



5V0-91.20^{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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

Which reputation has the highest priority in Cloud Endpoint Standard?

- A. Unknown
- B. Adware/PUP Malware
- C. Known Malware
- D. Ignore

Correct Answer: C

QUESTION 2

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

TIME	TYPE	EVENT
1:07:21 pm May 18, 2020	regmod	The script C:\programdata\amazon\ssm\instancedat a\4-04a386fae63ff52ea\document\orchestration\3558 ba56-0438-4df0-83ba-02a1c16cab28\patchwindows\ s cript.ps1 attempted to modify the Windows Registry Key (Value Name = "REGISTRYMACHINE\SOFTWARE\Microso ft\Windows NT\CurrentVersion\Notifications\Data\418 A073AA3BC3475").

ALERT DETAILS
Alert ID: UQKYCOTO
Reason: The application updater.exe invoked another application (install.ps1). A Deny Policy Action was applied.
First seen: 1:06:27 pm May 18, 2020
Policy: Policy applied

PROCESS
_script.ps1
CMD: C:\Windows\System32\WindowsPowerShell\ InputFormat:None -NonInteractive - NoProfile -ExecutionPolicy unrestricted -f C:\ProgramData\Amazon\SSM\InstanceD...
Effective Reputation: NOT_LISTED
Run by: NT AUTHORITY\SYSTEM
Unverified
Techniques: system_policy, has_packed_code, unknown_app, mibre_t1086_powershell

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 3

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 4

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 5

An administrator wants to find instances where the binary is unsigned. Which term will accomplish this search?

- A. NOT process_publisher:FILE_SIGNATURE_STATE_SIGNED
- B. NOT process_publisher_state:FILE_SIGNATURE_STATE_SIGNED
- C. process_publisher_state:FILE_SIGNATURE_STATE_NOT_SIGNED
- D. process_publisher:FILE_SIGNATURE_STATE_NOT_SIGNED

Correct Answer: B

[5V0-91.20 Study Guide](#)

[5V0-91.20 Exam Questions](#)

[5V0-91.20 Braindumps](#)