Question 1

Which two statements about troubleshooting installation and upgrade problems are true? (Choose two.)

Options:

A) A common cause of ESM Server installation problems is the failure to confirm connectivity to WildFire before running the installer.

B) A common cause of Traps endpoint agent installation problems is the failure to configure the SSL option correctly.

C) ESM Server services will shut down if they are not licensed within 24 hours of being started.

D) Use MSIEXEC with appropriate flags to get more logging detail at installation time.

Answer:

A, B

Question 2

Which three file types will be uploaded automatically to WildFire for examination? (Choose three.)

Options:

A) Application data files that trigger preventions

B) Executables with no previous verdict in the ESM deployment

C) Executables with a verdict overridden by the administrator

D) Executables allowed to run because their publisher is trusted

E) Executables allowed to run by local analysis

F) Application data files opened by the end user

Answer:

A, E, F

Question 3

Question Type: MultipleChoice

Which three statements about the trusted publisher mechanism are true? (Choose three.)

Options:

A) The trusted-publisher mechanism blocks executables from running unless they are signed by a trusted publisher.

B) The list of trusted publishers is maintained through content updates.

C) The trusted-publisher mechanism takes precedence over verdict overrides by administrators.

D) The trusted-publisher mechanism is called whenever an executable file would otherwise get an Unknown or No Connection verdict.

E) The trusted-publisher mechanism allows trusted signed executables to run without seeking a WildFire verdict.

F) No executable will be affected by the trusted-publisher mechanism unless it is signed by a publisher on a list maintained by Palo Alto Networks.

Answer:

B, C, D

Question 4

Question Type: MultipleChoice

Which is the correct set of prerequisite software components for a production deployment of Endpoint Security Manager?

Options:

A) IIS, .NET, Microsoft SQL Server or SQLite, and an active WildFire subscription

B) IIS, .NET, and Microsoft SQLite

C) IIS, .NET, and any relational database

D) IIS, .NET, Microsoft SQL Server, and an SMTP email server

E) IIS, .NET, and Microsoft SQL Server

Answer:

E

Question 5

Question Type: **MultipleChoice**

What are two ways to prevent exploits? (Choose two.)

Options:

A) Return-Oriented Programming

B) Address Space Layout Randomization

C) Heap Spray

D) Anti-Spyware Location and Removal

E) Retained Original Process

F) Buffer Overflow

G) Data Execution Prevention

Answer:

A, F

Question 6

Question Type: MultipleChoice

Which two statements about targeted attacks are true? (Choose two.)

Options:

A) Exploits typically target vulnerabilities for which there are no patches.

B) Targeted attacks typically employ a combination of software exploits and malware.

C) Computer users can protect themselves effectively against targeted attacks by keeping their systems fully patched and their antivirus signature databases up to date.

D) Attackers may gather information about their intended victims using social media.

Answer:

A, B

Question 7

What can be used to change the uninstall passwords of agents after the initial installation of the ESM Server and the endpoint agent software?

Options:

A) Using the Advanced tab of the Traps endpoint agent console

B) Using an agent action in ESM Console

C) Using an ESM Server setting in ESM Console

D) Using the command 'dbconfig server uninstallpassword' on ESM Server

Answer:

C

Question 8

Question Type: **MultipleChoice**

How does an administrator make a Tech Support File?

Options:

A) Click the 'Create ZIP' button on the Logs page in ESM Console

B) Click the 'Generate' button on the Settings page in ESM Console

C) Use dbconfig on ESM Server

D) Use cytool on the endpoint

Question 9

Question Type: MultipleChoice

Which statement about Malware verdicts is true?

Options:

A) If WildFire is not available when the active ESM server tries to reach it for a verdict on a file, the endpoint will get a verdict from local analysis.

B) If the ESM server is not available when the Traps agent tries to reach it for a verdict on a file, the file status is marked as Benign.

C) The end user can use the Traps console to override a verdict of Malicious.

D) Local analysis verdicts take precedence over WildFire verdicts.

Answer:

A