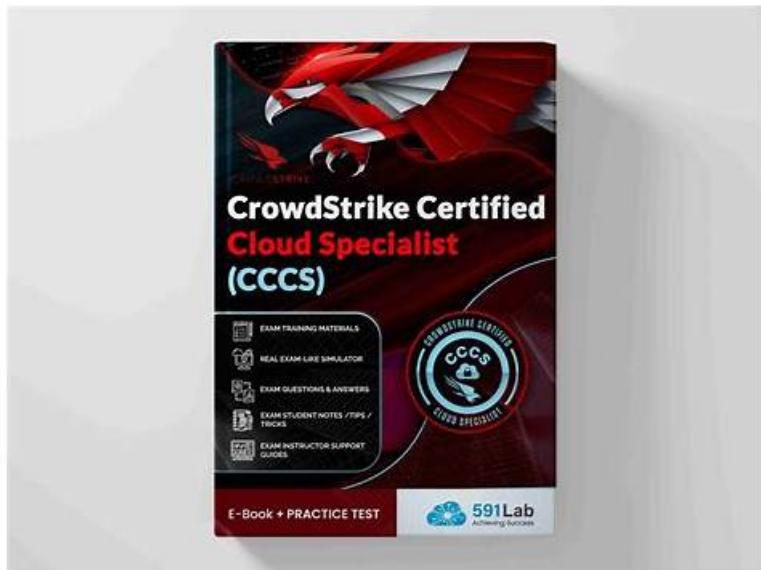# Pass Your CCCS-203b CrowdStrike Certified Cloud Specialist Exam on the First Try with VCE4Plus

Our company keeps pace with contemporary talent development and makes every learners fit in the needs of the society. Based on advanced technological capabilities, our CCCS-203b study materials are beneficial for the masses of customers. Our experts have plenty of experience in meeting the requirement of our customers and try to deliver satisfied CCCS-203b Exam guides to them. Our CCCS-203b exam prepare is definitely better choice to help you go through the test.

Our CCCS-203b study guide is verified by professional expert, therefore they cover the most of knowledge points. By using the exam dumps of us, you can get a full training for the exam. CCCS-203b exam dumps also have free update for 365 days after payment, and the update version will send to your email automatically. Furthermore, we have the online and offline chat service stuff, they can give you reply of your questions about the CCCS-203b Exam Dumps. Also, you can send your problem by email, we will give you answer as quickly as we can.

>> New CCCS-203b Test Question <<

Reliable CCCS-203b Exam Camp & CCCS-203b Valid Learning Materials

VCE4Plus is a very wonderful and effective platform to give chances to our worthy clients who want to achieve their expected scores and gain their CCCS-203b certifications. With our professional experts' tireless efforts, ourCCCS-203b exam torrent is equipped with a simulated examination system with timing function, allowing you to examine your learning results at any time, keep checking for defects, and improve your strength. Whether you are a student or an office worker, you can be satisfied here, and you will never regret if you choose our CCCS-203b Exam Torrent.

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	• 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	• 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	• 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 5	• 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.
Topic 6	• 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.

CrowdStrike Certified Cloud Specialist Sample Questions (Q21-Q26):

NEW QUESTION # 21
Which of the following is a requirement for enabling the Kubernetes Admission Controller for the CrowdStrike Kubernetes and Container Sensor?

- A. Pod-level annotations must be added to all running workloads.
- B. The Admission Controller requires direct integration with the underlying host operating system kernel.
- C. Role-Based Access Control (RBAC) must be configured to grant the Admission Controller permissions to intercept and modify API requests.
- D. The Admission Controller must be deployed as a Custom Resource Definition (CRD).

Answer: C

Explanation:
Option A: The Kubernetes Admission Controller requires appropriate RBAC permissions to function correctly. These permissions allow it to validate and enforce policies by intercepting and potentially modifying API requests to the Kubernetes API server. Without the correct RBAC configuration, the Admission Controller cannot enforce security controls or policies effectively.
Option B: While annotations might be used for other configuration purposes, they are not a requirement for enabling the Admission Controller.
Option C: This is incorrect because Admission Controllers are not CRDs. They are built-in or webhook-based components of Kubernetes.
Option D: This is incorrect as Admission Controllers operate at the API level and have no dependency on the host operating system kernel.

NEW QUESTION # 22
While reviewing a container image for vulnerabilities, which of the following steps ensures that vulnerabilities in installed software packages are detected and addressed effectively?

