Vendor: Palo Alto Networks

Exam Code:PSE-ENDPOINT

Exam Name:PSE: Endpoint – Professional

Version: Demo

QUESTION 1

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 2

In a scenario that macOS Traps logs failed to be uploaded to the forensic folder, where will the user on the macOS host be able to find to collected logs?

A. /ProgramData/Cyvera/Logs

B. /ProgramData/Cyvera/Everyone/Temp

C. /Library/Application Support/Cyvera/BITS Uploads/

D. /Library/Application Support/PaloAltoNetworks/Traps/Upload/

Correct Answer: D

QUESTION 3

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 4

An administrator has installed Traps 4.0. The administrator wants to test the malware protections provided. What sample should they use to test the protections provided by Traps?

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

B. A toolbar package known to be flagged as grayware by Traps

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

D. An MS Office document which contains a ransomware macro

Correct Answer: D

QUESTION 5

What is the default interval for Traps agents to communicate via heartbeat to the ESM?

A. Every 1 Minute

B. Every 1 Hour

C. Every 1 Day

D. Every 1 year

Correct Answer: B

QUESTION 6

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 7

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 8

Files are not getting a WildFire verdict.

What is one way to determine whether there is a BITS issue?

A. Check the upload status in the hash control screen.

B. Run a telnet command between Traps agent and ESM Server on port 2125.

C. Use PowerShell to test upload using HTTP POST method.

D. Initiate a "Send support file" from the agent.

Correct Answer: C

QUESTION 9

The administrator has downloaded the Traps_macOS_4.x.x.zip file. What are the next steps needed to successfully install the Traps 4.x for macOS agent?

A. Push the Traps_macOS_4.x.x.zip to the target endpoint(s), unzip it, and execute Traps.pkg

B. Unzip the Traps_macOS_4.x.x.zip, push the Traps pkg file to the target endpoint(s) and execute Traps.pkg

C. Create a one time action to install the Traps_macOS_4.x.x.zip file on the target endpoint(s)

D. Create an installation package using Traps_macOS_4.x.x on ESM, download the installationpackage.zip, push the installationpackage.zip to target endpoint(s), unzip it, and execute Traps.pkg

Correct Answer: D

QUESTION 10

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

Correct Answer: AC

QUESTION 11

Assume a Child Process Protection rule exists for powershell.exe in Traps v 4.0. Among the items on the blacklist is ipconfig.exe. How can an administrator permit powershell.exe to execute ipconfig.exe without altering the rest of the blacklist?

A. add ipconfig.exe to the Global Child Processes Whitelist, under Restriction settings.

B. Uninstall and reinstall the traps agent.

C. Create a second Child Process Protection rule for powershell.exe to whitelist ipconfig.exe.

D. Remove ipconfig.exe from the rule\\'s blacklist.

Correct Answer: A

QUESTION 12

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