DirectCertify

Unlock Your Potential, Certify Your Success

CrowdStrike

CCFA-200b Exam

CrowdStrike Falcon Administrator

Exam Latest Version: 6.0

DEMO Version

Full Version Features:

• 90 Days Free Updates

• 30 Days Money Back Guarantee

• Instant Download Once Purchased

• 24 Hours Live Chat Support

Full version is available at link below with affordable price.

https://www.directcertify.com/crowdstrike/ccfa-200b

Question 1. (Multi Select)

Which use cases are appropriate for configuring a Falcon workflow?

(Choose two)

A: Forwarding detection data to a SIEM system
B: Updating endpoint hostnames
C: Modifying policy priorities
D: Alerting a SOC team when high-severity detections

Correct Answer: A, D

Question 2. (Single Select)

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

Explanation:

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. [CrowdStrike Falcon User Guide], page 40.

Question 3. (Single Select)

Custom IOA rules are defined using which syntax?

A: Glob
B: PowerShell
C: Yara
D: Regex

Correct Answer: D

Explanation:

Regex guidelines
https://falcon.crowdstrike.com/documentation/68/detection-and-prevention-policies#regex

Question 4. (Single Select)

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

Explanation:

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 5. (Single Select)

How do you assign a Prevention policy to one or more hosts?

A: Create a new policy and assign it directly to those hosts on the Host Management page
B: Modify the users roles on the User Management page
C: Ensure the hosts are in a group and assign that group to a custom Prevention policy
D: Create a new policy and assign it directly to those hosts on the Prevention policy page

Correct Answer: C

Explanation:

The administrator can assign a Prevention policy to one or more hosts by ensuring the hosts are in a group and assigning that group to a custom Prevention policy. This allows users to apply different prevention settings and options to different groups of hosts based on their needs and preferences. The other options are either incorrect or not applicable to assigning a Prevention policy. [CrowdStrike Falcon User Guide], page 34.

DirectCertify

Unlock Your Potential, Certify Your Success

Full version is available at link below with affordable price.

https://www.directcertify.com/crowdstrike/ccfa-200b

30% Discount Coupon Code: LimitedTime2025