VCE & PDF
Pass4itSure.com

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.pass4itsure.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

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 2

You are evaluating the most appropriate Prevention Policy Machine Learning slider settings for your environment. In your testing phase, you configure the Detection slider as Aggressive. After running the sensor with this configuration for 1 week of testing, which Audit report should you review to determine the best Machine Learning slider settings for your organization?

A. Prevention Policy Audit Trail

B. Prevention Policy Debug

C. Prevention Hashes Ignored

D. Machine-Learning Prevention Monitoring

Correct Answer: A

QUESTION 3

When a host is placed in Network Containment, which of the following is TRUE?

A. The host machine is unable to send or receive network traffic outside of the local network

B. The host machine is unable to send or receive network traffic except to/from the Falcon Cloud and traffic allowed in the Firewall Policy

C. The host machine is unable to send or receive any network traffic

D. The host machine is unable to send or receive network traffic except to/from the Falcon Cloud and any resources allowlisted in the Containment Policy

Correct Answer: D

QUESTION 4

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

QUESTION 5

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