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

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

QUESTION 1

How do you find a list of inactive sensors?

A. The Falcon platform does not provide reporting for inactive sensors

B. A sensor is always considered active until removed by an Administrator

C. Run the Inactive Sensor Report in the Host setup and management option

D. Run the Sensor Aging Report within the Investigate option

Correct Answer: D

QUESTION 2

Which of the following Machine Learning (ML) sliders will only detect or prevent high confidence malicious items?

A. Aggressive

B. Cautious

C. Minimal

D. Moderate

Correct Answer: C

QUESTION 3

What is the purpose of a containment policy?

A. To define which Falcon analysts can contain endpoints

B. To define the duration of Network Containment

C. To define the trigger under which a machine is put in Network Containment (e.g. a critical detection)

D. To define allowed IP addresses over which your hosts will communicate when contained

Correct Answer: C

QUESTION 4

How can a Falcon Administrator configure a pop-up message to be displayed on a host when the Falcon sensor blocks, kills or quarantines an activity?

A. By ensuring each user has set the "pop-ups allowed" in their User Profile configuration page

B. By enabling "Upload quarantined files" in the General Settings configuration page

C. By turning on the "Notify End Users" setting at the top of the Prevention policy details configuration page

D. By selecting "Enable pop-up messages" from the User configuration page

Correct Answer: C

QUESTION 5

What is the primary purpose of using glob syntax in an exclusion?

A. To specify a Domain be excluded from detections

B. To specify exclusion patterns to easily exclude files and folders and extensions from detections

C. To specify exclusion patterns to easily add files and folders and extensions to be prevented

D. To specify a network share be excluded from detections

Correct Answer: B