Reveal (x) 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 **Laden Sie PCAP+-Sitzungsschlüssel herunter**.
5. klicken **Laden Sie PCAP+-Sitzungsschlüssel herunter**.

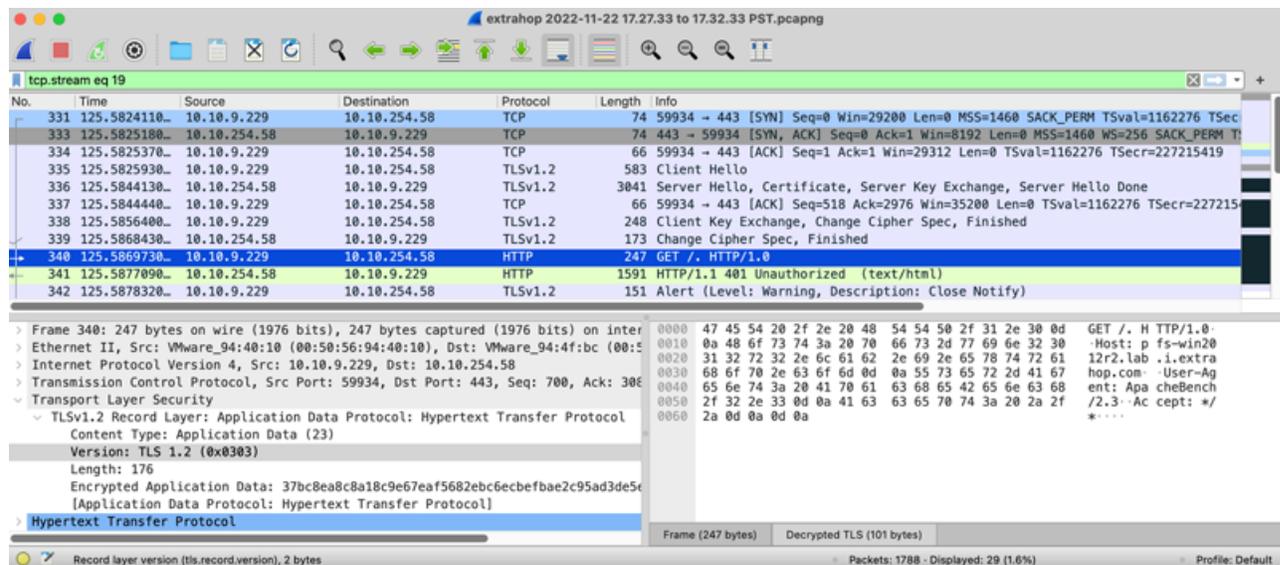
Die pcapng-Datei wird automatisch auf Ihren Computer heruntergeladen und der Vorgang zum Herunterladen des Sitzungsschlüssels wird aufgezeichnet in [Audit-Log](#).

Wenn keine Sitzungsschlüssel für die heruntergeladene PCAP verfügbar sind, wird **Laden Sie PCAP+-Sitzungsschlüssel herunter** 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, **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.



Auslöser

Trigger bestehen aus benutzerdefiniertem Code, der automatisch bei Systemereignissen über die ExtraHop Trigger API ausgeführt wird. Sie können über die Trigger-API einen Trigger schreiben, bei dem es sich um einen JavaScript-Block handelt, 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:

- Erstelle 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 Benutzeragent-Daten, die von einem HTTP Anfrage ist keine Metrik, die in das ExtraHop-System integriert ist. Die ExtraHop Auslöser API bietet jedoch eine HTTP-Eigenschaft für Benutzeragenten , mit der Sie einen Trigger schreiben können, der Benutzeragentendaten als benutzerdefinierte Metrik sammelt.
- Generieren [Aufzeichnungen](#) und schreiben Sie sie in einen Datenspeicher, um sie langfristig zu speichern und abzurufen.
- 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-Nutzlasten von nicht unterstützten Daten zuzugreifen und diese 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 dann klicken **Auslöser**. Auf der Trigger-Seite können Sie [einen Auslöser erstellen](#) oder klicken Sie auf das Häkchen neben einem Auslöser, um [Bearbeiten Sie die Trigger-Konfiguration](#) oder [das Trigger-Skript ändern](#).

