Free Questions for PSE-Endpoint by certscare

Shared by Medina on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

What is the default interval for Traps agents to communicate via heartbeat to the ESM?

Options:

A- Every 1 Minute

B- Every 1 Hour

C- Every 1 Day

D- Every 1 year

Answer:

B

Question 2

Question Type: **MultipleChoice**

In a scenario that macOS Traps logs failed to be uploaded to the forensic folder, where will the user on the macOS host be able to find to collected logs?

Options:

A- /ProgramData/Cyvera/Logs

B- /ProgramData/Cyvera/Everyone/Temp

C- /Library/Application Support/Cyvera/BITS Uploads/

D- /Library/Application Support/PaloAltoNetworks/Traps/Upload/

Answer:

D

Question 3

Question Type: **MultipleChoice**

An Administrator has identified an EPM-triggered false positive and has used the Create Rule button from within the relevant entry in the Security Events > Preventions > Exploits tab. What is the result of the created rule?

Options:

A- The new rule stops all EPM injection into the faulted process.

B- The new rule stops all EPM injection into processes on the machine on which the prevention was triggered.

C- The new rule excludes the endpoint from Traps protection.

D- The new rule will include the EPM that raised the prevention, the process that triggered the prevention, the machine on which the prevention was triggered, and a descriptive name for the rule.

Answer:

B

Question 4

Question Type: **MultipleChoice**

A deployment contains some machines that are not part of the domain. The Accounting and Sales departments are two of these.

How can a policy of WildFire notification be applied to Accounting, and a policy of WildFire prevention be applied to Sales, while not affecting any other WildFire policies?

Options:

A- Create the rules and use the Objects tab to add Accounting and Sales to each rule they should apply to.

B- Create a condition for an application found on an Accounting machine. Use that condition for the Accounting groups rule, and create the rule tor Sales without any conditions.

C- Create two rules for WildFire: one for prevention, and one for notification. Make sure the Accounting rule is numbered higher.

D- Create group-specific registry entries on endpoints. Use these registry entries to create conditions for the WildFire rules

Answer:

C

Question 5

Question Type: **MultipleChoice**

An administrator would like to add Google Chrome and Google Chrome Helper to the exploit prevention policy for macOS. In order to achieve this task, which option should be added to the macOS protected processes list?

Options:

A- chrome app

B- google chrome and google chrome helper

C- chrome*

D- google chrome

Answer:

B

Question 6

Question Type: **MultipleChoice**

Which version of .NET Framework is required as a prerequisite when installing Traps agent on Windows 7?

Options:

A- .NET Framework 4.5

B- .NET Framework 3.5.1

C- .NET Framework 2.0

D- .NET Framework 4.0

Answer:

B

Question 7

Question Type: MultipleChoice

The administrator has added the following whitelist to the WildFire Executable Files policy.

*\mysoftware.exe

What will be the result of this whitelist?

Options:

A- users will not be able to run mysoftware.exe.

B- mysoftware.exe will be uploaded to WildFire for analysis

C- mysoftware.exe will not be analyzed by WildFire regardless of the file location.

D- mysoftware.exe will not be analyzed by WildFire, but only if executed from the C drive.

Answer:

B

Question 8

Question Type: **MultipleChoice**

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?

Options:

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

Question 9

Question Type: MultipleChoice

Assume a Child Process Protection rule exists for powershell.exe in Traps v 4.0. Among the items on the blacklist is ipconfig.exe. How can an administrator permit powershell.exe to execute ipconfig.exe without altering the rest of the blacklist?

Options:

A- add ipconfig.exe to the Global Child Processes Whitelist, under Restriction settings.

B- Uninstall and reinstall the traps agent.

C- Create a second Child Process Protection rule for powershell.exe to whitelist ipconfig.exe.

D- Remove ipconfig.exe from the rule's blacklist.

Answer:

A

20%
DISCOUNT