Paquets

Publié: 2023-12-05

Un paquet réseau est une petite quantité de données envoyée sur des réseaux TCP/IP (Transmission Control Protocol/Internet Protocol). Le système ExtraHop vous permet de collecter, de rechercher et de télécharger en permanence ces paquets à l'aide d'une appliance Trace, ce qui peut être utile pour détecter les intrusions sur le réseau et autres activités suspectes.

Vous pouvez rechercher et télécharger des paquets depuis la page Paquets du système ExtraHop et via le Recherche par paquets 🗷 ressource dans l' API REST ExtraHop. Les paquets téléchargés peuvent ensuite être analysés par le biais d'un outil tiers, tel que Wireshark.

Note: Si vous ne possédez pas d'appliance Trace, vous pouvez toujours collecter des paquets via déclencheurs . Voir Initiez des captures de paquets de précision pour analyser les conditions de fenêtre zéro . à titre d'exemple.

Requête de paquets

Lancez une requête rapide par paquet en cliquant sur **Paquets** depuis le menu supérieur. Le système ExtraHop interroge tous les paquets et affiche la page Packet Query. Si vous modifiez l'intervalle de temps, la requête recommence. Chaque extrémité de la barre grise affiche un horodateur, qui est déterminé par l'intervalle de temps actuel. L' heure sur la droite indique le point de départ de la requête et l'heure sur la gauche indique le point de terminaison de la requête. La barre bleue indique la plage de temps pendant laquelle le système a détecté des paquets. Vous pouvez faire glisser le pointeur pour zoomer sur une période dans la barre bleue afin de réexécuter une requête pendant l'intervalle de temps sélectionné.

La figure suivante fournit une vue d'en	mble de la page Packet	Query et de ses fonctionnalités :
---	------------------------	-----------------------------------

Set time in	terval Fil	ter the resu	ılts		5	Start a	packet (query	glob selec	an IP addres al search fiel ct Search Pao	ss in the d and ther :kets	1	
*@ExtraHop Reveal(x)	c	verview Dashb	oards Detections	Alerts	Assets	Records	Packets			Search		D 🏟 🖸 🗄	1.0 87
Last 5 minutes 👻	Packet Query Results												
Refine Results	Packet Query										523,918 packets	(550.81 MB)	
135.140.88.252 (194.39 MB) 26.17.51.149 (160.55 MB) 48.37.4.32 (134.46 MB) 92.245.56.97 (87.25 MB) 192.168.53.165 (78.72 MB) 192.168.53.165 (78.72 MB)	From Feb 23, 1:51:02 pm BPF • = •		A	id Filter	Trunca	ted to 523,91	8 packets 0		Until Fe	eb 23, 1:56:02 pm	Download here are no session ith this packet quer	PCAP keys associated y	
192.168.20.168 (77.85 MB) 192.168.114.18 (77.79 MB) 69.200.115.45 (59.92 MB) 192.168.156.133 (12.77 MB)	Previewing 100 packets around Feb 23, 1:56:02.961 pm												
	Time	Src IP	Dst IP	IP Proto	Src Port	Dst Port	Flags	Bytes	Src MAC	Dst MAC	EtherType	VLAN ID	
192.168.65.39 (11.77 MB)	2022-02-23 13:56:02.961	186.167.50.1	121.111.2.174	TCP	443	48688	ACK	70	DC:6F:D0:59:EF:0E	A2:64:89:11:F3:8	3 IPv4	783	
192.168.247.124 (11.19 MB) 192.168.111.2 (9.46 MB)	2022-02-23 13:56:02.961	3.35.130.204	21.211.155.79	тср	48688	443	ACK	1,433	3B:0E:09:09:45:17	71:EE:94:BD:5C:8	3 IPv4		
192.168.77.181 (9.01 MB) 192.168.225.167 (5.96 MB)	2022-02-23 13:56:02.961	78.35.222.158	31.153.158.181	TCP	48688	443	ACK	1,433	71:9A:F2:91:87:26	DC:F4:D1:BA:46:	ió IPv4		
192.168.44.199 (5.96 MB)	2022-02-23 13:56:02.961	142.183.184	118.82.23.240	TCP	48688	443	ACK	1,433	24:6E:A0:46:9A:DC	A1:4F:11:A9:37:F	2 IPv4		
192.168.204.130 (5.36 MB) 192.168.102.33 (5.31 MB) 192.168.102.33 (5.31 MB) 192.168.197.209 (4.34 MB) + 833 more > IPv6 ff02-2 (9.47 KB) ff02-2 (6.21 KB) ff02-2 (6.21 KB) ff02-2 (6.21 KB) ff02-2 (5.21 KB) ff02-3 (5.21	2022-02-23 13:56:02.961	192.168.226	192.168.185.1	TCP	8081	52352	PSHACK	90	8F:0A:71:51:56:E8	C9:84:C4:2F:2F:9	A IPv4		
	2022-02-23 13:56:02.961	97.111.51.66	191.13.40.66	TCP	48688	443	ACK	1,433	9E:66:75:AA:31:55	B3:2E:66:AD:80:8	E IPv4		
	2022-02-23 13:56:02.961	92.13.1.59	21.198.123.176	TCP	443	48688	ACK	70	26:64:47:AF:35:8E	C1:35:C2:BB:0D:/	4 IPv4	783	
	2022-02-23 13:56:02.961	220.171.24.1	35.158.243.117	TCP	48688	443	ACK	1,433	A9:6E:7A:61:E9:C2	48:89:89:31:7A:9	7 IPv4		
	2022-02-23 13:56:02.961	192.168.62.34	7.174.159.166	UDP	48388	7351		181	3F:B1:05:6F:2C:FE	E7:A1:A3:EB:2E:0	0 IPv4	1020	
	2022-02-23 13:56:02.961	222.224.218	148.147.36.243	TCP	443	48688	ACK	70	7C:03:D2:5F:19:79	E2:F3:03:D4:21:E	PV4	783	
	100 packet preview											н • ⊳	ł



Conseilltrer les paquets avec la syntaxe du filtre de paquets Berkeley **Z**.

Il existe plusieurs emplacements dans le système ExtraHop à partir desquels vous pouvez lancer une requête de paquet :

• Tapez une adresse IP dans le champ de recherche globale, puis sélectionnez l'icône Search Packets 💿 .



• Cliquez Paquets sur la page d'un équipement.



 Cliquez sur l'icône Packets

 à côté de n'importe quel enregistrement sur la page de résultats d'une requête d'enregistrement.

	Time ↓	Record Type
۲	2022-02-23 15:04:08.999	DNS Response
	2022-02-23 15:04:08.999	DNS Request
۲	2022-02-23 15:04:08.998	Flow
۲	2022-02-23 15:04:08.998	Flow
	2022-02-23 15:04:08.998	SSL Close

• Cliquez sur une adresse IP ou un nom d'hôte dans n'importe quel graphique contenant des métriques relatives aux octets ou aux paquets du réseau par adresse IP pour afficher un menu contextuel. Cliquez ensuite sur l'icône Packets () pour demander l'équipement et l'intervalle de temps.

🕶 ExtraHop

