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.certbus.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

Which statement should be used when constructing queries in Carbon Black Audit and Remediation, Live Query?

A. ALTER

B. UPDATE

C. REMOVE

D. SELECT

Correct Answer: D

QUESTION 2

An administrator needs to query all endpoints in the HR group for instances of an obfuscated copy of

cmd.exe.

Given this Enterprise EDR query:

process_name:cmd.exe AND device_group:HR AND NOT enriched:true

Which example could be added to the query to provide the desired results?

A. NOT process_name:cmd.exe

B. NOT process_original_filename:cmd.exe

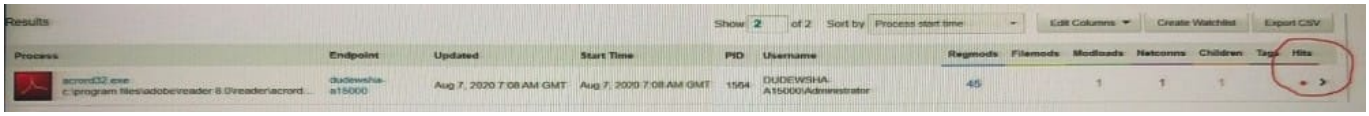
C. NOT process_company_name:cmd.exe

D. NOT process_internal_name:cmd.exe

Correct Answer: A

QUESTION 3

Refer to the exhibit, noting the circled red dot:



What is the meaning of the red dot under Hits in the Process Search page?

A. Whether the execution of the process resulted in a syslog hit

B. Whether the execution of the process resulted in a sensor hit

C. Whether the execution of the process resulted in matching hits for different users

D. Whether the execution of the process resulted in a feed hit

Correct Answer: C

QUESTION 4

A Carbon Black administrator received an alert for an untrusted hash executing in the environment. Which two information items are found in the alert pane? (Choose two.)

A. Launch Live Query

B. Launch process analysis

C. User quarantine

D. Add hash to banned list

E. IOC short name

Correct Answer: AB

QUESTION 5

Which statement filters data to only return rows where the publisher of the software includes VMware anywhere in the name?

A. WHERE publisher = "%VMware%"

B. WHERE publisher = "%VMware"

C. WHERE publisher LIKE "VMware%"

D. WHERE publisher LIKE "%VMware%"

Correct Answer: D

QUESTION 6

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 7

How often do watchlists run?

A. Every 10 minutes

B. Every 5 minutes

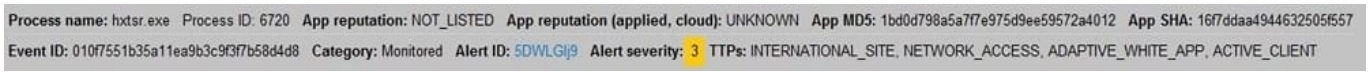
C. Watchlists can be configured to run at scheduled intervals

D. Every 30 minutes

Correct Answer: C

QUESTION 8

An administrator observes the following event detail in the Investigate tab for an application with an unknown reputation making network connections:



Upon further review of the event details returned, the reputation is observed as NOT_LISTED, and the applied (cloud) reputation is UNKNOWN.

Why is the applied (cloud) reputation UNKNOWN and not NOT_LISTED?

A. The sensor demoted the local reputation from UNKNOWN to NOT_LISTED based on the coud reputation.

B. NOT_LISTED was applied by the sensor after observing no cloud reputation, as evidenced by the applied cloud reputation UNKNOWN.

C. The application was UNKNOWN at the time of the event but then later determined to be NOT_LISTED.

D. The sensor demoted the local reputation from NOT_LISTED to UNKNOWN based on the cloud reputation.

Correct Answer: C

QUESTION 9

An administrator receives an alert with the TTP DATA_TO_ENCRYPTION.

What is known about the alert based on this TTP even if other parts of the alert are unknown?

A. A process attempted to delete encrypted data on the disk.

B. A process attempted to write a file to the disk.

C. A process attempted to modify a monitored file written by the sensor.

D. A process attempted to transfer encrypted data on the disk over the network.

Correct Answer: B

QUESTION 10

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 11

Which value should an administrator use when reviewing an alert to determine the file reputation at the time the event occurred?

A. Cloud Reputation (Initial)

B. Effective Reputation

C. Local Reputation

D. Cloud Reputation (Current)

Correct Answer: A

QUESTION 12

Review the following EDR query:

(parent_name:powershell.exe OR parent_name:cmd.exe) AND netconn_count:[l TO *]

Which process would show in the query results?

A. Processes invoked by Powershell.exe and cmd.exe with a single network connection event

B. Processes invoking Powershell.exe and cmd.exe with multiple network connection events

C. Processes invoked by Powershell.exe or cmd.exe with any number of network connection events

D. Processes invoking Powershell.exe or cmd.exe with multiple network connection events

Correct Answer: A

QUESTION 13

An administrator has updated a Threat Intelligence Report by turning it into a watchlist and needs to disable (Ignore) the old Threat Intelligence Report.

Where in the UI is this action not possible to perform?

A. Search Threat Reports Page

B. Threat Intelligence Feeds Page

C. Threat Report Page

D. Triage Alerts Page

Correct Answer: B

QUESTION 14

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

QUESTION 15

Which two statements are true about Carbon Black alerts? (Choose two.)

A. They can be grouped together.

B. Once received, it can be dismissed in bulk.

C. Once dismissed, the action cannot be undone.

D. Carbon Black does not generate alerts.

E. They are stored for 15 days.

Correct Answer: DE