# 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**

What is the purpose of using groups with Sensor Update policies in CrowdStrike Falcon?

A. To group hosts with others in the same business unit

B. To group hosts according to the order in which Falcon was installed, so that updates are installed in the same order every time

C. To prioritize the order in which Falcon updates are installed, so that updates are not installed all at once leading to network congestion

D. To allow the controlled assignment of sensor versions onto specific hosts

Correct Answer: D

**QUESTION 2**

You need to export a list of all deletions for a specific Host Name in the last 24 hours. What is the best way to do this?

A. Go to Host Management in the Host page. Select the host and use the Export Detections button

B. Utilize the Detection Resolution Dashboard. Use the filters to focus on the appropriate hostname and time, then export the results from the "Detection Resolution History" section

C. In the Investigate module, access the Detection Activity page. Use the filters to focus on the appropriate hostname and time, then export the results

D. Utilize the Detection Activity Dashboard. Use the filters to focus on the appropriate hostname and time, then export the results from the "Detections by Host" section

Correct Answer: C

**QUESTION 3**

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 4**

Which of the following is TRUE regarding Falcon Next-Gen AntiVirus (NGAV)?

A. Falcon NGAV relies on signature-based detections

B. Activating Falcon NGAV will also enable all detection and prevention settings in the entire policy

C. The Detection sliders cannot be set to a value less aggressive than the Prevention sliders

D. Falcon NGAV is not a replacement for Windows Defender or other antivirus programs

Correct Answer: D

**QUESTION 5**

Which of the following is NOT a way to determine the sensor version installed on a specific endpoint?

A. Use the Sensor Report to filter to the specific endpoint

B. Use Host Management to select the desired endpoint. The agent version will be listed in the columns and details

C. From a command line, run the sc query csagent -version command

D. Use the Investigate > Host Search to filter to the specific endpoint

Correct Answer: C

Reference: https://success.trendmicro.com/solution/1114876-viewing