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

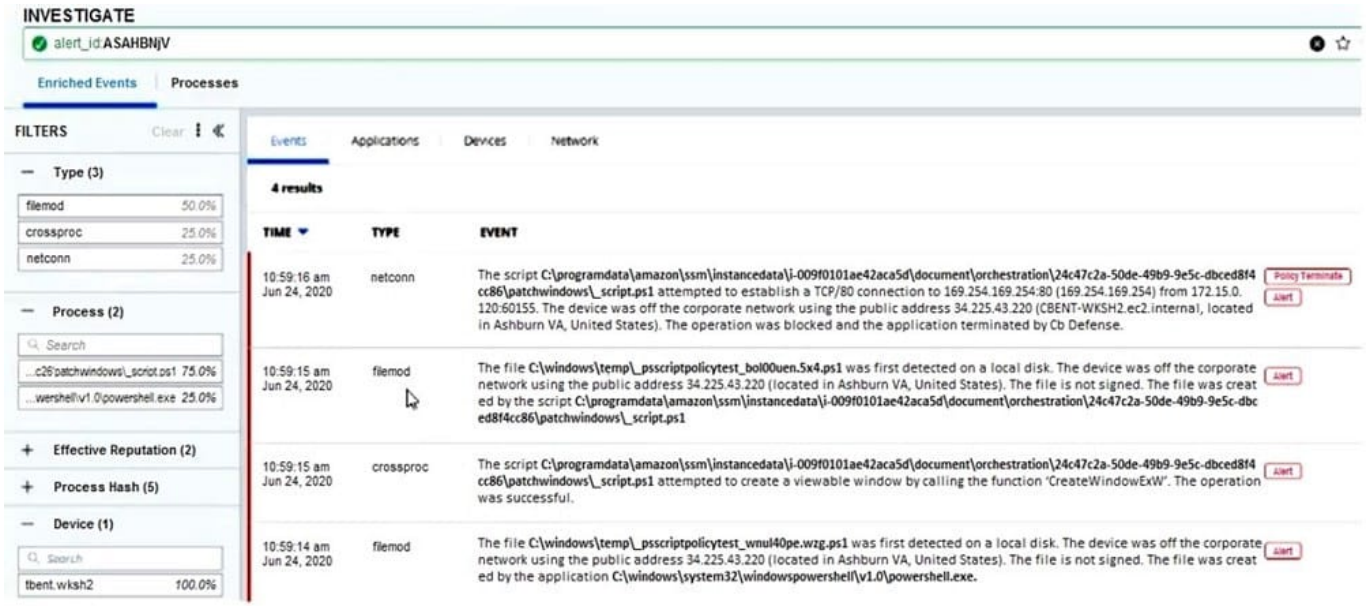
100% Passing Guarantee
100% Money Back Assurance

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:



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

5V0-91.20 Practice Test 5V0-91.20 Exam Questions 5V0-91.20 Braindumps