Palo Alto Networks PSE-Endpoint-Associate Exam

Volume: 24 Questions

Question No:1
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:2
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: B,C

Question No:3
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:4
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: A,B

Question No:5
Which two statements about troubleshooting installation and upgrade problems are true? (Choose two.)

A. A common cause of ESM Server installation problems is the failure to confirm connectivity to WildFire before running the installer.

B. A common cause of Traps endpoint agent installation problems is the failure to configure the SSL option correctly.

C. ESM Server services will shut down if they are not licensed within 24 hours of being started.

D. Use MSIEXEC with appropriate flags to get more logging detail at installation time.

Answer: A,B

Question No:6
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