CCCS-203b덤프 & CCCS-203b최신인증시험공부자료

그리고 Itcertkr CCCS-203b 시험 문제집의 전체 버전을 클라우드 저장소에서 다운로드할 수 있습니다: https://drive.google.com/open?id=1eTKi66JqirKrvID2fP9WEdsFLV_W5XBY

Itcertkr는 고객님께서 첫번째CrowdStrike CCCS-203b시험에서 패스할수 있도록 최선을 다하고 있습니다. 만일 어떤 이유로 인해 고객이 첫 번째 시도에서 실패를 한다면, Itcertkr는 고객에게CrowdStrike CCCS-203b덤프비용 전액을 환불 해드립니다.환불보상은 다음의 필수적인 정보들을 전제로 합니다.

만일CrowdStrike CCCS-203b인증시험을 첫 번째 시도에서 실패를 한다면 CrowdStrike CCCS-203b덤프비용 전액을 환불 할 것입니다. 만일 고객이 우리 제품을 구입하고 첫 번째 시도에서 성공을 하지 못 한다면 모든 정보를 확인한 후에 구매 금액 전체를 환불 할 것 입니다. 이러한 방법으로 저희는 고객에게 어떠한 손해도 주지 않을 것을 보장합니다.

>> CCCS-203b덤프 <<

CrowdStrike CCCS-203b최신 인증시험 공부자료 - CCCS-203b시험패스

Itcertkr의 도움으로 여러분은 많은 시간과 돈을 들이지 않으셔도 혹은 여러학원등을 다니시지 않으셔도 우리 덤프로 안전하게 시험을 통과하실 수 있습니다.CrowdStrike CCCS-203b시험자료는 우리 Itcertkr에서 실제시험에 의하여 만들어진 것입니다. 지금까지의 시험문제와 답과 시험문제분석 등입니다. Itcertkr에서 제공하는CrowdStrike CCCS-203b시험자료의 문제와 답은 실제시험의 문제와 답과 아주 비슷합니다.

CrowdStrike CCCS-203b 시험요강:

주제	소개
주제 1	• 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.
주제 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.
주제 3	• 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.
주제 4	• 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.

주제 5	• 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.

최신 CrowdStrike Certified Cloud Specialist CCCS-203b 무료샘플문제 (Q323-Q328):

질문 # 323
When registering a container registry in Falcon's Image Assessment feature, which of the following parameters is mandatory for a successful connection?

- A. The container registry's Base URL, authentication credentials, and a defined repository scan scope.
- B. The container registry's Base URL, authentication credentials, and a unique connection name.
- C. The container registry's Base URL, a scan rule for critical vulnerabilities, and a list of trusted images.
- D. The container registry's Base URL, authentication credentials, and an active Image Assessment policy.

정답：B

설명：
Option A: Registering a registry requires the Base URL to identify the registry, authentication credentials for access, and a unique connection name to distinguish it in the Falcon console.
Option B: An Image Assessment policy is configured after the registry connection is registered, not as part of the registration process.
Option C: While the Base URL and credentials are mandatory, the repository scan scope is optional and defined later in the scan policy.
Option D: These configurations are related to scan rules and policies, not to the connection setup itself.

질문 # 324
CrowdStrike pulls data via API from AWS, Azure, and GCP without an agent to identify misconfigurations.
What is the default scan interval set to for each cloud provider?

- A. Every 2 hours
- B. Every 24 hours
- C. Every 4 hours
- D. Every 6 hours

정답：C

설명：
CrowdStrike Falcon Cloud Security performs agentless cloud security posture management (CSPM) by integrating directly with cloud service providers such as AWS, Microsoft Azure, and Google Cloud Platform using native APIs. This approach allows Falcon to continuously assess cloud configurations, permissions, networking, storage, and identity controls without deploying sensors or agents.
By default, CrowdStrike configures cloud account scans to runevery 4 hours. This scan frequency is designed to strike a balance between near-real-time visibility and efficient API usage across cloud providers. Cloud environments are highly dynamic, with frequent changes to configurations, IAM policies, and services. A four-hour scan interval ensures that new misconfigurations or risky changes-such as overly permissive roles, exposed storage, or insecure network rules-are identified quickly enough to reduce exposure time.
Scanning more frequently could introduce unnecessary API throttling or operational overhead, while less frequent scans could delay detection of critical security gaps. The four-hour interval is therefore CrowdStrike' s recommended default for maintaining continuous visibility while preserving cloud provider performance and stability.
This default interval can be adjusted in certain scenarios, but unless explicitly changed,every 4 hoursis the standard scan cadence applied to AWS, Azure, and GCP environments.

