Pakete

Veröffentlicht: 2024-11-03

Ein Netzwerkpaket ist eine kleine Datenmenge, die über TCP/IP-Netzwerke (Transmission Control Protocol/Internet Protocol) gesendet wird. Das ExtraHop-System ermöglicht es Ihnen, diese Pakete kontinuierlich mit einer Trace-Appliance zu sammeln, zu durchsuchen und herunterzuladen. Dies kann nützlich sein, um Netzwerkeinbrüche und andere verdächtige Aktivitäten zu erkennen.

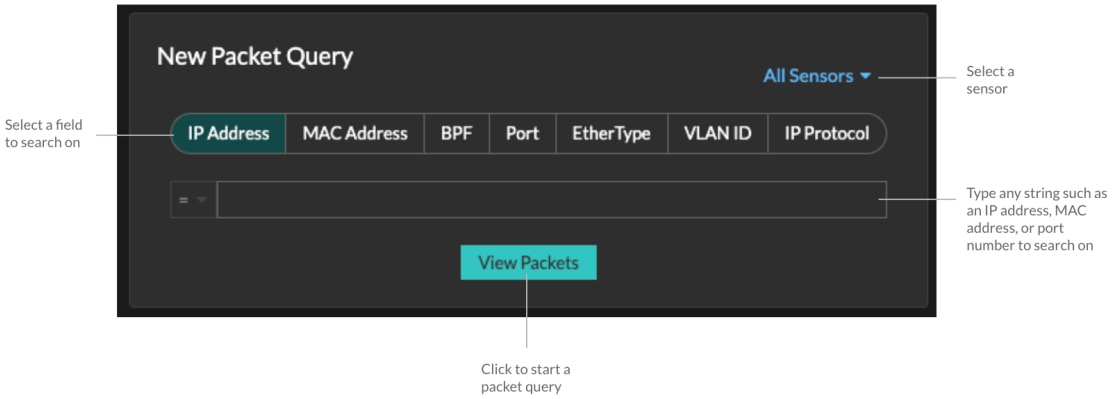
Sie können auf der Seite Pakete im ExtraHop-System nach Paketen suchen und diese herunterladen und über Paketsuche Ressource in der ExtraHop REST-API. Heruntergeladene Pakete können dann mit einem Drittanbieter-Tool wie Wireshark analysiert werden.

Hinweis: Wenn Sie keine Trace-Appliance haben, können Sie Pakete trotzdem über löst aus. siehe Initiieren Sie präzise Paketerfassungen, um Bedingungen ohne Fenster zu analysieren für ein Beispiel.

