Abfrage nach gespeicherten Datensätzen

Veröffentlicht: 2024-11-03

Sie können Datensätze, die im Recordstore gespeichert sind, mit einer Standardsuche oder mit AI Search Assistant abfragen.

- Erfahren Sie mehr über das Abfragen von Datensätzen mit einer Standardsuche.
- Erfahren Sie mehr über das Abfragen von Datensätzen mit dem AI Search Assistant.
- Informationen zum Abfragen eines bestimmten Datensatz finden Sie in unserer exemplarischen Vorgehensweise für Fehlende Webressourcen entdecken.
- Du kannst auch automatisiere diese Aufgabe über die REST-API.

Nächste Schritte

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

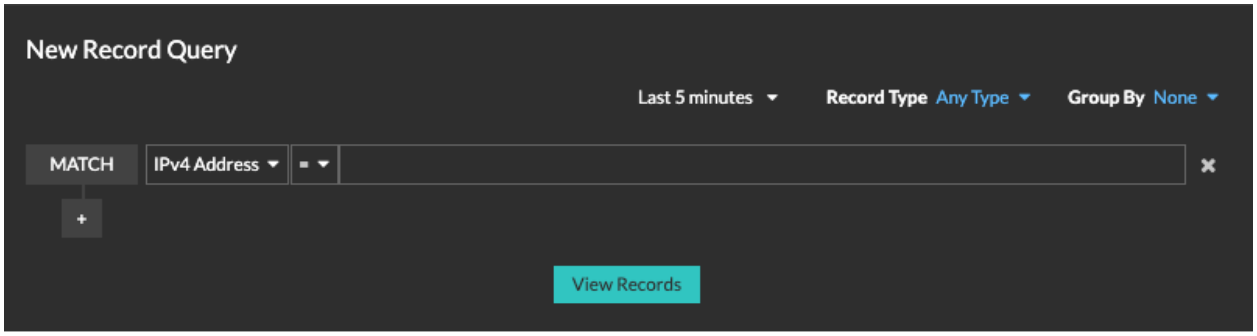
Datensätze mit einer Standardsuche abfragen

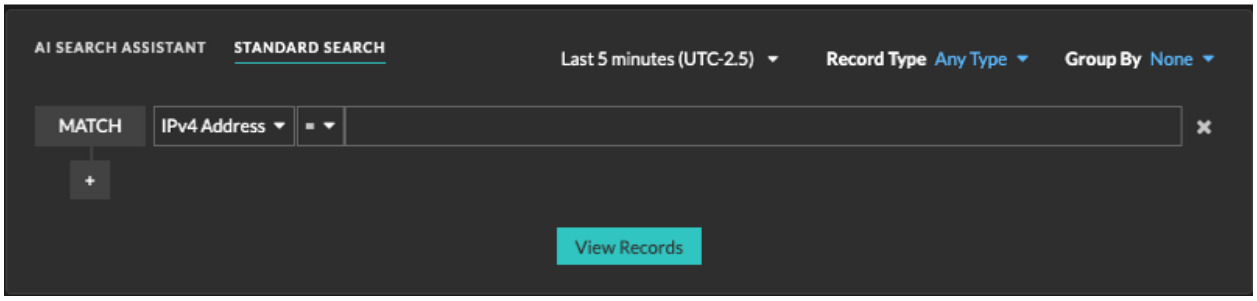
Auf der Seite „Datensätze“ können Sie einen komplexen Filter für die Suche nach Datensätzen erstellen.

Hier sind einige wichtige Dinge, die Sie über Datensatzabfragen mit der Standardsuche wissen sollten:

- Sie können mehrere Kriterien mit den Operatoren OR (Match Any), AND (Match All) und NOT angeben.
- Sie können Filter gruppieren und innerhalb jeder Gruppe auf vier Ebenen verschachteln.
- Sie können eine Filtergruppe bearbeiten, nachdem Sie sie erstellt haben, um die Suchergebnisse zu verfeinern.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Aufzeichnungen**.
   Wenn AI Search Assistant nicht aktiviert ist, wird der Abschnitt Neue Datensatzabfrage angezeigt.
   Wenn AI Search Assistant aktiviert ist, klicken Sie auf **Standardsuche**.



