

CCCS-203b Web-based Practice Exam



Nowadays, using computer-aided software to pass the CCCS-203b exam has become a new trend. Because the new technology enjoys a distinct advantage, that is convenient and comprehensive. In order to follow this trend, our company product such a CCCS-203b exam questions that can bring you the combination of traditional and novel ways of studying. The passing rate of our study material is up to 99%. If you are not fortune enough to acquire the CCCS-203b Certification at once, you can unlimitedly use our CCCS-203b product at different discounts until you reach your goal and let your dream comes true.

There are three different versions of our CCCS-203b exam questions: the PDF, Software and APP online. You can choose the version of CCCS-203b training guide according to your interests and habits. And if you buy the value pack, you have all of the three versions, the price is quite preferential and you can enjoy all of the study experiences. This means you can study CCCS-203b training engine anytime and anyplace for the convenience these three versions bring.

>> Test CCCS-203b Collection <<

Test CCCS-203b Collection - 100% 100% Pass-Rate Questions Pool

As you know, the low-quality latest CCCS-203b exam torrent may do harmful influence on you which may causes results past redemption. Whether you have experienced that problem or not was history by now. The free demos do honor to the perfection of our latest CCCS-203b exam torrent, and also a performance of our considerate after sales services. Those demos serve as epitomes of real CCCS-203b Quiz guides for your reference. In our demos, some examples or question points were enumerated as some representatives of our CCCS-203b test prep. How convenient and awesome of it!

CrowdStrike Certified Cloud Specialist Sample Questions (Q254-Q259):

NEW QUESTION # 254

You are concerned about an overprivileged cloud identity.

What steps should you take to identify issues with the account's permissions?

- A. Go to Falcon Users Roles and Permissions and filter for the identity to see any risky configurations related to its permissions
- **B. Go to Cloud Indicators of Misconfiguration and filter for the identity to see any risky configurations related to its permissions**
- C. Go to Cloud Indicators of Attack and filter for the identity to see any risky activity related to its permissions
- D. Go to Investigate User Search and filter for the specific identity to see any risky activity related to its permissions

Answer: B

Explanation:

To identify issues related to an overprivileged cloud identity, CrowdStrike Falcon Cloud Security directs users to Cloud Indicators of Misconfiguration (CIM). These indicators focus specifically on risky configurations, including excessive permissions, overly broad IAM roles, and violations of least-privilege principles.

By filtering Cloud Indicators of Misconfiguration for the specific identity, security teams can quickly identify misaligned permissions such as wildcard actions, unused privileges, or access that exceeds the role's intended function. This view is purpose-built for identifying configuration risk—not active attacks or behavioral anomalies.

Cloud Indicators of Attack (CIA) are used to detect suspicious or malicious activity, not static permission risk. Investigate User Search focuses on observed behavior rather than permission design. Falcon Users Roles and Permissions applies to Falcon console access, not cloud-provider IAM identities.

Therefore, the correct and CrowdStrike-aligned approach is to review Cloud Indicators of Misconfiguration for the identity in question.

NEW QUESTION # 255

What is the primary purpose of editing a cloud security posture policy in the Falcon platform?

- A. To deploy endpoint agents on unmanaged devices in the cloud.
- **B. To define compliance benchmarks and enforce them across cloud environments.**
- C. To disable logging for high-volume cloud services to save costs.
- D. To configure runtime protection for containers in Kubernetes clusters.

Answer: B

Explanation:

Option A: Endpoint agent deployment is managed separately and does not involve editing cloud security posture policies. These policies focus on assessing and maintaining compliance, not endpoint management.

Option B: Runtime protection for containers is handled by Falcon Container and Kubernetes Sensors, not cloud security posture policies. These policies focus on identifying and remediating misconfigurations in cloud environments.

Option C: Falcon Cloud Security Posture policies are designed to align cloud configurations with compliance frameworks (e.g., CIS, NIST). By editing these policies, administrators can customize rules to meet organizational or regulatory requirements and enforce compliance across multi-cloud environments.