Einen Auslöser planen

Das Schreiben eines Auslöser zur Erfassung benutzerdefinierter Metriken ist eine leistungsstarke Methode zur Überwachung Ihrer Anwendungs - und Netzwerkleistung. Trigger verbrauchen jedoch Systemressourcen und können die Systemleistung beeinträchtigen, und ein schlecht geschriebener Auslöser kann zu unnötiger Systemlast führen. Bevor Sie einen Auslöser erstellen, sollten Sie auswerten, was Ihr Auslöser bewirken soll, ermitteln, welche Ereignisse und Geräte zum Extrahieren der benötigten Daten erforderlich sind, 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 SSL-Zertifikate ab?
 - Erhält mein Netzwerk Verbindungen über nicht autorisierte Ports?
 - Wie viele langsame Transaktionen verzeichnet 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 existiert, 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 SSL-Verbindungen ausgeführt werden. Eine vollständige Liste der Systemereignisse finden Sie in [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 kommen, überprüfen Sie die Referenz, um sicherzustellen, dass die Eigenschaft, die Sie extrahieren möchten, verfügbar ist, oder um herauszufinden, welche Eigenschaften in einem Standard-CIFS-Datensatz gesammelt werden.
- Legen Sie fest, wie Sie die vom Auslöser gesammelten Daten visualisieren oder speichern möchten. Sie können beispielsweise Metriken auf einem anzeigen Dashboard oder von Protokoll, Sie können Aufzeichnungen an den Recordstore senden.
- Stellen Sie fest, ob bereits ein Auslöser existiert, der Ihren Anforderungen entspricht oder leicht geändert werden könnte. Beginnen Sie immer mit einem bereits vorhandenen Auslöser, wann immer dies möglich ist. Suchen Sie in den folgenden Ressourcen nach einem vorhandenen Auslöser:
 - [Bestehende Trigger auf der Trigger-Seite](#)
 - [Die ExtraHop Community-Foren](#)

Auslöser bauen

Wenn Sie feststellen, dass Sie einen neuen Auslöser erstellen müssen, machen Sie sich mit den folgenden Aufgaben vertraut, die abgeschlossen werden müssen:

- [Den Auslöser konfigurieren](#) um Details wie den Namen des Auslöser 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 auslösendes Ereignis.
- [Schreiben Sie das Trigger-Skript](#), das die Anweisungen angibt, die der Auslöser ausführt, wenn ein für den Auslöser konfiguriertes Systemereignis eintritt. Das Triggerskript kann Anweisungen für einfache Aufgaben wie die Erstellung einer benutzerdefinierten Gerätezählmetrik namens „slow_rsp“ oder für komplexere Aufgaben wie die Überwachung und Erfassung von Statistiken über die Cloud-Anwendungen, auf die in Ihrer Umgebung zugegriffen wird, bereitstellen.

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.
- [Überprüfen Sie die Diagramme zur Systemintegrität](#) für Trigger-Ausnahmen, Drops aus der Trigger-Warteschlange und unerwartete Aktivitäten.
- Vergewissern Sie sich, dass das Trigger-Skript dem entspricht [Leitfaden mit bewährten Methoden für Trigger](#) .

In Auslösern navigieren

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 das Debuggen aktiviert ist. Wenn das Debuggen aktiviert ist, werden die Ausgaben von Debug-Anweisungen im Trigger-Skript protokolliert [Debug-Log-Ausgabe](#).

Ereignisse

Die Systemereignisse, die dazu führen, dass der Auslöser ausgeführt wird, wie `HTTP_RESPONSE`.

Geändert

Das letzte Mal, dass der Auslöser geändert wurde.

Triggers

Name 41 results

<input type="checkbox"/>	Name ↑	Author	Description	Assignments	Status	Debug Log	Events	Modified
<input type="checkbox"/>	Active Direct...	ExtraHop	Custom metrics for Active Direct...	0	■ ENABLED	■ DISABLED	CIFS_RESPONSE, ...	2017-11-2
<input type="checkbox"/>	AD: DNS Ser...	ExtraHop	DNS service (SRV) resource reco...	0	■ DISABLED	■ DISABLED	DNS_REQUEST, D...	2018-08-2
<input type="checkbox"/>	AD: Group Po...	ExtraHop	Group Policy custom metrics for ...	0	■ DISABLED	■ DISABLED	CIFS_RESPONSE	2018-08-2

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  }

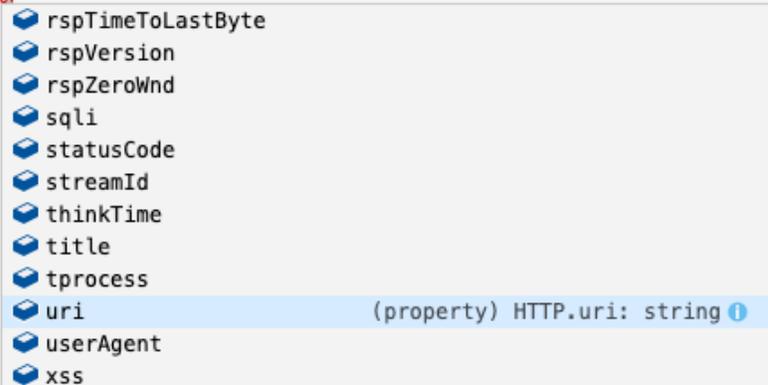
```

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:

