2026 Authoritative Amazon SCS-C03 Intereactive Testing Engine

One of the great features of our SCS-C03 training material is our SCS-C03 pdf questions. AWS Certified Security - Specialty exam questions allow you to prepare for the real SCS-C03 exam and will help you with the self-assessment. You can easily pass the SCS-C03 exam by using SCS-C03 dumps pdf. Moreover, you will get all the updated SCS-C03 Questions with verified answers. If you want to prepare yourself for the real AWS Certified Security - Specialty exam, then it is one of the most important ways to improve your SCS-C03 preparation level. We provide 100% money back guarantee on all SCS-C03 braindumps products.

Amazon SCS-C03 Exam Syllabus Topics:

Topic	Details
Topic 1	• Data Protection: This domain centers on protecting data at rest and in transit through encryption, key management, data classification, secure storage, and backup mechanisms.
Topic 2	• Infrastructure Security: This domain focuses on securing AWS infrastructure including networks, compute resources, and edge services through secure architectures, protection mechanisms, and hardened configurations.
Topic 3	• Incident Response: This domain addresses responding to security incidents through automated and manual strategies, containment, forensic analysis, and recovery procedures to minimize impact and restore operations.

>> SCS-C03 Intereactive Testing Engine <<

SCS-C03 Reliable Exam Pattern & Exam SCS-C03 Testking

Getting the AWS Certified Security - Specialty (SCS-C03) certification is the way to go if you're planning to get into Amazon or want to start earning money quickly. Success in the AWS Certified Security - Specialty (SCS-C03) exam of this credential plays an essential role in the validation of your skills so that you can crack an interview or get a promotion in an Amazon company. Many people are attempting the AWS Certified Security - Specialty (SCS-C03) test nowadays because its importance is growing rapidly.

Amazon AWS Certified Security - Specialty Sample Questions (Q48-Q53):

NEW QUESTION # 48
A company has a large fleet of Amazon Linux 2 Amazon EC2 instances that run an application processing sensitive data. Compliance requirements include no exposed management ports, full session logging, and authentication through AWS IAM Identity Center. DevOps engineers occasionally need access for troubleshooting.
Which solution will provide remote access while meeting these requirements?

- A. Use Systems Manager Automation to temporarily open remote access ports.
- B. Enable EC2 Instance Connect and configure security groups accordingly.
- C. Grant access to the EC2 serial console and allow IAM role access.
- D. Assign an EC2 instance role that allows access to AWS Systems Manager. Create an IAM policy that grants access to Systems Manager Session Manager and assign it to an IAM Identity Center role.

Answer: D

Explanation:
AWS Systems Manager Session Manager provides secure, auditable shell access to EC2 instances without opening inbound ports.
According to AWS Certified Security - Specialty guidance, Session Manager records all session activity to CloudWatch Logs or Amazon S3 and integrates with IAM Identity Center for centralized authentication.
This solution meets all requirements: no exposed ports, full audit logging, and identity-based access control.
EC2 Instance Connect and serial console access do not integrate with Identity Center and may expose management paths.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
AWS Systems Manager Session Manager
AWS IAM Identity Center Integration

NEW QUESTION # 49
A company runs a web application on a fleet of Amazon EC2 instances in an Auto Scaling group. Amazon GuardDuty and AWS Security Hub are enabled. The security engineer needs an automated response to anomalous traffic that follows AWS best practices and minimizes application disruption.
Which solution will meet these requirements?

- A. Use EventBridge to invoke a Lambda function that removes the affected instance from the Auto Scaling group and isolates it with a restricted security group.
- B. Use EventBridge to disable the instance profile access keys.
- C. Use Security Hub to update the subnet network ACL to block traffic.
- D. Send GuardDuty findings to Amazon SNS for email notification.

Answer: A

Explanation:
AWS incident response best practices emphasize isolating compromised resources rather than immediately terminating them.
According to AWS Certified Security - Specialty documentation, removing an instance from an Auto Scaling group prevents replacement loops, while applying a restrictive security group isolates the instance for forensic analysis.
Using Amazon EventBridge to trigger an AWS Lambda function enables automated, consistent responses to GuardDuty findings.
This approach minimizes disruption to the application because healthy instances continue serving traffic while the affected instance is isolated.
Disabling credentials or modifying network ACLs can have broader impact on unrelated workloads. SNS notifications alone do not provide response automation.
AWS recommends isolate-and-investigate patterns for EC2 incident response.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
Amazon GuardDuty Automated Responses
AWS Incident Response Playbooks

NEW QUESTION # 50
A company's data scientists use Amazon SageMaker with datasets stored in Amazon S3. Data older than 45 days must be removed according to policy.
Which action should enforce this policy?

