Pakete

Veröffentlicht: 2023-12-05

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.

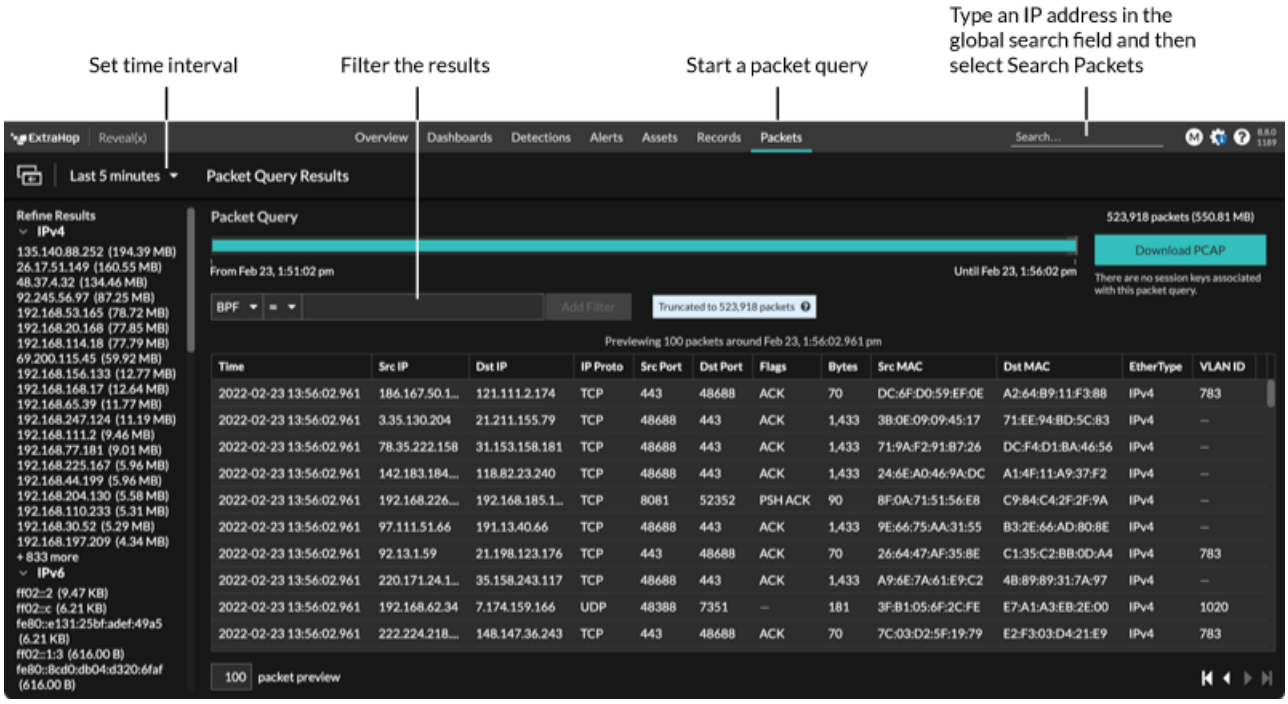
Sie können auf der Paketseite im ExtraHop-System nach Paketen suchen und diese herunterladen. Paketsuche Ressource in der ExtraHop REST API. Heruntergeladene Pakete können dann mit einem Drittanbieter-Tool wie Wireshark analysiert werden.

Hinweis: Wenn Sie keine Trace-Appliance haben, können Sie 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.

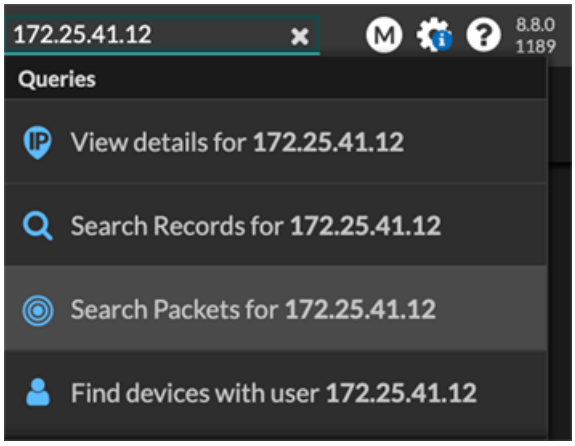
Die folgende Abbildung bietet einen Überblick über die Seite „Paketabfrage“ und ihre Funktionen:



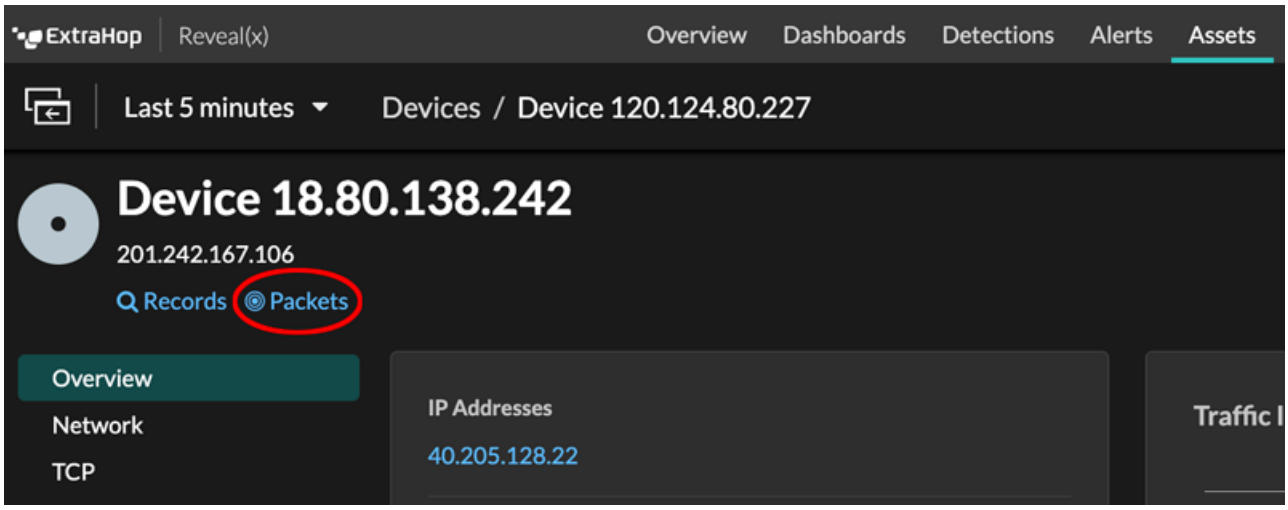
Hinweis: Pakete mit der Berkeley-Paketfilter-Syntax filtern.