```

debug (HTTP.);

```



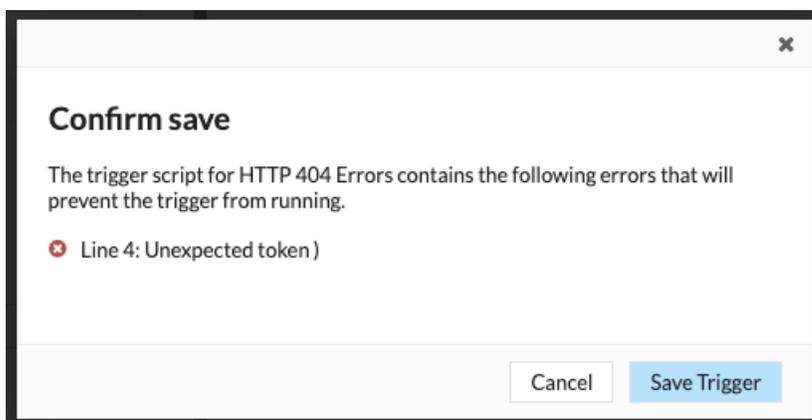
The image shows an autocomplete dropdown menu for the code `debug (HTTP.);`. The dropdown lists various properties and methods of the HTTP object, including `rspTimeToLastByte`, `rspVersion`, `rspZeroWnd`, `sqli`, `statusCode`, `streamId`, `thinkTime`, `title`, `tprocess`, `uri` (highlighted), `userAgent`, and `xss`. The `uri` property is highlighted in blue and includes the text `(property) HTTP.uri: string` and a small information icon.

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	<p>Gibt die Anzahl der Byte an, die pro Paket erfasst werden sollen. Die Gefangennahme beginnt mit dem ersten Byte im Paket. Nur diese Option angeben wenn das Trigger-Skript die PCAP durchführt.</p> <p>Ein Wert von 0 gibt an, dass das Capture alle Bytes in jedem sammeln soll Paket.</p>	<p>Alle Ereignisse mit Ausnahme der folgenden Liste werden unterstützt:</p> <ul style="list-style-type: none"> ALERT_RECORD_COMMIT METRIC_CYCLE_BEGIN METRIC_CYCLE_END FLOW_REPORT NEW_APPLICATION NEW_DEVICE SESSION_EXPIRE
L7-Nutzdatenbyte zum Puffer	<p>Gibt die maximale Anzahl von Nutzdaten-Bytes an, die gepuffert werden sollen.</p> <p> Hinweis: Wenn mehrere Trigger laufen auf demselben Ereignis, der Auslöser mit dem Der höchste Wert für L7-Payload (Byte to Buffer) bestimmt das Maximum Payload für dieses Ereignis für jeden Auslöser.</p>	<ul style="list-style-type: none"> CIFS_REQUEST CIFS_RESPONSE HTTP_REQUEST HTTP_RESPONSE ICA_TICK LDAP_RESPONSE
Bytes in der Zwischenablage	Gibt die Anzahl der Byte an, die in einer Citrix-Zwischenablage gepuffert werden sollen Übertragung.	<ul style="list-style-type: none"> ICA_TICK
Metrischer Zyklus	<p>Gibt die Länge des Metrik Zyklus an, ausgedrückt in Sekunden. Die folgenden Werte sind gültig:</p> <ul style="list-style-type: none"> 30sec 5min 1hr 24hr 	<ul style="list-style-type: none"> METRIC_CYCLE_BEGIN METRIC_CYCLE_END METRIC_RECORD_COMMIT
Metrische Typen	Gibt den Metriktyp anhand des Rohmetriknamens an, z. B. <code>extrahop.device.http_server</code> . Geben Sie mehrere an Metrik	<ul style="list-style-type: none"> ALERT_RECORD_COMMIT METRIC_RECORD_COMMIT

Option	Beschreibung	Unterstützte Ereignisse
Auslöser bei jeder Flow-Turn ausführen	<p>Typen in einer kommagetrennten Liste.</p> <p>Aktiviert die PCAP auf jedem Fluss abbiegen.</p> <p>Die Analyse pro Spielzug analysiert kontinuierlich die Kommunikation zwischen zwei Endpunkten, um einen einzelnen Nutzdatenpunkt zu extrahieren aus dem Fluss.</p> <p>Wenn diese Option aktiviert ist, alle Werte spezifiziert für Übereinstimmende Zeichenfolge für den Client und Übereinstimmende Zeichenfolge auf dem Server Optionen sind ignoriert.</p>	<ul style="list-style-type: none"> • SSL_PAYLOAD • TCP_PAYLOAD
Portbereich des Clients	<p>Gibt den Client-Portbereich an.</p> <p>Gültige Werte liegen zwischen 0 und 65535.</p>	<ul style="list-style-type: none"> • SSL_PAYLOAD • TCP_PAYLOAD • UDP_PAYLOAD
