Aufzeichnungen

Veröffentlicht: 2024-09-26

Datensätze sind strukturierte Informationen über Transaktions-, Nachrichten- und Netzwerkflüsse, die generiert und vom ExtraHop-System an einen Recordstore gesendet werden. Nachdem Ihre Aufzeichnungen gesammelt und gespeichert wurden, können Sie sie im gesamten ExtraHop-System abfragen.

Aufzeichnungen werden auf zwei Protokollebenen gesammelt: L3 und L7. L3- (oder Fluss-) Datensätze zeigen Transaktionen auf Netzwerkebene zwischen zwei Geräten über das IP-Protokoll. L7-Datensätze zeigen Transaktionen, die nachrichtenbasiert (wie ActiveMQ, DNS und DHCP), transaktional (wie HTTP, SMB und NFS) und sitzungsbasiert (wie TLS und ICA) sind.

Wenn Sie beispielsweise fünfzig HTTP 503-Fehler hätten, würden die zugehörigen HTTP-Transaktionen Details über die URL, den Server, den Client, der die Anfrage gesendet hat, usw. enthalten. Diese Details können Ihnen helfen, das zugrunde liegende Problem zu identifizieren.

Video: Sehen Sie sich die entsprechende Schulung an: Aufzeichnungen

Bevor du anfängst

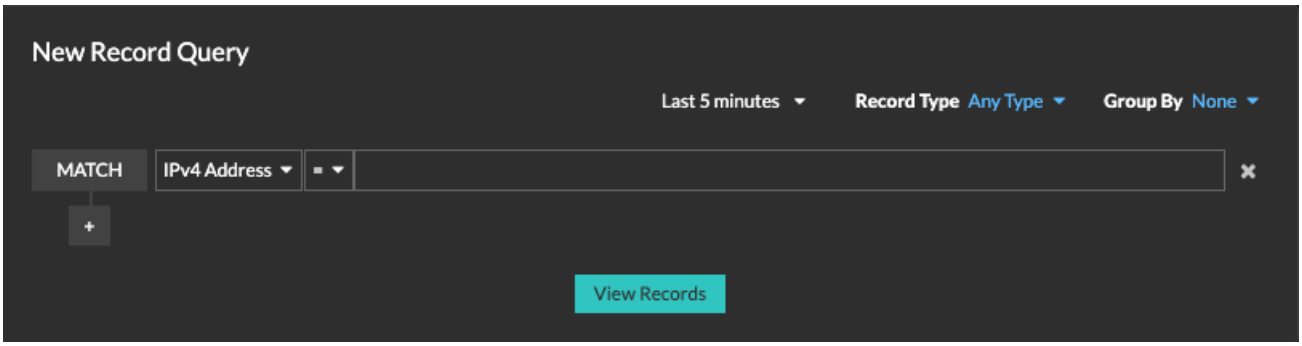
- Sie müssen einen konfigurierten Recordstore haben, z. B. ExtraHop Recordstore, Splunk, Google BigQuery, oder CrowdStrike Falcon LogScale.
- Sie können nur einen Recordstore für das ExtraHop-System konfigurieren.
- Ihr ExtraHop-System muss für das Sammeln und Speichern konfiguriert sein Flussaufzeichnungen oder L7-Datensätze.

In Datensätzen navigieren

Auf der Hauptseite „Datensätze“ werden mehrere Möglichkeiten zur Abfrage von gespeicherten Datensätzen angezeigt. klicken **Rekorde** aus dem oberen Menü, um loszulegen.

Standardsuche

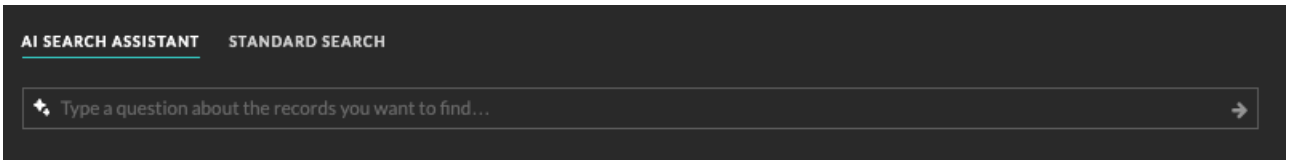
Fragen Sie mit einer Standardsuche nach Datensätzen ab, um einen komplexen Filter zu erstellen, indem Sie die Operatoren „AND“ und „OR“ mit zusätzlichen Filteroptionen wie Datensatztyp und Zeitintervall kombinieren . Erfahren Sie mehr über das Abfragen von Datensätzen mit einer Standardsuche.



