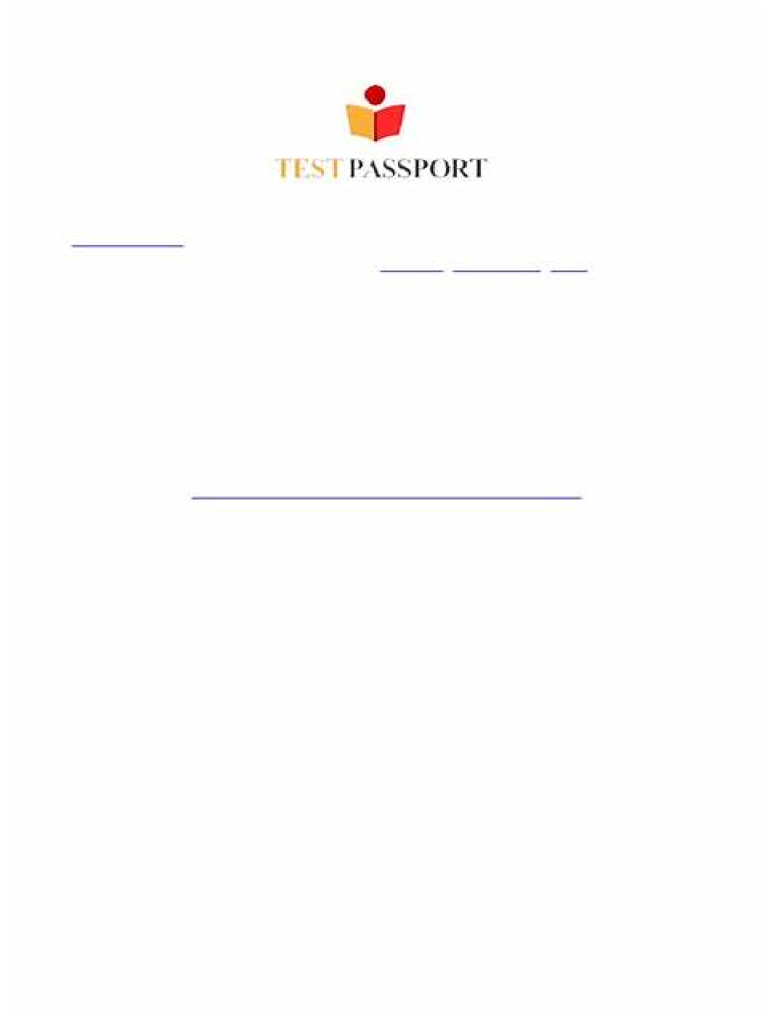
CCCS-203b Exam Online - Exam CCCS-203b Flashcards



The client can try out and download our CCCS-203b training materials freely before their purchase so as to have an understanding of our product and then decide whether to buy them or not. The website pages of our product provide the details of our CCCS-203b learning questions. You can see the demos which are part of the all titles selected from the test bank and the forms of the questions and answers and know the form of our software on the website pages of our study materials.

CrowdStrike CCCS-203b Exam Syllabus Topics:

Topic	Details
Topic 1	- 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 2	- 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 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	- 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.

>> CCCS-203b Exam Online <<

Exam CCCS-203b Flashcards - Latest CCCS-203b Exam Bootcamp

You can set time to test your study efficiency, so that you can accomplish your test within the given time when you are in the real CCCS-203b exam. Moreover, you can adjust yourself to the exam speed and stay alert according to the time-keeper that we set on our CCCS-203b training materials. Therefore, you can trust on our CCCS-203b Study Guide for this effective simulation function will eventually improve your efficiency and assist you to succeed in the CCCS-203b exam. Just have a try on our free demo of CCCS-203b exam questions!

CrowdStrike Certified Cloud Specialist Sample Questions (Q285-Q290):

NEW QUESTION # 285
An organization has a custom IOM rule in Falcon Cloud Security to detect SSH connections from unauthorized IP addresses.
However, the security team needs to update the rule to exclude a newly added internal IP range.
What is the correct way to update this rule?

- A. Delete the existing IOM rule and create a new one with the updated IP range.
- B. Edit the IOM rule directly in the Falcon Cloud Security Console.
- C. Disable the IOM rule and configure AWS Security Groups to handle IP whitelisting instead.
- D. Use the Falcon CLI to modify the IOM rule in the underlying infrastructure.

