HPE2-W05Q&As

Implementing Aruba IntroSpect

Pass HP HPE2-W05 Exam with 100% Guarantee

QUESTION 1

An IntroSpect installation has been up for a day. While validating the log sources, you see an Aruba Firewall log source configured on a Packet Processor that has shown up on the interface in the analyzer. While evaluating conversation data you notice there is no eflow data from AMON. You log into the controller and confirm there is user activity in the dashboard.

Would this be a correct statement about this situation? (The Packet Processor has been configured correctly.)

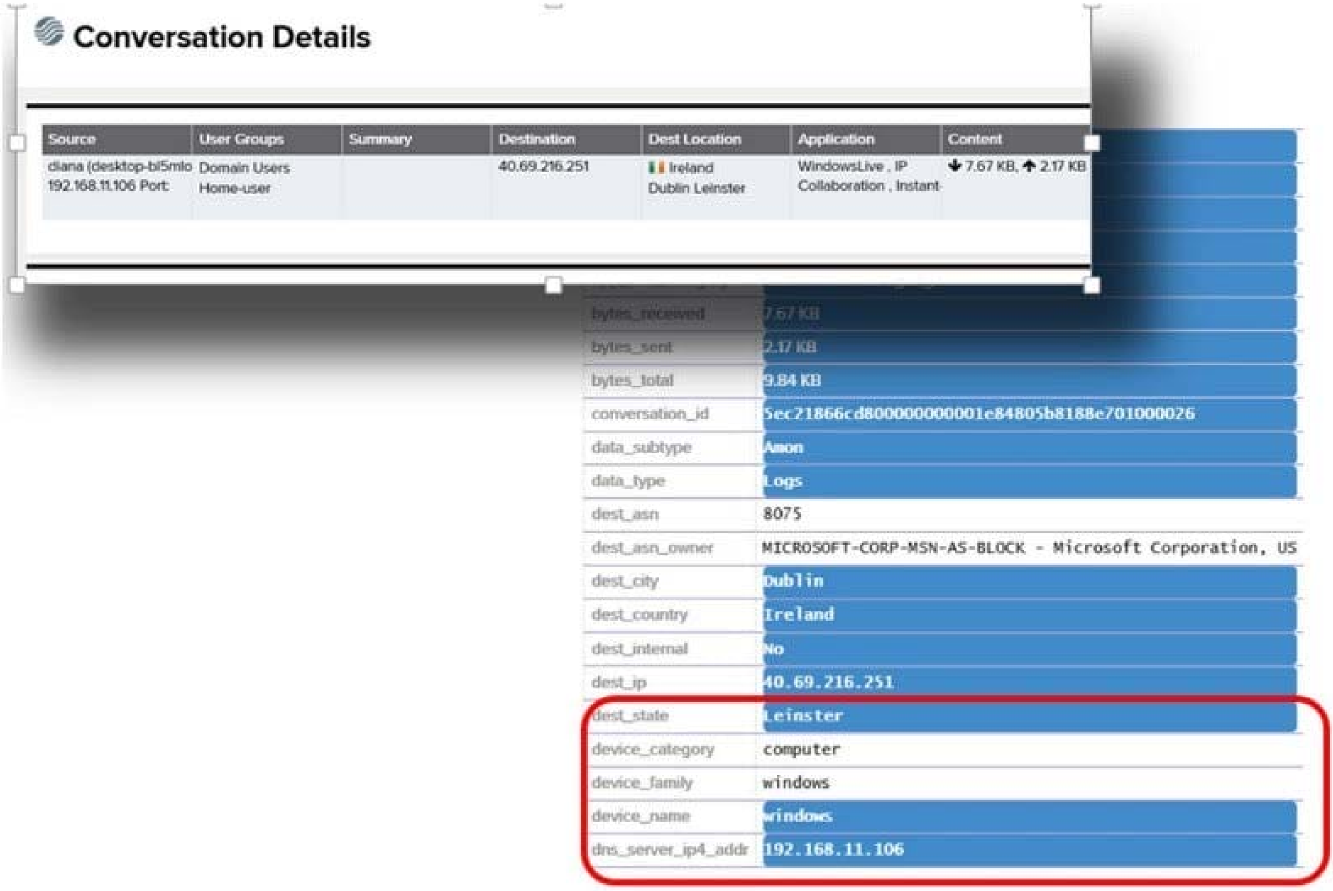
A. Yes

B. No

Correct Answer: B

QUESTION 2

Refer to the exhibit.



Conversation Details

Source	User Groups	Summary	Destination	Dest Location	Application	Content
diana (desktop-bl5mlo 192.168.11.106 Port:	Domain Users Home-user		40.69.216.251	Ireland Dublin Leinster	WindowsLive , IP Collaboration , Instant	↓ 7.67 KB, ↑ 2.17 KB

bytes_received	7.67 KB
bytes_sent	2.17 KB
bytes_total	9.84 KB
conversation_id	5ec21866cd800000000001e84805b8188e701000026
data_subtype	Amon
data_type	Logs
dest_asn	8075
dest_asn_owner	MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation, US
dest_city	Dublin
dest_country	Ireland
dest_internal	No
dest_ip	40.69.216.251
dest_state	Leinster
device_category	computer
device_family	windows
device_name	windows
dns_server_ip4_addr	192.168.11.106

You are a security analyst for a company that has deployed an Aruba infrastructure, such as Mobility Controllers, ClearPass, and Airwave. Recently they have deployed Aruba IntroSpect for security analytics. You are looking at the conversation details of an entity. Is this statement correct about the details highlighted? (These details came from the ClearPass server and it has been integrated as a context server in the IntroSpect.)