KI-Suchassistent

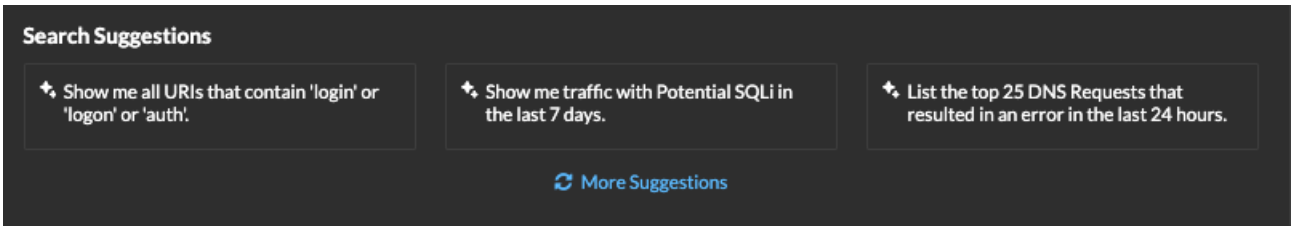
AI Search Assistant hilft Ihnen bei der Suche nach Datensätzen mit Fragen, die in natürlicher, alltäglicher Sprache verfasst sind, sodass Sie im Vergleich zur Erstellung einer Standardsuchabfrage mit denselben Kriterien schnell komplexe Abfragen erstellen können. Der AI Search Assistant muss

von Ihrem ExtraHop-Administrator aktiviert werden.Erfahren Sie mehr über das Abfragen von Datensätzen mit dem AI Search Assistant.



Vorschläge für die Suche

Das ExtraHop-System bietet mehrere Suchvorschläge mit vorgefertigten Filtern , mit denen Sie häufig verwendete Datensatzsuchen effizienter durchführen können. Klicken Sie auf eine vorgeschlagene Suche, um die Abfrage anzuwenden und sofort Datensätze anzuzeigen, oder klicken Sie auf **Weitere Vorschläge** für mehr Optionen.