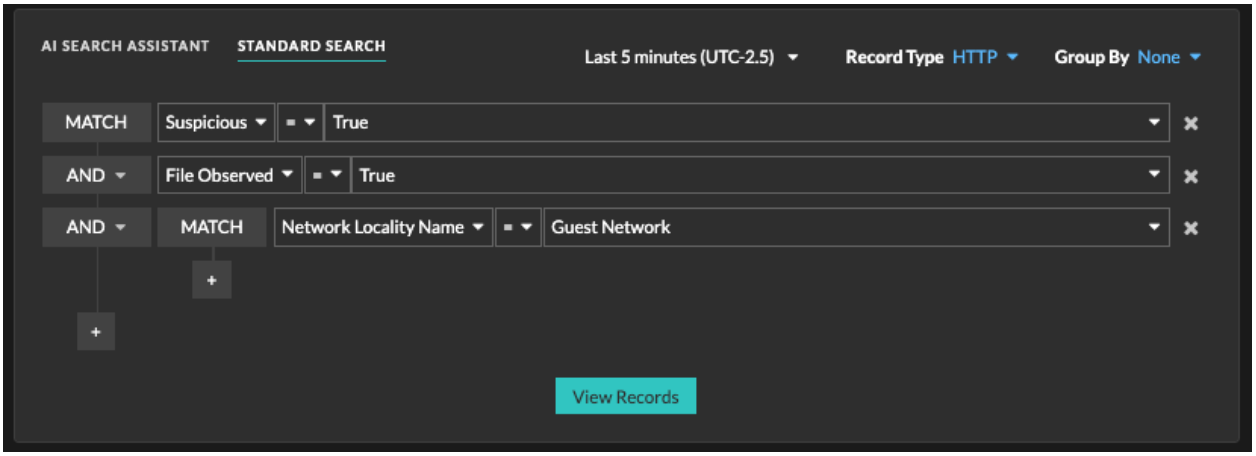


3. Wählen Sie das Zeitintervall aus, nach dem Sie suchen möchten.

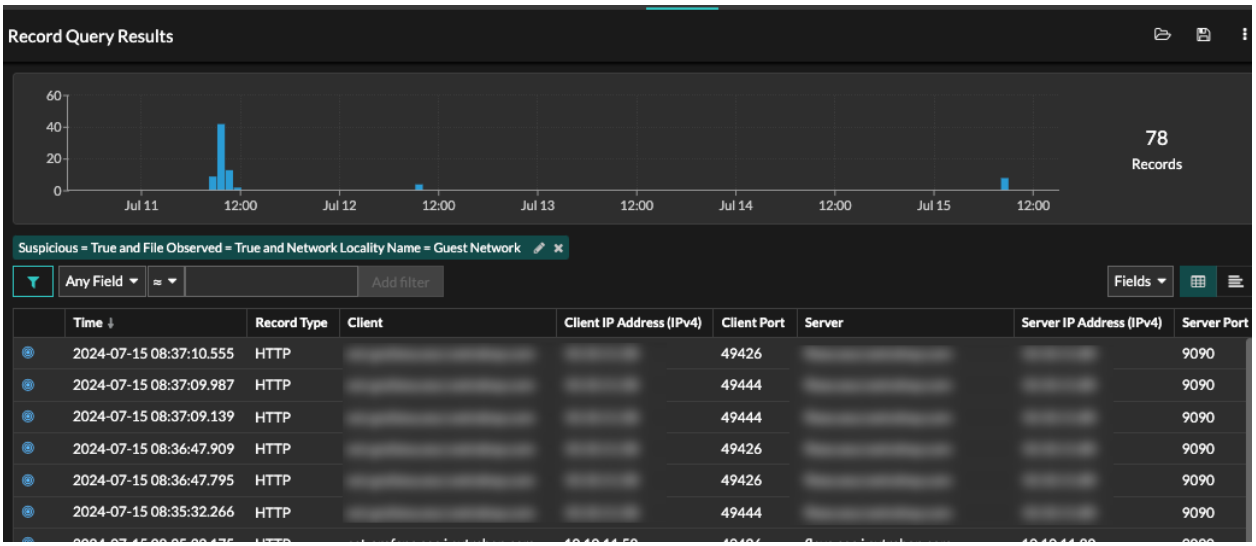
   Das Zeitintervall, das Sie auswählen, ändert die in der globaler Zeitwähler.
4. Aus dem **Datensatztyp** Wählen Sie im Drop-down-Menü einen oder mehrere der Datensatztypen aus, für deren Erfassung und Speicherung Ihr ExtraHop-System konfiguriert ist.
5. Aus dem **Gruppieren nach** Wählen Sie im Dropdownmenü eine Option aus, um anzugeben, wie Sie die Ergebnisse gruppieren möchten. Die angezeigten Optionen sind mit den von Ihnen ausgewählten Datensatztypen verknüpft.

