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.passapply.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

How do you assign a Prevention policy to one or more hosts?

A. Create a new policy and assign it directly to those hosts on the Host Management page

B. Modify the users roles on the User Management page

C. Ensure the hosts are in a group and assign that group to a custom Prevention policy

D. Create a new policy and assign it directly to those hosts on the Prevention policy page

Correct Answer: C

QUESTION 2

When the Notify End Users policy setting is turned on, which of the following is TRUE?

A. End users will not be notified as we would not want to notify a malicious actor of a detection. This setting does not exist

B. End users will be immediately notified via a pop-up that their machine is in-network isolation

C. End-users receive a pop-up notification when a prevention action occurs

D. End users will receive a pop-up allowing them to confirm or refuse a pending quarantine

Correct Answer: C

QUESTION 3

An analyst is asked to retrieve an API client secret from a previously generated key. How can they achieve this?

A. The API client secret can be viewed from the Edit API client pop-up box

B. Enable the Client Secret column to reveal the API client secret

C. Re-create the API client using the exact name to see the API client secret

D. The API client secret cannot be retrieved after it has been created

Correct Answer: B

QUESTION 4

Which of the following is an effective Custom IOA rule pattern to kill any process attempting to access www.badguydomain.com?

A. .*badguydomain.com.*

B. \Device\HarddiskVolume2*.exe -SingleArgument www.badguydomain.com /kill

C. badguydomain\.com.*

D. Custom IOA rules cannot be created for domains

Correct Answer: B

QUESTION 5

What impact does disabling detections on a host have on an API?

A. Endpoints with detections disabled will not alert on anything until detections are enabled again

B. Endpoints cannot have their detections disabled individually

C. DetectionSummaryEvent stops sending to the Streaming API for that host

D. Endpoints with detections disabled will not alert on anything for 24 hours (by default) or longer if that setting is changed

Correct Answer: D