Aufzeichnungen

Veröffentlicht: 2024-01-31

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, CIFS und NFS) und sitzungsbasiert (wie SSL 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.

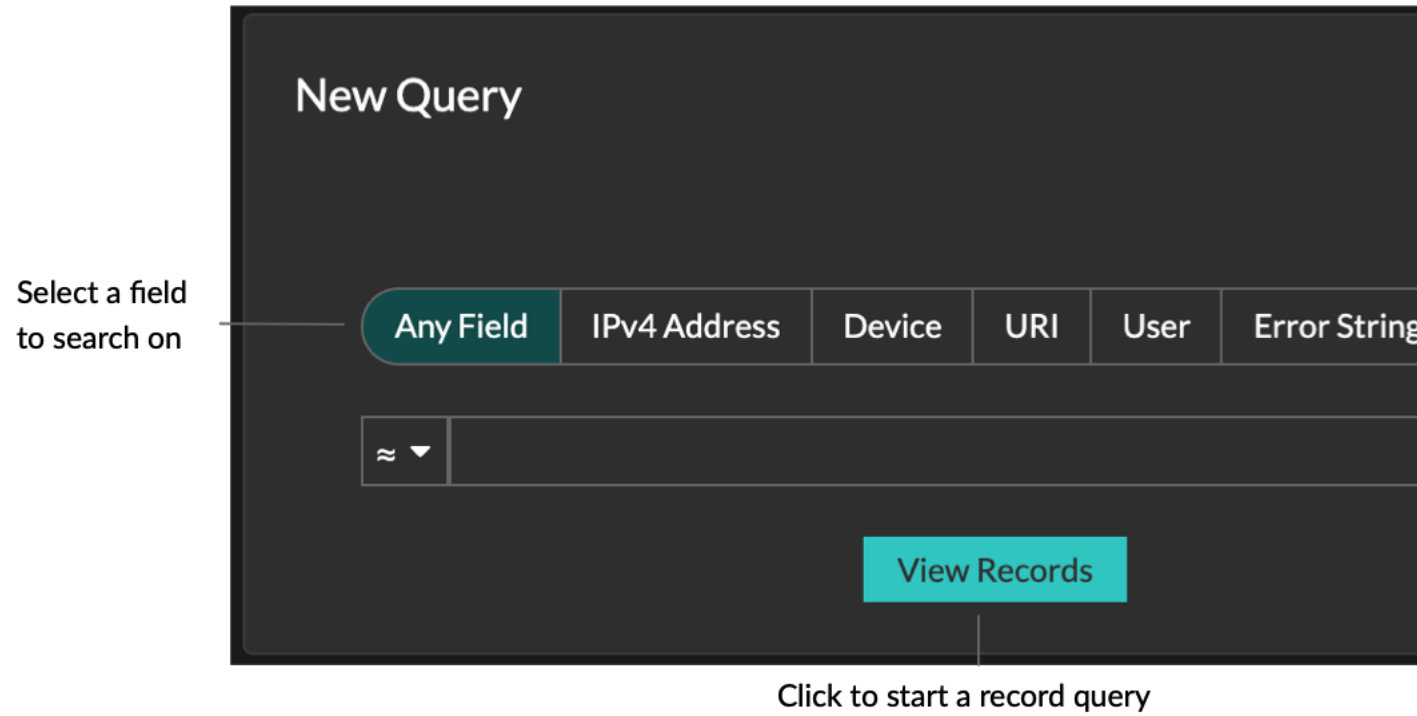
Video: Sehen Sie sich die entsprechende Schulung an: Aufzeichnungen