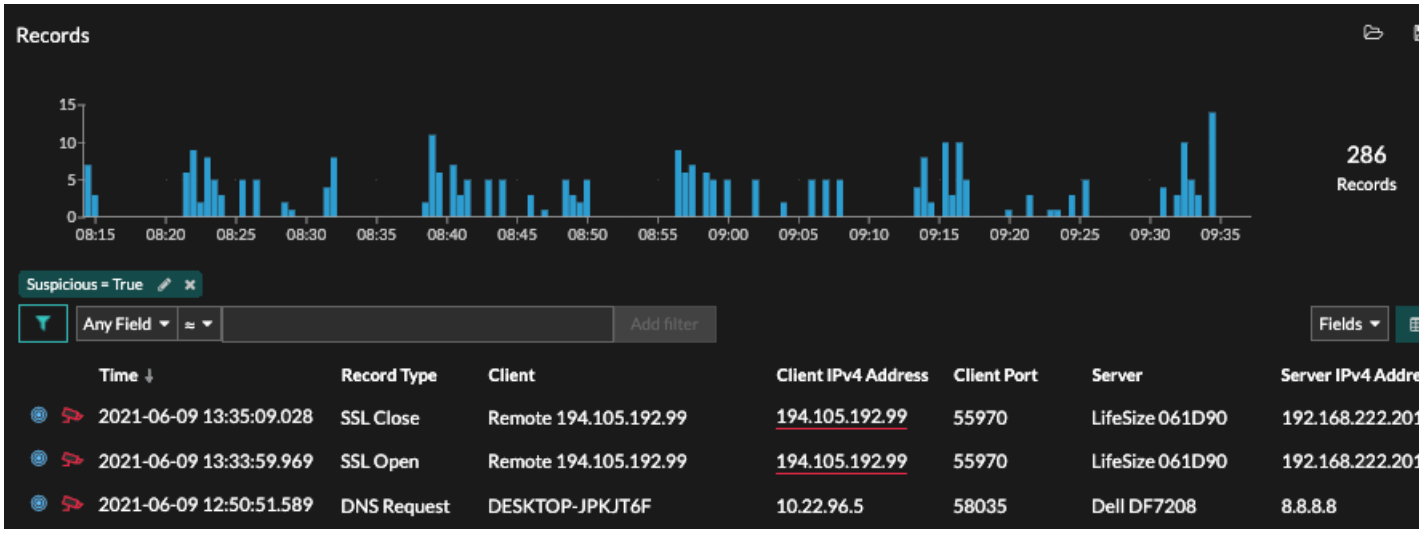
Gespeicherte Abfragen

Sie können auch eine zuvor gespeicherte Abfrage aus der Liste auf der Seite Datensätze auswählen und sofort Datensätze anzeigen, oder Sie können auf das Ordnersymbol klicken in der oberen rechten Ecke der Seite, um alle gespeicherten Abfragen anzuzeigen.

Hinweis: Um eine Datensatzabfrage für eine benutzerdefinierte Metrik zu erstellen, müssen Sie zunächst die Datensatzbeziehung definieren, indem Sie Verknüpfung der benutzerdefinierten Metrik mit einem Datensatztyp.

Ergebnisse einer Datensatzabfrage anzeigen

Nachdem Sie die Abfrage abgeschickt haben, werden die Ergebnisse auf der Hauptseite „Datensätze “ angezeigt.



Hinweis: Eine Abfrage kann Millionen von Datensätzen basierend auf dem Zeitintervall und den Filterkriterien zurückgeben. Wenn eine Abfrage die maximale Anzahl von Abfrageergebnissen überschreitet, wird eine gekürzte Anzahl von Datensätzen angezeigt (nur ExtraHop-Recordstore). Beispielsweise führen Abfragen aus dem Standardfilter Beliebiges Feld häufig zu einer sehr großen Anzahl von Ergebnissen und können sich auf die Leistung auswirken.

Hier sind einige Möglichkeiten, wie Sie die Ergebnisse von Datensatzabfragen aufschlüsseln können:

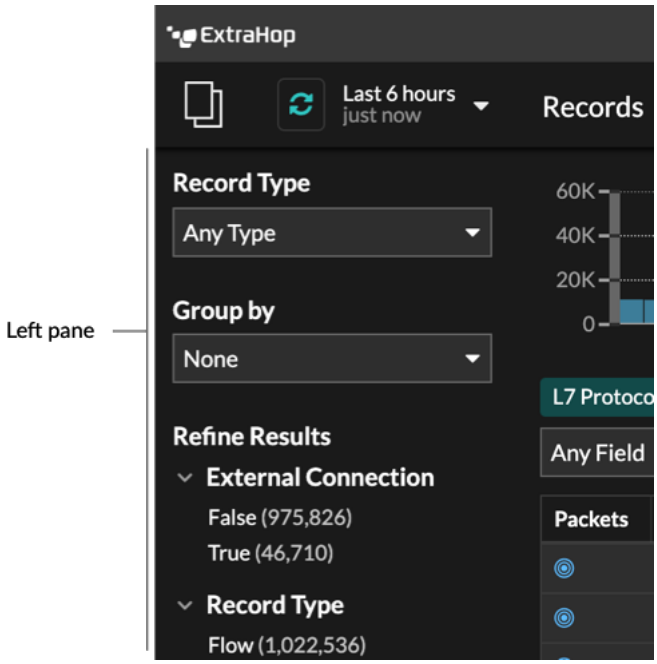
- Zeigen Sie im Datensatzdiagramm mit der Maus auf ein Zeitintervall, um die Anzahl der Datensätze anzuzeigen, oder klicken und ziehen Sie über das Diagramm, um die Ergebnisse der Datensatzabfrage auf ein bestimmtes Zeitintervall einzugrenzen.
- Klicken Sie auf einen Hostnamen oder eine IP-Adresse, um Details zum Gerät oder Externer Endpunkt anzuzeigen.
- Datensätze, die verdächtige IP-Adressen, Hostnamen und URIs enthalten, werden mit einem roten Kamerasymbol angezeigt. Klicken Sie auf das Kamerasymbol, um es anzuzeigen Bedrohungsinformationen für's Datensatz.
- Klicken Sie auf ein Paketsymbol, um eine zu starten Paketabfrage das wird durch diesen Datensatz gefiltert.
- Datensatzergebnisse werden standardmäßig in einer Tabelle angezeigt. Klicken Sie auf die Tabellenansicht oder die ausführliche Ansicht Symbole zum Umschalten der Anzeige.
- Eine Abfrage wird automatisch angehalten, wenn die Anzahl der gescannten oder zurückgegebenen Datensatzbytes extrem groß ist. Wenn die Abfrage angehalten ist, zeigt sie die neuesten Datensätze an. klicken **Abfrage fortsetzen** um die Suche fortzusetzen.
- Klicken Sie auf **Felder** Dropdownliste, um der Datensatzansicht zusätzliche Datensatzinformationen hinzuzufügen.
- Klicken und ziehen Sie in der Tabellenansicht die Spaltenüberschriften, um die Datensatzinformationen anzuordnen.
- Bewerben einfach oder erweiterte Filter um potenzielle Probleme zu finden, z. B. zu lange Bearbeitungszeiten oder ungewöhnliche Antwortgrößen.

