Paloalto Networks

Exam PSE-Endpoint

PSE: Endpoint – Professional

Version: 7.0

[Free Questions]

Question No : 40

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

Answer: B

Question No : 41

An administrator has a critical group of systems running Windows XP SP3 that cannot be upgraded. The administrator wants to evaluate the ability of Traps to protect these systems and the word processing applications running on them.

How should an administrator perform this evaluation?

A. Run a known 2015 flash exploit on a Windows XP SP3 VM, and run an exploitation tool that acts as a listener. Use the results to demonstrate Traps capabilities.
B. Run word processing exploits in a Windows 7 VM in a controlled and isolated environment. Document indicators of compromise and compare to Traps protection capabilities.
C. Prepare a Windows 7 VM. Gather information about the word processing applications, determine if some of them are vulnerable, and prepare a working exploit for at least one of them. Execute with an exploitation tool.
D. Gather information about the word processing applications and run them on a Windows XP SP3 VM. Determine if any of the applications are vulnerable and run the exploit with an exploitation tool.

Answer: A

Question No : 42

An administrator is concerned about rogue installs of Internet Explorer.

Which policy can be created to assure that Internet Explorer can only run from the \Program Files \Internet Explorer \directory?

A. An execution path policy to blacklist iexplore.exe, and whitelist entry for %programfiles%\iexplore.exe
B. An execution path policy to blacklist *\iexplore.exe. Trusted signers will allow the default iexplore.exe
C. A whitelist of *\iexplore.exe with an execution path restriction, and a blackfirst of %system%\iexplore.exe
D. An execution path policy to blacklist *\iexplore.exe, and a whitelist entry for %programfiles%\Internet Explorer\iexplore.exe

Answer: D

Question No : 43

A large manufacturer is planning to roll out Traps to 75,000 endpoints. Their environment consists of three major sites with 24,000 endpoints each, plus about 3,000 remote endpoints in smaller remote locations using always-on VPN connections to a single one of the major sites. The customer wants to minimize network traffic between the major sites, but all endpoints have internet access. The customer is looking for a centrally managed solution with common reporting and management for all endpoints in the environment.

Which design option would be appropriate for this environment?

A. Place the Traps database. ESM Console and two ESM core servers in the large site hosting the VPN gateway, and force all endpoints to use VPN at all times.
B. Place the Traps database, ESM Console and seven ESM core servers in a public-cloud environment where the ESM Core servers are accessible from the internet.
C. Place a Traps database, ESM Console and an ESM core server in each of the three large sites.
D. Place the Traps database and ESM Console in one of the major sites, and one ESM core server in each of the three major sites.

Answer: D

Question No : 44

To ensure that the Traps VDI tool can obtain verdicts for all unknown files what are the things that needs to be checked? Assuming ESM Console and ESM Server are on different servers. (Choose two.)

A. ESM Server can access WildFire Server

B. Endpoint can access WildFire Server
C. ESM Console can access WildFire Server
D. Endpoint can access ESM Server

Answer: A,D

Question No : 45

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

Answer: D