PSE-ENDPOINT^{Q&As}

PSE: Endpoint – Professional

Pass Palo Alto Networks PSE-ENDPOINT Exam with 100% Guarantee

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

https://www.pass4itsure.com/pse-endpoint.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

QUESTION 1

From the ESM console, which two ways can an administrator verify that their installed macOS agents are functional? (Choose two.)

A. Click the Settings Tab > Agent > Installation Package to view the agents installed.

B. Click the Dashboard Tab, and refer to the Computer Distribution and Version window

C. Click the Monitor Tab > Agent > Health. Sort by OS and look for the macOS endpoints

D. Click the Monitor Tab > Data Retrieval

Correct Answer: AC

QUESTION 2

An administrator has decided to test Traps functionality using malware samples in an isolated nonproduction environment. In order to effectively test Traps, what three types of samples should the administrator avoid? (Choose three.)

A. A sample with a low number of hits in Virus Total.

B. An MS Office document which contains a ransomware macro.

C. A sample known to be flagged as grayware by Traps.

D. A freeware video application which spawns malicious processes.

E. A sample known to generate false positives in the production environment.

Correct Answer: ABE

QUESTION 3

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

Correct Answer: B

QUESTION 4

A retail company just purchased Traps for its 8,000 endpoints. Many of its users work remotely. The company is not using any VPN solution, but would still like to manage all endpoints regardless where they are. Which two aspects should be part of the recommendation? (Choose two.)

A. As each ESM Core server can handle up to 30,000 endpoints, use at least 1 ESM Core server internally and 1 ESM core server in the DMZ for external endpoints.

B. Placing an ESM Core server in the DMZ or in a cloud hosting service allows external endpoints to connect to it, even without a VPN client.

C. Protection for remote endpoints is currently not supported. Since the ESM servers can only be installed in an internal network, endpoints without VPN will not be able to connect to it.

D. If there is no connection to the ESM Core server, Traps agents automatically connect to WildFire and endpoints are fully protected. No additional ESM Core servers are needed.

Correct Answer: AB

QUESTION 5

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.

Correct Answer: D

Latest PSE-ENDPOINT Dumps

PSE-ENDPOINT VCE Dumps

PSE-ENDPOINT Exam Questions