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.leads4pass.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 is searching for any child processes of email clients with this query in Carbon Black Enterprise EDR:

parent_name:outlook.exe OR parent_name:thunderbird.exe OR parent_name:eudora.exe The administrator would like to modify this query to only show child processes that do not have a known reputation in the Carbon Black Cloud.

Which search field can be added to the query to show the desired results?

A. process_integrity_level

B. process_reputation

C. process_privileges

D. process_cloud_reputation

Correct Answer: B

QUESTION 2

An Enterprise EDR administrator has created a custom Watchlist and wants to add a custom query to a report in the custom Watchlist.

From which page can the administrator add this custom query?

A. Policies

B. Watchlists

C. Investigate

D. Cloud Analysis

Correct Answer: C

QUESTION 3

Which actions are available for Permissions?

A. Approve, Upload, No Upload

B. Deny Operation, Terminate Process

C. Allow, Allow and Log, Bypass

D. Performs any Operation, Runs or is running

Correct Answer: C

QUESTION 4

Review the following EDR query:

parent_name:outlook.exe AND -alliance_score_srstrust:* AND -digsig_result: "Signed\\'

Which process would show in the query results?

A. Processes invoked by outlook.exe that have an SRS Trust value and that are digitally signed.

B. Processes invoking outlook.exe that do not have an SRS Trust value and that are not digitally signed.

C. Processes invoked by outlook.exe that do not have an SRS Trust value and that are not digitally signed.

D. Processes invoking outlook.exe that have an SRS Trust value and that are not digitally signed.

Correct Answer: D

QUESTION 5

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 6

An analyst is investigating an alert within the Enterprise EDR console and needs to take action on it. Which three actions are available to take on the alert? (Choose three.)

A. Ignore alert

B. Dismiss

C. Dismiss on all devices if grouping is enabled

D. Edit watchlist

E. Save report

F. Notifications history

Correct Answer: BCE

Reference: https://community.carbonblack.com/t5/Knowledge-Base/Carbon-Black-Cloud- How-to-DismissAlerts/ta-p/51766

QUESTION 7

How long will Live Queries in Carbon Black Audit and Remediation run before timing out?

A. 30 days

B. 14 days

C. 180 days

D. 7 days

Correct Answer: D

QUESTION 8

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 9

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 10

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 11

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 12

Which wildcard configuration applies a policy to all files and subfolders in a specific folder in Endpoint Standard?

A. C:\Program Files\example\$$

B. C:\Program Files\example**

C. C:\Program Files\example\$

D. C:\Program Files\example*

Correct Answer: B

Reference: https://community.carbonblack.com/t5/Knowledge-Base/Endpoint-Standard-How-to-CreatePolicy-Blocking-Isolation-and/ta-p/65941

QUESTION 13

Review the following search:

childproc_name:"rundll32.exe" AND -digsig_result:"Signed" AND path:c:\windows*

What is this search looking for?

A. Processes being launched by rundll32.exe running out of the windows directory that are not signed

B. Instances of rundll32.exe running out of the windows directory that are not signed

C. Instances of rundll32.exe running out of the windows directory that are signed

D. Processes launching rundll32.exe running out of the windows directory that are not signed

Correct Answer: A

Reference: https://www.carbonblack.com/blog/hunting-the-white-rabbit-detecting-metasploitmeterpreterusing-carbon-black/

QUESTION 14

Which strategy should be used to purge inactive bans from the web console?

A. Schedule an add-hoc cron job to remove

B. Use a pre-configured system cron job daily to remove them

C. Run the cbbannlng script on the EDR server

D. Go to the hashes page on the web console and remove them

Correct Answer: C

QUESTION 15

An administrator needs to manage a group of sensors from within the console.

Which three actions are available for sensors within the Sensor Group? (Choose three.)

A. Move to group

B. Disable

C. Restart

D. Ban

E. Uninstall

F. Share Settings

Correct Answer: ACE