Ace Your Exam Preparation with ActualPDF CrowdStrike CCFA-200b Exam Questions

P.S. Free 2026 CrowdStrike CCFA-200b dumps are available on Google Drive shared by ActualPDF: https://drive.google.com/open?id=1ou8J8_Xvy0wTICwg0lWud_0dIwl4T5ps

Once you have practiced and experienced the quality of our CCFA-200b exam preparation, you will remember the serviceability and usefulness of them. For the excellent quality of our CCFA-200b training questions explains why our CCFA-200b practice materials helped over 98 percent of exam candidates get the certificate you dream of successfully. Believe me with our CCFA-200b Guide quiz, you will be more confident to pass the exam in the shortest time with ease.

Each IT person is working hard for promotion and salary increases. It is also a reflection of the pressure of modern society. We should use the strength to prove ourselves. Participate in the CrowdStrike CCFA-200b exam please. In fact, this examination is not so difficult as what you are thinking. You only need to select the appropriate training materials. ActualPDF's CrowdStrike CCFA-200b Exam Training materials is the best training materials. Select the materials is to choose what you want. In order to enhance your own, do it quickly.

>> Best CCFA-200b Study Material <<

Pass Guaranteed Quiz CrowdStrike - CCFA-200b - CrowdStrike Certified Falcon Administrator - 2024 Version –Reliable Best Study Material

As long as you study with our CCFA-200b training braindump, then you will find that it is designed to deepened the understanding of the users and memory. Simple text messages, deserve to go up colorful stories and pictures beauty, make the CCFA-200b test guide better meet the zero basis for beginners, let them in the relaxed happy atmosphere to learn more useful knowledge, more good

combined with practical, so as to achieve the state of unity. It is easy to pass with our CCFA-200b Practice Questions as our pass rate of CCFA-200b exam material is more than 98%.

CrowdStrike CCFA-200b Exam Syllabus Topics:

Topic	Details
Topic 1	• Host Management and Setup: This domain addresses filtering and organizing hosts, disabling detections and understanding their effects, managing Reduced Functionality Mode situations, locating inactive sensors and their retention, and utilizing relevant management reports.
Topic 2	• User Management: This domain covers determining appropriate roles for console access, creating and assigning roles with specific permissions, and managing API keys for platform access.
Topic 3	• Group Creation: This domain covers assigning endpoints to appropriate groups for policy application and following best practices for managing host group structures.
Topic 4	• Policy Application: This domain encompasses configuring prevention policies for security posture, sensor update policies, RTR audit policies, containment policies with IP exclusions, and managing quarantined files.
Topic 5	• Workflows: This domain focuses on configuring automated workflows that execute predefined actions when specific triggers or conditions are met.
Topic 6	• Sensor Deployment: This domain focuses on verifying installation prerequisites, applying default policies and best practices, uninstalling sensors, and troubleshooting sensor issues across supported operating systems.
Topic 7	• Dashboards and Reports: This domain covers understanding different sensor report types and their use cases, and interpreting various audit logs for tracking platform activities.

CrowdStrike Certified Falcon Administrator - 2024 Version Sample Questions (Q68-Q73):

NEW QUESTION # 68
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 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"
- B. Using the API, gather the list of SHA256 or MD5 hashes for each binary and then upload them, setting them all to "Never Allow"
- C. 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
- D. 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.

Answer: D

Explanation:
The best way to ensure that a list of 100 hashes that are not malicious but your company has deemed to be inappropriate for work computers are not allowed to run in your environment is to use 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. This will allow Falcon to block the execution of these hashes on the hosts using this policy. The other options are either incorrect or not efficient to achieve this goal.

NEW QUESTION # 69
Where should you look to find the history of the successes and failures for any Falcon Fusion workflows?

- A. Falcon Ul Audit Trail
- B. Custom Alert History
- C. Workflow Audit log
- D. Workflow Execution log

Answer: D

Explanation:
The place where you can find the history of the successes and failures for any Falcon Fusion workflows is the Workflow Execution log. The Workflow Execution log in the Workflow Management option allows you to view the status and results of workflow executions triggered by detection events. You can filter the log by workflow name, status, start and end time, and detection ID. You can also view the details of each execution, including the actions performed, the output received, and any errors encountered. This log can help you troubleshoot potential failures or issues with your workflows.

NEW QUESTION # 70
What will happen to a host that is not part of any group which has a prevention policy assigned to it?

- A. The host will send a notification to the Falcon Administrator to assign a prevention policy
- B. The host will apply a sensor-based policy to prevent a majority of known threats
- C. The host will disable the falcon sensor
- D. The host will apply the default prevention policy

Answer: D

NEW QUESTION # 71
On the Host management page which filter could be used to quickly identify all devices categorized as a "Workstation" by the Falcon Platform?

- A. Type
- B. Platform
- C. Hostname
- D. Status

Answer: A

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 domain.

NEW QUESTION # 72
What least privilege role should be given to a user who needs to extract files with RTR?

- A. Real Time Responder - Administrator
- B. Real Time Responder - Active Responder
- C. Falcon Security Lead
- D. Falcon Investigator

Answer: B

Explanation:
The least privilege role for extracting files with RTR is Real Time Responder - Active Responder . The Active Responder role includes the ability to use the get command to retrieve files from endpoints, along with additional response commands beyond read-only reconnaissance. The RTR Administrator role can also extract files, but it grants broader capabilities such as creating custom

scripts, uploading files with put, and directly running executables, so it is not least privilege. Falcon Security Lead and Falcon Investigator are detection and investigation roles but do not provide the required RTR command authority by themselves. CCFA role design emphasizes giving users only the permissions needed to complete the task. For file extraction, Active Responder is sufficient and appropriately scoped.

NEW QUESTION # 73
.....