# 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.geekcert.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**

You have been provided with a list of 100 hashes that are not malicious but your company has deemed to be inappropriate for work computers. They have asked you to ensure that they are not allowed to run in your environment. You have

chosen to use Falcon to do this.

Which is the best way to accomplish this?

A. Using the Support Portal, create a support ticket and include the list of binary hashes, asking support to create an "Execution Prevention" rule to prevent these processes from running

B. Using Custom Alerts in the Investigate App, create a new alert using the template "Process Execution" and within that rule, select the option to "Block Execution"

C. Using IOC Management, gather the list of SHA256 or MD5 hashes for each binary and then upload them. Set all hashes to "Block" and ensure that the prevention policy these computers are using includes the option for "Custom Blocking" under Execution Blocking.

D. Using the API, gather the list of SHA256 or MD5 hashes for each binary and then upload them, setting them all to "Never Allow"

Correct Answer: C

**QUESTION 2**

You need to export a list of all deletions for a specific Host Name in the last 24 hours. What is the best way to do this?

A. Go to Host Management in the Host page. Select the host and use the Export Detections button

B. Utilize the Detection Resolution Dashboard. Use the filters to focus on the appropriate hostname and time, then export the results from the "Detection Resolution History" section

C. In the Investigate module, access the Detection Activity page. Use the filters to focus on the appropriate hostname and time, then export the results

D. Utilize the Detection Activity Dashboard. Use the filters to focus on the appropriate hostname and time, then export the results from the "Detections by Host" section

Correct Answer: C

**QUESTION 3**

Which of the following best describes the Default Sensor Update policy?

A. The Default Sensor Update policy does not have the "Uninstall and maintenance protection" feature

B. The Default Sensor Update policy is only used for testing sensor updates

C. The Default Sensor Update policy is a "catch-all" policy

D. The Default Sensor Update policy is disabled by default

Correct Answer: C

**QUESTION 4**

The alignment of a particular prevention policy to one or more host groups can be completed in which of the following locations within Falcon?

A. Policy alignment is configured in the "Host Management" section in the Hosts application

B. Policy alignment is configured only once during the initial creation of the policy in the "Create New Policy" pop-up window

C. Policy alignment is configured in the General Settings section under the Configuration menu

D. Policy alignment is configured in each policy in the "Assigned Host Groups" tab

Correct Answer: D

**QUESTION 5**

When uninstalling a sensor, which of the following is required if the \\'Uninstall and maintenance protection\\' setting is enabled within the Sensor Update Policies?

A. Maintenance token

B. Customer ID (CID)

C. Bulk update key

D. Agent ID (AID)

Correct Answer: A