Palo Alto Networks

PSE-ENDPOINT Exam

Palo Alto Networks PSE: Endpoint – Professional Exam

Thank you for Downloading PSE-ENDPOINT exam PDF Demo

You can Buy Latest PSE-ENDPOINT Full Version Download

https://www.certkillers.net/Exam/PSE-ENDPOINT

Version: 8.0

Question: 1

A company wants to implement a new Virtual Desktop Infrastructure (VDI) in which the endpoints are protected with Traps. It must select a VDI platform that is supported by Palo Alto Networks for Traps use.
Which two platform are supported? (Choose two.)

A. Citrix XenDesktop
B. VMware Horizon View
C. Listeq
D. Nimboxx

Answer: A, B

Question: 2

A customer plans to test the malware prevention capabilities of Traps. It has defined this policy.
•   Local analysis is enabled
•   Quarantining of malicious files is enabled
•   Files are to be uploaded to WildFire
No executables have been whitelisted or blacklisted in the ESM Console Hash Control screen.
Malware sample A has a verdict of Malicious in the WildFire service. Malware sample B is unknown to WildFire.
Which behavior will result?

A. WildFire will block sample A as known malware; sample B will be blocked as an unknown binary while the file is analyzed by WildFire for a final verdict.
B. Hash Control already knows sample A locally in the endpoint cache and will block it. Sample B will not be blocked by WildFire, but will be blocked by the local analysis engine.
C. WildFire will block sample A as known malware, and sample B will compromise the endpoint because it is new and ESM Server has not obtained the required signatures.
D. WildFire will block sample A as known malware; sample B will not be blocked by WildFire, but will be evaluated by the local analysis engine and will or will not be blocked, based on its verdict, until WildFire analysis determines the final verdict.

Answer: D

Question: 3

An administrator receives a number of email alerts indicating WildFire has prevented a malicious activity. All the prevention events refer to launching an Install Wizard that has received a benign verdict from WildFire. All prevention events are reported on a subset of endpoints, that have recently been migrated Mom another Traps deployment.
Which two troubleshooting actions are relevant to this investigation? (Choose two.)

A. Check that the servers xml file has been cleared on the migrated endpoints.
B. Check that the ClientInfoHash tag has been cleared on the migrated endpoints.
C. Check that the actions xml file has not been cleared on the migrated endpoints.
D. Check that the WildFire cache has been cleared on the migrated endpoints.

Answer: A, D

Question: 4

An administrator is installing ESM Core 4.0. The SQL Server is running on a non-standard port (36418). The database connection validation is failing. The administrator has entered the following information:
Server Name: Servername\Instance
Database: TrapsDB
User Name: Domain\Account
What is causing the failure?

A. The database name "TrapsDB" is unsupported
B. The instance name should not be specified
C. The non-standard port needs to be specified in the format TrapsDB,36418
D. The destination port cannot be configured during installation

Answer: B

Question: 5

The ESM policy is set to upload unknowns to WildFire. However, when an unknown is executed the Upload status in ESM Console never displays "Upload in progress", and the verdict remains local analysis or unknown. Even clicking the upload button and checking in does not resolve the Issue. A line in the log file suggests not being able to download a file from "https:/ESMSERVER/BitsUploads/… to C:\ProgramData\Cyvera\Temp\..."
Which solution fixes this problem?

A. Restart BITS service on the endpoint
B. Restart BITS service on ESM
C. Remove and reinstall all the agents without SSL

D. In the ESM Console, use the FQDN in multi ESM

Answer: B

Question: 6

When planning to test a software exploit using a Metasploit module, what two options should be considered about the victim host to ensure success?

A. USB port version of the victim host
B. Speed and make of the victim's RAM
C. software version of the target application
D. platform, architecture, and patch level of the victim host

Answer: A, C

Thank You for trying PSE-ENDPOINT PDF Demo

To Buy Latest PSE-ENDPOINT Full Version Download visit link below

https://www.certkillers.net/Exam/PSE-ENDPOINT

Start Your PSE-ENDPOINT Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further discount on your purchase. Test your PSE-ENDPOINT preparation with actual exam questions.