

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.leads4pass.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 active compromise is detected on an endpoint. Due to current policies, the compromise was detected but not terminated.

What would be an appropriate action to end the current communication between the device and the attacker?

- A. Uninstall the sensor
- B. Place the system into bypass mode
- C. Place the system into Quarantine D. Remotely scan the endpoint

Correct Answer: B

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)

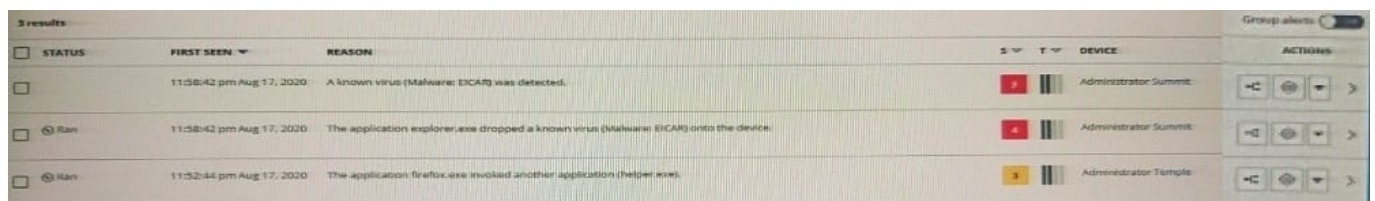
Which field can be added to this query to filter the results by signature status?

- A. childproc_publisher_state
- B. process_publisher
- C. childproc_reputation
- D. process_publisher_state

Correct Answer: C

QUESTION 3

An analyst navigates to the alerts page in Endpoint Standard and sees the following:



STATUS	FIRST SEEN	REASON	S	T	DEVICE	ACTIONS
<input type="checkbox"/>	11:58:42 pm Aug 17, 2020	A known virus (Malware: EICAR) was detected.	1		Administrator Summit	[Icons]
<input type="checkbox"/> Ran	11:58:42 pm Aug 17, 2020	The application explorer.exe dropped a known virus (Malware: EICAR) onto the device.	4		Administrator Summit	[Icons]
<input type="checkbox"/> Ran	11:52:44 pm Aug 17, 2020	The application firefox.exe invoked another application (helper.exe).	1		Administrator Temple	[Icons]

What does the yellow color represent on the left side of the row?

- A. It is an alert from a watchlist rather than the analytics engine.
- B. It is a threat alert and warrants immediate investigation.
- C. It is an observed alert and may indicate suspicious behavior.
- D. It is a dismissed alert within the user interface.

Correct Answer: A

QUESTION 4

What does the Aggressive setting do when configured in Local Scan Settings?

- A. It adds a temporary reputation.
- B. It scans all files on execution.
- C. It scans new files on first execution.
- D. It enables signature updates for the scanner.

Correct Answer: C

Reference: <https://community.carbonblack.com/t5/Knowledge-Base/Endpoint-Standard-How-ToConfigure-Local-AV-Scan/ta-p/89051>

QUESTION 5

After an emergency, what does the Restore computer button do on the App Control Home page?

- A. Move all computers to the original Enforcement level
- B. Move all computers to High Enforcement level
- C. Move all computers to Low Enforcement level
- D. Move all computers to Medium Enforcement level

Correct Answer: A

QUESTION 6

How long will Live Queries in Carbon Black Audit and Remediation run before timing out?

- A. 30 days
- B. 14 days
- C. 180 days
- D. 7 days

Correct Answer: D

QUESTION 7

A process is writing numerous interesting files that never actually execute.

Which rule type can the administrator define that will prevent reporting these file creations?

- A. Performance Optimization
- B. File Creation Control (Suppress)
- C. Expert (Tag Process, Terminate Process)
- D. Execute Ignore

Correct Answer: A

QUESTION 8

Why would a sensor have a status of "Inactive"?