Zu puffernde Client-Bytes	<p>Gibt die Anzahl der Client-Bytes an, die gepuffert werden sollen.</p> <p>Der Wert von Diese Option kann nicht auf 0 gesetzt werden, wenn der Wert von Server-Bytes zum Puffern Option ist auch auf 0 setzen.</p>	<ul style="list-style-type: none"> • SSL_PAYLOAD • TCP_PAYLOAD
Suchzeichenfolge für den Client-Puffer	<p>Gibt die Formatzeichenfolge an, die angibt, wann begonnen werden soll Pufferung von Client-Daten. Gibt das gesamte Paket auf einer Zeichenfolge zurück Spiel.</p> <p>Sie können die Zeichenfolge als Text oder Hexadezimalzahlen angeben. Zum Beispiel beide <code>ExtraHop</code> und <code>\x45\x78\x74\x72\x61\x48\x6F\x70</code> sind gleichwertig. Hexadezimalzahlen sind keine Groß-/Kleinschreibung empfindlich.</p> <p>Jeder für diese Option angegebene Wert wird ignoriert wenn der Pro Spielzug oder</p>	<ul style="list-style-type: none"> • SSL_PAYLOAD • TCP_PAYLOAD • UDP_PAYLOAD

Option	Beschreibung	Unterstützte Ereignisse
	Auslöser ausführen auf allen UDP Paketoption ist aktiviert.	
Portbereich des Servers	Gibt den Serverportbereich an. Gültige Werte sind 0 bis 65535.	<ul style="list-style-type: none"> SSL_PAYLOAD TCP_PAYLOAD UDP_PAYLOAD
Server-Bytes zum Puffer	Gibt die Anzahl der Server-Bytes an, die gepuffert werden sollen. Der Wert von Diese Option kann nicht auf 0 gesetzt werden, wenn der Wert von Zu puffernde Client-Bytes Option ist auch auf 0 setzen.	<ul style="list-style-type: none"> SSL_PAYLOAD TCP_PAYLOAD
Suchzeichenfolge für den Serverpuffer	Gibt die Formatzeichenfolge an, die angibt, wann begonnen werden soll Pufferung von Serverdaten. Sie können die Zeichenfolge als Text angeben oder Hexadezimalzahlen. Zum Beispiel beide <code>ExtraHop</code> und <code>\x45\x78\x74\x72\x61\x48\x6F\x70</code> sind gleichwertig. Hexadezimalzahlen sind keine Groß-/Kleinschreibung empfindlich. Jeder für diese Option angegebene Wert wird ignoriert wenn der Pro Spielzug oder Auslöser ausführen auf allen UDP Option ist aktiviert.	<ul style="list-style-type: none"> SSL_PAYLOAD TCP_PAYLOAD UDP_PAYLOAD
Auslöser für alle UDP-Pakete ausführen	Ermöglicht die Erfassung aller UDP-Datagramme.	<ul style="list-style-type: none"> UDP_PAYLOAD
Führen Sie FLOW_CLASSIFY für ablaufende, nicht klassifizierte Flows aus	Ermöglicht die Ausführung des Ereignis nach Ablauf, um Metriken zu sammeln zum Flüsse die vorher nicht klassifiziert wurden ablaufend.	<ul style="list-style-type: none"> FLOW_CLASSIFY
Externe Typen	Gibt die Typen der externen Daten an, die der Auslöser verarbeitet. Das Der Auslöser wird nur ausgeführt, wenn die Nutzlast ein Typfeld mit einem von enthält die angegebenen Werte. Geben Sie mehrere Typen	<ol style="list-style-type: none"> EXTERNAL_DATA

Option	Beschreibung	Unterstützte Ereignisse
	durch Kommas getrennt an auflisten.	

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:

PROBLEMS DEBUG LOG

