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

How is a new Alert of type Event Alert created whenever an endpoint is added or deleted and send emails for the App Control admin whenever these events occur?

A. Add filter in Event Properties for Subtype Endpoint added and Endpoint deleted. Click Create and add the App Control admin email, and then click Create and. Exit.

B. Add filter in Event Properties for Subtype Computer added and Computer deleted. Add the App Control admin email, and then click Create and Exit.

C. Add filter in Event Properties for Subtype Computer added and Computer deleted. Click Create and add the App Control admin email, and then click Create and Exit.

D. Add filter in Event Properties for Subtype Computer modified. Add the App Control admin email, and then click Create and Exit.

Correct Answer: D

QUESTION 2

A security policy states to enable Live Response by default across the enterprise. However, the team identified critical systems which should not support Live Response due to risk. The team needs to disable Live Response on selected systems.

From which page can this goal be accomplished?

A. Policy

B. API Access

C. Endpoints

D. Roles

Correct Answer: D

QUESTION 3

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 4

There is a requirement to block ransomware when a sensor is offline. Which blocking and isolation rule fulfills this requirement?

A. Known Malware --> Performs ransomware-like behavior --> Terminate process

B. Not Listed Application --> Performs ransomware-like behavior --> Deny operation

C. Suspect Malware --> Performs ransomware-like behavior --> Deny operation

D. Unknown Application --> Performs ransomware-like behavior --> Terminate process

Correct Answer: A

QUESTION 5

Review the following query:

path:c:\program\ files\ \(x86\)\microsoft

How would this query input term be interpreted?

A. c:\program files x86\microsoft

B. c:rogram files (x86)icrosoft

C. c:rogramfilesx86icrosoft

D. c:\program files (x86)\microsoft

Correct Answer: D