- A. The sensor has not checked in within the last 30 days.
- B. The sensor has been uninstalled from the endpoint for more than 30 days.
- C. The device has been put in bypass for the last 30 days.
- D. The sensor has been in disabled mode for more than 30 days.

Correct Answer: A

QUESTION 9

Which wildcard configuration applies a policy to all files and subfolders in a specific folder in Endpoint Standard?

- A. C:\Program Files\example\\$\$

B. C:\Program Files\example**

C. C:\Program Files\example\\$

D. C:\Program Files\example*

Correct Answer: B

Reference: <https://community.carbonblack.com/t5/Knowledge-Base/Endpoint-Standard-How-to-CreatePolicy-Blocking-Isolation-and/ta-p/65941>

QUESTION 10

An administrator is creating a query per policy for Audit and Remediation. The administrator ran several recommended queries already but notices they are unable to run the same recommended query for one of their policies. The run button is grayed out.

Which statement correctly explains why the run button is unavailable?

A. The sensors in the policy do not support the table or query.

B. The administrator needs the use live query permission.

C. The number of consecutive running queries is limited.

D. The query or table is not supported within osquery.

Correct Answer: B

QUESTION 11

Which strategy should be used to purge inactive bans from the web console?

A. Schedule an add-hoc cron job to remove

B. Use a pre-configured system cron job daily to remove them

C. Run the cbbanning script on the EDR server

D. Go to the hashes page on the web console and remove them

Correct Answer: C

QUESTION 12

An Enterprise EDR administrator wants to use Watchlists curated by VMware Carbon Black and other

threat intelligence specialists.

How should the administrator add these curated Watchlists from the Watchlists page?

- A. Click Add Watchlists, and input the URL(s) for the desired Watchlists.
- B. Click Take Action, select Edit, and select the desired Watchlists.
- C. Click Take Action, and select Subscribe for the desired Watchlists.
- D. Click Add Watchlists, on the Subscribe tab select the desired Watchlists, and click Subscribe.

Correct Answer: A

Reference: https://www.google.com/url?sa=t&drct=j&andq=andescr=sandsource=webandcd=andved=2ahUKEwj1tW404XvAhWZRhUIHSygB74QFjADegQIExADandurl=https%3A%2F%2Fcommunity.carbonblack.com%2Fgbouw27325%2Fattachments%2Fgbouw27325%2Fproduct-docs-news%2F1913%2F18%2FEnterprise%2520EDR%2520Getting%2520Started.pdf&usg=AOvVaw2_M7opfEgUallfutBZChvk (5)

QUESTION 13

Which Live Query statement is properly constructed?

- A. SELECT * FROM \\users\\
- B. select * from *:
- C. select from users;
- D. SELECT * FROM users;

Correct Answer: D

QUESTION 14

An incorrectly constructed watchlist generates 10,000 incorrect alerts.

How should an administrator resolve this issue?

- A. Delete the watchlist to automatically clear the alerts, and then create a new watchlist with the correct criteria.
- B. From the Triage Alerts Page, use the facets to select the watchlist, click the Wrench button to "Mark all as Resolved False Positive", and then update the watchlist with the correct criteria.
- C. Update the Triage Alerts Page to show 200 alerts, click the Select All Checkbox, click the "Dismiss Alert(s)" button for each page, and then update the watchlist with the correct criteria.
- D. From the Watchlists Page, select the offending watchlist, click "Clear Alerts" from the Action menu, and then update the watchlist with the correct criteria.

Correct Answer: B

QUESTION 15

Which two statements are true regarding Live Response? (Choose two.)

- A. Live Response can only be initiated through the user interface.
- B. Live Response supports one user per session on an endpoint.
- C. Live Response opens an SSH session with the remote device.
- D. Live Response requires both view and manage permissions to use.
- E. Live Response utilizes the same channel for sensor-server communications.

Correct Answer: AE

[Latest 5V0-91.20 Dumps](#)

[5V0-91.20 Study Guide](#)

[5V0-91.20 Braindumps](#)