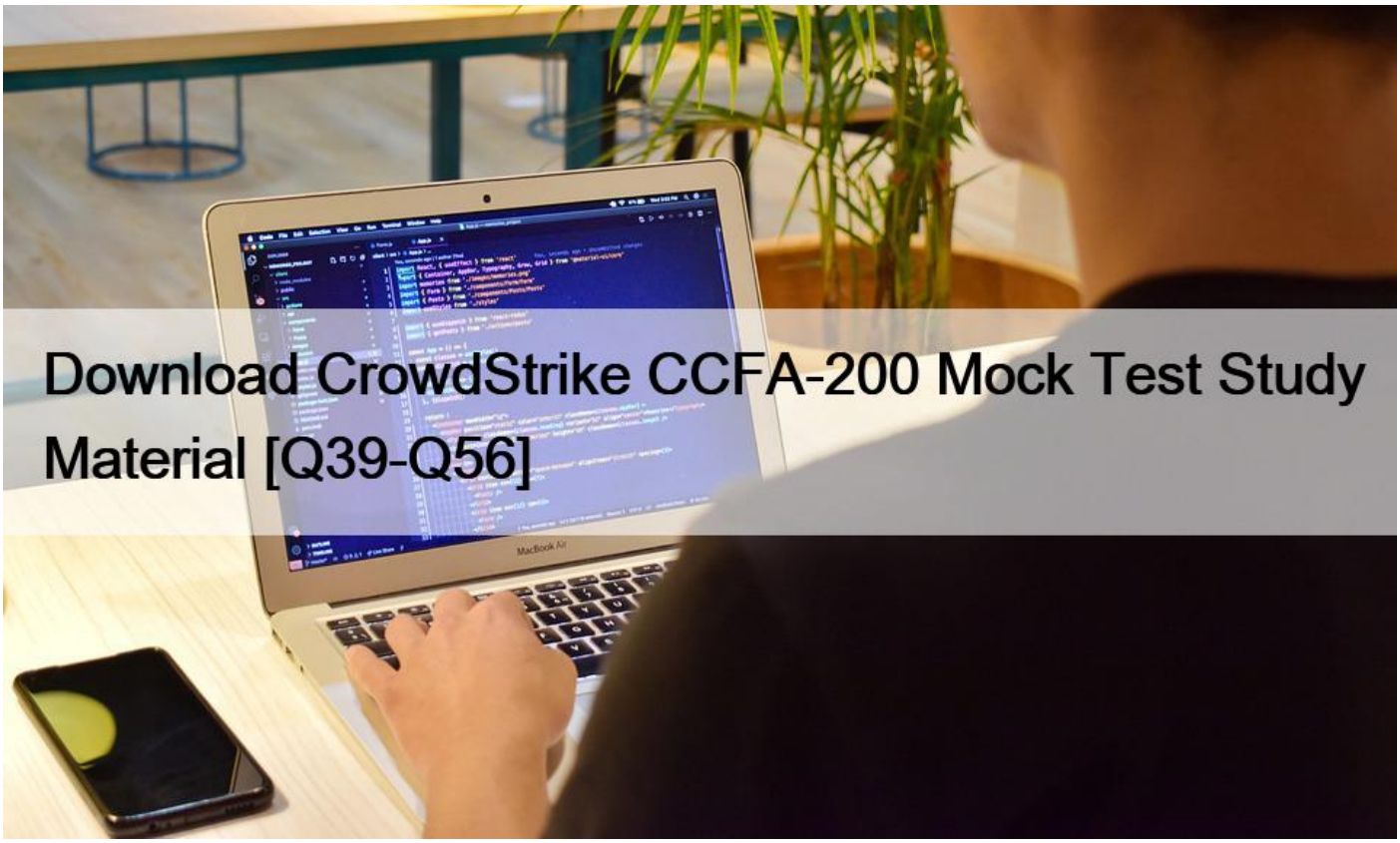
Download CrowdStrike CCFA-200 Mock Test Study Material [Q39-Q56



Download CrowdStrike CCFA-200 Mock Test Study Material
CCFA-200 Questions Prepare with Learning Information

NEW QUESTION 39

Which of the following is TRUE of the Logon Activities Report?
* Shows a graphical view of user logon activity and the hosts the user connected to
* The report can be filtered by computer name
* It gives a detailed list of all logon activity for users
* It only gives a summary of the last logon activity for users

NEW QUESTION 40

What is the most common cause of a Windows Sensor entering Reduced Functionality Mode (RFM)?
* Falcon console updates are pending
* Falcon sensors installing an update
* Notifications have been disabled on that host sensor
* Microsoft updates

Explanation

The most common cause of a Windows Sensor entering Reduced Functionality Mode (RFM) is Microsoft updates. RFM occurs when the sensor detects a change in the operating system that requires a reboot to complete. Microsoft updates are one of the common causes of such a change. The other options are either incorrect or not related to RFM. Reference: CrowdStrike Falcon User Guide, page 30.