Option D: While logging configurations can impact costs, cloud security posture policies do not handle logging management. This is done through cloud provider settings, not Falcon policies.

NEW QUESTION # 256

Which of the following describes the behavior of a runtime protection policy applied to containerized workloads in CrowdStrike Falcon?

- A. Works only with specific container orchestration platforms like Kubernetes.
- B. Requires manual signature updates to detect threats in the runtime environment.
- C. Blocks all system calls from container processes by default.
- **D. Monitors and prevents known malicious activities in real-time within the container environment.**

Answer: D

Explanation:

Option A: Runtime protection focuses on detecting and mitigating malicious activities, such as privilege escalation attempts or unauthorized network connections, in real-time.

Option B: Blocking all system calls would render containers non-functional. Runtime protection policies are designed to monitor and selectively block only malicious or suspicious activities.

Option C: Runtime protection policies are platform-agnostic and can protect containers regardless of the orchestration platform being used, including Kubernetes, Docker Swarm, or others.

Option D: CrowdStrike Falcon uses a combination of signature-based and behavior-based detection techniques, with automatic updates to threat intelligence, removing the need for manual signature updates.

NEW QUESTION # 257

A company uses Falcon Cloud Security to enforce policies for AWS, Azure, and Google Cloud environments. The security team wants to create a policy that ensures all storage buckets across these cloud providers are not publicly accessible.

What should be the scope of the security policy to achieve this?

- **A. Apply a multi-cloud policy with the "Storage Security" category.**
- B. Apply the policy to AWS only.
- C. Apply the policy to Azure only.
- D. Apply separate policies for each cloud provider with the "Network Security" category.

Answer: A

Explanation:

Option A: While creating separate policies for each cloud provider is technically possible, using the "Network Security" category would not directly address storage bucket accessibility. It would unnecessarily complicate policy management.

Option B: Multi-cloud policies in Falcon Cloud Security allow the creation of unified rules across AWS, Azure, and GCP. The "Storage Security" category is specifically designed for securing storage buckets, ensuring that they are not publicly accessible.

Option C: Limiting the policy to AWS would not ensure protection for storage buckets in Azure and GCP.

The requirement specifies a multi-cloud approach.

Option D: Focusing solely on Azure would leave AWS and GCP buckets unprotected, violating the stated requirement.

NEW QUESTION # 258

How can you delete a registry connection from the CrowdStrike Falcon console without affecting other registry connections?

- A. Use the "Bulk Delete" option to remove all registry connections, including the one you want to delete.
- **B. Navigate to the "Image Assessment" page, select the specific registry connection, and click "Delete."**
- C. Disable the "Image Assessment" feature globally and then remove the registry details.
- D. Remove all associated images from the registry before attempting to delete the connection.

Answer: B

Explanation:

Option A: Deleting associated images from the registry is not a prerequisite for removing a registry connection in CrowdStrike. The connection can be removed independently.

Option B: The "Image Assessment" page allows users to manage individual registry connections.

Deleting a specific connection can be done here without affecting other connections.

Option C: Disabling "Image Assessment" globally is not required to delete a specific registry connection. This action would unnecessarily impact all registry integrations.

Option D: The "Bulk Delete" option removes all registry connections, which is not suitable if you only want to delete one specific connection.

NEW QUESTION # 259

.....

The most notable feature of our CCCS-203b learning quiz is that they provide you with the most practical solutions to help you learn the exam points of effortlessly and easily, then mastering the core information of the certification course outline. Their quality of our CCCS-203b Study Guide is much higher than the quality of any other materials, and questions and answers of CCCS-203b training

CCCS-203b Free Practice Exams: <https://www.dumpstorrent.com/CCCS-203b-exam-dumps-torrent.html>

We pretty much took everything that we were being offered, CCCS-203b Caveats and Limitations, We promise we will never share your information to the third part without your permission.

Covers 100% Composite Exams CCCS-203b Critical Information

[illegible]