PSE: Endpoint Associate training for Traps 4.0

Paloalto Networks PSE-Endpoint-Associate

Version Demo
Total Questions: 10

https://dumpsboss.com
support@dumpsboss.com

PSE-Endpoint-Associate

PSE: Endpoint Associate training for Traps 4.0

QUESTION NO: 1

In which two ways does Traps complement Palo Alto Networks perimeter protection? (Choose two.)

A. Endpoints are sometimes operated by their users outside the corporate network perimeter.

B. ESM servers send information about threats directly to Palo Alto Networks firewalls.

C. Traps endpoints send information about threats directly to Palo Alto Networks firewalls.

D. Information about threats from both Palo Alto Networks firewalls and Traps endpoints flows into a shared threat intelligence cloud.

Answer: BC

QUESTION NO: 2

A user receives an email with an attached data file containing an exploit. What is it's likely effect? (Choose two.)

A. The exploit can work only if a corresponding application is installed on the user's system.

B. The exploit can do damage only if it downloads a piece of malware.

C. The exploit can work only if it begins with a buffer overflow.

D. The exploit might be launched merely by previewing the attachment.

Answer: AB

QUESTION NO: 3

The Traps product and documentation use the terms "malware" and "exploit" in a very specific way. Which two statements are true? (Choose two.)

A. Exploits attempt to take advantage of a vulnerability in code.

B. The primary vector for exploits is .exe files.

C. Malware consists of application data files containing malicious code.

D. Malware consists of malicious executable files that do not rely on exploit techniques.

Answer: AC

QUESTION NO: 4

Which statement about Malware verdicts is true?

A. If WildFire is not available when the active ESM server tries to reach it for a verdict on a file, the endpoint will get a verdict from local analysis.

B. If the ESM server is not available when the Traps agent tries to reach it for a verdict on a file, the file status is marked as Benign.

C. The end user can use the Traps console to override a verdict of Malicious.

D. Local analysis verdicts take precedence over WildFire verdicts.

Answer: A

QUESTION NO: 5

What does ROP stand for?

A. Return-Oriented Programming

B. Rules of Prevention

C. Restriction on Process

D. Retained Original Process

Answer: A

QUESTION NO: 6

Which two of the following TLS/SSL configurations are valid in a Traps 3.4 deployment? Choose two correct answers.

A. ESM Server configured for TLS/SSL; endpoint configured for TLS/SSL

B. ESM Server NOT configured for TLS/SSL; endpoint configured for TLS/SSL

C. ESM Server configured for TLS/SSL; endpoint NOT configured for TLS/SSL

D. ESM Server NOT configured for TLS/SSL; endpoint NOT configured for TLS/SSL

Answer: AB

QUESTION NO: 7

The administrator uses Restrictions to do what in the ESM Console?

A. restrict which processes will be protected by which EPMs.

B. restrict the execution of executable files.

C. restrict which administrators can set policies.

D. restrict the information displayed to users when the Traps agent blocks an exploit.

Answer: A

QUESTION NO: 8

By default, where are log entries for the ESM Server and the ESM Console stored?

A. In XML-formatted text files on the server

B. In flat text files on the server

C. In a connected SIEM system

D. In Panorama

E. In the Windows event log on the server

Answer: A

QUESTION NO: 9

What can be used to change the uninstall passwords of agents after the initial installation of the ESM Server and the endpoint agent software?

A. Using the Advanced tab of the Traps endpoint agent console

B. Using an agent action in ESM Console

C. Using an ESM Server setting in ESM Console

D. Using the command "dbconfig server uninstallpassword" on ESM Server

Answer: C

QUESTION NO: 10

How does an administrator make a Tech Support File?

A. Click the "Create ZIP" button on the Logs page in ESM Console

B. Click the "Generate" button on the Settings page in ESM Console

C. Use dbconfig on ESM Server

D. Use cytool on the endpoint

Answer: B

QUESTION NO: 11