Bevor du anfängst

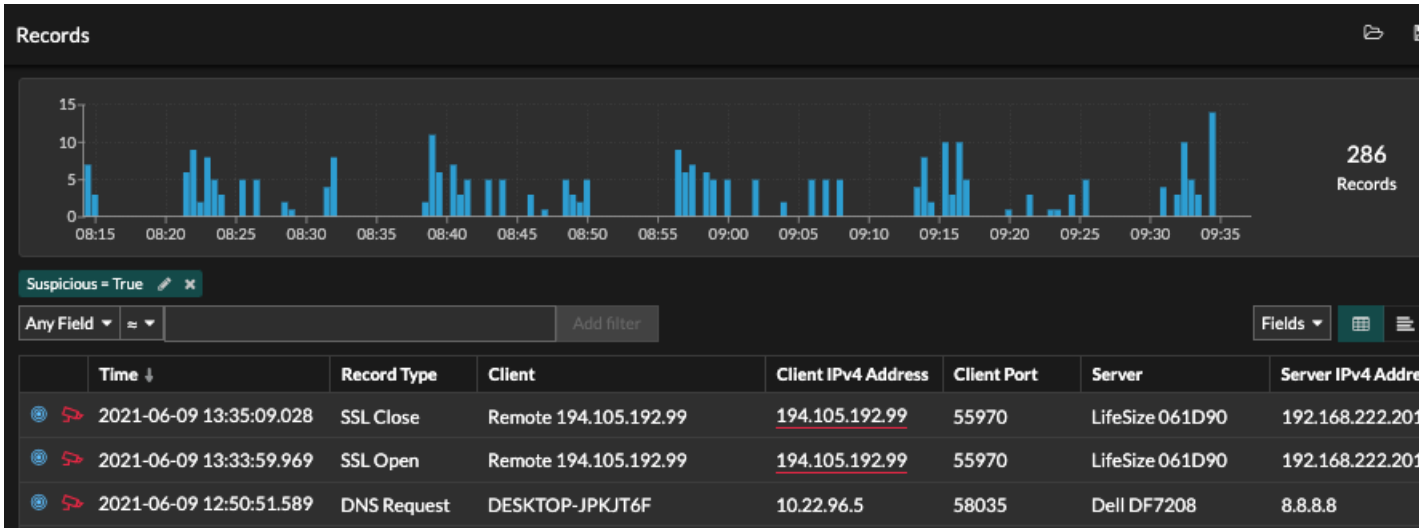
- Sie müssen einen konfigurierten Recordstore haben, z. B. ExtraHop Recordstore, Splunk, Google BigQuery, oder CrowdStrike Falcon LogScale.
- Sie können nur einen Recordstore für das ExtraHop-System konfigurieren.
- Ihr ExtraHop-System muss für das Sammeln und Speichern konfiguriert sein Flussaufzeichnungen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

In Datensätzen navigieren

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.



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 einzugrenzen.

- 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.

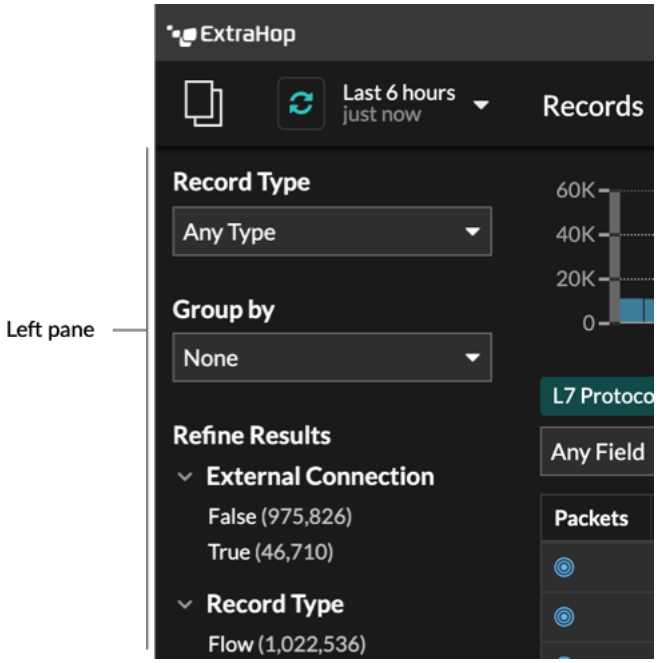
Wenn Sie versuchen, Datensätze nach einfachen Kriterien zu filtern (wenn Sie beispielsweise alle HTTP-Transaktionen von einem einzigen Server haben möchten, der 404-Dateien generiert hat), können Sie eine einfache Abfrage auf eine der folgenden Arten erstellen:

- 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.

