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

How can an analyst disregard alerts on multiple devices with the least amount of administrative effort?

A. Select the "Dismiss on all devices" option.

B. Make a note in the Notes/Tags option.

C. Search by hash and dismiss.

D. Turn off the Group Alerts option.

Correct Answer: D

Reference: https://www.google.com/url?sa=tandrct=jandq=andesrc=sandsource=webandcd=andcad=rjaanduact=8andved=2ahUKEwjv6pryl4XvAhWagVwKHTCMDTEQFjAAegQIARADandurl=https%3A%2F%2Fcommunity.carbonblack.com%2Ft5% 2FKnowled ge-Base%2FCarbon-Black-Cloud-How-to-Dismiss-Alerts%2Fta-p%2F51766andusg=AOvVaw2x1mST1tWpuASUMLmFhyuI (80)

QUESTION 2

Review the following search:

childproc_name:"rundll32.exe" AND -digsig_result:"Signed" AND path:c:\windows*

What is this search looking for?

A. Processes being launched by rundll32.exe running out of the windows directory that are not signed

B. Instances of rundll32.exe running out of the windows directory that are not signed

C. Instances of rundll32.exe running out of the windows directory that are signed

D. Processes launching rundll32.exe running out of the windows directory that are not signed

Correct Answer: A

Reference: https://www.carbonblack.com/blog/hunting-the-white-rabbit-detecting-metasploitmeterpreterusing-carbon-black/

QUESTION 3

An administrator needs to manage a group of sensors from within the console.

Which three actions are available for sensors within the Sensor Group? (Choose three.)

A. Move to group

B. Disable

C. Restart

D. Ban

E. Uninstall

F. Share Settings

Correct Answer: ACE

QUESTION 4

An administrator is reviewing an alert about a known and required application in the environment. The application has been given the reputation of PUP, with the alert reason being that the PUP was detected. As a result, this application is matching policy blocking and isolation rules for PUPs in the environment and Is not behaving as expected.

Which step should the administrator take to remediate this situation?

A. Add the file to the Approved List and Dismiss alert

B. Add the file to the Approved List

C. Dismiss the alert

D. Add the file to the Banned List and Delete application

Correct Answer: C

QUESTION 5

Which list below captures all Enforcement Levels for App Control policies?

A. Critical, Lockdown, Monitored, Tracking, Banning

B. High Enforcement, Medium Enforcement, Low Enforcement

C. High Enforcement, Medium Enforcement, Low Enforcement, None (Visibility), None (Disabled)

D. Control, Local Approval, Disabled

Correct Answer: C

Reference: https://www.google.com/url?
sa=tandrct=jandq=andesrc=sandsource=webandcd=andved=2ahUKEwiFsPPz04XvAhWRsnEKHV4lBuk
QFjABegQIAhADandurl=https%3A%2F%2Fcommunity.carbonblack.com%2Fgbouw27325%2Fattachments %
2Fgbouw27325%2Fproduct-docs-news%F2961%2F1%2FVMware%2520Carbon%2520Black%
2520App%2520Control%25208.5.0%2520User%2520Guide.pdfandusg=AOvVaw3es_0JTc8-_BifNR4iFiGl

(6)

[5V0-91.20 PDF Dumps](#) [5V0-91.20 Study Guide](#) [5V0-91.20 Braindumps](#)