Perfect CCCS-203b Latest Exam Experience - Easy and Guaranteed CCCS-203b Exam Success

CrowdStrike CCCS-203b Certification has great effect in this field and may affect your career even future. CrowdStrike Certified Cloud Specialist real questions files are professional and high passing rate so that users can pass the exam at the first attempt. High quality and pass rate make us famous and growing faster and faster.

CrowdStrike CCCS-203b Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• Pre-Runtime Protection: This domain covers managing registry connections, selecting image assessment methods, and analyzing assessment reports to identify malware, CVEs, leaked secrets, Dockerfile misconfigurations, and vulnerabilities before deployment.
Topic 3	• 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 4	• 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 5	• 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 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.

Test CCCS-203b Result, CCCS-203b Test Engine

The version of APP and PC of our CCCS-203b exam torrent is also popular. They can simulate real operation of test environment and users can test CCCS-203b test prep in mock exam in limited time. They are very practical and they have online error correction and other functions. The characteristic that three versions of CCCS-203b Exam Torrent all have is that they have no limit of the number of users, so you don't encounter failures anytime you want to learn our CCCS-203b quiz guide. The three different versions can help customers solve any questions and meet their all needs.

CrowdStrike Certified Cloud Specialist Sample Questions (Q347-Q352):

NEW QUESTION # 347
What capability does the Kubernetes Admission Controller provide within CrowdStrike Falcon Cloud Security?

- A. Encrypts data in motion
- B. Monitors IAM user behavior
- C. Schedules container scans
- D. Blocks or allows container deployments based on policy

Answer: D

NEW QUESTION # 348
Which of the following scenarios represents a security risk that CrowdStrike Identity Analyzer (CIEM) is designed to identify and address?

- A. A network security group is configured to allow inbound traffic on port 443
- B. An IAM role with permissions to delete all cloud resources is assigned to multiple non-human identities
- C. A serverless function has a concurrency limit set to 100 executions
- D. An encrypted storage bucket is accessed by an authorized application

Answer: B

Explanation:
Option A: Allowing inbound traffic on port 443 (HTTPS) is a standard practice for secure web services. While this could be a misconfiguration if unnecessary, it falls under network security rather than identity management, which is the focus of CIEM.
Option B: Concurrency settings relate to resource performance and scalability, not identity or entitlement management. CIEM does not monitor or manage execution limits for serverless functions.
Option C: CIEM is specifically designed to detect and analyze overly permissive roles and identities, particularly when sensitive permissions (like resource deletion) are assigned to multiple non-human identities. This scenario poses a significant security risk if those identities are compromised or misused.
Option D: This is an expected and secure behavior when proper access policies are in place.
CIEM would not flag this as an issue since the access is authorized and aligns with standard operational practices.

NEW QUESTION # 349
Which of the following is a requirement for deploying the Kubernetes and Container Sensor in a Kubernetes cluster?

- A. The cluster must have at least three nodes with GPU support.
- B. The sensor requires a DaemonSet to be deployed within the Kubernetes cluster.
- C. The cluster must have the kube-proxy component disabled.
- D. All workloads in the cluster must use privileged containers.

Answer: B

Explanation:
Option A: Requiring all workloads to use privileged containers would create unnecessary security risks. The Kubernetes and Container Sensor can secure non-privileged containers, which is the recommended best practice for containerized workloads.
Option B: Disabling the kube-proxy component is not required for deploying the Kubernetes and Container Sensor. Kube-proxy is an essential component of Kubernetes networking, and its removal would break cluster functionality.
Option C: The Kubernetes and Container Sensor is typically deployed as a DaemonSet to ensure that a sensor pod is running on each node in the Kubernetes cluster. This enables comprehensive monitoring and threat detection across all workloads in the cluster. The DaemonSet is a standard Kubernetes construct for deploying cluster-wide services.
Option D: GPU support is not a requirement for deploying the Kubernetes and Container Sensor.
GPU nodes are only necessary for specific workloads, such as machine learning applications, and are unrelated to the sensor's deployment.

NEW QUESTION # 350
You want to customize the GKE autopilot policy by updating the detection severity (Critical) and the detection type (CIS benchmark deviation) along with Vulnerability ExPRT.ai severities (Critical).
Which combination will trigger the prevention?

- A. Vulnerability ExPRT.ai severities (Critical), Detection severity (Critical), Image misconfigurations
- B. Vulnerability ExPRT.ai severities (Critical), Detection severity (Critical)
- C. Vulnerability ExPRT.ai severities (Critical), Detection severity (Critical), Detection type (CIS benchmark deviation)

Answer: C

Explanation:
InFalcon Cloud Security, prevention actions are triggered whenall configured enforcement criteriawithin a policy are met. When customizing theGKE Autopilot policy, enforcement requires alignment across vulnerability intelligence, detection severity, and compliance context.
By setting:
* Vulnerability ExPRT.ai severity = Critical
* Detection severity = Critical
* Detection type = CIS benchmark deviation
you ensure that bothrisk-based vulnerability intelligenceandcompliance deviation severitythresholds are satisfied. This combination confirms that the issue is not only severe but also represents a critical deviation from an accepted security benchmark, justifying prevention.
Omitting the detection type or replacing it with image misconfiguration alone does not meet the enforcement logic required for policy-triggered prevention.
Therefore,Option Cis the correct combination that triggers prevention.

NEW QUESTION # 351
Which feature of the CrowdStrike Identity Analyzer enables administrators to identify privileged accounts that are not protected by multi-factor authentication (MFA)?

- A. Privilege Monitoring Dashboard
- B. Privileged Account MFA Audit
- C. Non-MFA Account Report
- D. Account Activity Insights

Answer: B

Explanation:
Option A: The Privileged Account MFA Audit feature is specifically designed to analyze privileged accounts and identify those that are not secured by MFA. This is the most accurate tool for the scenario described.
Option B: This feature focuses on user behavior and activity trends, such as login attempts or API usage. It does not assess MFA status or privilege levels, making it unsuitable for this task.
Option C: Although this may sound relevant, there is no dedicated "Non-MFA Account Report" feature in the CrowdStrike Identity Analyzer. This option may confuse users who assume generic reporting capabilities include MFA-specific filters.
Option D: While the Privilege Monitoring Dashboard provides insights into privileged accounts, it does not specifically identify whether these accounts are protected by MFA. Its focus is on tracking access levels and changes to privilege assignments.

NEW QUESTION # 352
.....