질문 # 325
An organization is integrating CrowdStrike Falcon Cloud Security with Kubernetes to enhance workload protection using an

admission controller.
What is a critical requirement for successfully deploying Falcon's Kubernetes admission controller?

- A. The Kubernetes cluster must be configured to allow only manually approved API requests before the admission controller can take effect.
- B. The admission controller must be registered with the Kubernetes API server as either a mutating or validating webhook to enforce security policies.
- C. The admission controller must be configured to modify the etcd database directly to prevent unauthorized resource creation.
- D. The admission controller must be deployed as a sidecar container in every pod to enforce security policies dynamically.

정답： B

설명:
Option A: Admission controllers in Kubernetes function as webhooks that the API server invokes during resource creation. They can be either mutating webhooks, which modify API requests, or validating webhooks, which approve or deny them based on security policies. Falcon Cloud Security leverages this functionality to enforce security policies on workload deployment, preventing misconfigurations, vulnerabilities, and non-compliant images from being deployed.
Option B: Admission controllers do not modify etcd directly. They operate at the request validation stage before data is stored in etcd, ensuring that only compliant and secure configurations proceed.
Option C: Admission controllers are not deployed as sidecar containers in every pod. Instead, they act as centralized services that interact with the API server to validate and enforce security rules before pod creation.
Option D: API requests are not manually approved before admission controllers take effect.
Instead, the webhook-based controller evaluates and either modifies or denies requests automatically.

질문 # 326
What action should a security engineer prioritize to mitigate the risks of unassessed container images running in production using CrowdStrike Falcon?

- A. Use Threat Intelligence Feeds to Block Threats at the Network Level
- B. Enable Image Drift Detection with Runtime Visibility
- C. Run a Manual Audit of Deployed Containers
- D. Implement Network Segmentation for All Workload

정답： B

설명:
Option A: Threat intelligence feeds enhance detection of malicious activity, but they are not specifically tailored for identifying unassessed container images in runtime environments.
Option B: CrowdStrike Falcon includes drift detection, which identifies when a running container image deviates from its baseline configuration or assessment status. This real-time feature allows security teams to pinpoint unassessed images and mitigate risks proactively. Runtime visibility ensures any image running without prior assessment is flagged.
Option C: Manual audits are time-consuming and prone to human error. They lack the scalability and real-time capabilities provided by tools like CrowdStrike Falcon for detecting unassessed images in runtime.
Option D: While network segmentation can limit the impact of compromised containers, it does not address identifying or mitigating risks from unassessed images directly.

질문 # 327
You are performing a dry run of an automated remediation workflow designed to disable AWS security groups that allow unrestricted inbound traffic.
Which step ensures that the dry run accurately evaluates the workflow without impacting resources?

- A. Enable "Dry Run Mode" in Falcon Fusion to simulate actions without applying them.
- B. Use CloudTrail logs to manually verify the workflow actions post-execution.
- C. Deploy the workflow to a non-production environment for testing.
- D. Temporarily revoke permissions to ensure the workflow cannot make changes.

정답： A

설명:
Option A: Enabling "Dry Run Mode" in Falcon Fusion is the correct step for simulating workflow actions without making changes to the actual resources. This mode allows you to verify that the workflow logic functions as expected, including detecting findings and simulating remediation steps, without impacting live environments.
Option B: Revoking permissions may prevent accidental changes, but it does not allow you to test the workflow logic fully, as the dry run mode simulates actions while still validating permissions.
Option C: While testing in a non-production environment is a valid practice, it is not equivalent to a dry run, which explicitly avoids making changes.
Option D: Reviewing logs is important for auditing, but it does not replace the need for a dry run, which provides upfront validation without impacting resources.

질문 # 328
......

CrowdStrike인증 CCCS-203b시험은 IT업종종사분들에게 널리 알려진 유명한 자격증을 취득할수 있는 시험과목입니다. CrowdStrike인증 CCCS-203b시험은 영어로 출제되는만큼 시험난이도가 많이 높습니다.하지만 Itcertkr의 CrowdStrike인증 CCCS-203b덤프만 있다면 아무리 어려운 시험도 쉬워집니다. 오르지 못할 산도 정복할수 있는게 Itcertkr제품의 우점입니다. Itcertkr의CrowdStrike인증 CCCS-203b덤프로 시험을 패스하여 자격증을 취득하면 정상에 오를수 있습니다.