CCFA-200$^{Q\&As}$

CrowdStrike Certified Falcon Administrator

Pass CrowdStrike CCFA-200 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/ccfa-200.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CrowdStrike Official Exam Center

QUESTION 1

What can the Quarantine Manager role do?

A. Manage and change prevention settings

B. Manage quarantined files to release and download

C. Manage detection settings

D. Manage roles and users

Correct Answer: B

QUESTION 2

You want to create a detection-only policy. How do you set this up in your policy\\'s settings?

A. Enable the detection sliders and disable the prevention sliders. Then ensure that Next Gen Antivirus is enabled so it will disable Windows Defender.

B. Select the "Detect-Only" template. Disable hash blocking and exclusions.

C. You can\\'t create a policy that detects but does not prevent. Use Custom IOA rules to detect.

D. Set the Next-Gen Antivirus detection settings to the desired detection level and all the prevention sliders to disabled. Do not activate any of the other blocking or malware prevention options.

Correct Answer: D

QUESTION 3

You have determined that you have numerous Machine Learning detections in your environment that are false positives. They are caused by a single binary that was custom written by a vendor for you and that binary is running on many endpoints. What is the best way to prevent these in the future?

A. Contact support and request that they modify the Machine Learning settings to no longer include this detection

B. Using IOC Management, add the hash of the binary in question and set the action to "Allow"

C. Using IOC Management, add the hash of the binary in question and set the action to "Block, hide detection"

D. Using IOC Management, add the hash of the binary in question and set the action to "No Action"

Correct Answer: B

QUESTION 4

Which of the following is a valid step when troubleshooting sensor installation failure?

A. Confirm all required services are running on the system

B. Enable the Windows firewall

C. Disable SSL and TLS on the host

D. Delete any available application crash log files

Correct Answer: A

QUESTION 5

Which of the following is TRUE of the Logon Activities Report?

A. Shows a graphical view of user logon activity and the hosts the user connected to

B. The report can be filtered by computer name

C. It gives a detailed list of all logon activity for users

D. It only gives a summary of the last logon activity for users

Correct Answer: C