```
[Fri Jun 17 10:18:58] www.seattlefoodtruck.com/wp-content/uploads/2019/03/Nibbles.jpg
[Fri Jun 17 10:18:57] www.seattlefoodtruck.com/wp-content/themes/Impreza/framework/fonts/fontawesome-webfont.woff2
[Fri Jun 17 10:18:57] www.seattlefoodtruck.com/wp-content/uploads/2019/04/Xplosive-600x425.jpg
[Fri Jun 17 10:18:45] www.seattlefoodtruck.com/food-trucks/nibbles/
[Fri Jun 17 10:18:45] www.seattlefoodtruck.com/wp-content/uploads/2019/03/BuddhaBruddah-600x425.jpg
[Fri Jun 17 10:18:45] www.seattlefoodtruck.com/wp-content/uploads/2019/01/Thai-U-Up-600x425.jpg
[Fri Jun 17 10:18:39] www.seattlefoodtruck.com/wp-content/uploads/2019/02/MiniTheDoughnut-600x425.jpg
```

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.

PROBLEMS DEBUG LOG

```
[Wed Jun 12 15:50:59] Line 11: Uncaught Error: Second argument must be object
[Wed Jun 12 15:51:29] Line 11: Uncaught Error: Second argument must be object
[Wed Jun 12 15:51:59] Line 11: Uncaught Error: Second argument must be object
[Wed Jun 12 15:52:29] Line 11: Uncaught Error: Second argument must be object
```

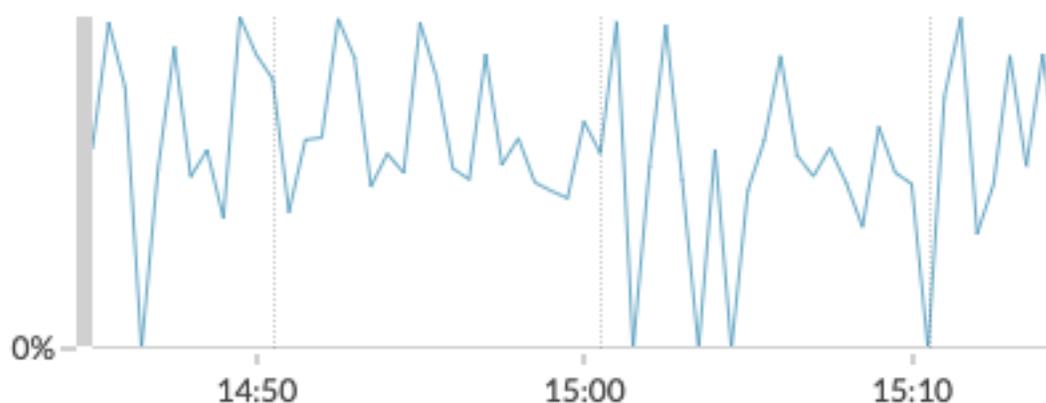
Die Leistung eines einzelnen Auslöser anzeigen

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-Leistungsdigramm angezeigt, in dem die Anzahl der Zyklen aufgezeichnet wird, die der Auslöser innerhalb eines bestimmten Zeitintervalls verbraucht hat.

Capture Trigger Load



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.
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.

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

Mit ExtraHop-Bundles können Sie dem ExtraHop-System vorkonfigurierte Anpassungen hinzufügen.

Bevor Sie beginnen

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 **Bündel**.
4. klicken **Paket hochladen**.
5. In der Paket hochladen Fensterbereich, klicken **Wählen Sie Datei**, und wählen Sie dann die Bundle-JSON-Datei aus, die Sie hochladen möchten.
Es werden Details zum Inhalt des Paket 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 Benachrichtigungen und Auslöser werden zu den ausgewählten Websites hinzugefügt. Sie können Anpassungen jedoch nur in dem ExtraHop-System anzeigen, aktivieren und konfigurieren, auf dem das Paket installiert wurde .

- b) Wählen Sie den **Inbegriffene Aufgaben anwenden** Checkbox.
Diese Option weist das Paket den im Bundle enthaltenen Metrikquellen zu. In den meisten Fällen ist es am besten, die Standardzuweisungen anzuwenden.
- c) Wählen Sie den **Bestehenden Inhalt überschreiben** Checkbox.
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 **Installieren**.

Nächste Schritte

- Aktiviere irgendeinen [löst aus](#) im Bundle enthalten.
- Beliebiges konfigurieren [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.

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 **Bündel**.
3. Auf dem Bündel Seite, klick **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, das eine neuere Firmware-Version erfordert, 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. Auslöser, Dashboards und Benachrichtigungen. 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 außer dem aus, auf das Sie geklickt haben.

SHIFT + Klick

Wählen Sie alle Elemente außer dem, auf das Sie geklickt haben, ab.

5. klicken **Speichern**.

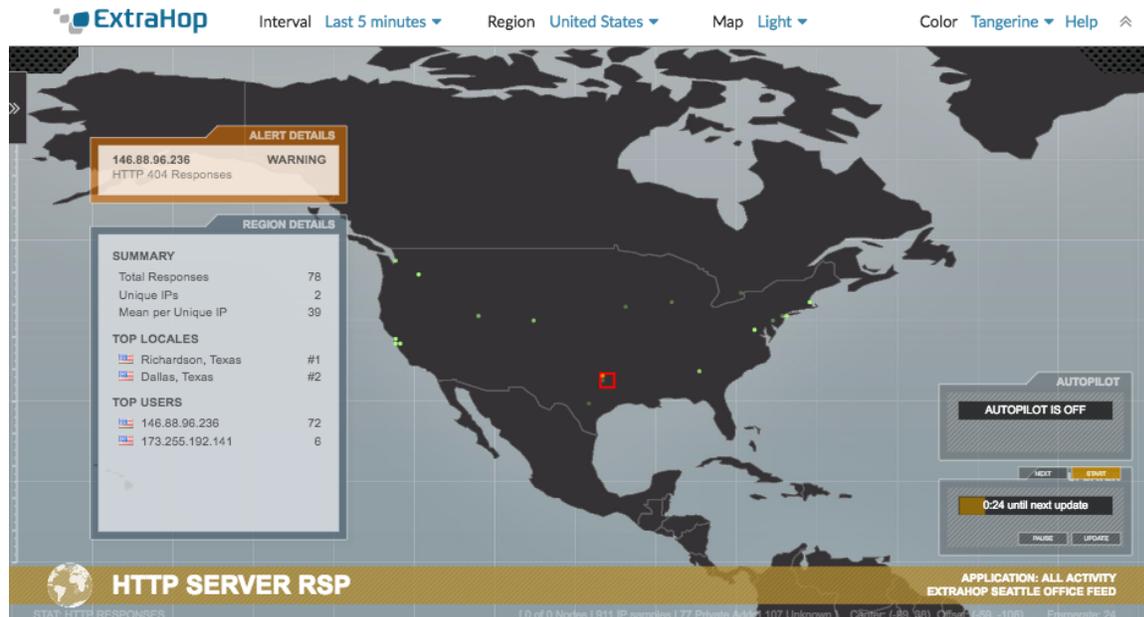
Sie können die von Ihnen erstellte Bundle-JSON-Datei herunterladen, indem Sie das Paket aus der Liste auswählen und dann auf **Paket herunterladen** aus dem rechten Bereich.

Nächste Schritte

- [Installieren Sie Ihr Paket auf einem anderen ExtraHop-System](#)