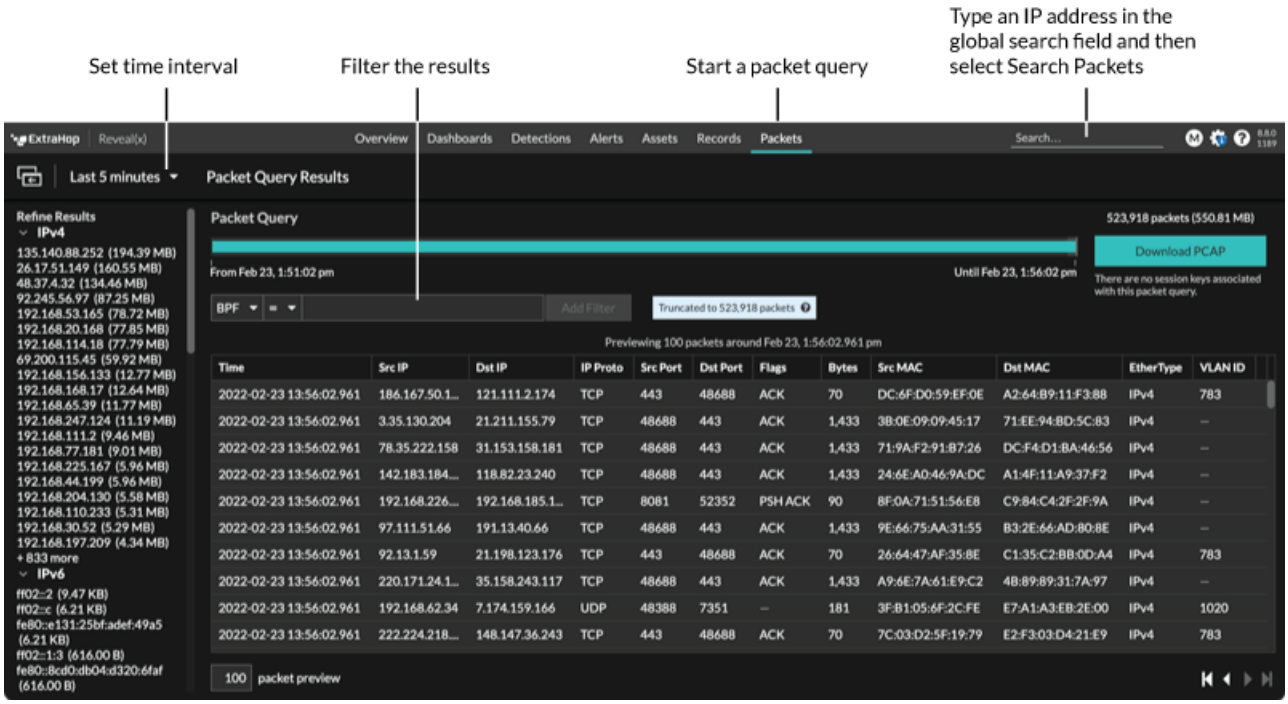
Video: Sehen Sie sich die entsprechende Schulung an: Pakete

In Paketen navigieren

Klicken Sie **Pakete** aus dem oberen Menü, um eine neue Paketabfrage zu erstellen. Auf der Seite Neue Paketabfrage können Sie einen Filter angeben.



Die Ergebnisse erscheinen auf der Hauptseite Pakete Seite. Starten Sie eine weitere Paketabfrage, indem Sie auf **Pakete** wieder aus dem Hauptmenü.



Wenn Sie das Zeitintervall ändern, beginnt die Abfrage erneut. An beiden Enden des grauen Balkens wird ein Zeitstempel angezeigt, der durch das aktuelle Zeitintervall bestimmt wird. Die Uhrzeit auf der rechten Seite zeigt den Startpunkt der Abfrage an und die Uhrzeit auf der linken Seite zeigt den Endpunkt der Abfrage an. Der blaue Balken gibt den Zeitraum an, in dem das System Pakete gefunden hat. Sie können einen Zeitraum in der blauen Leiste durch Ziehen vergrößern, um eine Abfrage für das ausgewählte Zeitintervall erneut auszuführen.

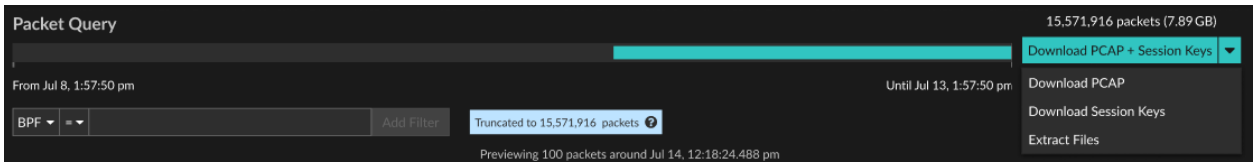
Hinweis: Pakete mit der Berkeley-Paketfilter-Syntax filtern.

Hinweis: Sie können nur Pakete anzeigen, die den von Ihrem ExtraHop-Administrator gewährten Rechten entsprechen. Wenn Sie Ihre erwarteten Abfrageergebnisse nicht sehen, wenden Sie sich an Ihren ExtraHop-Administrator.

Pakete werden heruntergeladen

Sie können die Abfrageergebnisse zusammen mit den TLS-Sitzungsschlüsseln und den Paketen zugehörigen Dateien zur Analyse in eine Paketerfassungsdatei (PCAP-Datei) herunterladen.

