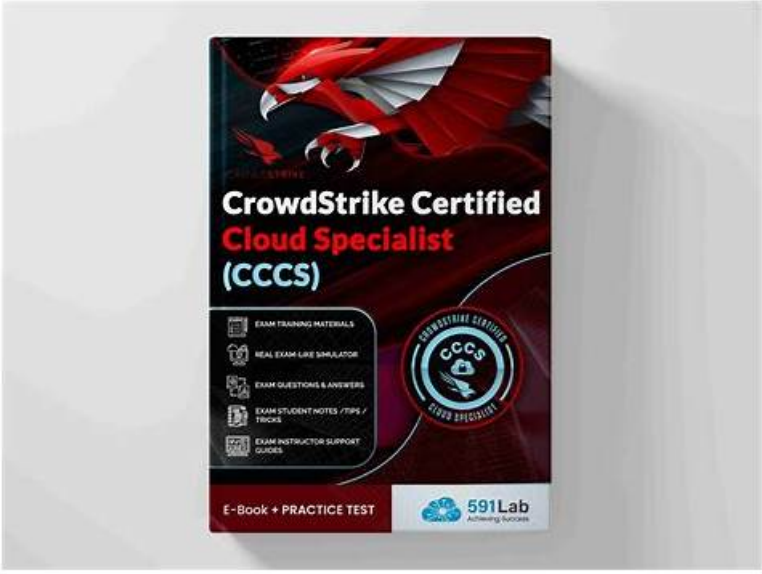
CrowdStrike Certified Cloud Specialist Updated Study Material & CCCS-203b Online Test Simulator & CrowdStrike Certified Cloud Specialist Valid Exam Answers



Actual4Cert regularly updates CrowdStrike Certified Cloud Specialist (CCCS-203b) practice exam material to ensure that it keeps in line with the test. In the same way, Actual4Cert provides a free demo before you purchase so that you may know the quality of the CrowdStrike Certified Cloud Specialist (CCCS-203b) dumps. Similarly, the Actual4Cert CrowdStrike Certified Cloud Specialist (CCCS-203b) practice test creates an actual exam scenario on each and every step so that you may be well prepared before your actual CrowdStrike Certified Cloud Specialist (CCCS-203b) examination time. Hence, it saves you time and money.

CrowdStrike CCCS-203b Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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	• 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.

Latest Upload CrowdStrike CCCS-203b Exam Objectives Pdf: CrowdStrike Certified Cloud Specialist | CCCS-203b Downloadable PDF

It is acknowledged that there are numerous CCCS-203b learning questions for candidates for the exam, however, it is impossible for you to summarize all of the key points in so many materials by yourself. But since you have clicked into this website for CCCS-203b practice materials you need not to worry about that at all because our company is especially here for you to solve this problem. With our CCCS-203b Exam Questions, you will pass your exam just in one go for we are the most professional team in this career for over ten years.

CrowdStrike Certified Cloud Specialist Sample Questions (Q358-Q363):

NEW QUESTION # 358
Your organization is onboarding a new multi-cloud environment with AWS, Azure, and Google Cloud. The security team wants to ensure that all cloud accounts are registered efficiently while maintaining strong security controls.
Which of the following methods is the most secure and efficient approach for registering cloud accounts in this scenario?

- A. Leverage single sign-on (SSO) integration with multi-factor authentication (MFA) for automatic registration.
- B. Manually register each cloud account separately in the CrowdStrike Falcon platform.
- C. Use API-based bulk registration with role-based access controls (RBAC).
- D. Allow users to self-register their cloud accounts using an open registration link.

Answer: C

Explanation:
Option A: Manually registering each cloud account separately is inefficient, especially in multi- cloud environments. This method does not scale well and is prone to human error, increasing the risk of misconfigurations.
Option B: Allowing users to self-register through an open registration link poses significant security risks. It can lead to unauthorized access and increases the attack surface, making the environment susceptible to account takeovers.
Option C: While SSO with MFA enhances authentication security, it is not specifically designed for cloud account registration. It may be useful for user authentication but does not provide the automation and scalability required for efficient multi-cloud registration.
Option D: Using API-based bulk registration with RBAC ensures a secure and automated process, reducing manual effort and enforcing least privilege access. RBAC allows for fine- grained permissions, ensuring only authorized entities can register cloud accounts.

NEW QUESTION # 359
What is a primary function of the Containers and Images Compliance dashboard in CrowdStrike's Cloud Security platform?

