HPE2-W05 Q&As

Implementing Aruba IntroSpect

Pass HP HPE2-W05 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/hpe2-w05.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

You have been asked to provide a Bill of Materials (BoM) for a mature small business with two sites. The IT Director prefers all hardware to be on-premise but is open to cloud-based solution. In conversations with the IT staff, you determine that the main site has approximately 550 network devices and 400 users. All users are in Active Directory. Eighty of the users use a Pulse Secure VPN to work remotely.

The second site is a warehouse operation with approximately 40 users and another 10 users that use Pulse Secure VPN. All wireless is using Aruba Networks Instant APs. There are Active Directory servers at both sites. All logs are currently being gathered into Splunk. The team feels that they can properly monitor the corporate site network with a single tap port on a central switch at the main office. There will be a network tap at the remote site. Is this a suggestion you would make to the customer? (The customer should install the Fixed Configuration Analyzer at the main site, along with a Packet Processor in the data center and a single Packet Processor at the warehouse site.)

A. Yes

B. No

Correct Answer: A

QUESTION 2

You are troubleshooting ClearPass with IntroSpect, and you notice that in Access Tracker the IntroSpect Logon Logoff actions profile is executing. However, the ClearPass Log Source on the IntroSpect Analyzer is showing dropped entries.

Would this be a good troubleshooting step? (Confirm that the ClearPass context action is sending the User name, MAC Address, Entity Type, and User Role)

A. Yes

B. No

Correct Answer: B

QUESTION 3

A network administrator is looking for an option to set the maximum data retention period to 180 days in the IntroSpect Analyzer. Is this a correct statement about data retention in IntroSpect? (The data retention period cannot exceed 90 days.)

A. Yes

B. No

Correct Answer: B

QUESTION 4

A company wants to integrate ClearPass with the IntroSpect. Is this a supported version? (ClearPass 6.7.4.)

A. Yes

B. No

Correct Answer: B

QUESTION 5

Arube IntroSpect establishes different types of baselines to perform user or device behavior analysis. Is this a correct description of a baseline that IntroSpect establishes? (Individual history baseline: this typically takes 10 to 14 days to establish a "steady state" that can be used.)

A. Yes

B. No

Correct Answer: A

QUESTION 6

Would this be a proper correlation between entity and attack stage? (There is an alert for port scans by an entity, and you correlate that to a malware doing recon.)

A. Yes

B. No

Correct Answer: B

QUESTION 7

You are configuring a ClearPass Cluster to send endpoint context to an IntroSpect Analyzer for the wireless network. You want to test the setup after you have installed the XML file with the enforcement profiles and actions. Can this method be used to test that the setup is functioning correctly? (Connect to the wireless network, and send a test authentication from a test device/user in the network. Observe the results in Access Tracker.)

A. Yes

B. No

Correct Answer: A

QUESTION 8

You are deploying a new IntroSpect Packet Processor in your data center. It is not communicating with the analyzer in

the same data center. You think that you have entered the host name of the analyzer incorrectly while bootstrapping the packet processor. Would this be a logical next step? (Enter a new host name with the command #>/opt/niara/analyzer/lib/hadoop/rename-an-node {analyzer FQDN} in the CLI.)

A. Yes

B. No

Correct Answer: A

Reference: https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Default.aspx? EntryId=27256

QUESTION 9

The company has a DMZ with an application server where customers can upload and access their product orders. The security admin wants to know how you configure IntroSpect to monitor this server. Should this be part of your plan? (Configure the server in the DMZ as a High Value Asset in Menu>Configuration>Analytics>Correlator Config>so that IntroSpect will monitor the server for access patterns.)

A. Yes

B. No

Correct Answer: B

QUESTION 10

While investigating alerts in the Analyzer you notice a host desktop with a low risk score has been sending regular emails from an internal account to the same external account. Upon investigation you see that the emails all have attachments. Would this be correct assessment of the situation? (Your next step should be to find what user account logs into this desktop, and look at activity of their devices this user has access to.)