Download-Optionen sind im Drop-down-Menü oben rechts verfügbar. Klicken Sie auf eine Option, damit Ihr Browser die Datei auf Ihren lokalen Computer herunterladen kann.



Hier sind einige Überlegungen zum Herunterladen von Paketen und Extrahieren von Dateien:

- Die im Dropdownmenü angezeigten Download-Optionen hängen von Ihren Abfrageergebnissen ab. Wenn den Paketen beispielsweise keine Sitzungsschlüssel zugeordnet sind, werden möglicherweise nur Optionen zum Herunterladen von PCAP und zum Extrahieren von Dateien angezeigt.
- Downloads enthalten nur Pakete, die den von Ihrem ExtraHop-Administrator gewährten Rechten entsprechen. Wenn Sie beispielsweise zwei Sensoren abfragen, aber von Ihrem Administrator

eingeschränkter Zugriff auf einen der Sensoren zugewiesen wurde, enthält Ihr Download nur die Paket-Header des Sensor mit beschränktem Zugriff.

- Wenn du Sitzungsschlüssel herunterladen, können Sie die Paketerfassungsdatei in einem Tool wie Wireshark öffnen, das die Sitzungsschlüssel anwenden und die entschlüsselten Pakete anzeigen kann.
- Dateiextraktion (auch bekannt als File Carving) ist verfügbar, wenn Dateien in Paketen mit HTTP- oder SMB-Einträgen beobachtet werden.

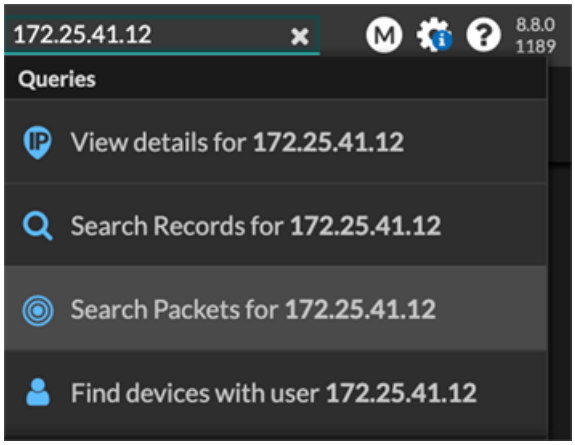
  Hinweis: Auf der Seite „ Datensätze“ können Sie nach HTTP- oder SMB-Datensatztypen suchen und nach beobachteter Datei filtern. Klicken Sie auf das Paketsymbol neben dem Datensatz, der Dateien enthält, die Sie extrahieren möchten.
- Extrahierte Dateien werden in einer ZIP-Datei heruntergeladen und enthalten unverschlüsselten Originalinhalt, der schädliche Daten enthalten kann. Zum Öffnen der entpackten ZIP-Dateien ist ein Passwort erforderlich. Das Passwort ist in der RevealX Enterprise oder RevealX 360 Administrationseinstellungen und können von Ihrem ExtraHop-Administrator abgerufen werden.
- Wenn Sie Ihre erwarteten Download-Optionen nicht sehen, wenden Sie sich an Ihren ExtraHop-Administrator. Sie haben keinen oder nur eingeschränkten Zugriff auf Sensoren, die Ihnen nicht über die Sensorzugriffskontrolle zugewiesen wurden. Darüber hinaus können Ihre Download-Optionen durch Modulzugriff und Benutzerrechte eingeschränkt werden. Der Modulzugriff und die für jede Download-Option erforderlichen Rechte werden in der folgenden Tabelle beschrieben:

Option herunterladen	Modul erforderlich	Rechte für Paketforensik erforderlich
PCAP+-Sitzungsschlüssel herunterladen	NDR oder NPM	Pakete und Sitzungsschlüssel
PCAP herunterladen	NDR oder NPM	Nur Pakete
PCAP-Header herunterladen	NDR oder NPM	Nur Paket-Header
PCAP-Slices herunterladen	NDR oder NPM	Nur Paketsegmente
Sitzungsschlüssel herunterladen	NDR oder NPM	Pakete und Sitzungsschlüssel
Dateien extrahieren	NDR	Nur Pakete oder Pakete und Sitzungsschlüssel

