5V0-91.20 Q&As

VMware Carbon Black Portfolio Skills

Pass VMware 5V0-91.20 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/5v0-91-20.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by VMware Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

An analyst wants to block an application\\'s specific behavior but does not want to kill the process entirely as it is heavily used on workstations. The analyst needs to use a Blocking and Isolation Action to ensure that the process is kept alive while blocking further unwanted activity.

Which Blocking and Isolation Action should the analyst use to accomplish this goal?

A. Log Operation

B. Deny Operation

C. Terminate Process

D. Block Process

Correct Answer: B

QUESTION 2

What is the meaning, if any, of the event Report write (removable media)?

A. This event would never occur. App Control does not report activity on removable media.

B. A Policy\\'s device control setting `Block writes to unapproved removable media\\' is set to Report Only. The event details show the process, file name, and hash modified or deleted on the removable media.

C. A Policy\\'s device control setting `Block writes to unapproved removable media\\' is set to Report Only. The event details show the process and file name modified or deleted on the unapproved removable media.

D. A Policy\\'s device control setting `Block writes to unapproved removable media\\' is set to Enabled. The event details show the process, file name, and hash modified or deleted on the removable media.

Correct Answer: C

QUESTION 3

An Enterprise EDR administrator is reviewing the Investigate page and believes they are receiving false positive hits from specific watchlist.

Which three options reduce future false positive hits from this watchlist? (Choose three.)

A. Disable/remove the IOC associated with the false positives.

B. Disable/remove the report associated with the false positives.

C. Dismiss the watchlist hit.

D. Select edit watchlist and uncheck alert on hits.

E. Modify policy rules to exclude the false positive directory.

F. Disable the watchlist associated with the false positives.

Correct Answer: ABD

QUESTION 4

Review the following query:

path:c:\program\ files\ \(x86\)\microsoft

How would this query input term be interpreted?

A. c:\program files x86\microsoft

B. c:rogram files (x86)icrosoft

C. c:rogramfilesx86icrosoft

D. c:\program files (x86)\microsoft

Correct Answer: D

QUESTION 5

How often do watchlists run?

A. Every 10 minutes

B. Every 5 minutes

C. Watchlists can be configured to run at scheduled intervals

D. Every 30 minutes

Correct Answer: C

QUESTION 6

What is the maximum number of binaries (hashes) that can be banned using the web console?

A. 500

B. 600

C. 300

D. 400

Correct Answer: C

QUESTION 7

Which reputation has the highest priority in Cloud Endpoint Standard?

A. Unknown

B. Adware/PUP Malware

C. Known Malware

D. Ignore

Correct Answer: C

QUESTION 8

When dismissing alerts, when should an administrator select "If alert occurs in the future, automatically dismiss it from all devices"?

A. When the administrator wishes to mark the alert instance as a false positive

B. When the administrator wishes to be notified again to this behavior

C. When the administrator wishes to apply this action to all future alerts from the device

D. When the administrator wishes to remove the alert

Correct Answer: C

QUESTION 9

Given the following query:

SELECT * FROM users WHERE UID >= 500;

Which statement is correct?

A. This query limits the number of columns to display in the results.

B. This query filters results sent to the cloud.

C. This query is missing a parameter for validity.

D. This query returns all accounts found on systems.

Correct Answer: A

QUESTION 10

A watchlist generates a false positive on the Triage Alerts page, so the watchlist must be updated. How should this task be accomplished?

A. One can update watchlists directly on the Triage Alerts Page using the pencil icon.

B. One can update watchlists from the Process Search Page.

C. Open the process analysis page and select the Add Watchlist Exclusion option from the Actions menu.

D. Open the Watchlist Page and click the pencil button associated with the watchlist.

Correct Answer: A

QUESTION 11

Given an event rule: Approve nVidia Drivers, changes the local state to Approved for file writes or execution blocks when the publisher is NVIDIA Corporation. How is an alert created that is triggered whenever an nVidia driver is approved by the event rule?

A. Add a new Alert of type Event Alert. Set Subtype to New unapproved file to computer and Execution block (unapproved file) and Publisher to NVIDIA Corporation. Click Create and add email recipients.

B. Click Create Alert on the event rule Approve nVidia Drivers details page. Click Create and add email recipients. Create and Exit.

C. Click Create Alert on the event rule Approve nVidia Drivers details page. Add email recipients. Create and Exit.

D. Create a custom rule name Approve nVidia that approves writes or blocks when the publisher is NVIDIA Corporation. Create an alert for rule name Approve nVidia. Click Create and add email recipients.

Correct Answer: B

QUESTION 12

How can an analyst disregard alerts on multiple devices with the least amount of administrative effort?

A. Select the "Dismiss on all devices" option.

B. Make a note in the Notes/Tags option.

C. Search by hash and dismiss.

D. Turn off the Group Alerts option.

Correct Answer: D

Reference: https://www.google.com/url?sa=tandrct=jandq=andesrc=sandsource=webandcd=andcad=rjaanduact=8andved=2ahUKEwjv6pryl4XvAhWagVwKHTCMDTEQFjAAegQIARADandurl=https%3A%2F%2Fcommunity.carbonblack.com%2Ft5% 2FKnowled ge-Base%2FCarbon-Black-Cloud-How-to-Dismiss-Alerts%2Fta-p%2F51766andusg=AOvVaw2x1mST1tWpuASUMLmFhyuI (80)

QUESTION 13

An authorized administrator plans to remove the App Control agent from a computer. Which Enforcement Level must a computer be in before the agent can be uninstalled?

A. Visibility

B. None (Disabled)

C. Any Enforcement Level

D. Low Enforcement

Correct Answer: C

QUESTION 14

An analyst has investigated two alerts on two separate HR workstations and found that notepad.exe has established communication to another IP address.

Which rule will kill notepad.exe entirely if this activity is detected in the future?

A. **\system32\notepad.exe --> Communicates over the network --> Terminate process

B. **\system32\notepad.exe --> Runs or is Running --> Deny operation

C. **/system32/notepad.exe --> Runs or is Running --> Terminate process

D. **/system32/notepad.exe--> Communicates over the network --> Deny operation

Correct Answer: C

QUESTION 15

Which reputation is processed with the lowest priority for Endpoint Standard?

A. Local White

B. Known Malware

C. Trusted White

D. Common White

Correct Answer: B