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

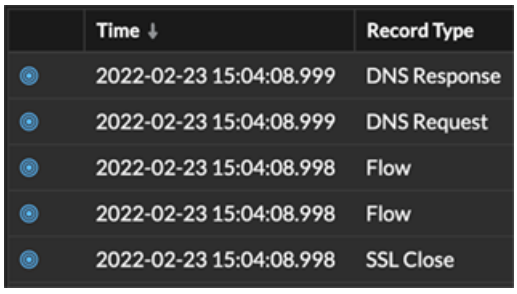
- Geben Sie eine IP-Adresse in das globale Suchfeld ein und wählen Sie dann das Symbol Pakete suchen .



- klicken **Pakete** auf einer Geräteseite.

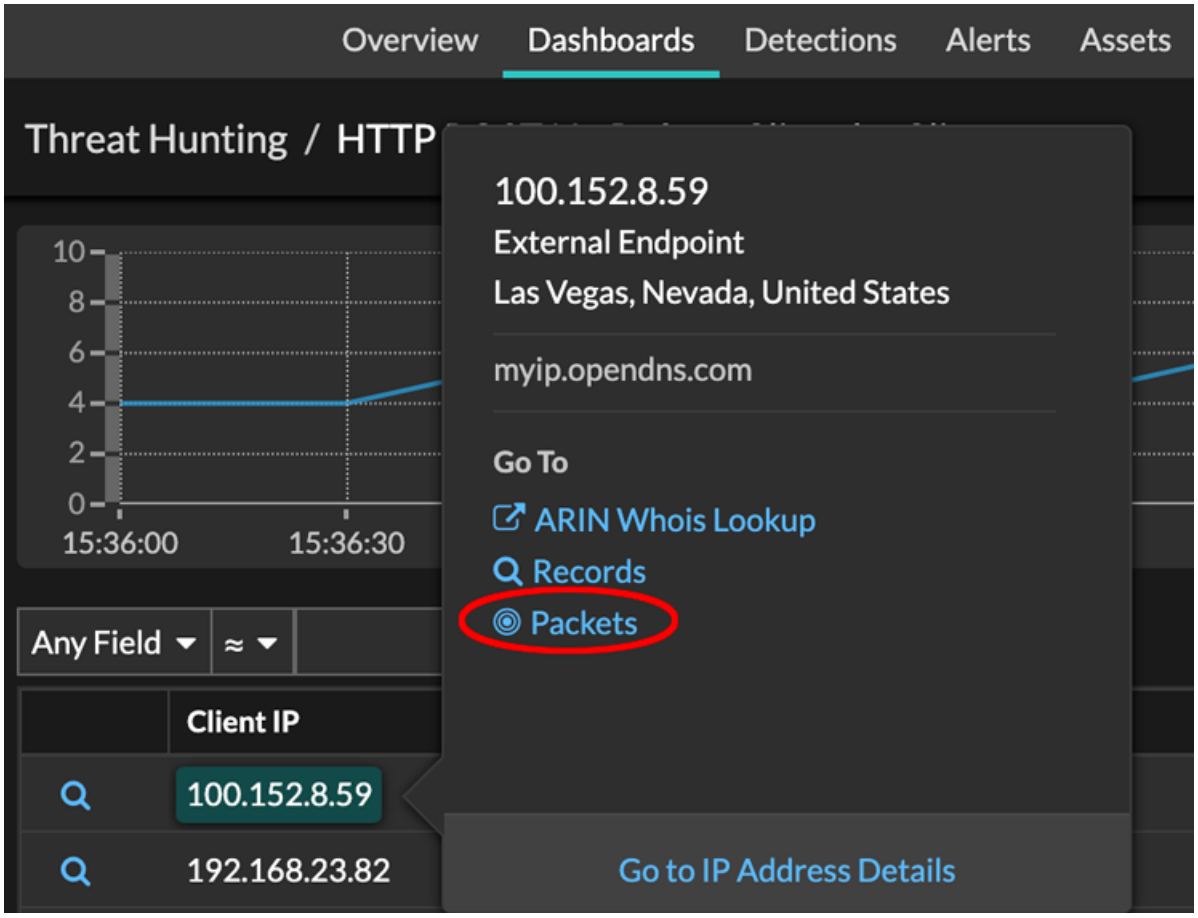


- Klicken Sie auf das Paketsymbol neben einem beliebigen Datensatz auf der Ergebnisseite einer Datensatzabfrage.



	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.


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