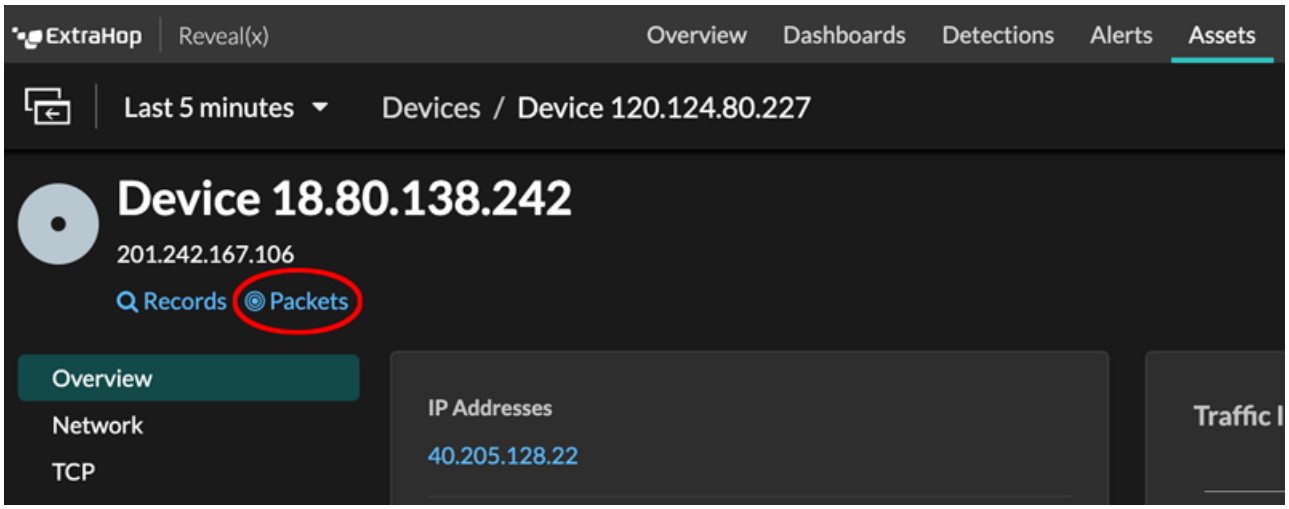
Pakete im ExtraHop-System abfragen

Die Seite Pakete bietet zwar schnellen Zugriff, um alle Pakete abzufragen, aber es gibt Indikatoren und Links, über die Sie im gesamten ExtraHop-System eine Paketabfrage starten können.

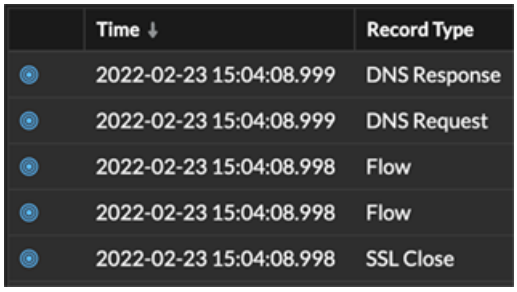
- Geben Sie eine IP-Adresse in das globale Suchfeld ein und wählen Sie dann das Symbol Pakete durchsuchen .



- Klicken Sie **Pakete** auf einer Geräteseite.

