Free Questions for PSE-Endpoint-Associate by actualtestdumps

Shared by Cochran on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

In the Traps product, what does the term "Service Protection" mean?

Options:

A- the protection of a specified process

B- the ability of one ESM Server to take over for another

C- the protection of a process running on a Windows Server system

D- the ability of the Traps agent to make itself tamper-proof

Answer:

A

Question 2

Question Type: MultipleChoice

A user receives an email that has piece of malware as an attachment. Choose the true statement.

Options:

A- The piece of malware can work only if a corresponding application is on the user's system.

B- The piece of malware can do damage only if it makes a connection to a command-and-control server.

C- The piece of malware can work only if it begins with a buffer overflow.

D- The piece of malware can work only if the user opens the attachment.

Answer:

C

Question 3

Question Type: MultipleChoice

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 4

Question Type: **MultipleChoice**

What can a Traps content update include? (Choose three.)

Options:

A- New EPMs

B- Updates to the local-analysis model

C- New trusted root certificates

D- New default policy rules

E- New trusted publishers

F- New Traps endpoint drivers

Answer:

B, C, D

Question 5

Question Type: MultipleChoice

Which two statements about Local Analysis are true? (Choose two.)

Options:

A- Traps endpoint agents build a local analysis model based on the executables they detect.

B- Local analysis is called to validate all verdicts on executable files before the files are allowed to run.

C- Palo Alto Networks uses machine-learning techniques in its labs to build the local analysis model.

D- Local analysis is called whenever an executable file would otherwise get an Unknown or No Connection verdict.

Answer:

C, D

Question 6

Question Type: MultipleChoice

What is the maximum supported number of endpoints per ESM Server in a Traps 3.4 deployment?

Options:

A- 350

B- 16,000

C- 10,000

D- 80,000

Answer:

D

Question 7

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

Answer:

B

Question 8

Question Type: MultipleChoice

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 9

Question Type: MultipleChoice

By default, where are log entries for the ESM Server and the ESM Console stored?

Options:

A- In XML-formatted text files on the server

B- In flat text files on the server

C- In a connected SIEM system

D- In Panorama

E- In the Windows event log on the server

Answer:

A

Question 10

Question Type: **MultipleChoice**

The administrator uses Restrictions to do what in the ESM Console?

Options:

A- restrict which processes will be protected by which EPMs.

B- restrict the execution of executable files.

C- restrict which administrators can set policies.

D- restrict the information displayed to users when the Traps agent blocks an exploit.

Answer:

A

Question 11

Question Type: MultipleChoice

Which two of the following TLS/SSL configurations are valid in a Traps 3.4 deployment? Choose two correct answers.

Options:

A- ESM Server configured for TLS/SSL; endpoint configured for TLS/SSL

B- ESM Server NOT configured for TLS/SSL; endpoint configured for TLS/SSL

C- ESM Server configured for TLS/SSL; endpoint NOT configured for TLS/SSL

D- ESM Server NOT configured for TLS/SSL; endpoint NOT configured for TLS/SSL

Answer:

A, B

Question 12

Question Type: MultipleChoice

What does ROP stand for?

Options:

A- Return-Oriented Programming

B- Rules of Prevention

C- Restriction on Process

D- Retained Original Process

Answer:

A