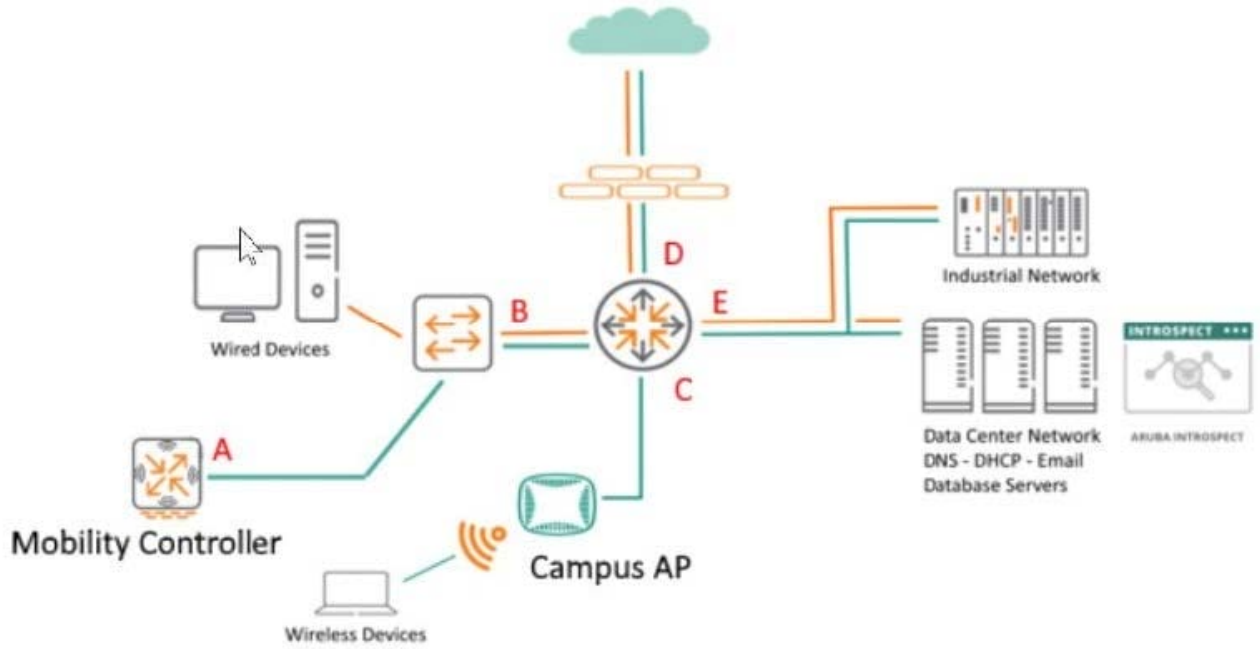
A. Yes

B. No

Correct Answer: B

QUESTION 11

Refer to the exhibit.



You are monitoring network traffic and considering DNS flow patterns. Where is a good location to place the Network Tap or Taps? (Location C.)

A. Yes

B. No

Correct Answer: A

QUESTION 12

A network administrator is looking for an option to set the maximum data retention period to 180 days in the IntroSpect Analyzer. Is this a correct statement about data retention in IntroSpect? (The default data retention period is set at 30 days, and this cannot be changed.)

A. Yes

B. No

Correct Answer: A

QUESTION 13

In a conversation with a colleague you are asked to give them an idea of what type of monitor source you would use for each attack stage.

1. Reconnaissance
2. Entry or Compromise
3. Command and Control
4. Lateral Movement
5. Escalation
6. Execution

Would this be a correct correlation? (For "Command and Control" you can monitor DNS through AMON on the Aruba Mobility Controllers.)

A. Yes

B. No

Correct Answer: B

QUESTION 14

An analyst notices that a disabled user account has been enabled. Is this an action that the analyst should take? (Allow the system to run for 15 days to establish a historical baseline, and determine if this account is a threat.)

A. Yes

B. No

Correct Answer: B

QUESTION 15

You are planning to configure ClearPass to send endpoint context to IntroSpect. You need to create a checklist of functions that must be enabled in ClearPass to support this. Is this an option that is required? (System Monitor Service.)

A. Yes

B. No

Correct Answer: B