DUMPSARENA

VMware Carbon Black Portfolio Skills

VMware 5V0-91.20

Version Demo

Total Demo Questions: 10

Total Premium Questions: 56

Buy Premium PDF

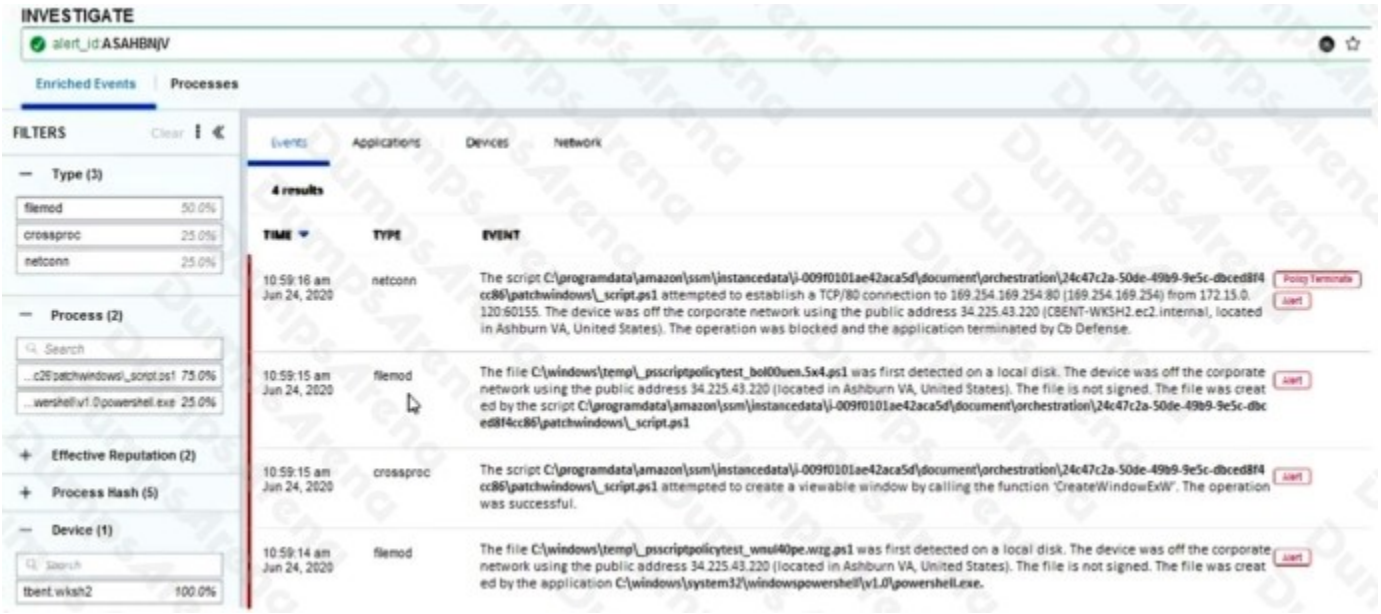
https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

An analyst is investigating a specific alert in Endpoint Standard. The analyst selects the investigate button from the alert triage page and sees the following:



Which statement accurately characterizes this situation?

