5V0-91.20$^{\text{Q\&As}}$

VMware Carbon Black Portfolio Skills

Pass VMware 5V0-91.20 Exam with 100% Guarantee

QUESTION 1

Examine the following EDR query:

file_desc:"Windows Command Processor" AND -process_name:cmd.exe

Which process will show in the query results?

A. Any process named something other than cmd.exe with the file description of "Windows Command Processor"

B. Any process with the binary file description "Windows Command Processor"

C. Any process with the binary file description "Windows Command Processor" named cmd.exe

D. Any process named cmd.exe

Correct Answer: C

QUESTION 2

Which enforcement level does not block unapproved files but will block files that have been specifically banned?

A. Medium Enforcement

B. Disabled

C. Visibility

D. Low Enforcement

Correct Answer: B

Explanation: The protection level applied to computers running the App Control Agent. A range of levels from High (Block Unapproved) to None (Disabled) enable you to specify the level of file blocking required.

QUESTION 3

Given an event rule: Approve nVidia Drivers, changes the local state to Approved for file writes or execution blocks when the publisher is NVIDIA Corporation. How is an alert created that is triggered whenever an nVidia driver is approved by the event rule?

A. Add a new Alert of type Event Alert. Set Subtype to New unapproved file to computer and Execution block (unapproved file) and Publisher to NVIDIA Corporation. Click Create and add email recipients.

B. Click Create Alert on the event rule Approve nVidia Drivers details page. Click Create and add email recipients. Create and Exit.

C. Click Create Alert on the event rule Approve nVidia Drivers details page. Add email recipients. Create and Exit.

D. Create a custom rule name Approve nVidia that approves writes or blocks when the publisher is NVIDIA Corporation. Create an alert for rule name Approve nVidia. Click Create and add email recipients.

Correct Answer: B

QUESTION 4

An active compromise is detected on an endpoint. Due to current policies, the compromise was detected but not terminated.

What would be an appropriate action to end the current communication between the device and the attacker?

A. Uninstall the sensor

B. Place the system into bypass mode

C. Place the system into Quarantine D. Remotely scan the endpoint

Correct Answer: B

QUESTION 5

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

A. Process ID

B. Event ID

C. Priority Score

D. Alert ID

Correct Answer: B

QUESTION 6

Review this EDR query:

childproc_name:whoami.exe AND childproc_name:hostname.exe AND childproc_name:tasklist.exe AND childproc_name:ipconfig.exe

Which process would show in the query results?

A. Any process invoked by whoami.exe, hostname.exe, tasklist.exe, and ipconfig.exe

B. Any process invoked by whoami.exe, hostname.exe, tasklist.exe, or ipconfig.exe

C. Any process invoking whoami.exe, hostname.exe, tasklist.exe, or ipconfig.exe

D. Any process invoking whoami.exe, hostname.exe, tasklist.exe, and ipconfig.exe

Correct Answer: D

QUESTION 7

What are the three available methods in VMware Carbon Black App Control by which an endpoint (agent) can be assigned to a specific policy? (Choose three.)

A. By pushing the designated GPO script

B. Via DASCLI command

C. By installing the agent via SCCM

D. Manual policy assignment

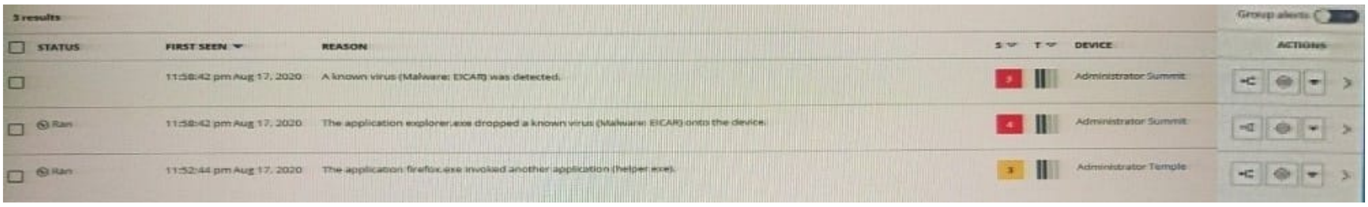
E. By branded/policy-specific installer

F. By Active Directory Mapping

Correct Answer: CDF

QUESTION 8

An analyst navigates to the alerts page in Endpoint Standard and sees the following:



3 results

□	STATUS	FIRST SEEN	REASON	S	T	DEVICE	ACTIONS
□		11:58:42 pm Aug 17, 2020	A known virus (Malware: EICAR) was detected.	3		Administrator Summit	
□	Ran	11:58:42 pm Aug 17, 2020	The application explorer.exe dropped a known virus (Malware: EICAR) onto the device.	4		Administrator Summit	
□	Ran	11:52:44 pm Aug 17, 2020	The application firefox.exe invoked another application (helper.exe).	3		Administrator Temple	

What does the yellow color represent on the left side of the row?

A. It is an alert from a watchlist rather than the analytics engine.

B. It is a threat alert and warrants immediate investigation.

C. It is an observed alert and may indicate suspicious behavior.

D. It is a dismissed alert within the user interface.

Correct Answer: A

QUESTION 9

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 10

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 11

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 12

An analyst has investigated two alerts on two separate HR workstations and found that notepad.exe has established communication to another IP address.

Which rule will kill notepad.exe entirely if this activity is detected in the future?

A. **\system32\notepad.exe --> Communicates over the network --> Terminate process

B. **\system32\notepad.exe --> Runs or is Running --> Deny operation

C. **/system32/notepad.exe --> Runs or is Running --> Terminate process

D. **/system32/notepad.exe--> Communicates over the network --> Deny operation

Correct Answer: C

QUESTION 13

There is a need to ignore all activity at an application path. Which rule definition should be used to address this need?

A. Application at Path, Performs any operation, Bypass

B. Application at Path, Runs or is Running, Bypass

C. Application at Path, Runs or is Running, Allow and Log

D. Application at Path, Performs any operation, Allow and Log

Correct Answer: A

Reference: https://community.carbonblack.com/t5/Knowledge-Base/Carbon-Black-Cloud-Console-How-toSetup-Exclusions-in-the/ta-p/42334

QUESTION 14

Review the following query:

path:c:\program\ files\ \(x86\)\microsoft

How would this query input term be interpreted?

A. c:\program files x86\microsoft

B. c:rogram files (x86)icrosoft

C. c:rogramfilesx86icrosoft

D. c:\program files (x86)\microsoft

Correct Answer: D

QUESTION 15

An incorrectly constructed watchlist generates 10,000 incorrect alerts.

How should an administrator resolve this issue?

A. Delete the watchlist to automatically clear the alerts, and then create a new watchlist with the correct criteria.

B. From the Triage Alerts Page, use the facets to select the watchlist, click the Wrench button to "Mark all as Resolved False Positive", and then update the watchlist with the correct criteria.

C. Update the Triage Alerts Page to show 200 alerts, click the Select All Checkbox, click the "Dismiss Alert(s)" button for each page, and then update the watchlist with the correct criteria.

D. From the Watchlists Page, select the offending watchlist, click "Clear Alerts" from the Action menu, and then update the watchlist with the correct criteria.

Correct Answer: B