Answer: B

Explanation:
Option A: Deleting and recreating the rule is inefficient and could lead to downtime or loss of historical data. The rule should be edited instead.
Option B: There is no CLI functionality for modifying IOM rules in Falcon Cloud Security. All IOM rule management is handled through the console.
Option C: Falcon Cloud Security provides a straightforward interface for editing existing custom IOM rules, including modifying IP ranges or other parameters.
Option D: AWS Security Groups are not a replacement for Falcon Cloud Security's IOM rules.
Security Groups are limited to network-level access control and do not offer the runtime detection capabilities of IOM rules.

NEW QUESTION # 286
What is the most critical prerequisite when registering a cloud account with CrowdStrike Falcon?

- A. A dedicated IAM role or user with the appropriate permissions must be created and configured for integration.
- B. The cloud account must have administrator-level access to all resources within the environment.
- C. The Falcon agent must be installed on all virtual machines in the cloud account before registration.
- D. All cloud account users must be enrolled in Falcon platform authentication prior to registration.

Answer: A

Explanation:
Option A: It is not necessary for all users in the cloud account to be enrolled in Falcon platform authentication. Only the role or user performing the integration needs access.
Option B: Administrator-level access is not required and is considered a poor security practice.
CrowdStrike's design uses least-privilege access to minimize exposure.
Option C: To register a cloud account with CrowdStrike Falcon, a dedicated IAM role (for AWS) or service principal (for Azure) must be configured with the appropriate permissions for CrowdStrike integration. This ensures secure, granular access to the necessary resources for monitoring without over-provisioning access rights.
Option D: Installing the Falcon agent on virtual machines is not a prerequisite for account registration. The registration process focuses on cloud API integration, not individual agent deployment.

NEW QUESTION # 287

Your organization has identified several accounts that do not have Multi-Factor Authentication (MFA) enabled, using CrowdStrike's CIEM.
Which of the following actions would be the most effective first step to mitigate the security risk associated with these accounts?

- A. Set up an alert system to monitor non-MFA accounts for unusual activity.
- B. Assign "read-only" permissions to non-MFA accounts to limit their impact.
- C. Use CIEM to enforce MFA policies across all accounts.
- D. Disable all non-MFA accounts immediately to prevent unauthorized access.

Answer: C

Explanation:
Option A: Restricting permissions to "read-only" does not address the core issue of MFA enforcement. These accounts remain vulnerable to unauthorized access, especially if they are compromised.
Option B: Monitoring unusual activity is a reactive measure and does not mitigate the risk posed by non-MFA accounts. Proactively enforcing MFA policies is a better strategy for reducing exposure.
Option C: Using CIEM to enforce MFA policies ensures a consistent and automated approach to improving account security. This method reduces the likelihood of human error and applies a scalable solution to protect all accounts, aligning with best practices for cloud identity management.
Option D: While disabling non-MFA accounts might reduce risk temporarily, it can disrupt business operations. A more measured approach, such as enforcing MFA, is preferable to balance security and functionality.

NEW QUESTION # 288

A security team using CrowdStrike Falcon Runtime Protection wants to detect and respond to Indicators of Attack (IOAs) in their containerized environment. Which of the following is the best approach for detecting IOAs in real-time?

- A. Block all incoming network connections to containerized workloads to prevent potential attacks.
- B. Rely exclusively on Kubernetes audit logs to identify threats within the environment.
- C. Monitor system calls and process behaviors in runtime to detect anomalous activity indicative of an attack.
- D. Only analyze static container images for known vulnerabilities before deployment.

Answer: C

Explanation:
Option A: CrowdStrike Falcon Runtime Protection detects Indicators of Attack (IOAs) by monitoring system calls, process behaviors, and runtime activities in containers. This allows Falcon to identify anomalous activity, privilege escalation attempts, and suspicious behaviors indicative of an attack.
Option B: Blocking all network traffic would break legitimate communications and is not a practical security measure. Instead, Falcon applies behavioral analytics to detect suspicious network activity dynamically.
Option C: Static analysis alone is insufficient for detecting IOAs, as runtime threats may emerge after deployment, including zero-day attacks and living-off-the-land techniques.
Option D: While Kubernetes audit logs provide useful insights, they do not capture all IOAs, particularly those at the process and system call level within containers.

NEW QUESTION # 289

What happens to the data and alerts linked to a cloud account after it is deprovisioned from the Falcon console?

- A. All data and alerts associated with the account are immediately and permanently deleted.
- B. Data is archived for 30 days and then permanently deleted.
- C. Historical data and alerts remain accessible, but new data collection stops.
- D. The cloud account's data remains visible only if the account is re-registered within 7 days.

