5V0-91.20Q&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.pass2lead.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

Given the following query:

SELECT hostname, cpu_type, cpu_brand, cpu_physical_cores, cpu_logical_cores, cpu_microcode, (1.0 * physical_memory / (1000*1000*1000)) AS physical_mem_gb, hardware_vendor, hardware_model, hardware_version, hardware_serial FROM system_info;

Which statement Is correct?

A. This query combines data from several different tables.

B. This query customizes the results returned by the system.

C. This query is missing a filter option.

D. This query shows data from the physical_mem_gb column.

Correct Answer: C

QUESTION 2

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 3

Which statement correctly defines the results of ignoring a feed report?

A. Ignoring a feed report will ignore future instances of that report.

B. Ignoring a feed report will ignore all indicators in other threat reports.

C. Ignoring a feed report will also ignore the threat intelligence feed.

D. Ignoring a feed report will remove all instances of the report.

Correct Answer: C

QUESTION 4

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=2ahUKEwjv6pryl4XvAhW
agVwKHTCMDTEQFjAAegQIARADandurl=https%3A%2F%2Fcommunity.carbonblack.com%2Ft5% 2FKnowled ge-
Base%2FCarbon-Black-Cloud-How-to-Dismiss-Alerts%2Fta-p%
2F51766andusg=AOvVaw2x1mST1tWpuASUMLmFhyuI (80)

QUESTION 5

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 6

App Control System Health email alerts for excessive agent backlog are occurring hourly.

This is overwhelming the analysts, and they would like to reduce the notifications.

How can the analyst reduce the unneeded alerts?

A. Set the email address for subscribers to an invalid email.

B. Change reminder email to daily or disabled.

C. Disable the alert.

D. Delete the alert.

Correct Answer: B

QUESTION 7

This search is entered into the process search page: notepad.exe Which three statements about this query are true? (Choose three.)

A. Only processes named notepad.exe will be returned.

B. Since a field name is not selected, query performance will be impacted.

C. A field identifier is required for all criteria within a process search.

D. The search will fail with an error.

E. All processes containing the text notepad.exe in any default field.

F. Processes with registry modifications containing notepad.exe would be retuned.

Correct Answer: BEF

QUESTION 8

An Endpoint Standard administrator is working with an IT team to explicitly permit specific applications from the environment using both the IT Tools and Certs Approved List features.

Once applied, which reputation would these applications be classified under for processing?