A. These events are tied to an observed alert within the user interface.

B. The policy had no blocking and isolation rules set.

C. The events shown will all have the same event ID, correlating them to the alert.

D. Each event listed contributed to the overall alert score and severity.

ANSWER: D

QUESTION NO: 2

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

A. ALTER

B. UPDATE

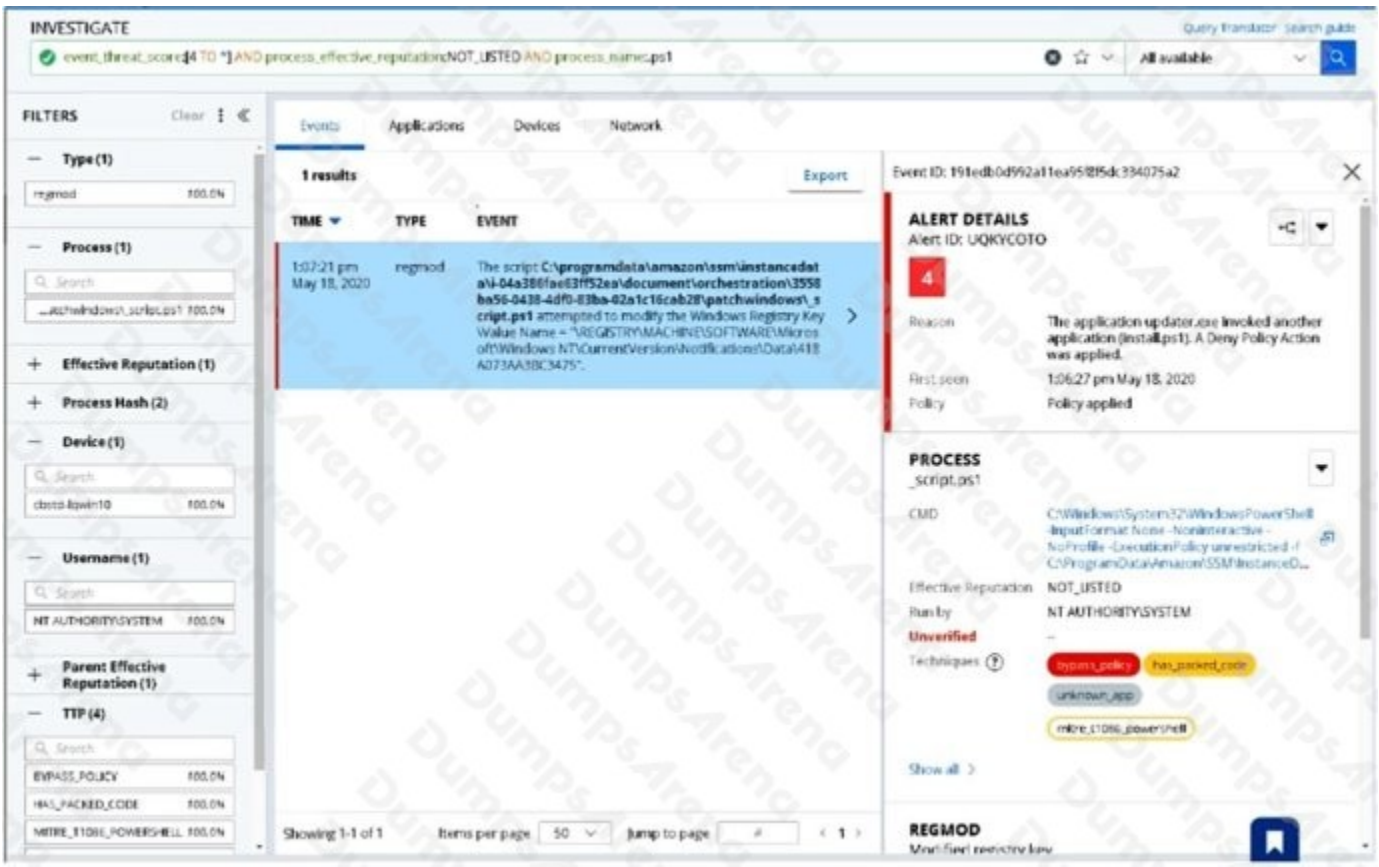
C. REMOVE

D. SELECT

ANSWER: D

QUESTION NO: 3

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.

ANSWER: A D F

QUESTION NO: 4

In which two ways can the tamper protection on an App Control agent be disabled when diagnosing agent issues or removing the agent? (Choose two.)

A. From the Computer Details page on the web console

B. From the Files on Computers page on the web console

C. Run authenticated DasCLI on Windows command prompt

D. Run RepCLI on Windows command prompt

E. From the File Catalog page on the web console

ANSWER: A C

Explanation:

Reference: https://community.carbonblack.com/t5/Knowledge-Base/App-Control-How-to-Disable-Enable-Tamper-Protection/ta-p/37220

QUESTION NO: 5

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.

ANSWER: B

Explanation:

Reference:
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjZ_N65jIXvAhUFYcAKHbu4ChUQFjAAegQIAhAD&url=https%3A%2F%

2Fcommunity.carbonblack.com%2Fgbouw27325%2Fattachments%2Fgbouw27325%2Fproduct-docs-news%2F3142%2F25%2FCarbon%2520Black%2520Cloud%2520-%2520Endpoint%2520Advanced%2520User%2520Guide.pdf&usg=AOvVaw2N-B7YFQA_I7hj-HvB5Hf6 (47)

QUESTION NO: 6

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: 7

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: 8

An Enterprise EDR administrator wants to use Watchlists curated by VMware Carbon Black and other threat intelligence specialists.

How should the administrator add these curated Watchlists from the Watchlists page?

A. Click Add Watchlists, and input the URL(s) for the desired Watchlists.

B. Click Take Action, select Edit, and select the desired Watchlists.

C. Click Take Action, and select Subscribe for the desired Watchlists.

D. Click Add Watchlists, on the Subscribe tab select the desired Watchlists, and click Subscribe.

ANSWER: A

Explanation:

Reference:
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjl1tW404XvAhWZRhUIHSygB74QFjADegQIExAD&url=https%3A%2F%

2Fcommunity.carbonblack.com%2Fgbouw27325%2Fattachments%2Fgbouw27325%2Fproduct-docs-news%2F1913%2F18%2FEnterprise%2520EDR%2520Getting%

2520Started.pdf&usg=AOvVaw2_M7opfEgUaIfutBZChvk (5)

QUESTION NO: 9

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: 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