Answer: C

Explanation:
Option A: Data visibility is not tied to re-registration within a specific timeframe. Historical data is retained regardless of whether the account is re-registered or permanently deprovisioned. This answer introduces an unnecessary restriction.
Option B: CrowdStrike retains historical data for compliance and forensic purposes. Immediate and permanent deletion would

hinder post-deprovisioning investigations or audits, which is not the intended behavior of the Falcon platform.
Option C: There is no automatic data archival or deletion process tied to deprovisioning a cloud account in Falcon. Historical data remains accessible for an extended period, as determined by organizational data retention policies.
Option D: When a cloud account is deprovisioned from Falcon, the platform stops collecting new data and generating alerts for the account. However, historical data and alerts are retained for compliance and auditing purposes. This ensures organizations can review past activity and investigate incidents even after the account is deprovisioned.

NEW QUESTION # 290
......

Our CCCS-203b guide torrent has gone through strict analysis and summary according to the past exam papers and the popular trend in the industry and are revised and updated according to the change of the syllabus and the latest development conditions in the theory and the practice. The CCCS-203b exam questions have simplified the sophisticated notions. The software boosts varied self-learning and self-assessment functions to check the learning results. The software of our CCCS-203b Test Torrent provides the statistics report function and help the students find the weak links and deal with them.

Exam CCCS-203b Flashcards: https://www.testsdumps.com/CCCS-203b_real-exam-dumps.html

- CCCS-203b Reliable Exam Braindumps □ Certification CCCS-203b Test Answers □ Dumps CCCS-203b Free Download □ Search for ▸ CCCS-203b ◂ and obtain a free download on { www.vceengine.com } □CCCS-203b Reliable Exam Braindumps
- Pass Guaranteed 2026 CrowdStrike CCCS-203b: CrowdStrike Certified Cloud Specialist Unparalleled Exam Online □ Easily obtain free download of ✔ CCCS-203b □✔□ by searching on 【 www.pdfvce.com 】 □CCCS-203b Reliable Test Voucher
- Pass Guaranteed 2026 CrowdStrike CCCS-203b: CrowdStrike Certified Cloud Specialist Unparalleled Exam Online □ Copy URL □ www.pdfdumps.com □ open and search for ➡ CCCS-203b □□□ to download for free □Reliable CCCS-203b Exam Cram
- 100% Pass CrowdStrike - Accurate CCCS-203b - CrowdStrike Certified Cloud Specialist Exam Online □ Search for ▸ CCCS-203b ◂ and download exam materials for free through □ www.pdfvce.com □ □Exam Topics CCCS-203b Pdf
- Pass Guaranteed 2026 CrowdStrike CCCS-203b: CrowdStrike Certified Cloud Specialist Unparalleled Exam Online ⌨ 【 www.testkingpass.com 】 is best website to obtain ✔ CCCS-203b □✔□ for free download □Certification CCCS-203b Test Answers
- CrowdStrike Certified Cloud Specialist cexamkiller practice dumps - CCCS-203b test training reviews □ Open ➠ www.pdfvce.com □ and search for ➥ CCCS-203b □ to download exam materials for free ☮CCCS-203b Reliable Exam Braindumps
- CCCS-203b Training Online □ CCCS-203b Exam Topic □ CCCS-203b Training Online □ Search for 【 CCCS-203b 】 and obtain a free download on { www.testkingpass.com } □CCCS-203b Exam Topic
- Exam CCCS-203b Cost □ Certification CCCS-203b Test Answers □ Exam CCCS-203b Cost □ Search for □ CCCS-203b □ on 「 www.pdfvce.com 」 immediately to obtain a free download □CCCS-203b Latest Study Guide
- Reliable CCCS-203b Exam Cram □ CCCS-203b Practice Exam Online □ CCCS-203b Test Cram □ Download □ CCCS-203b □ for free by simply searching on ➤ www.validtorrent.com □ □Latest CCCS-203b Dumps Ppt
- Pass Guaranteed Quiz 2026 CrowdStrike CCCS-203b: CrowdStrike Certified Cloud Specialist – Reliable Exam Online □ Open website ☀ www.pdfvce.com □☀□ and search for ➥ CCCS-203b □ for free download □CCCS-203b Exam Topic
- Free PDF Quiz 2026 Marvelous CCCS-203b: CrowdStrike Certified Cloud Specialist Exam Online □ Download ➡ CCCS-203b □□□ for free by simply entering □ www.practicevce.com □ website □Exam Topics CCCS-203b Pdf
- interncorp.in, infocode.uz, www.stes.tyc.edu.tw, myportal.utt.edu.tt, lms.col1920.co.uk, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes