5V0-91.20Q&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

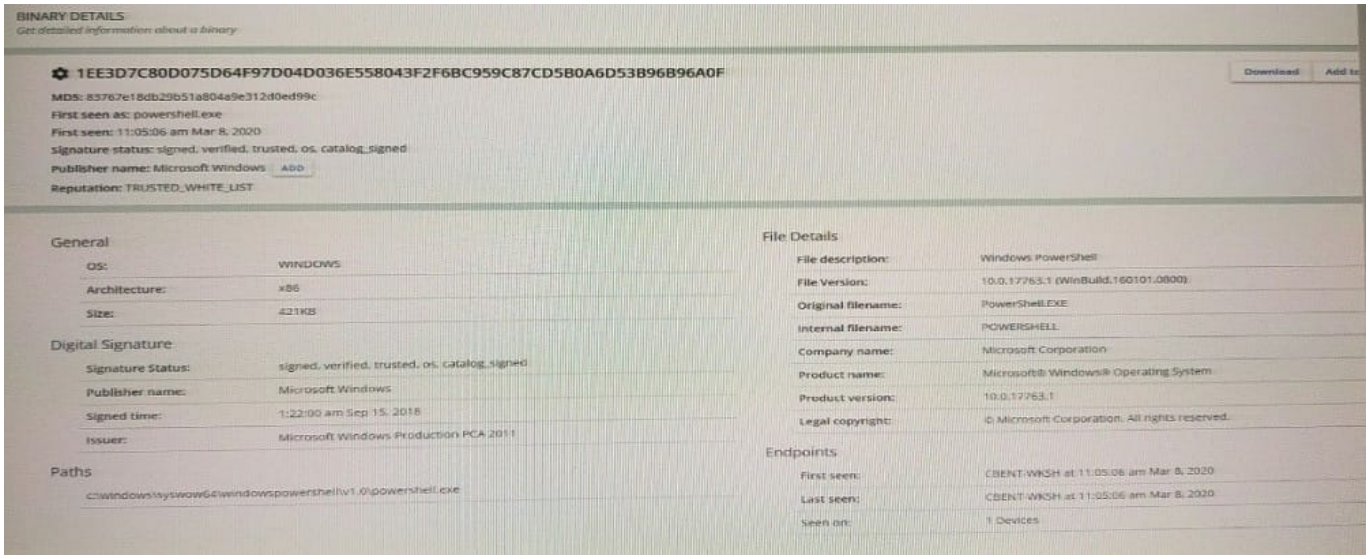
100% Passing Guarantee
100% Money Back Assurance

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

An analyst is investigating an alert within Enterprise EDR. The alert is tied to an unusual process name. When navigating to the binary details page, for the binary used in the alert, the analyst sees the following:



The analyst wants to find any instances of this process executing regardless of the process name used.

Which two details from the binary can be used to search for the application regardless of the seen name? (Choose two.)

A. The binary\\'s hash

B. The path

C. The original filename

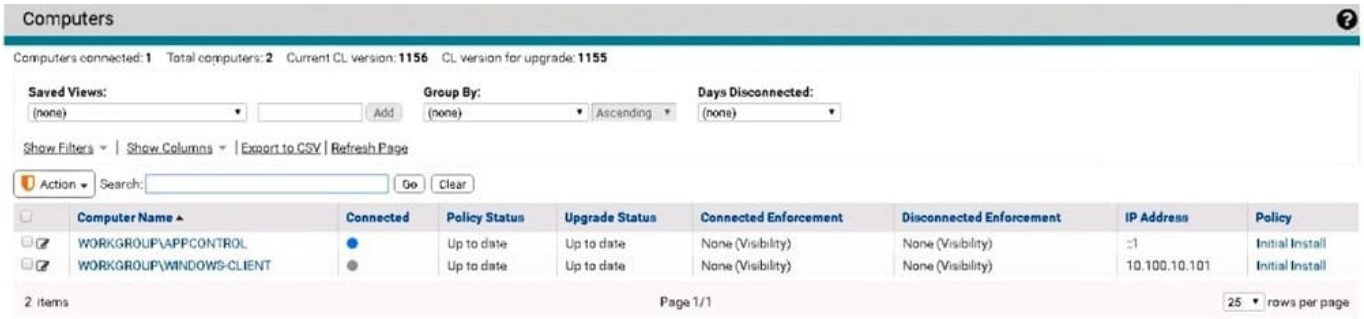
D. The product version

E. The publisher name

Correct Answer: BD

QUESTION 2

An administrator is troubleshooting App Control agent issues. When navigating to the Computer Details page, the administrator sees the following: What is the status of the WINDOWS-CLIENT agent?



A. Connected and Up to date

B. Disconnected and Up to date

C. Connected but unsupported

D. Connected but health check failed

Correct Answer: B

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

What are three ways to ignore a feed report within the EDR user interface? (Choose three.)

A. Threat Reports Details page

B. Threat Intelligence Feeds page

C. Investigations page

D. Search Threat Reports page

E. Alert Dashboard page

F. After marking a feed alert as a false positive

Correct Answer: ABF

Reference: https://community.carbonblack.com/t5/Knowledge-Base/EDR-How-to-Customize-a-Feed-toPrevent-False-Positives/ta-p/64413

QUESTION 5

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