Verfeinern Sie Ihren Datensatzabfragefilter

Es gibt eine Reihe von Möglichkeiten, Ihren Datensatzabfragefilter zu verfeinern, um genau die Datensätze zu finden, nach denen Sie suchen. Die folgenden Abschnitte beschreiben jede Methode und zeigen Beispiele, mit denen Sie sich zunächst vertraut machen können.

Filtern der Datensatzergebnisse aus dem linken Bereich

Nachdem alle verfügbaren Datensätze für das gewählte Zeitintervall auf der Seite Datensätze angezeigt wurden, können Sie im linken Bereich filtern, um Ihre Ergebnisse zu verfeinern.



Das **Typ des Datensatzes** Das Drop-down-Menü zeigt eine Liste aller Datensatztypen an, für deren Erfassung und Speicherung Ihr ExtraHop-System konfiguriert ist. Ein Datensatztyp bestimmt, welche Daten gesammelt und im Recordstore gespeichert werden.

Hinweis: Da Sie einen Auslöser schreiben müssen, um Datensätze zu sammeln, benötigen Sie eine Möglichkeit, den Typ der zu sammelnden Daten zu identifizieren. Es gibt integrierte Datensatztypen, die alle verfügbaren bekannten Felder für ein Protokoll sammeln. Sie können mit einem integrierten Datensatztyp (z. B. HTTP) beginnen und einen Auslöser schreiben, der nur die Felder für dieses Protokoll erfasst, die für Sie von Bedeutung sind (wie URI und Statuscode). Fortgeschrittene Benutzer können auch einen benutzerdefinierten Datensatztyp erstellen, wenn sie proprietäre Informationen sammeln müssen, die über einen integrierten Datensatztyp nicht verfügbar sind.

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

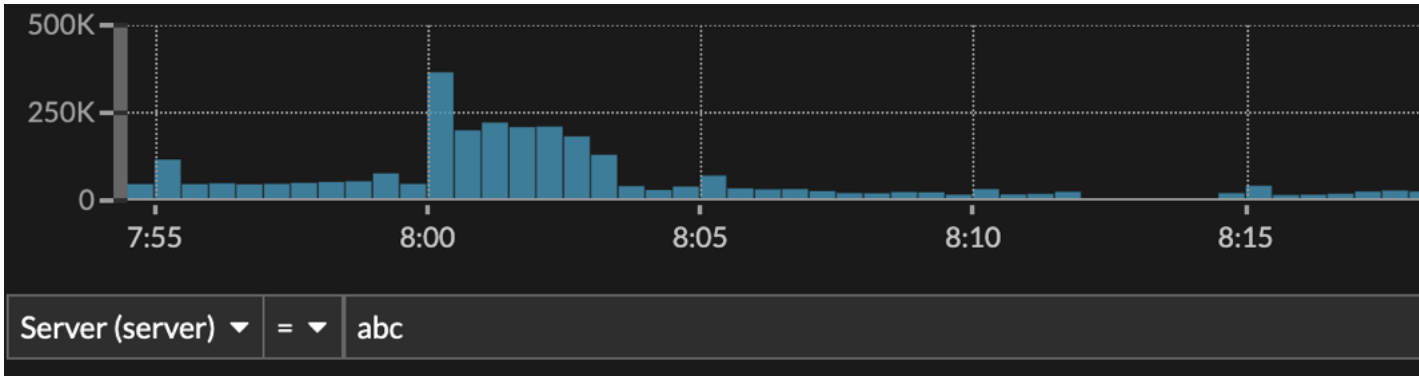
Das **Ergebnisse verfeinern** Dieser Abschnitt zeigt Ihnen eine Liste gängiger Datensatzfilter für den ausgewählten Datensatztyp mit der Anzahl der Datensätze, die dem Filter in Klammern entsprechen.

