Quiz 2026 CrowdStrike CCCS-203b–Professional Accurate Prep Material

2026 Latest Exams4Collection CCCS-203b PDF Dumps and CCCS-203b Exam Engine Free Share: https://drive.google.com/open?id=1EnJDsxParN-IavONywv-CEvntWVpa95H

We have the first-rate information safety guarantee system for the buyers who buy the CCCS-203b questions and answers of our company, we can ensure that the information of your name, email, or product you buy. We respect the private information of every customer, and we won't send the junk information to you to bother. Besides, you will get CCCS-203b Questions and answers downloading link within ten minutes, and our system will send you the update version to your mailbox.

CrowdStrike CCCS-203b Exam Syllabus Topics:

Topic	Details
Topic 1	• Falcon Cloud Security Features and Services: This domain covers understanding CrowdStrike's cloud security products (CSPM, CWP, ASPM, DSPM, IaC security) and their integration, plus one-click sensor deployment and Kubernetes admission controller capabilities.
Topic 2	• Remediating and Reporting Issues: This domain addresses identifying remediation steps for findings, using scheduled reports for cloud security, and utilizing Falcon Fusion SOAR workflows for automated notifications.
Topic 3	• Runtime Protection: This domain focuses on selecting appropriate Falcon sensors for Kubernetes environments, troubleshooting deployments, and identifying misconfigurations, unassessed images, IOAs, rogue containers, drift, and network connections.
Topic 4	• Findings and Detection Analysis: This domain covers evaluating security controls to identify IOMs, vulnerabilities, suspicious activity, and persistence mechanisms, auditing user permissions, comparing configurations to benchmarks, and discovering unmanaged public-facing assets.
Topic 5	• Cloud Security Policies and Rules: This domain addresses configuring CSPM policies, image assessment policies, Kubernetes admission controller policies, and runtime sensor policies based on specific use cases.
Topic 6	• Cloud Account Registration: This domain focuses on selecting secure registration methods for cloud environments, understanding required roles, organizing resources into cloud groups, configuring scan exclusions, and troubleshooting registration issues.

>> CCCS-203b Accurate Prep Material <<

CCCS-203b Hot Spot Questions & Test CCCS-203b Dump

The CrowdStrike Certified Cloud Specialist (CCCS-203b) PDF dumps are suitable for smartphones, tablets, and laptops as well. So you can study actual CrowdStrike Certified Cloud Specialist (CCCS-203b) questions in PDF easily anywhere. Exams4Collection updates CrowdStrike Certified Cloud Specialist (CCCS-203b) PDF dumps timely as per adjustments in the content of the actual CrowdStrike CCCS-203b exam.

CrowdStrike Certified Cloud Specialist Sample Questions (Q193-Q198):

NEW QUESTION # 193
After manually scanning an image using the CrowdStrike Falcon command-line tool, how can you view the scan results?

- A. Scan results are automatically sent to your email associated with the Falcon account.
- B. Use the command falcon image-scan --results <image_id> to fetch the scan results.
- C. Run falconctl results --scan-id <scan_id> to retrieve scan results directly.
- D. Check the "Image Scans" tab in the Falcon console for a detailed report.

Answer: D

Explanation:
Option A: The falconctl tool is used for endpoint management, not for retrieving scan results.
Additionally, --scan-id is not a valid flag in this context.
Option B: CrowdStrike does not automatically send scan results via email. Results are viewed through the console or programmatically retrieved using APIs.
Option C: The falcon image-scan command does not have a --results flag. Results must be viewed in the Falcon console or through an API query.
Option D: The "Image Scans" tab in the Falcon console is the primary location for viewing detailed results of manual or automated scans. This interface provides comprehensive information, including vulnerabilities and remediation steps.

NEW QUESTION # 194
An organization is using CrowdStrike's CIEM/Identity Analyzer to assess its cloud environment.
During the analysis, it identifies several issues.
Which of the following would be flagged as a primary concern?

- A. Firewall misconfigurations allowing unrestricted inbound traffic.
- B. Data stored in unencrypted cloud storage buckets.
- C. Instances of unused roles with administrative privileges.
- D. Outdated operating systems running on virtual machines.