- A. Checking for updates to the container orchestration platform.
- B. Running a static analysis scan on the container image.
- C. Relying on the image author's documentation to identify vulnerabilities.
- D. Comparing the image against a trusted, verified base image.

Answer: B

Explanation:
Option A: Image authors may provide useful information, but relying solely on their documentation is risky. They might not have updated their documentation with the latest vulnerability information, and the analysis would lack thoroughness.
Option B: While keeping the orchestration platform updated is important, this does not address vulnerabilities within the container image itself. The two are separate layers of the container ecosystem.
Option C: Static analysis scanning tools are purpose-built to analyze container images for vulnerabilities in installed packages, libraries, and dependencies. They use vulnerability databases (e.g., CVE databases) to identify known issues, enabling you to patch or replace insecure packages before deploying the image.
Option D: Comparing images can help identify deviations but does not specifically identify vulnerabilities in installed packages. A static analysis scan is more comprehensive and accurate for this purpose.

NEW QUESTION # 23

Which of the following is the correct method to obtain credentials from an approved container registry for image assessment in Falcon Cloud Security?

- A. Download the credentials file from the Falcon Cloud Security dashboard.
- B. Manually retrieve credentials from the Kubernetes Secret store.
- C. Use the CLI tool provided by the container registry to generate a service account token.
- D. Enable auto-login for the container registry using Docker Hub credentials.

Answer: C

Explanation:

Option A: Most container registries, such as Amazon ECR, Google Container Registry (GCR), or Docker Hub, provide CLI tools or APIs to generate service account tokens for programmatic access. This is the standard way to securely retrieve credentials for integration with Falcon Cloud Security.

Option B: Manually retrieving credentials from Kubernetes Secrets is error-prone and may not comply with security best practices for accessing registries.

Option C: Auto-login features like Docker's CLI-based credential storage are not suitable for enterprise-grade security and are not part of the approved procedure for image assessments.

Option D: The Falcon Cloud Security dashboard does not provide registry credentials. Users must retrieve these credentials directly from the container registry.

NEW QUESTION # 24

Which of the following steps is required to successfully integrate the Falcon CWPP Image Scanning Script with a CI/CD pipeline for image assessment?

- A. Use the Falcon API to fetch a unique API token and store it in the pipeline configuration file.
- B. Modify the pipeline script to execute the Image Scanning Script during the post-deployment phase.
- C. Schedule the script to run daily on the production environment's container images.
- D. Install the Falcon CWPP agent on all developer machines.

Answer: A

Explanation:

Option A: Image scanning should occur before deployment to identify vulnerabilities early in the development lifecycle. Running the script post-deployment defeats the purpose of proactive security measures.

Option B: While the Falcon CWPP agent is part of the larger CrowdStrike solution, it is not required for the Image Scanning Script's integration into a CI/CD pipeline. The scanning process is executed during pipeline stages and doesn't depend on agents on developer machines.

Option C: Image assessments should be part of the CI/CD pipeline to detect vulnerabilities during development. Running scans on production images introduces unnecessary risk and is not the intended use case of the Image Scanning Script.

Option D: To authenticate the Image Scanning Script with the Falcon platform, a unique API token is required. This token allows secure communication between the CI/CD pipeline and the Falcon API, enabling image assessments to occur seamlessly. Failure to include this step results in authentication issues, causing the script to fail.

NEW QUESTION # 25

After performing an image assessment in Falcon Cloud Security, which of the following is a typical actionable recommendation?

- A. Disable unused Kubernetes Admission Controllers.
- B. Limit the number of pods per node to prevent resource exhaustion.
- C. Update container images to address identified critical vulnerabilities.
- D. Apply a pod security policy to restrict privileged containers.

Answer: C

Explanation:

Option A: Admission Controllers provide security and compliance enforcement, and disabling them would reduce security posture rather than align with image assessment results.

Option B: Applying pod security policies is a general security best practice but is not directly derived from an image assessment.
Option C: Image assessments identify vulnerabilities and provide actionable recommendations, such as updating base images or dependencies to mitigate critical security risks.
Option D: Limiting pods per node is a capacity management measure, not an outcome of image assessments focused on vulnerabilities.

NEW QUESTION # 26
......

To become more powerful and struggle for a new self, getting a professional CCCS-203b certification is the first step beyond all questions. We suggest you choose our CCCS-203b test prep ----an exam braindump leader in the field. Since we release the first set of the CCCS-203b quiz guide, we have won good response from our customers and until now---a decade later, our products have become more mature and win more recognition. And our CCCS-203b Exam Torrent will also be sold at a discount from time to time and many preferential activities are waiting for you.