NEW QUESTION 41

On the Host management page which filter could be used to quickly identify all devices categorized as a

“Workstation” by the Falcon Platform?
* Status
* Platform
* Hostname
* Type

Explanation

The filter that could be used to quickly identify all devices categorized as a “Workstation” by the Falcon Platform on the Host Management page is Type. The Type filter allows you to filter hosts by their device type, such as workstation, server, or domain controller. The device type is assigned to each host based on their Active Directory domain structure. You can use the Type filter to quickly identify all hosts that have the workstation type assigned in their domain2.

References: 2: Cybersecurity Resources | CrowdStrike

NEW QUESTION 42

How many “Auto” sensor version update options are available for Windows Sensor Update Policies?
* 1
* 2
* 0
* 3

NEW QUESTION 43

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?
* Create a Dynamic Group with Type=Workstation Assignment
* Create a Dynamic Group and Import All Workstations
* Create a Static Group and Import all Workstations
* Create a Static Group with Type=Workstation Assignment

Explanation

The best method to ensure all workstation hosts are added to the group is to create a Dynamic Group with Type=Workstation Assignment. A Dynamic Group is a group that automatically updates its membership based on certain criteria or filters. A Type=Workstation Assignment filter will match all hosts that have the workstation type assigned in their Active Directory domain. This way, any new or existing workstation hosts will be added to the group without manual intervention1.

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

NEW QUESTION 44

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?
* USB Device Policy
* Firewall Rule Group
* Containment Policy
* Machine Learning Exclusions

NEW QUESTION 45

You have a new patch server that should be reachable while hosts in your environment are network contained.

The server’s IP address is static and does not change. Which of the following is the best approach to updating the Containment Policy to allow this?
* Add an allowlist entry for the individual server’s MAC address
* Add an allowlist entry containing the host group that the server belongs to
* Add an allowlist entry for the individual server’s IP address
* Add an allowlist entry containing CIDR notation for the /24 network the server belongs to
Explanation

The best approach to updating the Containment Policy to allow a new patch server that should be reachable while hosts in your environment are network contained is to add an allowlist entry for the individual server’s IP address. An allowlist entry allows you to define a list of trusted IP addresses that can communicate with your contained hosts. This way, you can isolate a host from the network while still allowing it to access essential resources or services, such as a patch server. If the server’s IP address is static and does not change, adding an individual IP address is more precise and secure than adding a host group or a network range2.

References: 2: Cybersecurity Resources | CrowdStrike

NEW QUESTION 46

What is the most common cause of a Windows Sensor entering Reduced Functionality Mode (RFM)?
* Microsoft updates
* Notifications have been disabled on that host sensor
* Falcon console updates are pending
* Falcon sensors installing an update

NEW QUESTION 47

What is the purpose of using groups with Sensor Update policies in CrowdStrike Falcon?
* To group hosts with others in the same business unit
* To group hosts according to the order in which Falcon was installed, so that updates are installed in the same order every time
* To prioritize the order in which Falcon updates are installed, so that updates are not installed all at once leading to network congestion
* To allow the controlled assignment of sensor versions onto specific hosts

NEW QUESTION 48

Which Real Time Response role will allow you to see all analyst session details?
* Real Time Response – Read-Only Analyst

* None of the Real Time Response roles allows this
* Real Time Response -Active Responder
* Real Time Response -Administrator

Explanation

The Real Time Response role that will allow you to see all analyst session details is Real Time Response

-Administrator. A Real Time Response -Administrator is a role that has full access and control over the Real Time Response feature in Falcon, which allows you to remotely access and investigate hosts in real time. A Real Time Response -Administrator can view all analyst session details, such as session ID, host name, start and end time, commands executed, and output received. A Real Time Response -Administrator can also create, modify, delete, and assign scripts and commands to other analysts2.

References: 2: Cybersecurity Resources | CrowdStrike

NEW QUESTION 49

What is the purpose of the Machine-Learning Prevention Monitoring Report?

* It is designed to give an administrator a quick overview of machine-learning aggressiveness settings as well as the numbers of items actually quarantined
* It is the dashboard used by an analyst to view all items quarantined and to release any items deemed non-malicious
* It is the dashboard used to see machine-learning preventions, and it is used to identify spikes in activity and possible targeted attacks
* It is designed to show malware that would have been blocked in your environment based on different Machine-Learning Prevention settings

Explanation

Machine-Learning Prevention Monitoring dashboard: Use this dashboard to view malware that would have been blocked in your environment over the selected timeframe based on different Machine Learning Prevention settings (Cautious, Moderate, Aggressive or Extra Aggressive).

NEW QUESTION 50

Why is it important to know your company’s event data retention limits in the Falcon platform?

