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

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.geekcert.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

QUESTION 1

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

Correct Answer: AC

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

QUESTION 2

An administrator uses the following Enterprise EDR search query to show web browsers spawning nonbrowser child processes that connect over the network:

(parent_name:chrome.exe OR parent_name:iexplore.exe OR parent_name:firefox.exe) AND (NOT process_name:chrome.exe OR NOT process_name:iexplore.exe OR NOT process_name:firefox.exe)

Which field can be added to this query to filter the results by signature status?

A. childproc_publisher_state

B. process_publisher

C. childproc_reputation

D. process_publisher_state

Correct Answer: C

QUESTION 3

An Endpoint Standard administrator finds a binary in the environment and decides to manually add the file hash to the Banned List.

Which reputation does the file now have?

A. Suspect/Heuristic Malware

B. Company Black

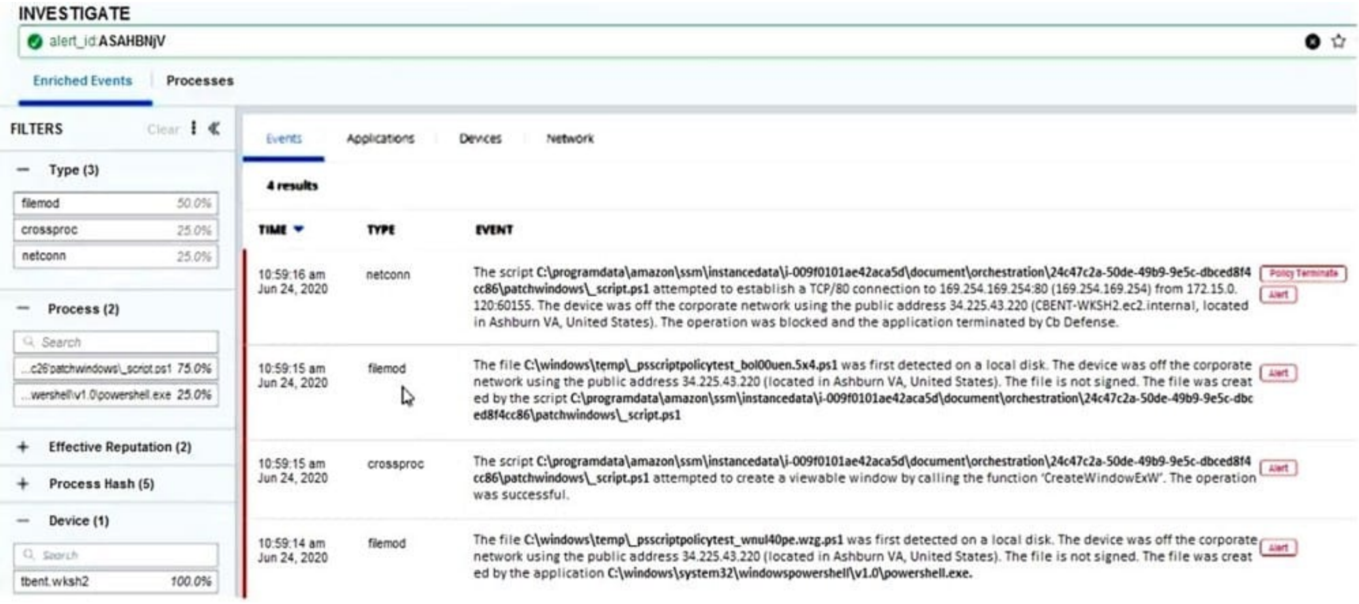
C. Adware/PUP Malware

D. Known Malware

Correct Answer: A

QUESTION 4

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:



Type (3)

filemod	50.0%
crossproc	25.0%
netconn	25.0%

Process (2)

...c26\patchwindows_script.ps1	75.0%
...wershell\v1.0\powershell.exe	25.0%

+ Effective Reputation (2)

+ Process Hash (5)

Device (1)

tbent.wksh2	100.0%

4 results

TIME	TYPE	EVENT	
10:59:16 am Jun 24, 2020	netconn	The script **C:\programdata\amazon\ssm\instancedata\i-009f0101ae42aca5d\document\orchestration\24c47c2a-50de-49b9-9e5c-dbced8f4cc86\patchwindows_script.ps1** attempted to establish a TCP/80 connection to 169.254.169.254:80 (169.254.169.254) from 172.15.0.120:60155. The device was off the corporate network using the public address 34.225.43.220 (CBENT-WKSH2.ec2.internal, located in Ashburn VA, United States). The operation was blocked and the application terminated by Cb Defense.	Policy Terminate Alert
10:59:15 am Jun 24, 2020	filemod	The file **C:\windows\temp_psscriptpolicytest_bol00uen.5x4.ps1** was first detected on a local disk. The device was off the corporate network using the public address 34.225.43.220 (located in Ashburn VA, United States). The file is not signed. The file was created by the script **C:\programdata\amazon\ssm\instancedata\i-009f0101ae42aca5d\document\orchestration\24c47c2a-50de-49b9-9e5c-dbced8f4cc86\patchwindows_script.ps1**	Alert
10:59:15 am Jun 24, 2020	crossproc	The script **C:\programdata\amazon\ssm\instancedata\i-009f0101ae42aca5d\document\orchestration\24c47c2a-50de-49b9-9e5c-dbced8f4cc86\patchwindows_script.ps1** attempted to create a viewable window by calling the function 'CreateWindowExW'. The operation was successful.	Alert
10:59:14 am Jun 24, 2020	filemod	The file **C:\windows\temp_psscriptpolicytest_wnul40pe.wzg.ps1** was first detected on a local disk. The device was off the corporate network using the public address 34.225.43.220 (located in Ashburn VA, United States). The file is not signed. The file was created by the application **C:\windows\system32\windowspowershell\v1.0\powershell.exe.**	Alert

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.

Correct Answer: D

QUESTION 5

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