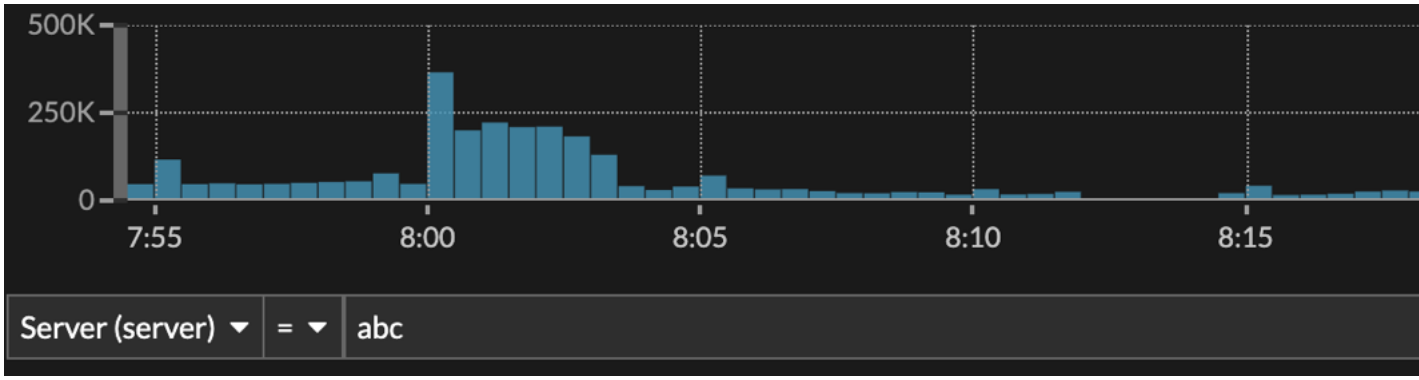
Hinweis: Da Sie zum Sammeln von Datensätzen einen Auslöser schreiben müssen, benötigen Sie eine Möglichkeit, die Art der Daten zu identifizieren, die Sie sammeln werden. Es gibt integrierte Datensatztypen, die alle verfügbaren bekannten Felder für ein Protokoll sammeln. Sie können mit einem integrierten 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.

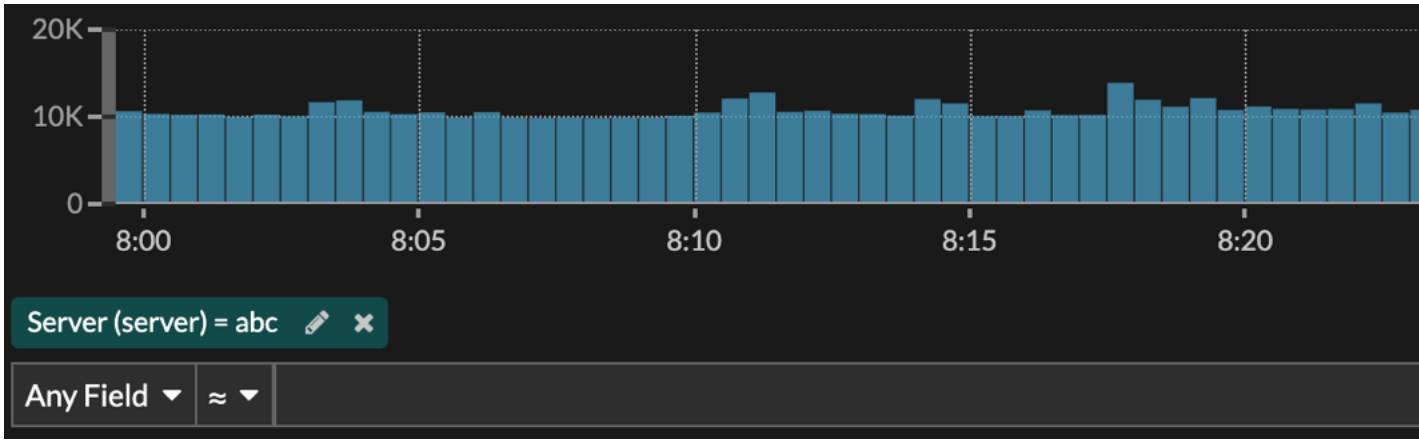
Die **Gruppieren nach** In der Dropdownliste finden Sie eine Liste mit Feldern, nach denen Sie den Datensatztyp weiter filtern können.

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.

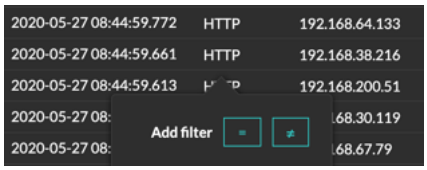
Die folgenden Operatoren können basierend auf dem ausgewählten Feldnamen ausgewählt werden:

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

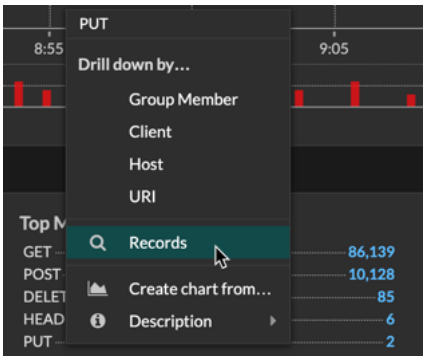
Sie können einen beliebigen Feldeintrag auswählen, der entweder in der Tabellenansicht oder in der ausführlichen Ansicht in Ihren Datensatzergebnissen angezeigt wird, und dann auf den Popup-Operator klicken, um den Filter hinzuzufügen. Filter werden unter der Diagrammzusammenfassung angezeigt (mit Ausnahme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



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.