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

You are beginning the rollout of the Falcon Sensor for the first time side-by-side with your existing security solution. You need to configure the Machine Learning levels of the Prevention Policy so it does not interfere with existing solutions

during the testing phase.

What settings do you choose?

A. Detection slider: Extra Aggressive Prevention slider: Cautious

B. Detection slider: Moderate Prevention slider: Disabled

C. Detection slider: Cautious Prevention slider: Cautious

D. Detection slider: Disabled Prevention slider: Disabled

Correct Answer: C

QUESTION 2

What is the purpose of precedence with respect to the Sensor Update policy?

A. Precedence applies to the Prevention policy and not to the Sensor Update policy

B. Hosts assigned to multiple policies will assume the highest ranked policy in the list (policy with the lowest number)

C. Hosts assigned to multiple policies will assume the lowest ranked policy in the list (policy with the highest number)

D. Precedence ensures that conflicting policy settings are not set in the same policy

Correct Answer: B

QUESTION 3

You want the Falcon Cloud to push out sensor version changes but you also want to manually control when the sensor version is upgraded or downgraded. In the Sensor Update policy, which is the best Sensor version option to achieve these requirements?

A. Specific sensor version number

B. Auto - TEST-QA

C. Sensor version updates off

D. Auto - N-1

Correct Answer: A

QUESTION 4

With Custom Alerts, it is possible to _____.

A. schedule the alert to run at any interval

B. receive an alert in an email

C. configure prevention actions for alerting

D. be alerted to activity in real-time

Correct Answer: D

QUESTION 5

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