Geomaps

Eine Geomap ist eine visuelle Darstellung der weltweiten Aktivitäten auf der Grundlage einer einzigen Zählung, Metrik. Das ExtraHop-System bestimmt die ursprüngliche IP-Adresse jeder Metrik Ereignis und zeichnet es auf einem regionalen Datenpunkt auf der Geomap auf.



Generieren Sie eine Geomap im Handumdrehen von einer Metrik-Detailseite aus. Sie können nur Geomaps für Zählmetriken generieren, die nach einer IP-Adresse aufgeschlüsselt werden können.

Regionale Details anzeigen

Eine auf einer Geomap verfolgte Metrik zeigt einen Datenpunkt für jeden Ort an, von dem die Metrikdaten stammen. Weisen Sie beispielsweise einer Geomap eine SSH-Sitzungsmetrik zu, um herauszufinden, ob SSH-Versuche von nicht autorisierten Orten kommen. Jeder Datenpunkt zeigt die IP-Adressen an, die die Anfragen gesendet haben. Klicken Sie auf einen Datenpunkt, um die folgenden regionalen Aktivitätsdetails anzuzeigen:

Zusammenfassung

Zeigt die folgenden Informationen zur Benutzeraktivität in der Region an:

- Die Gesamtzahl der IP-Adressen, auf die eine Antwort oder eine Anfrage gestellt wurde.
- Die Anzahl der eindeutigen IP-Adressen an der Gesamtzahl der Adressen.
- Die durchschnittliche oder durchschnittliche Anzahl von IP-Adressen pro eindeutiger IP-Adresse.

Top-Lokale

Zeigt die beiden wichtigsten Gebietschemas an, die in der Region die meisten Aktivitäten generieren. Locales sind Städte, die geografisch nahe beieinander liegen und in einer Region zusammengefasst werden können. In dem Fenster könnten beispielsweise Mountain View, Kalifornien, und Oakland, Kalifornien, als Top-Standorte für eine Region angezeigt werden.

Die besten Nutzer

Zeigt die sechs Benutzer an, die in der Region die meisten Aktivitäten generiert haben. Jeder Benutzer wird anhand der IP-Adresse identifiziert, und die Anzahl der von jeder IP-Adresse generierten Antworten oder Anfragen wird angezeigt.

Warnungsdetails anzeigen

Eine auf einer Geomap verfolgte Metrik kann mit einer oder mehreren verknüpft sein Warnungen. Wenn die Metrikaktivität die Warnbedingungen erfüllt, gibt das Erscheinungsbild des Datenpunkts den Schweregrad an. Die Schweregrad von Warnungen werden auf der Geomap durch die folgenden Farben dargestellt:

Grau

Zeigt an, dass keine benutzerdefinierten Benachrichtigungen konfiguriert sind oder dass die Warnungseinstellungen so konfiguriert sind, dass eine einzelne Alarm wird, wenn die Bedingungen erfüllt sind, auch wenn der Zustand andauert.

Grün

Zeigt an, dass keine benutzerdefinierten Warnungen konfiguriert sind oder dass eine Alarm mit dem Schweregrad Debug und Informationale generiert wurde.

Orange

Zeigt an, dass mindestens eine Alarm mit dem Schweregrad Hinweis oder Warnung generiert wurde.

Rot mit sich drehenden Kanten

Zeigt an, dass mindestens eine Alarm mit dem Schweregrad Fehler oder Kritisch generiert wurde.

Rot mit Sonarsignalen

Zeigt an, dass mindestens eine Alarm mit dem Schweregrad Notfall oder Warnung generiert wurde.

Wenn eine Alarm beispielsweise so konfiguriert ist, dass HTTP-Antworten auf einer Gruppe von Webservern überwacht werden, sodass jedes Mal, wenn die Fehlerquote 5% überschreitet, eine Benachrichtigung auf kritischer Ebene gesendet wird. Wenn Ihre Geomap HTTP-Antworten auf denselben Webservern verfolgt, werden Datenpunkte rot angezeigt, wobei sich die Kanten in jeder Region drehen, in der die Warnbedingung erfüllt ist.