   Wenn Sie beispielsweise HTTP-Datensätze nach Client gruppieren, werden in der Ergebnistabelle die Clients angezeigt, die in den Datensatztransaktionen gefunden wurden, sortiert nach der Häufigkeit, mit der dieser Client gefunden wurde.
6. Wählen Sie im Dropdownmenü Filterkriterien (die Standardeinstellung ist IPv4-Adresse) die ersten Kriterien aus, denen der Filter entsprechen soll. Die angezeigten Optionen sind mit den von Ihnen ausgewählten Datensatztypen verknüpft.
7. Optional: Klicken Sie auf das Plus-Symbol und wählen Sie **Filter hinzufügen** oder **Filtergruppe hinzufügen** um weitere Kriterien auf der obersten oder sekundären Ebene des Filters anzugeben.

   Eine neue Filtergruppe fügt dem Ergebnis des ursprünglichen Filters Kriterien hinzu. Wenn Sie beispielsweise nach HTTP-Transaktionen suchen, die verdächtig waren und Dateien enthielten, können Sie eine Filtergruppe hinzufügen, um die Ergebnisse auf Datensätze einzugrenzen, die einer bestimmten Netzwerklokalität zugeordnet sind.



8. Klicken Sie **Aufzeichnungen ansehen**.
   Die Ergebnisse der Aufzeichnungen werden auf der Hauptseite „Aufzeichnungen“ angezeigt.



Nächste Schritte

- Du kannst Abfrageergebnisse anzeigen und aufschlüsseln.
- Du kannst verfeinern Sie Ihren Datensatzabfragefilter.
- Sie können auf das Symbol Speichern klicken von oben rechts auf der Seite, um Ihren Filter für ein anderes Mal zu speichern.
- Sie können auf ein Paketsymbol neben einem Datensatz klicken, um einen zu starten Paketabfrage das nach diesem Datensatz gefiltert wird, oder klicken Sie auf den Abfrage-Link am Ende der Tabelle, um eine Paketabfrage für alle angezeigten Datensätze zu starten.

Datensätze mit AI Search Assistant abfragen

Mit dem AI Search Assistant können Sie nach Datensätzen mit Fragen suchen, die in natürlicher, alltäglicher Sprache verfasst sind. So können Sie im Vergleich zur Erstellung einer Standardsuchabfrage mit denselben Kriterien schnell komplexe Abfragen erstellen.

Wenn Sie beispielsweise abfragen: „Gab es in den letzten 7 Tagen verdächtige HTTP-Transaktionen mit Dateien?“ , die folgende AI Search Assistant-Abfrage wird angezeigt:

```
Time Interval = Last 2 days and Record Type = [HTTP]
Suspicious = True and File Observed = True
```

Hier sind einige Dinge, die Sie bei der Suche nach Geräten mit AI Search Assistant beachten sollten:

