Vendor: CrowdStrike

Exam Code:CCFA-200

Exam Name: CrowdStrike Certified Falcon Administrator

Version: Demo

QUESTION 1

What impact does disabling detections on a host have on an API?

A. Endpoints with detections disabled will not alert on anything until detections are enabled again

B. Endpoints cannot have their detections disabled individually

C. DetectionSummaryEvent stops sending to the Streaming API for that host

D. Endpoints with detections disabled will not alert on anything for 24 hours (by default) or longer if that setting is changed

Correct Answer: D

QUESTION 2

Where do you obtain the Windows sensor installer for CrowdStrike Falcon?

A. Sensors are downloaded from the Hosts > Sensor Downloads

B. Sensor installers are unique to each customer and must be obtained from support

C. Sensor installers are downloaded from the Support section of the CrowdStrike website

D. Sensor installers are not used because sensors are deployed from within Falcon

Correct Answer: B

QUESTION 3

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 4

An administrator creating an exclusion is limited to applying a rule to how many groups of hosts?

A. File exclusions are not aligned to groups or hosts

B. There is a limit of three groups of hosts applied to any exclusion

C. There is no limit and exclusions can be applied to any or all groups

D. Each exclusion can be aligned to only one group of hosts

Correct Answer: B

QUESTION 5

You have created a Sensor Update Policy for the Mac platform. Which other operating system(s) will this policy manage?

A. *nix

B. Windows

C. Both Windows and *nix

D. Only Mac

Correct Answer: C

Reference: https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/

QUESTION 6

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 7

What is the goal of a Network Containment Policy?

A. Increase the aggressiveness of the assigned prevention policy

B. Limit the impact of a compromised host on the network

C. Gain more visibility into network activities

D. Partition a network for privacy

Correct Answer: B

QUESTION 8

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: D

QUESTION 9

Custom IOA rules are defined using which syntax?

A. Glob

B. PowerShell

C. Yara

D. Regex

Correct Answer: B

QUESTION 10

Which is the correct order for manually installing a Falcon Package on a macOS system?

A. Install the Falcon package, then register the Falcon Sensor via the registration package

B. Install the Falcon package, then register the Falcon Sensor via command line

C. Register the Falcon Sensor via command line, then install the Falcon package

D. Register the Falcon Sensor via the registration package, then install the Falcon package

Correct Answer: C

QUESTION 11

What is the most common cause of a Windows Sensor entering Reduced Functionality Mode (RFM)?

A. Falcon console updates are pending

B. Falcon sensors installing an update

C. Notifications have been disabled on that host sensor

D. Microsoft updates

Correct Answer: C

QUESTION 12

What information is provided in Logan Activities under Visibility Reports?

A. A list of all logons for all users

B. A list of last endpoints that a user logged in to

C. A list of users who are remotely logged on to devices based on local IP and local port

D. A list of unique users who are remotely logged on to devices based on the country

Correct Answer: B