

CrowdStrike CCCS-203b Authentic Exam Questions - Valid Test CCCS-203b Vce Free



We also offer a free demo version that gives you a golden opportunity to evaluate the reliability of the CrowdStrike Certified Cloud Specialist (CCCS-203b) exam study material before purchasing. Vigorous practice is the only way to ace the CrowdStrike Certified Cloud Specialist (CCCS-203b) test on the first try. And that is what TrainingDumps CrowdStrike CCCS-203b practice material does. Each format of updated CrowdStrike CCCS-203b preparation material excels in its way and helps you pass the CrowdStrike Certified Cloud Specialist (CCCS-203b) examination on the first attempt.

Being devoted to this area for over ten years, our experts keep the excellency of our CrowdStrike Certified Cloud Specialist exam question like always. They are distinguished experts in this area who can beef up your personal capacity. By cutting through the clutter of tremendous knowledge, they picked up the essence into our CCCS-203b guide prep. Up to now our CCCS-203b real exam materials become the bible of practice material of this industry. Ten years have gone, and three versions have been made for your reference. They made the biggest contribution to the efficiency and quality of our CrowdStrike Certified Cloud Specialist practice materials, and they were popularizing the ideal of passing the exam easily and effectively. All CCCS-203b Guide prep is the successful outcomes of professional team.

>> CrowdStrike CCCS-203b Authentic Exam Questions <<

Valid Test CCCS-203b Vce Free | Valid CCCS-203b Test Registration

Overall, CCCS-203b is committed to helping candidates achieve success in the CrowdStrike CCCS-203b exam. Their goal is to save students time and money, and they guarantee that candidates who use their product will pass the CCCS-203b Exam on their first try. With the right study material and support team, passing the exam at the first attempt is an achievable goal.

CrowdStrike Certified Cloud Specialist Sample Questions (Q227-Q232):

NEW QUESTION # 227

While auditing a cloud image configured for deployment, which of the following findings represents a deployment misconfiguration?

- A. The image includes unused software packages.
- B. The image uses a private container registry with role-based access control (RBAC).

- C. The image has labels for versioning and maintainability metadata.
- D. The image lacks a health check directive in the Dockerfile.

Answer: A

Explanation:

Option A: While missing a health check directive is not ideal for production readiness, it is not a security misconfiguration. Health checks are primarily for operational monitoring and ensuring high availability.

Option B: This is a best practice to ensure only authorized users can access the image. It strengthens the security of the deployment pipeline and does not represent a misconfiguration.

Option C: Adding labels for versioning and maintainability metadata (e.g., LABEL version="1.0") is a best practice. It aids in managing image lifecycles and troubleshooting deployments. This does not constitute a misconfiguration.

Option D: Including unused software packages increases the attack surface and may introduce unnecessary vulnerabilities. Attackers could exploit unmaintained or outdated components, even if they are not actively used by the application. Removing unnecessary packages during the build process is a key security best practice.

NEW QUESTION # 228

As a security analyst, you are tasked with assessing the asset inventory in the CrowdStrike Falcon platform. You notice several unmanaged assets appearing in the inventory, identified only by IP addresses.

Which of the following actions would be the most appropriate to take next?

- A. Ignore these assets, as they are likely non-critical devices.
- **B. Activate Falcon sensor deployment to ensure visibility and management.**
- C. Block these IP addresses at the firewall to mitigate any potential threats.
- D. Tag the assets as "unmanaged" and move on to the next task.

Answer: B

Explanation:

Option A: Simply tagging the devices without further action does not address the potential security risks associated with unmanaged assets. Additional steps, such as identifying and deploying the Falcon sensor, are required.

Option B: Unmanaged devices pose significant security risks, regardless of their perceived criticality. Ignoring them could lead to blind spots in your security posture.

Option C: Blocking these devices at the firewall could disrupt legitimate operations, particularly if they are critical to business processes. Investigating and managing them is a better approach.

Option D: Deploying the Falcon sensor is the most appropriate action to ensure these unmanaged assets are properly monitored and secured. Without the Falcon sensor, these devices remain unprotected and could serve as attack vectors. This step ensures they are brought under management and included in the asset inventory for continuous monitoring.

NEW QUESTION # 229

Which of the following steps is essential when configuring an automated remediation dry run in CrowdStrike Falcon?

