# 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**

Under the "Next-Gen Antivirus: Cloud Machine Learning" setting there are two categories, one of them is "Cloud Anti-Malware" and the other is:

A. Adware and PUP

B. Advanced Machine Learning

C. Sensor Anti-Malware

D. Execution Blocking

Correct Answer: B

**QUESTION 2**

How does the Unique Hosts Connecting to Countries Map help an administrator?

A. It highlights countries with known malware

B. It helps visualize global network communication

C. It identifies connections containing threats

D. It displays intrusions from foreign countries

Correct Answer: B

**QUESTION 3**

Which of the following applies to Custom Blocking Prevention Policy settings?

A. Hashes must be entered on the Prevention Hashes page before they can be blocked via this policy

B. Blocklisting applies to hashes, IP addresses, and domains

C. Executions blocked via hash blocklist may have partially executed prior to hash calculation process remediation may be necessary

D. You can only blocklist hashes via the API

Correct Answer: C

**QUESTION 4**

Why is the ability to disable detections helpful?

A. It gives users the ability to set up hosts to test detections and later remove them from the console

B. It gives users the ability to uninstall the sensor from a host

C. It gives users the ability to allowlist a false positive detection

D. It gives users the ability to remove all data from hosts that have been uninstalled

Correct Answer: C

**QUESTION 5**

Your organization has a set of servers that are not allowed to be accessed remotely, including via Real Time Response (RTR). You already have these servers in their own Falcon host group. What is the next step to disable RTR only on these hosts?

A. Edit the Default Response Policy, toggle the "Real Time Response" switch off and assign the policy to the host group

B. Edit the Default Response Policy and add the host group to the exceptions list under "Real Time Functionality"

C. Create a new Response Policy, toggle the "Real Time Response" switch off and assign the policy to the host group

D. Create a new Response Policy and add the host name to the exceptions list under "Real Time Functionality"

Correct Answer: C

CCFA-200 PDF Dumps CCFA-200 VCE Dumps CCFA-200 Study Guide