A. Trusted White

B. Company White

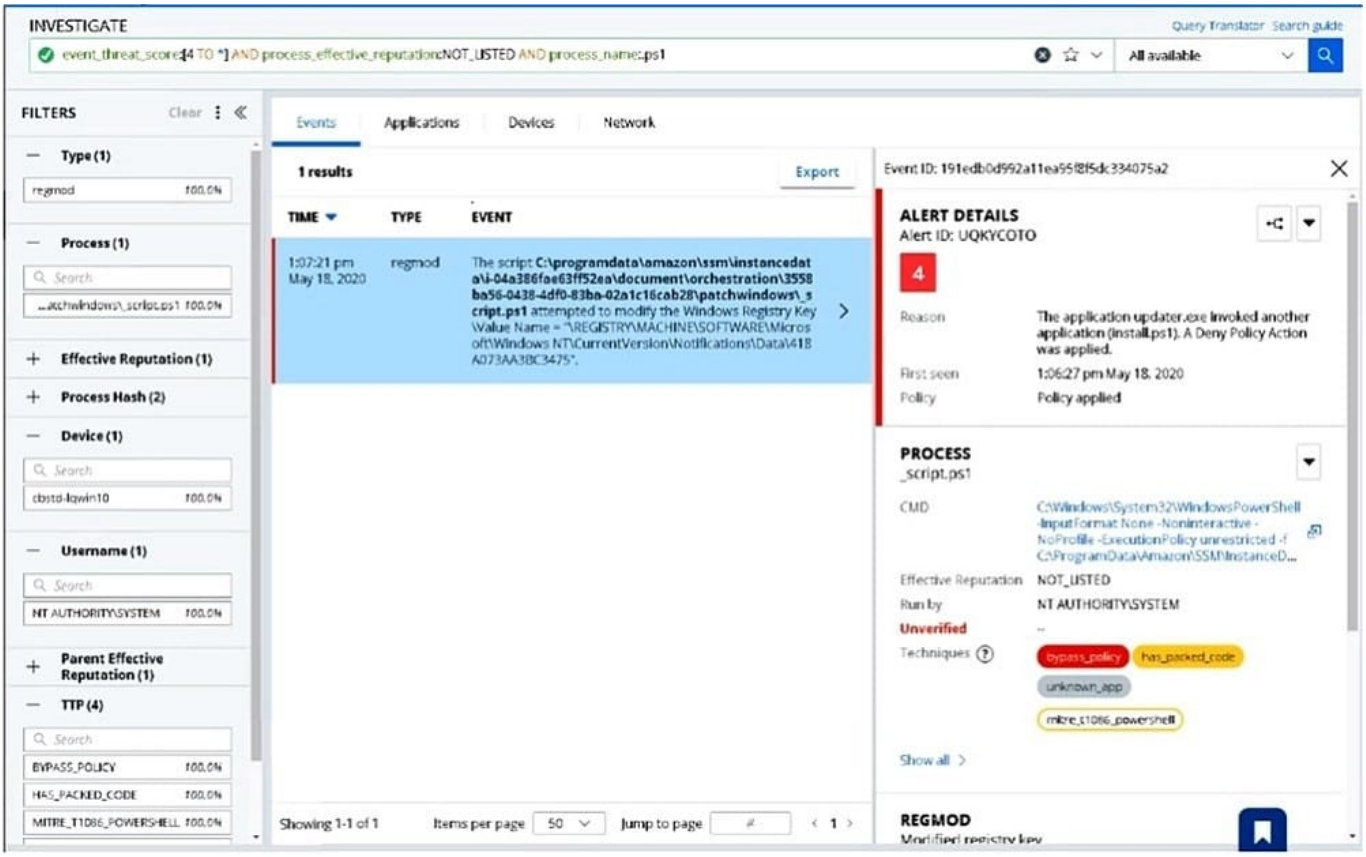
C. Local White

D. Common White

Correct Answer: A

QUESTION 9

An Endpoint Standard analyst runs the query in the graphic below:



Which three statements are true from the results shown? (Choose three.)

A. The process is a PowerShell process running a script with a .ps1 extension.

B. The process has a threat score greater than 4.

C. The process made a network connection to another system.

D. The process had a NOT_LISTED reputation at the time the event occurred.

E. The process was run under the NT_AUTHORITY\SYSTEM user context.

F. The process was able to inject code into another process.

Correct Answer: ADF

QUESTION 10

An administrator is creating a query per policy for Audit and Remediation. The administrator ran several recommended queries already but notices they are unable to run the same recommended query for one of their policies. The run button is grayed out.

Which statement correctly explains why the run button is unavailable?

A. The sensors in the policy do not support the table or query.

B. The administrator needs the use live query permission.

C. The number of consecutive running queries is limited.

D. The query or table is not supported within osquery.

Correct Answer: B

QUESTION 11

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 12

What does the Aggressive setting do when configured in Local Scan Settings?

A. It adds a temporary reputation.

B. It scans all files on execution.

C. It scans new files on first execution.

D. It enables signature updates for the scanner.

Correct Answer: C

Reference: https://community.carbonblack.com/t5/Knowledge-Base/Endpoint-Standard-How-ToConfigure-Local-AV-Scan/ta-p/89051

QUESTION 13

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.

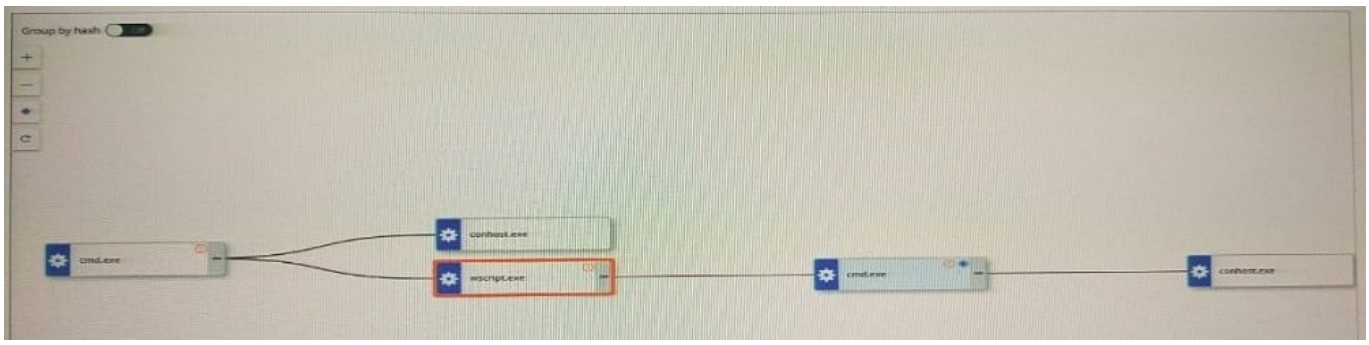
C. This query is missing a parameter for validity.

D. This query returns all accounts found on systems.

Correct Answer: A

QUESTION 14

An analyst is investigating an alert within Enterprise EDR on the process analysis page. The process tree can be seen below:



Which statement accurately characterizes this situation?

A. Conhost.exe has one or more child processes.

B. The solid line between the nodes denotes a process was injected into by another process.

C. Several nodes in this process tree have watchlist hits.

D. The analyst navigated to this process analysis page from the wscrlpt.exe process.

Correct Answer: B

QUESTION 15

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