- A. Tracks the network performance of containers and provides detailed network usage data
- B. Displays the list of all containers that are unsupported by Falcon Cloud Security with Containers
- C. Provides a visual summary of compliance across containers and images
- D. Allows users to automatically patch non-compliant containers and images

Answer: C

Explanation:
TheContainers and Images Compliance dashboardinFalcon Cloud Securityis designed to give security and DevOps teams avisual, aggregated view of compliance postureacross container images and running containers.
This dashboard summarizes compliance status against benchmarks such asCIS, organizational policies, and security best practices. It highlights compliant versus non-compliant images and containers, severity distribution, and trending risk, enabling teams to quickly assess overall posture and prioritize remediation.
The dashboard does not perform network monitoring, automatic patching, or unsupported container enumeration. Those functions are handled by other Falcon modules or operational workflows.
Therefore, itsprimary functionis toprovide a visual summary of compliance across containers and images
, makingOption Acorrect.

NEW QUESTION # 360
You are tasked with creating a Falcon Fusion workflow to notify your cloud operations team when a new detection is triggered for an unapproved cloud policy violation. What is the first step you should take in setting up this workflow?

- A. Select "Create New Workflow" from the Falcon Fusion console.
- B. Configure the notification channels for the cloud operations team.
- C. Define the trigger conditions for the workflow.
- D. Enable auto-remediation for the policy violation.

Answer: A

Explanation:
Option A: Configuring notification channels is a critical step, but it occurs after the initial workflow creation. Jumping directly to this step skips foundational aspects like defining triggers and conditions.
Option B: Triggers are vital to the workflow, but they can only be defined after the workflow has been created. Defining triggers before creating the workflow is not possible in Falcon Fusion.
Option C: Auto-remediation is an optional feature that can be added to a workflow, but it is not a required or initial step when creating a workflow.
Option D: The first step in creating a Falcon Fusion workflow is to select "Create New Workflow" from the Falcon Fusion console. This is where the entire workflow configuration process begins.
Starting here allows you to define subsequent steps like triggers, actions, and notification methods. Many users mistakenly believe they should start by configuring notification channels or defining triggers, but those steps come later in the workflow setup process.

NEW QUESTION # 361
When using the Identity Analyzer feature in CrowdStrike CIEM to identify inactive users, which data source is primarily used to assess inactivity?

- A. CrowdStrike Falcon sensor telemetry.
- B. Historical security alerts from CrowdStrike Falcon.
- C. Network traffic logs from connected endpoints.
- D. Audit trails of API calls and resource utilization.

Answer: D

Explanation:
Option A: Network traffic logs are related to endpoint or network-level activity, not specific to cloud identities or IAM behavior. CIEM focuses on cloud-specific activity data like API calls and resource usage, making this an irrelevant data source.
Option B: Security alerts focus on threats and anomalies, not routine user activity patterns. CIEM uses operational data like API calls and resource usage to assess inactivity, which makes security alerts irrelevant for this purpose.
Option C: Falcon sensor telemetry is used for endpoint detection and response, not cloud IAM activity. While it complements CIEM for overall security, it does not directly contribute to inactivity analysis.
Option D: CIEM's Identity Analyzer uses audit trails, including API call records and resource utilization data, to detect inactivity. This ensures a holistic understanding of user behavior and accurately identifies users who no longer engage with cloud resources. This approach reduces false positives and enhances the security posture by identifying legitimate inactive accounts.

NEW QUESTION # 362
What is a key benefit of Falcon Cloud Security's integration of its components within a single platform?

- A. It eliminates the need for traditional SIEM tools by storing all security logs in the Falcon platform.
- B. It allows for seamless encryption of all cloud data, ensuring compliance with GDPR and CCPA.
- C. It reduces the need for manual threat analysis by leveraging AI-powered threat detection and response.
- D. It provides a built-in firewall to secure cloud environments against external attacks.

Answer: C

Explanation:
Option A: While encryption is a critical aspect of cloud security, Falcon Cloud Security does not perform data encryption. Instead, it provides unified visibility, detection, and protection across cloud workloads and environments.
Option B: Falcon Cloud Security integrates with SIEM tools to enhance security operations but does not replace them entirely. It

collects telemetry and threat data, which can be shared with SIEM solutions for deeper analysis.
Option C: Falcon Cloud Security integrates AI and machine learning to automate threat detection and response, reducing the manual workload for security teams. This is a primary benefit of its unified platform approach.
Option D: Falcon Cloud Security is not a firewall. Instead, it focuses on endpoint protection, workload security, and threat detection, which complement network-based tools like firewalls.

NEW QUESTION # 363
......

Many students often start to study as the exam is approaching. Time is very valuable to these students, and for them, one extra hour of study may mean 3 points more on the test score. If you are one of these students, then CrowdStrike Certified Cloud Specialist exam tests are your best choice. Because students often purchase materials from the Internet, there is a problem that they need transport time, especially for those students who live in remote areas. When the materials arrive, they may just have a little time to read them before the exam. However, with CCCS-203b Exam Questions, you will never encounter such problems, because our materials are distributed to customers through emails.

CCCS-203b Downloadable PDF: https://www.actual4cert.com/CCCS-203b-real-questions.html