CrowdStrike Certified Falcon Administrator

CrowdStrike CCFA-200

Version Demo

Total Demo Questions: 10

Total Premium Questions: 96

QUESTION NO: 1

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

ANSWER: C

QUESTION NO: 2

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

ANSWER: C

QUESTION NO: 3

Which role will allow someone to manage quarantine files?

A. Falcon Security Lead

B. Detections Exceptions Manager

C. Falcon Analyst – Read Only

D. Endpoint Manager

ANSWER: B

QUESTION NO: 4

How are user permissions set in Falcon?

A. Permissions are assigned to a User Group and then users are assigned to that group, thereby inheriting those permissions

B. Pre-defined permissions are assigned to sets called roles. Users can be assigned multiple roles based on job function and they assume a cumulative set of permissions based on those assignments

C. An administrator selects individual granular permissions from the Falcon Permissions List during user creation

D. Permissions are token-based. Users request access to a defined set of permissions and an administrator adds their token to the set of permissions

ANSWER: B

QUESTION NO: 5

Which of the following best describes the Default Sensor Update policy?

A. The Default Sensor Update policy does not have the "Uninstall and maintenance protection" feature

B. The Default Sensor Update policy is only used for testing sensor updates

C. The Default Sensor Update policy is a "catch-all" policy

D. The Default Sensor Update policy is disabled by default

ANSWER: C

QUESTION NO: 6

Which of the following Machine Learning (ML) sliders will only detect or prevent high confidence malicious items?

A. Aggressive

B. Cautious

C. Minimal

D. Moderate

ANSWER: C

QUESTION NO: 7

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

ANSWER: B

QUESTION NO: 8

How do you disable all detections for a host?

A. Create an exclusion rule and apply it to the machine or group of machines

B. Contact support and provide them with the Agent ID (AID) for the machine and they will put it on the Disabled Hosts list in your Customer ID (CID)

C. You cannot disable all detections on individual hosts as it would put them at risk

D. In Host Management, select the host and then choose the option to Disable Detections

ANSWER: D

QUESTION NO: 9

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.

ANSWER: C

QUESTION NO: 10

To enhance your security, you want to detect and block based on a list of domains and IP addresses. How can you use IOC management to help this objective?

A. Blocking of Domains and IP addresses is not a function of IOC management. A Custom IOA Rule should be used instead

B. Using IOC management, import the list of hashes and IP addresses and set the action to Detect Only

C. Using IOC management, import the list of hashes and IP addresses and set the action to Prevent/Block

D. Using IOC management, import the list of hashes and IP addresses and set the action to No Action

ANSWER: C