

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.pass2lead.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 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 2

An administrator creating an exclusion is limited to applying a rule to how many groups of hosts?

- A. File exclusions are not aligned to groups or hosts
- B. There is a limit of three groups of hosts applied to any exclusion
- C. There is no limit and exclusions can be applied to any or all groups
- D. Each exclusion can be aligned to only one group of hosts

Correct Answer: B

QUESTION 3

Why is it critical to have separate sensor update policies for Windows/Mac/*nix?

- A. There may be special considerations for each OS
- B. To assist with testing and tracking sensor rollouts
- C. The network protocols are different for each host OS
- D. It is an auditing requirement

Correct Answer: D

QUESTION 4

The Logon Activities Report includes all of the following information for a particular user EXCEPT _____.

- A. the account type for the user (e.g. Domain Administrator, Local User)

- B. all hosts the user logged into
- C. the logon type (e.g. interactive, service)
- D. the last time the user's password was set

Correct Answer: D

QUESTION 5

If a user wanted to install an older version of the Falcon sensor, how would they find the older installer file?

- A. Older versions of the sensor are not available for download
- B. By emailing CrowdStrike support at support@crowdstrike.com
- C. By installing the current sensor and clicking the "downgrade" button during the install
- D. By clicking on "Older versions" links under the Host setup and management > Deploy > Sensor downloads

Correct Answer: D

[Latest CCFA-200 Dumps](#)

[CCFA-200 PDF Dumps](#)

[CCFA-200 VCE Dumps](#)