DUMPSsheet

Free Questions for PSE-Endpoint-Associate by dumpssheet

Shared by Morin on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which two statements about file hashes are true? (Choose two.)

Options:

A- WildFire populates ESM Server's cache with hashes of files known from other customers to be malicious.

B- The Traps agent caches the hashes of executable files for which it has verdicts.

C- ESM Servers send hashes of application data files to WildFire.

D- ESM Servers send hashes of executable files to WildFire.

Answer:

A, C

Question 2

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 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

Traps endpoints send which three items directly to the ESM Server over port 2125 by default? (Choose three.)

Options:

A- Requests for software update packages

B- Verdict requests

C- WildFire malware reports

D- Exploit prevention dumps

E- Prevention events

F- Heartbeats

Answer:

A, C, E

Question 5

Question Type: **MultipleChoice**

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 6

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 7

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 8

Question Type: **MultipleChoice**

Which two statements about advanced cyberthreats are true? (Choose two.)

Options:

A- It is very common for attacks to use previously unknown malware.

B- A zero-day vulnerability is defined as a security flaw of which the vulnerable product's vendor has no prior awareness.

C- It is impractical to protect against zero-day attacks.

D- A zero-day vulnerability is defined as a security flaw of which the vulnerable product's customers have no prior awareness.

Answer:

B, D