VCE & PDF
GeekCert.com

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.geekcert.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 administrator viewed and filtered the results of a completed query within the User Interface for Audit and Remediation. The administrator exported the results to create charts and other visuals for reporting. When viewing the exported results, the administrator noticed some results were missing from the data set.

Why did the administrator not have the full data set from the query?

A. Export applies to the data visible in the UI; filtering will impact the viewable data.

B. Export pulls all results; the query must not have covered all data required.

C. Export is limited to the first hundred rows, and the query had more rows than supported.

D. Export was used prior to the query completing, and some data is missing.

Correct Answer: D

QUESTION 2

An administrator needs to check configurations using Audit across several policies and locations within the organization.

How can the administrator run the query to only these specific devices?

A. Specify endpoints on the query by selecting the check box for each device.

B. Specify endpoints on the query by typing the sensor name into the text box, selecting the device. Repeat as necessary for all devices.

C. Specify the policy for the endpoints on the query, and then select the check box for each device.

D. Specify the policy for the endpoints on the query, and then type the sensor name into the text box, selecting the devices. Repeat as necessary for all devices.

Correct Answer: D

QUESTION 3

While an administrator is reviewing an alert, the device is observed beaconing to an unknown destination. Which action should be taken to stop this behavior?

A. Deregister the sensor

B. Put the device in Bypass mode

C. Place the device in Quarantine

D. Assign the application to the Approved List

Correct Answer: B

QUESTION 4

A process has created a number of interesting (executable) files in one sequence.

In addition to the event Subtype \\'New Unapproved File to Computer\\', what other event subtype is likely to be associated with this sequence?

A. File Upload Completed

B. New File Discovered on Startup

C. File Group Created

D. File Properties Modified

Correct Answer: B

QUESTION 5

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