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 role allows a user to connect to hosts using Real-Time Response?

A. Endpoint Manager

B. Falcon Administrator

C. Real Time Responder ?Active Responder

D. Prevention Hashes Manager

Correct Answer: C

The role that allows a user to connect to hosts using Real-Time Response is Real Time Responder ?Active Responder. This role allows users to use the "Connect to Host" feature to gather additional information from the host, as well as

execute commands and scripts on the host. The other roles do not have this capability. Reference:

[CrowdStrike Falcon User Guide], page 18.

QUESTION 2

You have a Windows host on your network in Reduced functionality mode (RFM). While the system is in RFM, which of the following is TRUE?

A. System monitoring will be unavailable

B. Event reporting will be unavailable

C. Prevention patterns will not be triggered

D. Some detection patterns and preventions will not be triggered

Correct Answer: D

The option that is true when a Windows host is in Reduced Functionality Mode (RFM) is that some detection patterns and preventions will not be triggered. RFM is a mode that limits the sensor\\'s functionality due to license expiration, network connectivity loss, or certificate validation failure. When a Windows sensor is in RFM, it will only provide basic prevention capabilities, such as blocking known malware hashes and preventing script execution from the %TEMP% directory. The sensor will not send any telemetry or detection events to the Falcon platform, and will not receive any policy or update changes from the Falcon cloud. This means that some detection patterns and preventions that rely on telemetry, machine learning, or cloud analysis will not be triggered. References: : [Falcon Administrator Learning Path | Infographic | CrowdStrike]

QUESTION 3

Which of the follow should be used with extreme caution because it may introduce additional security risks such as malware or other attacks which would not be recorded, detected, or prevented based on the exclusion syntax?

A. Sensor Visibility Exclusion

B. Machine Learning Exclusions

C. IOC Exclusions

D. IOA Exclusions

Correct Answer: D

The option that should be used with extreme caution because it may introduce additional security risks such as malware or other attacks which would not be recorded, detected, or prevented based on the exclusion syntax is IOA Exclusions. An IOA (indicator of attack) exclusion allows you to define custom rules for excluding suspicious behavior from detection or prevention based on process execution, file write, network connection, or registry events. However, using IOA exclusions may reduce the visibility and protection of the Falcon sensor, as it may allow malicious activity to bypass the sensor\\'s detection and prevention capabilities. Therefore, you should use IOA exclusions with extreme caution and only when necessary2. References: 2: Cybersecurity Resources | CrowdStrike

QUESTION 4

When creating an API client, which of the following must be saved immediately since it cannot be viewed again after the client is created?

A. Base URL

B. Secret

C. Client ID

D. Client name

Correct Answer: B

When creating an API client, the secret must be saved immediately since it cannot be viewed again after the client is created. The secret is a randomly generated string that is used to authenticate the API client along with the client ID. The other options are either incorrect or can be viewed or modified later. Reference: CrowdStrike Falcon User Guide, page 54.

QUESTION 5

On a Windows host, what is the best command to determine if the sensor is currently running?

A. sc query csagent

B. netstat -a

C. This cannot be accomplished with a command

D. ping falcon.crowdstrike.com

Correct Answer: A

On a Windows host, the best command to determine if the sensor is currently running is sc query csagent. This command will show the status of the csagent service, which is responsible for running the sensor on Windows systems. The output of this command will indicate if the service is running, stopped, or paused. If the service is running, the

sensor is also running3. References: 3: How to Become a CrowdStrike Certified Falcon Administrator