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

Where do you obtain the Windows sensor installer for CrowdStrike Falcon?

A. Sensors are downloaded from the Hosts > Sensor Downloads

B. Sensor installers are unique to each customer and must be obtained from support

C. Sensor installers are downloaded from the Support section of the CrowdStrike website

D. Sensor installers are not used because sensors are deployed from within Falcon

Correct Answer: A

The Windows sensor installer for CrowdStrike Falcon can be downloaded from the Hosts > Sensor Downloads page in the Falcon console. This page allows you to download different sensor versions and installers for various operating systems and platforms, as well as view installation instructions and release notes. The other options are either incorrect or not available. Reference: CrowdStrike Falcon User Guide, page 27.

QUESTION 2

With Custom Alerts, it is possible to _____.

A. schedule the alert to run at any interval

B. receive an alert in an email

C. configure prevention actions for alerting

D. be alerted to activity in real-time

Correct Answer: B

The reporting interval is predefined and cannot be changed. You can only enable/disable the custom alert feature and add/remove recipient email client for the alert/detection.

QUESTION 3

What is the purpose of precedence with respect to the Sensor Update policy?

A. Precedence applies to the Prevention policy and not to the Sensor Update policy

B. Hosts assigned to multiple policies will assume the highest ranked policy in the list (policy with the lowest number)

C. Hosts assigned to multiple policies will assume the lowest ranked policy in the list (policy with the highest number)

D. Precedence ensures that conflicting policy settings are not set in the same policy

Correct Answer: B

The purpose of precedence with respect to the Sensor Update policy is that hosts assigned to multiple policies will

assume the highest ranked policy in the list (policy with the lowest number). This means that if a host belongs to more than one group that has different Sensor Update policies assigned, it will use the policy that has the highest precedence (lowest number) among them. The other options are either incorrect or not related to precedence. Reference: CrowdStrike Falcon User Guide, page 38.

QUESTION 4

While a host is Network contained, you need to allow the host to access internal network resources on specific IP addresses to perform patching and remediation. Which configuration would you choose?

A. Configure a Real Time Response policy allowlist with the specific IP addresses

B. Configure a Containment Policy with the specific IP addresses

C. Configure a Containment Policy with the entire internal IP CIDR block

D. Configure the Host firewall to allowlist the specific IP addresses

Correct Answer: B

While a host is Network contained, the administrator can allow the host to access internal network resources on specific IP addresses to perform patching and remediation by configuring a Containment Policy with the specific IP addresses. This policy allows users to specify which ports, protocols and IP addresses are allowed or blocked during network containment. The other options are either incorrect or not related to network containment. Reference: [CrowdStrike Falcon User Guide], page 40.

QUESTION 5

When performing targeted filtering for a host on the Host Management Page, which filter bar attribute is NOT case-sensitive?

A. Username

B. Model

C. Domain

D. Hostname

Correct Answer: D

When performing targeted filtering for a host on the Host Management Page, the filter bar attribute that is not case-sensitive is Hostname. The Hostname attribute allows you to filter hosts by their computer name or DNS name. The Hostname filter is not case- sensitive, meaning that it will match hosts regardless of the capitalization of their names. For example, filtering by hostname=DESKTOP-1234 will match hosts with names such as DESKTOP-1234, desktop-1234, or Desktop12342. References: 2: Cybersecurity Resources | CrowdStrike