A. Yes

B. No

Correct Answer: B

QUESTION 3

A security analyst is monitoring the traffic which is accessing internal and external resources. They find abnormal activity, indicating communication between a compromised internal user(host) and internal infrastructure, and found a suspicious malware activity. Is this a correct attack stage classification for this activity? (Infection.)

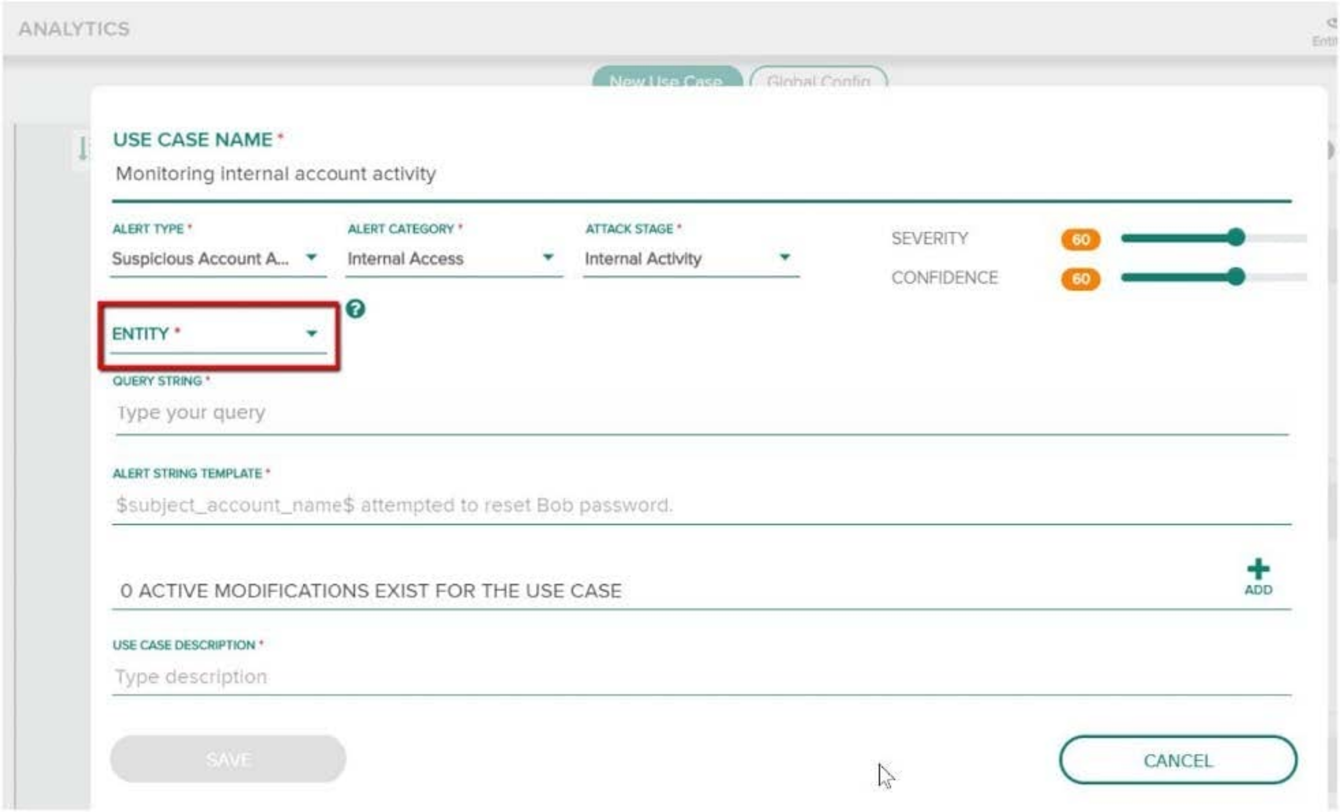
A. Yes

B. No

Correct Answer: A

QUESTION 4

Refer to the exhibit.



USE CASE NAME *
Monitoring internal account activity

ALERT TYPE *
Suspicious Account A...

ALERT CATEGORY *
Internal Access

ATTACK STAGE *
Internal Activity

SEVERITY 60

CONFIDENCE 60

ENTITY *

QUERY STRING *
Type your query

ALERT STRING TEMPLATE *
$subject_account_name$ attempted to reset Bob password.

0 ACTIVE MODIFICATIONS EXIST FOR THE USE CASE

USE CASE DESCRIPTION *
Type description

You have been assigned a task to monitor, analyze, and find those entities who are trying to access internal resources without having valid user credentials. You are creating an AD-based use case to look for this activity. Could you use this entity type to accomplish this? (Host name.)

A. Yes

B. No

Correct Answer: A

QUESTION 5

While validating the data sources in a new IntroSpect installation, you have confirmed that the network tap

data is correct and there are AMON log sources for both firewall and DNS.

When you lock in the Entity360, you see the usernames from Active Directory.

However, when you look under E360 > activity > for any user accounts there is no information under

"Activity Card" and "Authentication" for any user. When you filter the Entity360 for IP address and look at

the Activity screen you do see activity on the "Activity Card".

Could this be a reason why you do not see the information but do not see activity? (The log broker could

be configured incorrectly and not sending authentication logs to IntroSpect.)

A. Yes

B. No

Correct Answer: B

HPE2-W05 Practice Test HPE2-W05 Study Guide HPE2-W05 Exam Questions