Free Questions for PSE-Endpoint by certsinside

Shared by Simon on 12-12-2023

For More Free Questions and Preparation Resources

Question 1

Question Type: MultipleChoice

Files are not getting a WildFire verdict.

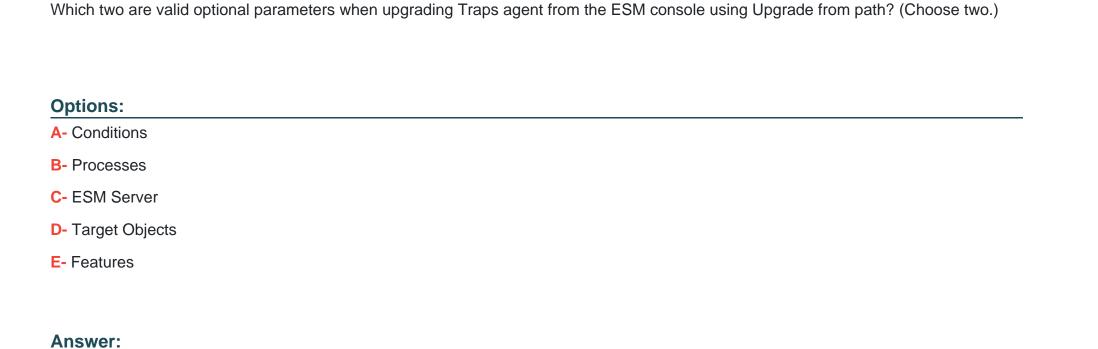What is one way to determine whether there is a BITS issue?

Options:

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

Answer:

C

Question 2

Question Type: MultipleChoice

Which two are valid optional parameters when upgrading Traps agent from the ESM console using Upgrade from path? (Choose two.)

Options:

A- Conditions

B- Processes

C- ESM Server

D- Target Objects

E- Features

Answer:

A, D

Question 3

Question Type: **MultipleChoice**

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 4

Question Type: MultipleChoice

An administrator has decided to test Traps functionality using malware samples in an isolated non-production environment. In order to effectively test Traps, what three types of samples should the administrator avoid? (Choose three.)

Options:

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

B- An MS Office document which contains a ransomware macro

C- A sample known to be flagged as grayware by Traps

D- A freeware video application which spawns malicious processes

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

Answer:

A, B, E

Question 5

Question Type: MultipleChoice

An ESM server's SSL certificate needs two Enhanced Key Usage purposes:

Client Authentication and _____

Options:

A- Server Authentication

B- File Recovery

C- IP Security User

D- IP Security Tunnel Termination

Answer:

A

Question 6

Question Type: MultipleChoice

Uploads to the ESM Sever are failing.

How can the mechanism for forensic and WildFire uploads be tested from the endpoint?

Options:

A- Use BITS commands in PowerShell to send a file to the ESM Server

B- Use curl to execute a POST operation

C- Use SCP commands from a ssh client to transfer a file to the ESM Server

D- Click Check-in now in the agent console

Answer:

D

Question 7

Question Type: **MultipleChoice**

A company is trying to understand which platform can be installed on their environment:

Select the three endpoints where Traps can be installed (Choose three).

Options:

A- Windows 10 LTSB with 2 GB RAM, 500MB free disk space and Intel Core i5 CPU

B- Windows 2000 SP4 with 1 GB RAM, 4 GB free disk space and Intel Pentium 4 CPU

C- Apple iPhone 6s

D- Windows Server 2012 R2 Standard Edition in FIPS Mode, with 4GB RAM, 20GB free disk space, running on VMware ESXi.

E- 15'' MacBook Pro running macOS 10.12 with 16GB RAM, Intel Core i7 CPU and 100GB tree disk space

Answer:

A, D, E