Das Verhalten einer Alarm wirkt sich auf die Datenpunkte auf der Geomap aus. Eine Alarm kann so konfiguriert werden, dass sie einmal ausgelöst wird, wenn die Alarmbedingung erfüllt ist, was zu einem einmaligen Datenpunkt auf der Karte führt. Oder eine Alarm kann so konfiguriert werden, dass sie in regelmäßigen Intervallen ausgelöst wird, solange die Warnbedingung erfüllt ist, was zu einem Datenpunkt führt, der den kontinuierlichen Status widerspiegelt.

Klicken Sie auf einen Datenpunkt, um die folgenden Warninformationen anzuzeigen:

- Die IP-Adressen, für die eine Alarm generiert wurde.
- Der Schweregrad der Alarm, der jeder IP-Adresse zugeordnet ist.
- Der Name der Alarm, die jeder IP-Adresse zugeordnet ist.

siehe [Alerts](#) für weitere Informationen zur Konfiguration von Warnmeldungen und Schweregraden von Warnungen.

Navigieren Sie in den Displaysteuerungen

Jede Geomap zeigt die folgenden Informationen und Steuerelemente an:

Bedienelemente anzeigen

Einstellungen, die das Aussehen der Geomap und den Zeitraum der angezeigten Daten bestimmen.

Aktivitätsdiagramme

Grafiken, die Benutzeraktivitäten in kleineren Datensätzen anzeigen.

Autopilot

Eine Funktion, die automatisch zwischen den acht Regionen mit den meisten Benutzeraktivitäten navigiert.

Aktualisierer

Ein Timer, der bis zur nächsten Aktualisierung der Daten auf der Geomap herunterzählt.

Weitere Informationen zu Geomaps finden Sie in der [Häufig gestellte Fragen zu Geomaps](#).

Generieren Sie eine Geomap

Das ExtraHop-System macht es Ihnen leicht, im Handumdrehen eine Geomap von einer Metrik-Detailseite aus zu erstellen. Das ExtraHop-System bestimmt die ursprüngliche IP-Adresse jeder Metrik Ereignis und zeichnet es auf einem regionalen Datenpunkt auf der Geomap auf.

Sie können nur Geomaps für Zählmetriken generieren, die nach einer IP-Adresse aufgeschlüsselt werden können.

Informationen darüber, wie Geomaps funktionieren und welche Informationen bereitgestellt werden, finden Sie unter [Geomaps](#).

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Gehen Sie zu dem Gerät, der Anwendung oder dem Dashboard, auf dem die Zählmetrik angezeigt wird, die Sie verfolgen möchten.
 - Um zu einer Geräteseite zu wechseln, klicken Sie auf **Vermögenswerte**, klicken **Geräte** oder **Gerätegruppen** im linken Bereich, und klicken Sie dann auf das gewünschte Gerät.
 - Um zu einer Anwendungsseite zu gelangen, klicken Sie auf **Vermögenswerte**, klicken **Bewerbungen** im linken Bereich, und klicken Sie dann auf die gewünschte Anwendung.
 - Um zu einem Dashboard zu gelangen, klicken Sie auf **Armaturenbretter**, und klicken Sie dann auf das gewünschte Dashboard.



Hinweis Wenn es kein Dashboard oder keine Quellseite gibt, auf der die gewünschte Zählmetrik angezeigt wird, [ein Diagramm erstellen](#) und füge es zu einem Dashboard.

3. Klicken Sie auf die Bezeichnung der Zählmetrik, um ein Kontextmenü zu öffnen, und wählen Sie dann den Schlüssel für die gewünschte Detail-Metrik aus der **Drilldown nach** Liste.

Je nach Metrik kann es sich bei den verfügbaren Schlüsseln um Client-, Server- oder IP-Schlüssel handeln.

Die Detailseite für die Quelle der Metrik wird angezeigt.

4. Klicken Sie auf **Geomap ansehen** knopf.
Die Geomap wird im Vollbildmodus auf einer neuen Browser-Registerkarte geöffnet.



Hinweis Sie können die Geomap-URL speichern oder mit einem Lesezeichen versehen, um schnell zu ihr zurückzukehren.

Anlage

Protokollmodule

Das ExtraHop-System stellt Metriken über die folgenden Arten von Protokollmodulen bereit:

Typ des Moduls	Protokolle
L2-L3 Metriken	<ul style="list-style-type: none"> • Multicast • IP • IPv6 • ICMP • ICMP v6