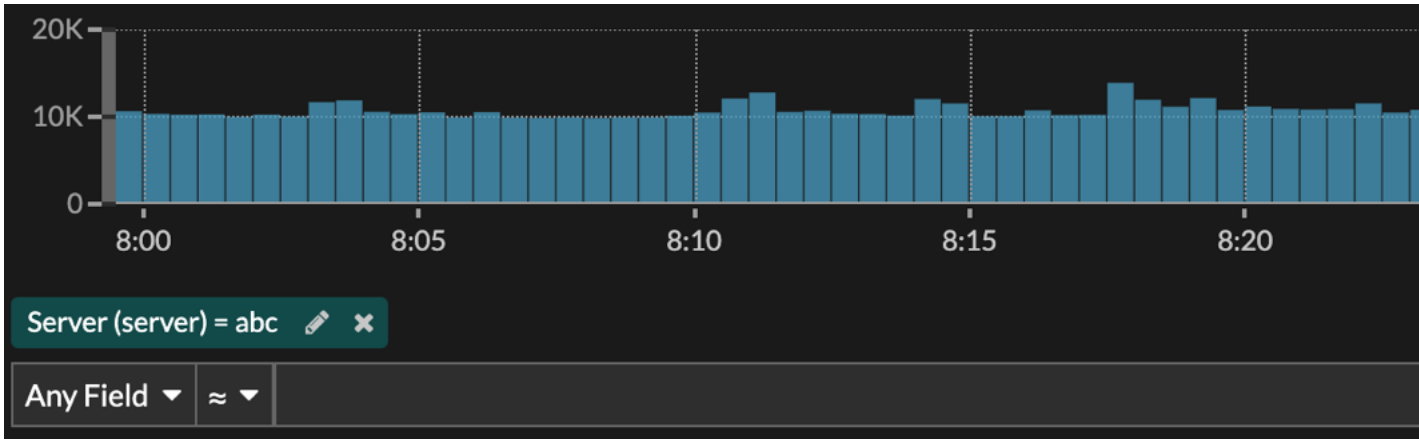
Filterung der Datensatzergebnisse durch das Dreifeld

Klicken Sie auf das Stiftsymbol um einen vorhandenen Filter zu bearbeiten, oder klicken Sie auf die Schaltfläche Advance Filter hinzufügen um einen neuen Filter hinzuzufügen.

In der **Anzeigename des Filters** Feld, Sie können einen beschreibenden Namen angeben, um den allgemeinen Zweck der Abfrage zu identifizieren.

Wählen Sie eine Kriterienoption aus dem Dropdownmenü aus (die Standardoption ist IPv4-Adresse), wählen Sie einen Operator aus (z. B. das Gleichheitszeichen (=)), und geben Sie dann den Suchwert ein. Klicken Sie **Filter hinzufügen**, und der Filter wird über der Filterleiste hinzugefügt.





Ihre Ergebnisse zeigen nur Datensätze, die dem Filter entsprechen.

