🕶 ExtraHop

ExtraHop Packet Basics

Forensic investigation in cloud environments is more critical than ever. Attacks evolve daily, and the number of advanced threats security teams are forced to confront continues to rise.

ExtraHop Packet Basics is a free network forensics offering that provides incident responders with packet capture (PCAP) for analysis, forensic investigation, threat hunting, and more.

Security Benefits of Packet Capture in Cloud Environments

With ExtraHop Packet Basics, cloud-focused security teams now have access to specific network packets before, during, and after incidents. Armed with richer forensic detail than what is available in logs and data from agents and firewalls, analysts can get to ground truth faster and fulfill chain-of-custody requirements.

Why Choose ExtraHop Packet Basics Free PCAP?

ExtraHop Packet Basics integrates with Amazon VPC Traffic Mirroring to begin providing incident responders and forensic investigators with copies of network packets as soon as it's deployed in an AWS environment. As a free tool, ExtraHop Packet Basics also removes the financial burden of adding PCAP to your existing incident response workflows.

You can select ExtraHop Packet Basics directly from <u>AWS Marketplace</u>, allowing you to deploy PCAP with the click of a button. Additionally, ExtraHop Packet Basics provides three key benefits:

			Filt	er =	-												
			BPF														
Packet Basks														000	85590 7041		
Last é hours Packet Query Results			EtherType												Upgrad	e to Reveal(a) 360 Learn Mor	e .
efree Results	Packet Query		IP Address														
2.18.1.181 (78.03 MB)	From Aug 3, 9:55:34 am		IP Aduress					_				_				/77.00	140
216249.6 (76.03 MB) 2.114.136.67 (1.04 MB)															66,300	packets (77.99	MF
216.237.149 (616.14 K8) 217.900 198 (106.06 K8) BPT + - +		IP Protocol				4,545 packets											
217.364.72 (105.85 KB) 46.545.233 (31.66 KB)							Provincing 100 packets around Aug 3, 3,53,41,007 pm								Download PCAP		
524.655244.712.54481 5224.57234.74158480 5221657234.6415880 52135746941580 52135748947110.55480 52137548947110.55480 3227545912.054480 3227545912.054480 3227545912.054480 3227545912.05480 322754912.05480 322757912.054912.05480 33427272105412.05480 33427272105412.05480 33427272105412.05480		Sec 17	MA	MAC Address		Peri	Dut Port	flip	Dytes	See MAC C	DIEMAC	EtherType	VLANID		Download PCAP		
	2021-08-00 15:51:47.850	172.1						PSHACK		0E8147.D2:23.A8	GESCADARSA45						
	2021-08-03 15:51:47.850	172.1	Port VLAN ID					PSHACK		0EB147.D2:23.AB	0E5CA0A89A65						
	2021-08-03 15:51:47.850	172.1					PSHACK		0E8147.D2:23.A8	GESCADABSA45							
	2021-08-03 15:51:47.850	172.1						PSHACK		0EB147:D2:23:AB	0650303838465						
	2021-08-03 15:51:47.851	172.1					PSHACK		0E/81/47/D2/23.A8	06/50/A0/48/94/65							
	2021-08-00 15:51:47.851	172.1			_			PSHADK		0E8147:D2:23:A8	08:50:40:48:94:65						
IP Protocol	2021-08-03 15:51:47:851										0E81.47.D2:23.AB						
P (78.00 ME) P 132.48 KE	2021-08-00 15:51:47.852							PSHACK			OESCADARSKAS						
Port	2021-08-03 15:51:47.852						58187	PSHACK			06:50:40:48:94:65						
TCP.80 (76.88 M8) TCP:48086 (40.99 M8) TCP:48088 (35.04 M8) TCP:58187 (1.04 M8)	2021-08-03 15:51:47.853	172.18		172.114.136.67			58187	PSHACK	270	0E8147.D2:23.A8							
	2021-08-03 15:51:47.853			172.114.136.67				PSHACK			GESCADABSA45						
P:22 (1.04 MII) P:57208 (616.14 KBI	2021-08-03 15:51:47:853	172.18		172.114.136.67			58187	PSHACK	270	0E8147.D2:23.AB							
P-44460 (104.61 KB) P-40920 (104.50 KB)	2021-08-03 15:51:47.853	172.18		172.114.135.67			58187	PSHADK	110		GESCADABSA45						
P:443 (73.96 KB) IP:123 (21.15 KB)	2021-08-03 15:51:47.854 2021-08-00 15:51:47.854	172.18		172.114.136.67		22 22	58187	PSHACK	270	0E8147.D2:23.A8	0ESCADABSA-65 0ESCADABSA-65						
P-53666 (18.63 KB)	2021-08-03 15:51:47.856	172.18		172.114.136.67		22	58187	PSHACK	270	0E8147.D2:23A8							
IPIS3 (11.33 KB) P-46396 (10.72 KB)	2021-08-03 15:51:47:856	172.18		172.114.136.67		22	58187	PSHACK	110		GESCADARSKIS						
P.56180 (10.68 KB) P.56248 (10.56 KB)	2021-08-03 15:51:47:857	172.18		172.114.136.67	109	22	58187	PSHACK	278	0EB147.02:23AB							
P.59948 (10.56 KB) P.49166 (10.50 KB)	2021-08-03 15:51:47.858	172.18		172.114.136.67			58187	PSHACK	270		05/50/40/48 90/65						
P-46495 (10.50 KB) P-46350 (10.44 KB)	2021-08-00 15:51:47.858	172.18		172.114.136.67		22	58187	PSHACK	110	058147.02:23 AB							
P:44458 (1.46 KB) 56 more	2021-08-03 15:51:47.858	172.18	1.181	172.114.136.67			58187	PSHACK		0E8147.D2:23.A8	06:50:40:48:94:65						
VLAN	2021-08-00 15:51:47.858			172.114.135.67				PSHACK		058147.02:23.48	OESCADALSA45						
Untagged (78.03 MB)	2021-08-03 15:51:47.859							PSHACK			0E5CA0.48.9A.65						
	100 packet preview															н н т	н

