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

Once an exclusion is saved, what can be edited in the future?

A. All parts of the exclusion can be changed

B. Only the selected groups and hosts to which the exclusion is applied can be changed

C. Only the options to "Detect/Block" and/or "File Extraction" can be changed

D. The exclusion pattern cannot be changed

Correct Answer: A

Once an exclusion is saved, all parts of the exclusion can be changed in the future. The administrator can edit an existing exclusion by selecting it from the Exclusions page and modifying any of its fields, such as pattern, type, option, group or host. The other options are either incorrect or not true of editing exclusions. Reference: CrowdStrike Falcon User Guide, page 37.

QUESTION 2

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: D

The API client secret cannot be retrieved after it has been created. The secret is only displayed once when the API client is created, and it cannot be viewed or edited later. Therefore, it is important to save the secret securely and use it along with the client ID to authenticate the API client. The other options are either incorrect or not possible. Reference: CrowdStrike Falcon User Guide, page 54.

QUESTION 3

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

The Unique Hosts Connecting to Countries Map helps an administrator to visualize global network communication. The map shows the number of unique hosts in your environment that have established network connections to different countries in the past 24 hours. You can use this map to identify unusual or suspicious network activity, such as connections to high-risk countries or regions, or connections from hosts that are not expected to communicate with external entities2. References: 2: Cybersecurity Resources | CrowdStrike

QUESTION 4

Which role is required to manage groups and policies in Falcon?

A. Falcon Host Analyst

B. Falcon Host Administrator

C. Prevention Hashes Manager

D. Falcon Host Security Lead

Correct Answer: B

The Falcon Host Administrator role is required to manage groups and policies in Falcon. This role allows users to create, edit and delete groups and policies, as well as assign them to hosts. The other roles do not have this capability.

Reference:

[CrowdStrike Falcon User Guide], page 17.

QUESTION 5

When would the No Action option be assigned to a hash in IOC Management?

A. When you want to save the indicator for later action, but do not want to block or allow it at this time

B. Add the indicator to your allowlist and do not detect it

C. There is no such option as No Action available in the Falcon console

D. Add the indicator to your blocklist and show it as a detection

Correct Answer: A

The No Action option can be assigned to a hash in IOC Management when you want to save the indicator for later action, but do not want to block or allow it at this time. This option will neither detect nor prevent the execution of the hash, but will keep it in the IOC list for future reference. The other options are either incorrect or not related to the No Action option. Reference: CrowdStrike Falcon User Guide, page 44.