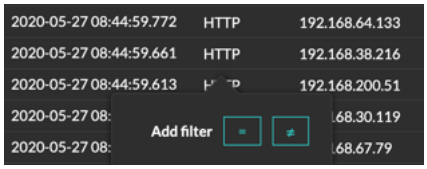
Die folgenden Operatoren können basierend auf dem ausgewählten Feldnamen ausgewählt werden:

Betreiber	Beschreibung
=	Ist gleich
≈	Ist nicht gleich
≈	Beinhaltet Wenn Datensätze in einem ExtraHop-Recordstore gespeichert sind, entspricht der Include-Operator ganzen Wörtern, die durch Leerzeichen und Satzzeichen getrennt sind. Beispielsweise würde eine Suche nach „www.extra“ auf „www.extra.com“, aber nicht auf „www.extrahop.com“ passen. Bei allen anderen Datensatzspeichern entspricht der Include-Operator Teilzeichenfolgen, einschließlich Leerzeichen und Satzzeichen. Beispielsweise würde eine Suche nach „www.extra“ mit „www.extrahop.com“ übereinstimmen, aber eine Suche nach „www extra“ würde nicht mit „www.extrahop.com“ übereinstimmen. Regex- und Platzhalterzeichen werden nicht unterstützt.

Betreiber	Beschreibung
≈/	Schließt aus Wenn Datensätze in einem ExtraHop-Recordstore gespeichert sind, entspricht der Ausschlussoperator ganzen Wörtern, die durch Leerzeichen und Satzzeichen getrennt sind. Beispielsweise würde eine Suche nach „extra“ zwar „www.extra.com“ ausschließen, aber nicht „www.extrahop.com“. Bei allen anderen Datensatzspeichern entspricht der Operator excludes Teilzeichenfolgen, einschließlich Leerzeichen und Satzzeichen. Beispielsweise würde eine Suche nach „www.extra“ „www.extrahop.com“ ausschließen, aber eine Suche nach „www extra“ würde „www.extrahop.com“ nicht ausschließen. Regex - und Platzhalterzeichen werden nicht unterstützt.
<	Weniger als
≤	Weniger als oder gleich
>	Größer als
≥	Größer als oder gleich
beginnt mit	Beginnt mit
existiert	Existiert
geht nicht	Existiert nicht

Direktes Filtern aus Datensatzergebnissen

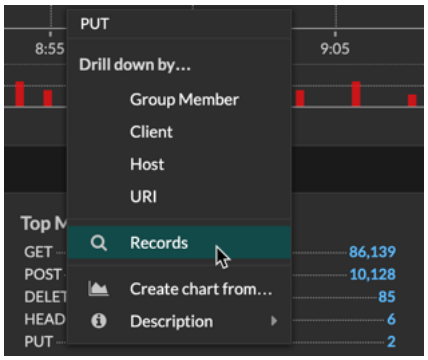
Sie können jeden Feldeintrag auswählen, der in Ihren Datensatzergebnissen entweder in der Tabellenansicht oder in der ausführlichen Ansicht angezeigt wird, und dann auf den Popup-Operator klicken, um den Filter hinzuzufügen. Filter werden unter der Diagrammzusammenfassung angezeigt (mit Ausnahme des Feld Datensatztyp, das im linken Bereich geändert wurde).



Datensätze im ExtraHop-System finden

- Geben Sie einen Suchbegriff in das globale Suchfeld oben auf dem Bildschirm ein und klicken Sie auf Datensätze durchsuchen, um eine Abfrage für alle gespeicherten Datensätze zu starten.
- Klicken Sie auf einer Geräteübersichtsseite auf **Rekorde** um eine nach diesem Gerät gefilterte Abfrage zu starten.
- Klicken Sie auf einer Übersichtsseite für Gerätegruppe auf **Aufzeichnungen ansehen** um eine nach dieser Gerätegruppe gefilterte Abfrage zu starten.

- Klicken Sie auf einer Erkennungskarte auf Datensätze anzeigen, um eine Abfrage zu starten, die mit den Transaktionen gefiltert wird, die mit der Erkennung verknüpft sind.
- Klicken Sie auf das Datensatzsymbol aus einem Diagramm-Widget, wie in der folgenden Abbildung dargestellt.



- Klicken Sie auf das Datensatzsymbol neben einer Detail-Metrik, nachdem Sie sich eine Top-Level-Metrik genauer angesehen haben. Klicken Sie beispielsweise nach der Aufschlüsselung der HTTP-Antworten nach Server auf das Symbol Datensätze, um eine Abfrage für Datensätze zu erstellen, die eine bestimmte Server-IP-Adresse enthalten.