



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

The screenshot shows the 'INVESTIGATE' interface for an alert with ID 'alert_id:ASAHBNIJ'. The interface is divided into a left sidebar with filters and a main content area with a table of events. The filters include Type (filemod, crossproc, netconn), Process (c2s\patchwindows_script.ps1, powershell.exe), Effective Reputation, Process Hash, and Device (tbent.wksh2). The event table has columns for TIME, TYPE, and EVENT. The events are as follows:

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-dbcd8f4cc86\patchwindows_script.ps1 attempted to establish a TCP/80 connection to 169.254.169.254:80 (169.254.169.254) from 172.15.0.120:50155. 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_bo100uen.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-dbcd8f4cc86\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-dbcd8f4cc86\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_wnu140pe.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 2

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 3

An administrator runs multiple queries on tables and combines the results after the fact to correlate data. The administrator needs to combine rows from multiple tables based on data from a related column in each table.

Which SQL statement should be used to achieve this goal?

- A. JOIN
- B. WHERE
- C. AS
- D. COMBINE

Correct Answer: A

QUESTION 4

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 5

Which reputation has the highest priority in Cloud Endpoint Standard?

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

Correct Answer: C



VCE & PDF

PassApply.com

<https://www.passapply.com/5v0-91-20.html>

2024 Latest passapply 5V0-91.20 PDF and VCE dumps Download

[5V0-91.20 Practice Test](#)

[5V0-91.20 Exam Questions](#)

[5V0-91.20 Braindumps](#)