- Eingabeaufforderungen werden denselben Datensatzfilterkriterien zugeordnet, die Sie beim Erstellen einer Standardsuche angeben.
- Eingabeaufforderungen können absolute und relative Zeitbereiche enthalten, z. B. „Zeige mir Traffic mit potenziellem SQLi in den letzten 7 Tagen“. Das aktuelle Jahr wird verwendet, wenn für ein Datum kein Jahr enthalten ist.
- Die Eingabeaufforderungen sollten so klar und präzise wie möglich sein. Wir empfehlen Ihnen, einige Variationen zu schreiben, um Ihre Ergebnisse zu maximieren.
- Das ExtraHop-System ist möglicherweise nicht in der Lage, eine Abfrage zu verarbeiten, die Anfragen nach Datensatzinformationen enthält, die außerhalb der verfügbaren Filter liegen.
- Das ExtraHop-System kann Benutzeranweisungen zur Produktverbesserung speichern. Wir empfehlen, dass Sie in Ihren Eingabeaufforderungen keine urheberrechtlich geschützten oder vertraulichen Daten angeben.
- Sie können die Abfragefilterkriterien bearbeiten, um die Suchergebnisse zu verfeinern.

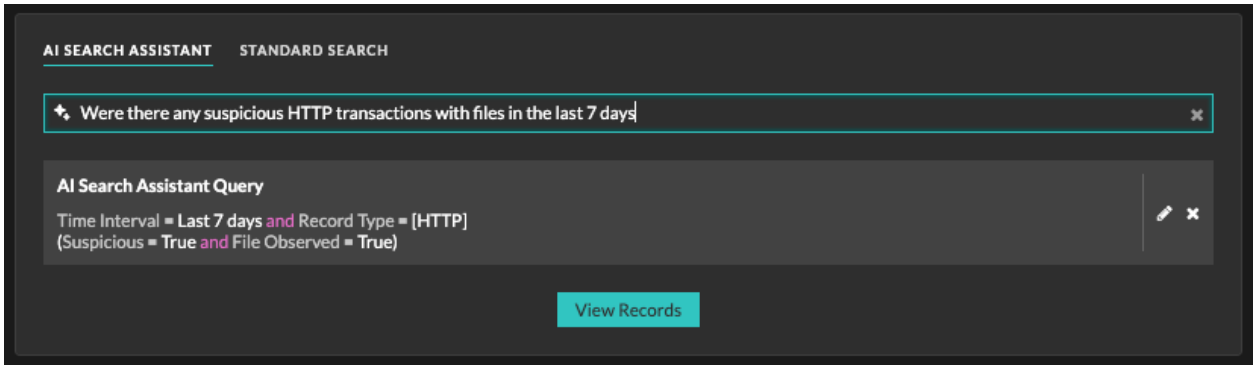
Bevor Sie beginnen

- Ihr ExtraHop-System muss verbunden mit ExtraHop Cloud Services.
- Der AI Search Assistant muss von Ihrem ExtraHop-Administrator aktiviert werden.

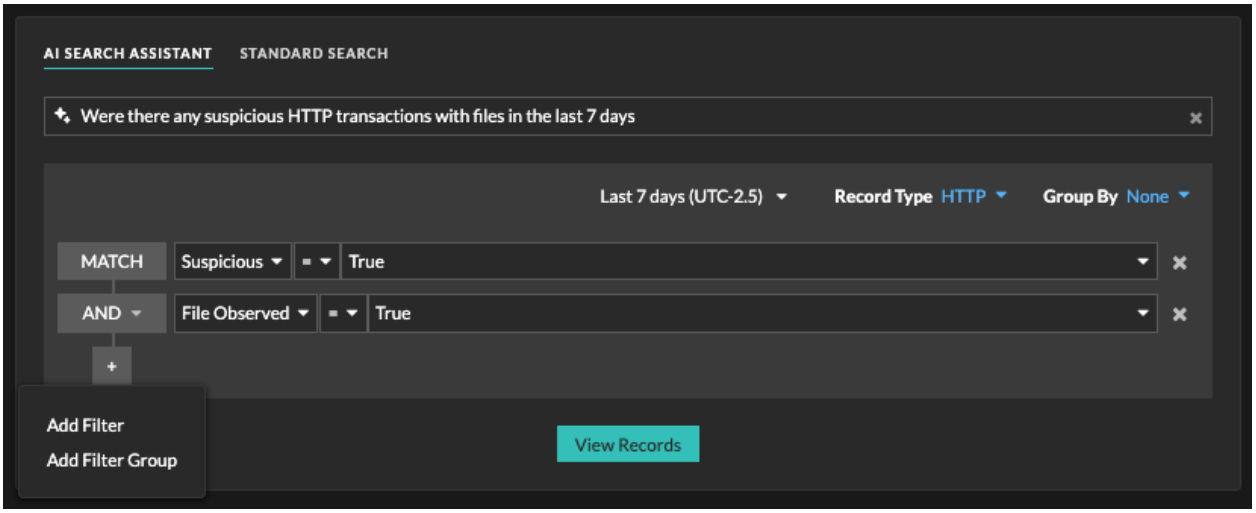
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Rekorde**.
3. Schreiben Sie eine Aufforderung in das Feld AI Search Assistant und drücken Sie die EINGABETASTE.

