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.leads4pass.com/ccfa-200.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What is the purpose of using groups with Sensor Update policies in CrowdStrike Falcon?

A. To group hosts with others in the same business unit

B. To group hosts according to the order in which Falcon was installed, so that updates are installed in the same order every time

C. To prioritize the order in which Falcon updates are installed, so that updates are not installed all at once leading to network congestion

D. To allow the controlled assignment of sensor versions onto specific hosts

Correct Answer: D

QUESTION 2

Custom IOA rules are defined using which syntax?

A. Glob

B. PowerShell

C. Yara

D. Regex

Correct Answer: B

QUESTION 3

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 4

Which option allows you to exclude behavioral detections from the detections page?

A. Machine Learning Exclusion

B. IOA Exclusion

C. IOC Exclusion

D. Sensor Visibility Exclusion

Correct Answer: A

QUESTION 5

What is the goal of a Network Containment Policy?

A. Increase the aggressiveness of the assigned prevention policy

B. Limit the impact of a compromised host on the network

C. Gain more visibility into network activities

D. Partition a network for privacy

Correct Answer: B