Free Questions for 5V0-93.22 by vceexamstest

Shared by Bennett on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An administrator has been tasked with preventing the use of unauthorized USB storage devices from being used in the environment.

Which item needs to be enabled in order to enforce this requirement?

Options:

A- Enable the Block access to all unapproved USB devices within the policies option.

B- Choose to disable USB device access on each endpoint from the Inventory page.

C- Select the option to block USB devices from the Reputation page.

D- Elect to approve only allowed USB devices from the USB Devices page.

Answer:

A

Question 2

Question Type: MultipleChoice

The use of leading wildcards in a query is not recommended unless absolutely necessary because they carry a significant performance penalty for the search.

What is an example of a leading wildcard?

Options:

A- filemod:system32/ntdll.dll

B- filemod:system32/*ntdll.dll

C- filemod:*/system32/ntdll.dll

D- filemod:system32/ntdll.dll*

Answer:

C

Question 3

Question Type: **MultipleChoice**

A script-based attack has been identified that inflicted damage to the corporate systems. The security administrator found out that the malware was coded into Excel VBA and would like to perform a search to further inspect the incident.

Where in the VMware Carbon Black Cloud Endpoint Standard console can this action be completed?

Options:

A- Endpoints

B- Settings

C- Investigate

D- Alerts

Answer:

C

Question 4

Question Type: **MultipleChoice**

Which port does the VMware Carbon Black sensor use to communicate to VMware Carbon Black Cloud?

Options:

A- 443

B- 80

C- 8443

D- 22

Answer:

A

Question 5

Question Type: MultipleChoice

An organization is implementing policy rules. The administrator mentions that one operation attempt must use a Terminate Process action.

Which operation attempt has this requirement?

Options:

A- Performs ransom ware-like behavior

B- Runs or is running

C- Scrapes memory of another process

D Invokes a command interpreter

Answer:

A

Question 6

Question Type: MultipleChoice

What is a security benefit of VMware Carbon Black Cloud Endpoint Standard?

Options:

A- Events and alerts are tagged with Carbon Black TTPs to provide context around attacks.

B- Firewall rule configuration are provided in the environment.

C- Data leakage protection (DLP) is enforced on endpoints or subsets of endpoints.

D- Customized threat feeds can be combined with other outside threat intelligence sources.

Answer:

A

Question 7

Question Type: MultipleChoice

A security administrator needs to remediate a security vulnerability that may affect the sensors. The administrator decides to use a tool that can provide interaction and remote access for further investigation.

Which tool is being used by the administrator?

Options:

A- CBLauncher

B- Live Response

C- PowerCLI

D- IRepCLI

Answer:

B

Question 8

Question Type: MultipleChoice

An administrator has determined that the following rule was the cause for an unexpected block:

[Suspected malware] [Invokes a command interpreter] [Terminate process]

All reputations for the process which was blocked show SUSPECT_MALWARE.

Which reputation was used by the sensor for the decision to terminate the process?

Options:

A- Initial Cloud reputation

B- Actioned reputation

C- Current Cloud reputation

D- Effective reputation

Answer:

D