CCFA-200$^{\text{Q\&As}}$

CrowdStrike Certified Falcon Administrator

Pass CrowdStrike CCFA-200 Exam with 100% Guarantee

QUESTION 1

How do you assign a policy to a specific group of hosts?

A. Create a group containing the desired hosts using "Static Assignment." Go to the Assigned Host Groups tab of the desired policy and dick "Add groups to policy." Select the desired Group(s).

B. Assign a tag to the desired hosts in Host Management. Create a group with an assignment rule based on that tag. Go to the Assignment tab of the desired policy and click "Add Groups to Policy." Select the desired Group(s).

C. Create a group containing the desired hosts using "Dynamic Assignment." Go to the Assigned Host Groups tab of the desired policy and select criteria such as OU, OS, Hostname pattern, etc.

D. On the Assignment tab of the desired policy, select "Static" assignment. From the next window, select the desired hosts (using fitters if needed) and click Add.

Correct Answer: C

QUESTION 2

Custom IOA rules are defined using which syntax?

A. Glob

B. PowerShell

C. Yara

D. Regex

Correct Answer: B

QUESTION 3

Why is it critical to have separate sensor update policies for Windows/Mac/*nix?

A. There may be special considerations for each OS

B. To assist with testing and tracking sensor rollouts

C. The network protocols are different for each host OS

D. It is an auditing requirement

Correct Answer: D

QUESTION 4

Even though you are a Falcon Administrator, you discover you are unable to use the "Connect to Host" feature to gather additional information which is only available on the host. Which role do you need added to your user account to have this capability?

A. Real Time Responder

B. Endpoint Manager

C. Falcon Investigator

D. Remediation Manager

Correct Answer: C

QUESTION 5

Where can you modify settings to permit certain traffic during a containment period?

A. Prevention Policy

B. Host Settings

C. Containment Policy

D. Firewall Settings

Correct Answer: C

QUESTION 6

In order to quarantine files on the host, what prevention policy settings must be enabled?

A. Malware Protection and Custom Execution Blocking must be enabled

B. Next-Gen Antivirus Prevention sliders and "Quarantine and Security Center Registration" must be enabled

C. Malware Protection and Windows Anti-Malware Execution Blocking must be enabled

D. Behavior-Based Threat Prevention sliders and Advanced Remediation Actions must be enabled

Correct Answer: C

QUESTION 7

One of your development teams is working on code for a new enterprise application but Falcon continually flags the execution as a detection during testing. All development work is required to be stored on a file share in a folder called "devcode."

What setting can you use to reduce false positives on this file path?

A. USB Device Policy

B. Firewall Rule Group

C. Containment Policy

D. Machine Learning Exclusions

Correct Answer: C

QUESTION 8

When creating a Host Group for all Workstations in an environment, what is the best method to ensure all workstation hosts are added to the group?

A. Create a Dynamic Group with Type=Workstation Assignment

B. Create a Dynamic Group and Import All Workstations

C. Create a Static Group and Import all Workstations

D. Create a Static Group with Type=Workstation Assignment

Correct Answer: A

QUESTION 9

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

QUESTION 10

You have an existing workflow that is triggered on a critical detection that sends an email to the escalation team. Your CISO has asked to also be notified via email with a customized message. What is the best way to update the workflow?

A. Clone the workflow and replace the existing email with your CISO\\'s email

B. Add a sequential action to send a custom email to your CISO

C. Add a parallel action to send a custom email to your CISO

D. Add the CISO\\'s email to the existing action

Correct Answer: B

QUESTION 11

You have been provided with a list of 100 hashes that are not malicious but your company has deemed to be inappropriate for work computers. They have asked you to ensure that they are not allowed to run in your environment. You have

chosen to use Falcon to do this.

Which is the best way to accomplish this?

A. Using the Support Portal, create a support ticket and include the list of binary hashes, asking support to create an "Execution Prevention" rule to prevent these processes from running

B. Using Custom Alerts in the Investigate App, create a new alert using the template "Process Execution" and within that rule, select the option to "Block Execution"

C. Using IOC Management, gather the list of SHA256 or MD5 hashes for each binary and then upload them. Set all hashes to "Block" and ensure that the prevention policy these computers are using includes the option for "Custom Blocking" under Execution Blocking.

D. Using the API, gather the list of SHA256 or MD5 hashes for each binary and then upload them, setting them all to "Never Allow"

Correct Answer: C

QUESTION 12

You want to create a detection-only policy. How do you set this up in your policy\\'s settings?

A. Enable the detection sliders and disable the prevention sliders. Then ensure that Next Gen Antivirus is enabled so it will disable Windows Defender.

B. Select the "Detect-Only" template. Disable hash blocking and exclusions.

C. You can\\'t create a policy that detects but does not prevent. Use Custom IOA rules to detect.

D. Set the Next-Gen Antivirus detection settings to the desired detection level and all the prevention sliders to disabled. Do not activate any of the other blocking or malware prevention options.

Correct Answer: D

QUESTION 13

Where in the Falcon console can information about supported operating system versions be found?

A. Configuration module

B. Intelligence module

C. Support module

D. Discover module

Correct Answer: C

QUESTION 14

Under the "Next-Gen Antivirus: Cloud Machine Learning" setting there are two categories, one of them is "Cloud Anti-Malware" and the other is:

A. Adware and PUP

B. Advanced Machine Learning

C. Sensor Anti-Malware

D. Execution Blocking

Correct Answer: B

QUESTION 15

Which of the following applies to Custom Blocking Prevention Policy settings?

A. Hashes must be entered on the Prevention Hashes page before they can be blocked via this policy

B. Blocklisting applies to hashes, IP addresses, and domains

C. Executions blocked via hash blocklist may have partially executed prior to hash calculation process remediation may be necessary

D. You can only blocklist hashes via the API

Correct Answer: C