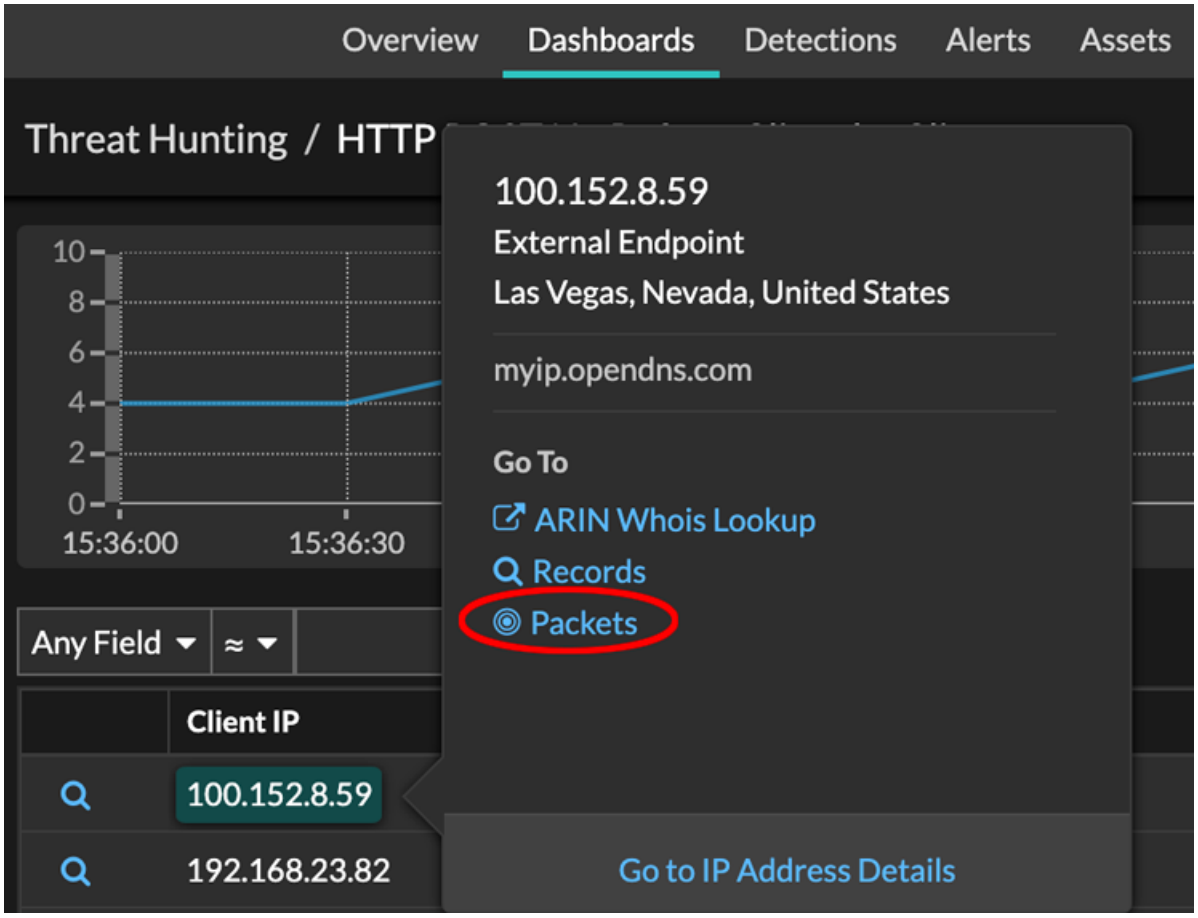


- Klicken Sie auf das Paketsymbol neben einem beliebigen Datensatz auf der Ergebnisseite einer Datensatzabfrage.



	Time ↓	Record Type
	2022-02-23 15:04:08.999	DNS Response
	2022-02-23 15:04:08.999	DNS Request
	2022-02-23 15:04:08.998	Flow
	2022-02-23 15:04:08.998	Flow
	2022-02-23 15:04:08.998	SSL Close

- Klicken Sie in einem Diagramm mit Metriken für Netzwerkbytes oder Pakete nach IP-Adresse auf eine IP-Adresse oder einen Hostnamen, um ein Kontextmenü aufzurufen. Klicken Sie dann auf das Paketsymbol um das Gerät und das Zeitintervall abzufragen.


Overview
Dashboards
Detections
Alerts
Assets
Threat Hunting / HTTP
100.152.8.59
External Endpoint
Las Vegas, Nevada, United States
myip.opendns.com
Go To
ARIN Whois Lookup
Records
Packets
10
8
6
4
2
0
15:36:00
15:36:30
Any Field
≈
Client IP
100.152.8.59
192.168.23.82
Go to IP Address Details