DUMPSARENA

VMware Carbon Black Portfolio Skills

VMware 5V0-91.20

Version Demo

Total Demo Questions: 10

Total Premium Questions: 57

Buy Premium PDF

https://dumpsarena.com

sales@dumpsarena.com

QUESTION NO: 1

An administrator wants to allow files to run from a network share.

Which rule type should the administrator configure?

A. Execute Prompt (Shared Path)

B. Trusted Path

C. Network Execute (Allow)

D. Write Approve (Network)

ANSWER: A

QUESTION NO: 2

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

ANSWER: A C E

Explanation:

Reference:
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjttoeA3ILvAhU6QhUIHZaND-YQFjAAegQIARAD&url=https%3A%2F%

2Fcommunity.carbonblack.com%2Fgbouw27325%2Fattachments%2Fgbouw27325%2Fproduct-docs-news%2F3020%2F1%2FCB_EDR_7.3_User_Guide.pdf&usg=AOvVaw23smt4s66MWHdv9jM2PYF- (86)

QUESTION NO: 3

Which Sensor Status under Endpoint Health indicates that a system's policy enforcement is disabled, and the sensor is not sending security event data to the cloud?

A. Quarantined

B. Deregistered

C. Inactive

D. Bypass

ANSWER: D

Explanation:

Reference: https://community.carbonblack.com/t5/Knowledge-Base/CB-Defense-What-Happens-When-Bypass-has-been-Enabled-on-the/ta-p/74905

QUESTION NO: 4

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.

ANSWER: B E F

QUESTION NO: 5

An administrator wants to query the status of the firewall for all endpoints. The administrator will query the registry key found here

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile.

To make the results easier to understand, the administrator wants to return either enabled or disabled for the results, rather than the value from the registry key.

Which SQL statement will rewrite the output based on a specific result set returned from the system?

A. CASE

B. AS

C. ALTER

D. SELECT

ANSWER: A

Explanation:

Reference: https://www.carbonblack.com/blog/8-live-queries-that-will-speed-up-your-next-pci-audit/

QUESTION NO: 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

ANSWER: B C E

Explanation:

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

QUESTION NO: 7

A company wants to implement the strictest security controls for computers on which the software seldom changes (i.e., servers or single-purpose systems).

Which Enforcement Level is the most fitting?

A. Low Enforcement

B. Medium Enforcement

C. High Enforcement

D. None (Visibility)

ANSWER: C

Explanation:

Reference:
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjapqGLiYXvAhUwQxUIHRn2BHYQFjALegQILxAD&url=https%3A%2F%

2Fcommunity.carbonblack.com%2Fgbouw27325%2Fattachments%2Fgbouw27325%2Fproduct-docs-news%2F1001%2F1%2Fbit9-userguide.pdf&usg=AOvVaw23gKlZGFcZ4y9AKAalm9Oj

QUESTION NO: 8

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

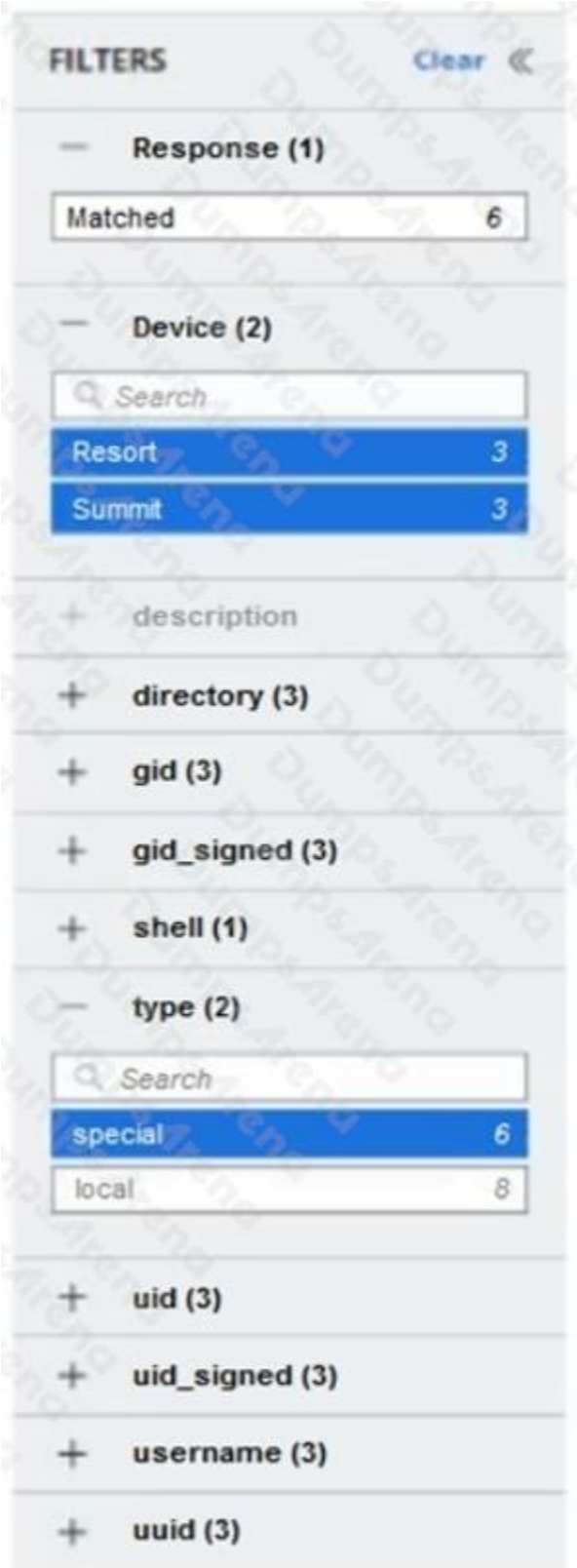
D. Add hash to banned list

E. IOC short name

ANSWER: A B

QUESTION NO: 9

Refer to the exhibit:



Which two logic statements correctly explain filtering within the UI? (Choose two.)

A. Filtering between fields is a logical OR

B. Filtering within the same field is a logical AND

C. Filtering between fields is a logical AND

D. Filtering between fields is a logical XOR

E. Filtering within the same field is a logical OR

ANSWER: A D

QUESTION NO: 10

Which identifier is shared by all events when an alert is investigated?

A. Process ID

B. Event ID

C. Priority Score

D. Alert ID

ANSWER: B