# 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**

Which of the following is TRUE of the Logon Activities Report?

A. Shows a graphical view of user logon activity and the hosts the user connected to

B. The report can be filtered by computer name

C. It gives a detailed list of all logon activity for users

D. It only gives a summary of the last logon activity for users

Correct Answer: C

**QUESTION 2**

What command should be run to verify if a Windows sensor is running?

A. regedit myfile.reg

B. sc query csagent

C. netstat -f

D. ps -ef | grep falcon

Correct Answer: B

**QUESTION 3**

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 4**

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 5**

Which option allows you to exclude behavioral detections from the detections page?

A. Machine Learning Exclusion

B. IOA Exclusion

C. IOC Exclusion

D. Sensor Visibility Exclusion

Correct Answer: A