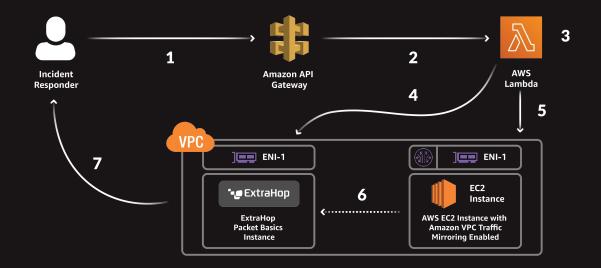
• Enhances incident response workflows with instant access to network packets.

- Enables PCAP for the packets needed for incident response and more.
- Reduces the amount of time and effort required to perform packet capture in the cloud.

Get ExtraHop Packet Basics for Free GET IT NOW ③

Start the Reveal(x) 360 Demo **START DEMO** ⊗

EXTRAHOP PACKET BASICS Incident Response Workflow



Respond intelligently

ExtraHop Packet Basics is designed for frictionless PCAP in AWS environments, helping incident responders make confident decisions about the steps to take to stop a threat. Here is one example of how an incident responder could use network packets from ExtraHop Packet Basics.

- 1. An incident responder identifies abnormal activity and submits an EC2 instance to investigate
- 2. The API Gateway interacts with an AWS Lambda
- 3. Given input, the Lambda triggers an action
- 4. The Lambda launches an ExtraHop Packet Basics instance
- 5. The Lambda also enables Amazon VPC Traffic Mirroring
- 6. Amazon VPC Traffic Mirroring forwards copies of network packets to the ExtraHop Packet Basics instance
- 7. The incident responder can now analyze packet data on the potentially compromised workload and take their next steps

Get ExtraHop Packet Basics for Free GETITNOW ⊙

Start the Reveal(x) 360 Demo **START DEMO** ⊙

ABOUT EXTRAHOP NETWORKS

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform uses cloud-scale AI to help enterprises detect and respond to advanced threats—before they can compromise your business. When you don't have to choose between protecting your business and moving it forward, that's security, uncompromised.

© 2021 ExtraHop Networks, Inc. All rights reserved. ExtraHop is a registered trademark of ExtraHop Networks, Inc. in the United States and/or other countries. All other products are the trademarks of their respective owners.

• ExtraHop

info@extrahop.com www.extrahop.com