   Hinweis: Klicken Sie auf das Suchaufforderungsfeld, um eine aktuelle Abfrage oder eine vorgeschlagene Suche auszuwählen.

   Der AI Search Assistant-Abfragefilter wird angezeigt.



4. Optional: Klicken Sie im Abschnitt AI Search Assistant Query auf das Bearbeitungssymbol um Ihre Abfragefilterkriterien zu verfeinern.



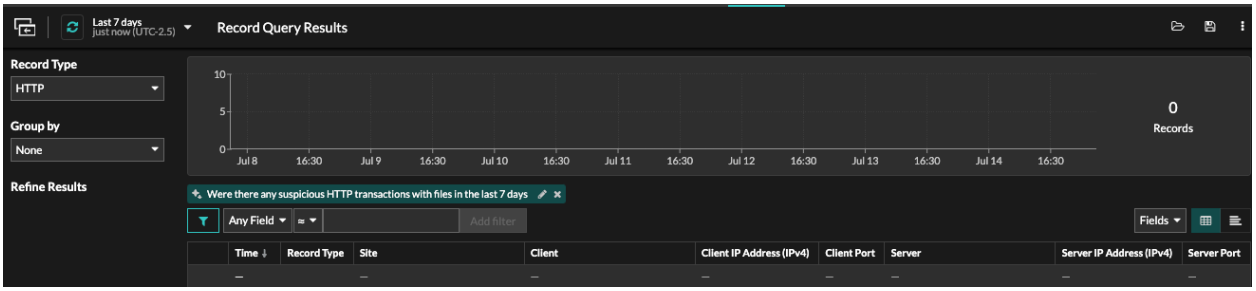
a) Bearbeiten Sie in der obersten Zeile das Zeitintervall, **Datensatztyp** oder **Gruppieren nach** Optionen.

b) Klicken Sie auf das Plus-Symbol und wählen Sie **Filter hinzufügen** oder **Filtergruppe hinzufügen** um weitere Kriterien auf der obersten oder sekundären Ebene des Filters anzugeben.

Eine neue Filtergruppe fügt dem Ergebnis des ursprünglichen Filters Kriterien hinzu. Wenn Sie beispielsweise nach verdächtigen HTTP-Datensätzen suchen, die Dateien enthielten, können Sie eine Filtergruppe hinzufügen, um die Ergebnisse auf Datensätze einzugrenzen, die einer bestimmten Netzwerklokalität zugeordnet sind.

c) Klicken Sie **Erledigt**.

5. Klicken Sie **Aufzeichnungen ansehen**.
Die Ergebnisse der Aufzeichnungen werden auf der Hauptseite „Aufzeichnungen“ angezeigt. Der Anzeigename des AI Search Assistant-Filters ist die Eingabeaufforderung, die Sie eingegeben haben und die über dem Dreifeld angezeigt wird.



Nächste Schritte

- Du kannst Abfrageergebnisse anzeigen und aufschlüsseln.
- Du kannst verfeinern Sie Ihren Datensatzabfragefilter.
- Sie können auf das Symbol Speichern klicken von oben rechts auf der Seite, um Ihren Filter für ein anderes Mal zu speichern.
- Sie können auf ein Paketsymbol neben einem Datensatz klicken, um einen zu starten Paketabfrage das nach diesem Datensatz gefiltert wird, oder klicken Sie auf den Abfrage-Link am Ende der Tabelle, um eine Paketabfrage für alle angezeigten Datensätze zu starten.