* This is not necessary; you simply select “All Time” in your query to search all data
* You will not be able to search event data into the past beyond your retention period
* Data such as process records are kept for a shorter time than event data
* Your query will require you to specify the data pool associated with the date you wish to search

NEW QUESTION 51

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

* Endpoints with detections disabled will not alert on anything until detections are enabled again
* Endpoints cannot have their detections disabled individually
* DetectionSummaryEvent stops sending to the Streaming API for that host
* Endpoints with detections disabled will not alert on anything for 24 hours (by default) or longer if that setting is changed

NEW QUESTION 52

What best describes what happens to detections in the console after clicking “Disable Detections” for a host from within the Host Management page?

* The detections for the host are removed from the console immediately and no new detections will display in the console going forward
* You cannot disable detections for a host
* Existing detections for the host remain, but no new detections will display in the console going forward
* Preventions will be disabled for the host

Explanation

The option that best describes what happens to detections in the console after clicking “Disable Detections” for a host from within the Host Management page is that the detections for the host are removed from the console immediately and no new detections will display in the console going forward. The “Disable Detections” feature allows you to enable or disable the detection and prevention capabilities of the Falcon sensor on a specific host. When you disable detections for a host, the sensor will stop sending any detection or prevention events to the Falcon console, and any existing events for that host will be removed from the console. When you enable detections for a host, the sensor will resume sending any new detection or prevention events to the Falcon console, but any previous events for that host will not be restored to the console1.

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

NEW QUESTION 53

You need to export a list of all deletions for a specific Host Name in the last 24 hours. What is the best way to do this?

* Go to Host Management in the Host page. Select the host and use the Export Detections button
* Utilize the Detection Resolution Dashboard. Use the filters to focus on the appropriate hostname and time, then export the results from the “Detection Resolution History” section
* In the Investigate module, access the Detection Activity page. Use the filters to focus on the appropriate hostname and time, then export the results
* Utilize the Detection Activity Dashboard. Use the filters to focus on the appropriate hostname and time, then export the results from the “Detections by Host” section

Explanation

The best way to export a list of all deletions for a specific Host Name in the last 24 hours is to go to the Investigate module, access the Detection Activity page, use the filters to focus on the appropriate hostname and time, then export the results. This will allow you to download a CSV file that contains information about all the detections that were deleted for that host in that time period. The other options are either incorrect or not related to exporting deletions. Reference: CrowdStrike Falcon User Guide, page 49.

NEW QUESTION 54

Which statement describes what is recommended for the Default Sensor Update policy?

* The Default Sensor Update policy should align to an organization’s overall sensor updating practice while leveraging Auto N-1 and Auto N-2 configurations where possible
* The Default Sensor Update should be configured to always automatically upgrade to the latest sensor version
* Since the Default Sensor Update policy is pre-configured with recommend settings out of the box, configuration of the Default Sensor Update policy is not required
* No configuration is required. Once a Custom Sensor Update policy is created the Default Sensor Update policy is disabled

Explanation

The statement that describes what is recommended for the Default Sensor Update policy is that the Default Sensor Update policy should align to an organization’s overall sensor updating practice while leveraging Auto N-1 and Auto N-2 configurations where possible. As explained in question 139, the Default Sensor Update policy is a “catch-all” policy that applies to any host that is not assigned to a specific Sensor Update policy.

Therefore, it is recommended that the Default Sensor Update policy should align to your organization’s overall sensor updating practice, such as how frequently and how quickly you want to update your sensors. It is also recommended that you leverage the Auto N-1 and Auto N-2 configurations, which allow you to automatically update your sensors to the latest or second-latest sensor version without requiring manual intervention1.

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

NEW QUESTION 55

Where in the console can you find a list of all hosts in your environment that are in Reduced Functionality Mode (RFM)?
* Host Dashboard
* Host Management > Filter for RFM
* Inactive Sensor Report
* Containment Policy

Explanation

The place in the console where you can find a list of all hosts in your environment that are in Reduced Functionality Mode (RFM) is Host Management > Filter for RFM. The Host Management page allows you to view and manage all hosts in your environment that have Falcon sensors installed. You can use the filter bar to filter hosts by various attributes, such as status, platform, type, or group. You can also filter hosts by health events, such as RFM, which is a mode that limits the sensor’s functionality due to license expiration, network connectivity loss, or certificate validation failure. By filtering for RFM, you can see a list of all hosts that are in this mode1.

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

NEW QUESTION 56

How do you assign a Prevention policy to one or more hosts?
* Create a new policy and assign it directly to those hosts on the Host Management page
* Modify the users roles on the User Management page
* Ensure the hosts are in a group and assign that group to a custom Prevention policy
* Create a new policy and assign it directly to those hosts on the Prevention policy page

Most Reliable CrowdStrike CCFA-200 Training Materials: https://www.braindumpsit.com/CCFA-200_real-exam.html]