L4-Metriken	<ul style="list-style-type: none"> • TCP • UDP
Benennung	DNS
Verzeichnisdienste	LDAP
Netz	<ul style="list-style-type: none"> • HTTP/HTTPS • AMF • SSL
Middleware	<ul style="list-style-type: none"> • MS-RPC • Memcache • IBMMQ
Datenbank	<ul style="list-style-type: none"> • IBM DB2 • IBM Informix • Microsoft SQL Server • MongoDB • MySQL • Orakel • PostgreSQL • Sybase ASE • Sybase IQ
Aufbewahrung	<ul style="list-style-type: none"> • iSCSI • CIFS • NFS
Übertragung von Dateien	FTP
Post	SMTP
Citrix VDI	<ul style="list-style-type: none"> • ICA • CGP
Branchenspezifische Protokolle	<ul style="list-style-type: none"> • Durchmesser • FIX

Typ des Moduls	Protokolle <ul style="list-style-type: none"> • HL7 • RADIUS • SMPP • Telnet
Entschlüsselung	Irgendein Protokoll verschlüsselt über einen Ende-zu-Ende-SSL-Kanal, kann mit dem SSL-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

In diesem Handbuch werden die folgenden gebräuchlichen Akronyme für Computer- und Netzwerkprotokolle verwendet.

Abkürzung	Vollständiger Name
AAA	Authentifizierung, Autorisierung und Abrechnung
AMF	Format der Aktionsmeldung
CIFS	Gemeinsames Internet-Dateisystem
CLI	Befehlszeilenschnittstelle
CPU	Zentrale Verarbeitungseinheit
DB	Datenbank
DHCP	Dynamisches Host-Konfigurationsprotokoll
DNS	Domainnamensystem
ERSPAN	Gekapselter RSPAN
FIX	Austausch von Finanzinformationen
FTP	FTP
HTTP	Hypertext-Übertragungsprotokoll
IBMMQ	IBM Nachrichtenorientierte Middleware
ICA	Unabhängige Computerarchitektur

Abkürzung	Vollständiger Name
IP	Internet-Protokoll
iSCSI	Internet-Systemschnittstelle für kleine Computer
L2	Schicht 2
L3	Schicht 3
L7	Schicht 7
LDAP	Lightweight Directory Access Protocol
MAC	Medienzugriffskontrolle
MIB	Informationsbasis für das Management
NFS	NFS
NVRAM	Nichtflüchtiger Direktzugriffsspeicher
RADIUS	Dial-In-Benutzerdienst mit Remoteauthentifizierung
RPC	Prozeduraufruf aus der Ferne
RPCAP	Paketerfassung aus der Ferne
RSS	Größe des Resident-Sets
SMPP	Peer-to-Peer-Protokoll für Kurznachrichten
SMTP	Einfaches Nachrichtenübertragungsprotokoll
SNMP	Einfaches Netzwerkmanagement-Protokoll
SPAN	Analysator für geschaltete Ports
SSD	Solid-State-Laufwerk
SSH	Sichere Shell
SSL	Sicherer Socket-Layer
TACACS+	Terminal Access Controller Zutrittskontrollsystem Plus
TCP	TCP
UI	Benutzerschnittstelle
VLAN	VLAN
VM	Virtuelle Maschine

Tastenkürzel

Mithilfe von Tastenkombinationen können Sie schnell im ExtraHop-System navigieren oder bestimmte Aktionen mit wenigen Tastenanschlägen ausführen.

Die folgenden Tastenkombinationen gelten für das gesamte ExtraHop-System.

Schlüssel	Aktion
?	Ein Hotkey-Hilfemenü ein- oder ausblenden
G dann S	Gehe zu Armaturenbrett

Schlüssel	Aktion
G dann A	Gehe zu Alerts
G dann P	Gehe zu Anwendungsmetriken
G dann N	Gehe zu Network Metrics
G dann D	Gehe zu Device Metrics
G dann G	Gehe zu Group Metrics
/	Weltweite Suche
O dann M	Offen Metric Explorer
G dann E	Gehe zu Einstellungen
G dann T	Gehe zum Trigger Editor
G dann H	Hilfe öffnen
O dann Q	Systeminformationen anzeigen
Strg+S	Widget-Konfiguration speichern

Die folgenden Tastenkombinationen gelten nur für Dashboards.

Schlüssel	Aktion
O dann L	Layoutmodus bearbeiten umschalten
O dann P	Dashboard-Eigenschaften anzeigen
C dann D	Kopieren Sie das aktuelle Dashboard
D dann D	Das aktuelle Dashboard löschen
O dann S.	Beschreibungen umschalten
Strg+Aufwärtspfeil+F	Präsentationsmodus umschalten
N dann D	Neues Dashboard erstellen
N dann F	Einen neuen Ordner erstellen
O dann D	Dock-Bearbeitungsmodus umschalten