Answer: C

Explanation:
Option A: CIEM/Identity Analyzer focuses on identifying risks related to permissions and roles in cloud environments. Unused roles, especially those with administrative privileges, represent a significant security risk as they can be exploited by malicious actors or abused inadvertently.
Identifying and remediating these issues aligns with CIEM's core purpose of ensuring least privilege access.
Option B: Misconfigured firewalls pose significant risks, but CIEM does not deal with network- level security. This would be addressed by network security tools like cloud firewalls or security groups.
Option C: Although critical for data security, encryption of storage is not the focus of CIEM. Tools specific to storage configuration and compliance are used for this purpose.
Option D: This is a vulnerability management issue, not an identity and permissions concern. It falls under the scope of VM monitoring or endpoint protection tools, not CIEM.

NEW QUESTION # 195
After identifying a risky Azure Service Principal using the CrowdStrike CIEM/Identity Analyzer, what is the most appropriate action

to mitigate the risk?

- A. Replace the Service Principal with a managed identity to eliminate credential-related risks.
- B. Immediately delete the Service Principal and its associated secrets.
- C. Rotate the Service Principal's credentials and reduce its permissions to the minimum necessary.
- D. Assign the Service Principal an "Owner" role for temporary troubleshooting purposes.

Answer: C

Explanation:
Option A: While managed identities are a secure alternative to Service Principals, this is not always feasible for existing workflows. It may require significant reconfiguration, making it a long- term consideration rather than an immediate action.
Option B: Assigning high-level permissions like "Owner" unnecessarily increases risk.
Troubleshooting should use roles with only the necessary permissions.
Option C: Deleting the Service Principal without understanding its purpose could disrupt workflows or critical services. A more measured approach is necessary to assess and mitigate risks.
Option D: Rotating credentials ensures that any compromised secrets are invalidated, while reducing permissions to the minimum necessary aligns with the principle of least privilege. This approach mitigates risks without disrupting the Service Principal's intended functionality.

NEW QUESTION # 196
An organization has deployed CrowdStrike Falcon on their cloud workloads, but they notice that real-time detection and blocking are not functioning as expected. Upon reviewing the deployment, they identify a configuration oversight.
Which of the following is the most likely reason that runtime protection is not working?

- A. The container runtime is using an unsupported version of Docker.
- B. The cloud workload protection policies are configured to monitor but not block threats.
- C. The Falcon sensor logs indicate no active threats were detected, meaning the deployment is successful.
- D. The Falcon Container Sensor was installed without enabling workload protection policies.

Answer: D

Explanation:
Option A: While some older versions of Docker may have compatibility issues, most modern Docker versions are supported by CrowdStrike Falcon. The issue is more likely a misconfiguration than a compatibility problem.
Option B: While a "monitor-only" policy can prevent blocking, it does not explain why real-time detection is not functioning. The absence of protection is likely due to a broader misconfiguration.
Option C: Even if the Falcon Sensor is installed correctly, runtime protection requires active security policies. If these policies are missing or misconfigured, the sensor will not enforce security actions, leading to ineffective threat prevention.
Option D: The absence of detected threats does not confirm that protection is working. It is possible that policies are misconfigured, and malicious activity is going unnoticed.

NEW QUESTION # 197
A security team wants to modify existing registry connection settings in CrowdStrike Falcon to enhance pre-runtime security protections.
Which of the following best describes the correct process for updating these settings?

- A. Allow all images from a registry once it has been added, even if authentication settings or security policies change.
- B. Edit the registry connection details in the Falcon console, update authentication credentials if necessary, and apply changes to scanning policies.
- C. Disable all scanning policies when making changes to registry settings to avoid configuration errors.
- D. Delete and recreate the registry connection from scratch every time a setting needs to be updated.

Answer: B

Explanation:
Option A: Simply adding a registry does not guarantee security. Administrators must continuously update policies and authentication settings as needed.
Option B: Deleting and recreating registry connections every time is unnecessary and can cause disruptions to security operations.

Editing is a more efficient approach.
Option C: Disabling scanning policies during configuration updates is risky. Instead, updates should be made carefully while maintaining security protections.
Option D: Administrators should edit registry connection details in the Falcon console, update authentication credentials as needed, and modify scanning policies to enhance security.

NEW QUESTION # 198
......

IavONywv-CEvntWVpa95H