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

Which of the following is TRUE regarding disabling detections for a host?

A. After disabling detections, the host will operate in Reduced Functionality Mode (RFM) until detections are enabled

B. After disabling detections, the data for all existing detections prior to disabling detections is removed from the Event Search

C. The DetectionSummaryEvent continues being sent to the Streaming API for that host

D. The detections for that host are removed from the console immediately. No new detections will display in the console going forward unless detections are enabled

Correct Answer: D

The option that is true regarding disabling detections for a host is that the detections for that host are removed from the console immediately. No new detections will display in the console going forward unless detections are enabled. This option is essentially a repetition of question 127 and its answer. Disabling detections for a host will remove any existing detections for that host from the console and prevent any new detections from appearing in the console until detections are enabled again1. References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 2

Why do Sensor Update policies need to be configured for each OS (Windows, Mac, Linux)?

A. To bundle the Sensor and Prevention policies together into a deployment package

B. Sensor Update policies are OS dependent

C. To assist with auditing and change management

D. This is false. One policy can be applied to all Operating Systems

Correct Answer: B

Sensor Update policies need to be configured for each OS (Windows, Mac, Linux) because Sensor Update policies are OS dependent. A Sensor Update policy is a policy that controls how and when the Falcon sensor is updated on a host.

Sensor Update policies are specific to each operating system type, as different operating systems have different sensor versions, features, and requirements. Therefore, you need to create and assign separate Sensor Update policies for

each operating system type in your environment1.

References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 3

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 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

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: A

"Disable Detections. This is helpful for users who want to set up hosts to test detections in the Falcon console and who later want to remove those old test detections from the"