- **A. Select a limited scope of affected resources to prevent wide-scale simulation**
- B. Enable enforcement mode to simulate real-world remediation
- C. Integrate third-party tools for enhanced dry run reporting
- D. Schedule the dry run to occur only during off-peak hours

Answer: A

Explanation:

Option A: While integration with third-party tools may enhance monitoring and reporting, it is not essential for performing a dry run. The primary goal of a dry run is to validate the workflow within the platform.

Option B: When performing a dry run, it is important to limit the scope of affected resources to ensure the simulation is manageable and does not inadvertently include unnecessary or unrelated areas. This allows for precise evaluation of the workflow's effectiveness and helps in identifying issues without impacting the overall environment.

Option C: While off-peak scheduling may reduce operational overhead, it is not an essential requirement for dry runs. The focus is on testing the workflow, regardless of the time it is run.

Option D: Enforcement mode is used for applying actual remediation actions, not for a dry run. A dry run avoids execution of real-world actions, focusing solely on simulation.

NEW QUESTION # 230

You are tasked with creating a custom compliance framework within the CrowdStrike platform.

Which of the following steps is essential to ensure the framework meets organizational compliance needs and remains adaptable over time?

- A. Define a baseline of security controls aligned with existing regulatory standards.
- B. Enable monitoring for endpoints but exclude periodic reporting.
- C. Limit the framework to addressing only one regulatory standard at a time.
- D. Use default CrowdStrike compliance templates without modifications.

Answer: A

Explanation:

Option A: Defining a baseline of security controls is a critical step in creating a custom compliance framework. This ensures that the framework aligns with existing regulations, industry standards, and organizational needs. A well-defined baseline also serves as a reference point for evaluating the effectiveness of the framework over time. Misalignment with regulations can lead to compliance gaps and legal repercussions.

Option B: Default templates provide a starting point, but they must be tailored to the organization's specific needs, regulatory landscape, and operational requirements. Using them without modifications may result in an incomplete or misaligned compliance framework.

Option C: A compliance framework should ideally address multiple standards, especially when overlaps exist, to streamline efforts and reduce redundancy. Limiting the scope to one standard at a time is inefficient and can increase operational complexity.

Option D: While endpoint monitoring is essential, excluding periodic reporting undermines the framework's ability to demonstrate ongoing compliance. Reporting helps identify deviations from compliance and facilitates audits.

NEW QUESTION # 231

After deploying the Falcon Container Sensor in your Kubernetes cluster, your team wants to understand its primary use cases.

Which of the following is a primary function of the Falcon Container Sensor in Kubernetes?

- A. Deploying application code to Kubernetes clusters securely.
- B. Automatically scaling Kubernetes pods based on security threats.
- C. Encrypting all data stored in Kubernetes Persistent Volumes (PVs).
- D. Monitoring container runtime activity and detecting malicious behavior.

Answer: D

Explanation:

Option A: The primary function of the Falcon Container Sensor is to monitor container runtime activity, identify anomalies, and detect potential threats or malicious behavior.

Option B: The Falcon Container Sensor does not control pod scaling. Kubernetes itself handles scaling based on resource usage, not security threats.

Option C: The sensor does not encrypt data in Persistent Volumes. Data encryption is managed by the storage provider or Kubernetes itself, not by the Falcon Container Sensor.

Option D: The Falcon Container Sensor is not responsible for deploying application code. It focuses on securing containerized workloads rather than application delivery.

NEW QUESTION # 232

.....

Our CCCS-203b exam questions are highly praised for their good performance. Customers often value the functionality of the product. After a long period of research and development, our CCCS-203b learning materials have been greatly optimized. We can promise you that all of our CCCS-203b practice materials are completely flexible. In addition, we have experts who specialize in research optimization, constantly update and improve our learning materials, and then send them to our customers. We take client's advice on CCCS-203b training prep seriously and develop it with the advices.

Valid Test CCCS-203b Vce Free: https://www.trainingdumps.com/CCCS-203b_exam-valid-dumps.html

CrowdStrike CCCS-203b Authentic Exam Questions It won't happen if you name them and we don't have them, After your

Improve Student Comprehension with a Client-first Approach to CCCS-203b Data Structures, The same rule applies on the outbound side, It won't happen if you name them and we don't have them.

CCCS-203b reliable test collection & CCCS-203b latest exam guide & CCCS-203b exam study solutions

[illegible]