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.leads4pass.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

The administrator has added the following whitelist to the WildFire Executable Files policy.

*\mysoftware.exe

What will be the result of this whitelist?

A. users will not be able to run mysoftware.exe.

B. mysoftware.exe will be uploaded to WildFire for analysis

C. mysoftware.exe will not be analyzed by WildFire regardless of the file location.

D. mysoftware.exe will not be analyzed by WildFire, but only if executed from the C drive.

Correct Answer: B

QUESTION 2

An Administrator has identified an EPM-triggered false positive and has used the Create Rule button from within the relevant entry in the Security Events > Preventions > Exploits tab. What is the result of the created rule?

A. The new rule stops all EPM injection into the faulted process.

B. The new rule stops all EPM injection into processes on the machine on which the prevention was triggered.

C. The new rule excludes the endpoint from Traps protection.

D. The new rule will include the EPM that raised the prevention, the process that triggered the prevention, the machine on which the prevention was triggered, and a descriptive name for the rule.

Correct Answer: B

QUESTION 3

An ESM server\\'s SSL certificate needs two Enhanced Key Usage purposes: Client Authentication and _____

A. Server Authentication

B. File Recovery

C. IP Security User

D. IP Security Tunnel Termination

Correct Answer: A

QUESTION 4

In a scenario where winword.exe, Microsoft Word application, is behaving abnormally, how would the administrator verify if Traps DLLs are injected to the process?

A. Run \\'cytool policy winword.exe

B. Use Process Explore to find Traps DLLs injected to the process

C. Open the add-ins tab in Word\\'s options to find Traps add-in

D. Use \\'Ninja mode\\' in the policy editing screen in the ESM to find winword.exe

Correct 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

Correct Answer: B

QUESTION 6

A deployment contains some machines that are not part of the domain. The Accounting and Sales

departments are two of these.

How can a policy of WildFire notification be applied to Accounting, and a policy of WildFire prevention be

applied to Sales, while not affecting any other WildFire policies?

A. Create the rules and use the Objects tab to add Accounting and Sales to each rule they should apply to.

B. Create a condition for an application found on an Accounting machine. Use that condition for the Accounting groups rule, and create the rule tor Sales without any conditions.

C. Create two rules for WildFire: one for prevention, and one for notification. Make sure the Accounting rule is numbered higher.

D. Create group-specific registry entries on endpoints. Use these registry entries to create conditions for the WildFire

rules.

Correct Answer: C

QUESTION 7

An administrator is testing an exploit that is expected to be blocked by the JIT Mitigation EPM protecting the viewer application in use. No prevention occurs, and the attack is successful. In which two ways can the administrator determine the reason for the missed prevention? (Choose two.)

A. Check in the HKLM\SYSTEM\Cyvera\Policy registry key and subkeys whether JIT Mitigation is enabled for this application

B. Check if a Just-In-Time debugger is installed on the system

C. Check that the Traps libraries are injected into the application

D. Check that all JIT Mitigation functions are enabled in the HKLM\SYSTEM\Cyvera\Policy\Organization \Process\Default registry key

Correct Answer: AC

QUESTION 8

An administrator can check which two indicators to verity that Traps for Mac is running correctly on an installed endpoint? (Choose two.)

A. Use cytool from the command line interface to display the running Traps agent services.

B. In the Activity Monitor, verify that CyveraSecvice is running

C. Ping other Traps agents from the macOS agent

D. Verity that the Traps agent icon is displayed on the macOS finder bar.

Correct Answer: BD

QUESTION 9

Once an administrator has successfully instated a Content Update, how is the Content Update applied to endpoint?

A. After Installation on the ESM, an Agent License renewal is required in order to trigger relevant updates.

B. After installation on the ESM, relevant updates occur at the next Heartbeat communication from each endpoint.

C. Installation of a Content Update triggers a proactive push of the update by the ESM server to all endpoints with licensed Traps Agents within the Domain.

D. The Traps Agent must be reinstalled on the endpoint in order to apply the content update. Existing Agents will not be able to take advantage of content updates.

Correct Answer: B

QUESTION 10

Which two enhanced key usage purposes are necessary when creating an SSL certificate for an ESM server? (Choose two.)

A. File Recovery

B. Server Authentication

C. Client Authentication

D. Key Recovery

Correct Answer: BC