- A. Create a scheduled Lambda function to delete old objects monthly.
- B. Configure S3 Intelligent-Tiering.
- C. Create a Lambda function triggered on object upload to delete old data.
- D. Configure an S3 Lifecycle rule to delete objects after 45 days.

Answer: D

NEW QUESTION # 51
A company's security engineer receives an abuse notification from AWS. The notification indicates that someone is hosting malware from the company's AWS account. After investigation, the security engineer finds a new Amazon S3 bucket that an IAM user created without authorization.
Which combination of steps should the security engineer take toMINIMIZE the consequencesof this compromise? (Select THREE.)

- A. Rotate or delete all AWS access keys.
- B. Take snapshots of all Amazon Elastic Block Store (Amazon EBS) volumes.
- C. Encrypt all AWS CloudTrail logs.
- D. Turn on Amazon GuardDuty.
- E. Change the password for all IAM users.
- F. Delete any resources that are unrecognized or unauthorized.

Answer: A,D,F

Explanation:
AWS incident response best practices emphasizerapid containment, credential revocation, and threat detectionto minimize the blast radius of a compromise. According to the AWS Certified Security - Specialty Official Study Guide, when unauthorized resources such as an Amazon S3 bucket hosting malware are discovered, immediate action must be taken to stop further misuse of the account and to prevent recurrence.
Rotating or deleting all AWS access keys (Option D)is a critical containment step. If an IAM user has been compromised, any long-term credentials associated with that user must be revoked immediately to prevent continued unauthorized access. AWS guidance explicitly lists access key rotation or deletion as a first- response action for suspected credential compromise.
Deleting unrecognized or unauthorized resources (Option F)directly removes the malicious infrastructure that is being abused. In this case, deleting the unauthorized S3 bucket immediately stops malware distribution and reduces reputational and compliance impact.
Turning on Amazon GuardDuty (Option B)enables continuous threat detection by analyzing CloudTrail events, VPC Flow Logs, and DNS logs. GuardDuty can identify additional malicious activity, compromised credentials, or persistence mechanisms that the attacker may have established. AWS documentation recommends enabling GuardDuty during or immediately after an incident to detect ongoing or future threats.
Option A does not reduce the impact of the current compromise. Option C is overly disruptive and not recommended; credential rotation should be targeted. Option E is unnecessary because there is no indication that EBS-backed compute resources are involved.
AWS incident response guidance clearly prioritizescredential revocation, malicious resource removal, and threat detectionto minimize consequences.
* AWS Certified Security - Specialty Official Study Guide
* AWS Incident Response Best Practices
* Amazon GuardDuty User Guide
* AWS IAM Security Best Practices

NEW QUESTION # 52
A company needs to detect unauthenticated access to its Amazon Elastic Kubernetes Service (Amazon EKS) clusters. The solution must require no additional configuration of the existing EKS deployment.
Which solution will meet these requirements with the LEAST operational effort?

- A. Install a third-party security add-on.
- B. Monitor CloudWatch Container Insights metrics for EKS.
- C. Enable AWS Security Hub and monitor Kubernetes findings.
- D. Enable Amazon GuardDuty and use EKS Audit Log Monitoring.

Answer: D

Explanation:
Amazon GuardDuty provides managed threat detection and supports EKS protection features that analyze Kubernetes audit logs to detect suspicious activity, including unauthorized or unauthenticated access attempts.
AWS Certified Security - Specialty documentation recommends GuardDuty for low-overhead detection because it is fully managed and does not require deploying agents or modifying application code. EKS Audit Log Monitoring is designed to consume and analyze relevant control plane audit events to identify anomalous or unauthorized actions against the cluster. Compared to third-party add-ons, GuardDuty reduces operational burden and remains fully within AWS managed services. Security Hub aggregates findings from services like GuardDuty but does not itself perform the detection. CloudWatch Container Insights focuses on performance and

operational metrics, not authentication security detections. Therefore, enabling GuardDuty with EKS Audit Log Monitoring provides the required detection with the least operational effort and without requiring additional configuration to the existing EKS workload beyond enabling the feature.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
Amazon GuardDuty EKS Protection and Audit Log Monitoring
AWS Threat Detection Best Practices for Kubernetes on AWS

NEW QUESTION # 53
......

The meaning of qualifying examinations is, in some ways, to prove the candidate's ability to obtain qualifications that show your ability in various fields of expertise. If you choose our SCS-C03 learning dumps, you can create more unlimited value in the limited study time, learn more knowledge, and take the exam that you can take. Through qualifying examinations, this is our SCS-C03 Real Questions and the common goal of every user, we are trustworthy helpers, so please don't miss such a good opportunity. The acquisition of Amazon qualification certificates can better meet the needs of users' career development, so as to bring more promotion space for users. This is what we need to realize.

SCS-C03 Reliable Exam Pattern: https://www.passtestking.com/Amazon/SCS-C03-practice-exam-dumps.html