Free Questions for 5V0-93.22 by go4braindumps

Shared by Jimenez on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

The administrator has configured a permission rule with the following options selected:

Application at path: C:\Program Files**

Operation Attempt: Performs any operation

Action: Bypass

What is the impact, if any, of using the wildcards in the application at path field?

Options:

A- Executable files in the 'Program Files' directory and subdirectories will be ignored.

B- Executable files in the 'Program Files' directory will be blocked.

C- Executable files in the 'Program Files' directory will be logged.

D- Executable files in the 'Program Files' directory will be subject to blocking rules.

Answer:

A

Question 2

Question Type: MultipleChoice

Is it possible to search for unsigned files in the console?

Options:

A- Yes, by using the search:

NOT process_publisher_state:FILE_SIGNATURE_STATE_SIGNED

B- No, it is not possible to return a query for unsigned files.

C- Yes, by using the search:

process_publisher_state:FILE_SIGNATURE_STATE_UNSIGNED

D.

Yes, by looking at signed and unsigned executables in the environment and seeing if another difference can be found, thus locating unsigned files in the environment.

Answer:

C

Question 3

Question Type: **MultipleChoice**

An administrator wants to find information about real-world prevention rules that can be used in VMware Carbon Black Cloud Endpoint Standard.

How can the administrator obtain this information?

Options:

A- Refer to an external report from other security vendors to obtain solutions.

B- Refer to the TAU-TIN's on the VMware Carbon Black community page.

C- Refer to the VMware Carbon Black Cloud sensor install guide.

D- Refer to VMware Carbon Black Cloud user guide.

Answer:

B

Question 4

Question Type: MultipleChoice

What are the highest and lowest file reputation priorities, respectively, in VMware Carbon Black Cloud?

Options:

A- Priority 1: Ignore, Priority 11: Unknown

B- Priority 1: Unknown, Priority 11: Ignore

C- Priority 1: Known Malware, Priority 11: Common White

D- Priority 1: Company Allowed, Priority 11: Not Listed/Adaptive White

Answer:

A

Question 5

Question Type: MultipleChoice

A user downloaded and executed malware on a system. The malware is actively exfiltrating data.

Which immediate action is recommended to prevent further exfiltration?

Options:

A- Check Security Advisories and Threat Research contents.

B- Place the device in quarantine.

C- Run a background scan.

D- Request upload of the file for analysis.

Answer:

B

Question 6

Question Type: **MultipleChoice**

Which command is used to immediately terminate a current Live Response session?

Options:

A- kill

B- detach -q

C- delete

D- execfg

Answer:

B

Question 7

Question Type: MultipleChoice

An administrator is investigating an alert and reads a summary that says:

The application powershell.exe was leveraged to make a potentially malicious network connection.

Which action should the administrator take immediately to block that connection?

Options:

A- Click Delete Application

B- Click Quarantine Asset

C- Click Export Alert

D- Click Drop Connection

Answer:

D

Question 8

Question Type: MultipleChoice

An administrator wants to block an application by its path instead of reputation. The following steps have already been taken:

Go to Enforce > Policies > Select the desired policy >

Which additional steps must be taken to complete the task?

Options:

A- Click Enforce > Add application path name

B- Scroll down to the Permissions section > Click Add application path > Enter the path of the desired application

C- Scroll down to the Blocking and Isolation section > Click Edit (pencil icon) for the desired Reputation

D- Scroll down to the Blocking and Isolation section > Click Add application path > Enter the path of the desired application

Answer:

D

Question 9

Question Type: **MultipleChoice**

What connectivity is required for VMware Carbon Black Cloud Endpoint Standard to perform Sensor Certificate Validation?

Options:

A- TCP/443 to GoDaddy OCSP and CRL URLs (crl.godaddy.com and ocsp.godaddy.com)

B- TCP/80 to GoDaddy OCSP and CRL URLs (crl.godaddy.com and ocsp.godaddy.com)

C- TCP/443 to GoDaddy CRL URL (crl.godaddy.com and ocsp.godaddy.com)

D- TCP/80 to GoDaddy CRL URL (crl.godaddy.com and ocsp.godaddy.com)

Answer:

A

Question 10

Question Type: **MultipleChoice**

Which VMware Carbon Black Cloud integration is supported for SIEM?

Options:

A- SolarWinds

B- LogRhythm

C- Splunk App

D- Datadog

Answer:

C

Question 11

Question Type: MultipleChoice

An administrator needs to use an ID to search and investigate security incidents in Carbon Black Cloud.

Which three IDs may be used for this purpose? (Choose three.)

Options:

A- Threat

B- Hash

C- Sensor

D- Event

E- User

F- Alert

Answer:

B, D, F

Question 12

Question Type: **MultipleChoice**

An administrator needs to create a search, but it must exclude "system.exe".

How should this task be completed?

Options:

A- #process_name:system.exe

B- *process_name:system.exe

C-

D- -process_name:system.exe

Answer:

D

20%
DISCOUNT