

Accurate SCS-C03 Study Material & Realistic 2026 Amazon Latest AWS Certified Security - Specialty Braindumps



BTW, DOWNLOAD part of Pass4Leader SCS-C03 dumps from Cloud Storage: <https://drive.google.com/open?id=1kj2vDmelqtzgG-RF8zfEflJ78OtnOJYP>

Our AWS Certified Security - Specialty exam tool can support almost any electronic device, from iPod, telephone, to computer and so on. You can use Our SCS-C03 test torrent by your telephone when you are travelling far from home; I think it will be very convenient for you. You can also choose to use our SCS-C03 study materials by your computer when you are at home. You just need to download the online version of our SCS-C03 study materials, which is not limited to any electronic device and support all electronic equipment in anywhere and anytime. At the same time, the online version of our AWS Certified Security - Specialty exam tool will offer you the services for working in an offline states, I believe it will help you solve the problem of no internet. If you would like to try our SCS-C03 Test Torrent, I can promise that you will improve yourself and make progress beyond your imagination.

Amazon SCS-C03 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">• Security Foundations and Governance: This domain addresses foundational security practices including policies, compliance frameworks, risk management, security automation, and audit procedures for AWS environments.
Topic 2	<ul style="list-style-type: none">• Detection: This domain covers identifying and monitoring security events, threats, and vulnerabilities in AWS through logging, monitoring, and alerting mechanisms to detect anomalies and unauthorized access.
Topic 3	<ul style="list-style-type: none">• 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.

>> Accurate SCS-C03 Study Material <<

Amazon SCS-C03 PDF Questions Exam Preparation and Study Guide

If you choose our SCS-C03 exam questions, then you can have a study on the latest information and technologies on the subject and you will definitely get a lot of benefits from it. Of course, the most effective point is that as long as you carefully study the SCS-C03 Study Guide for twenty to thirty hours, you can go to the exam. To really learn a skill, sometimes it does not take a lot of time. Come to buy our SCS-C03 practice materials and we teach you how to achieve your goals efficiently.

Amazon AWS Certified Security - Specialty Sample Questions (Q114-Q119):

NEW QUESTION # 114

A company has a single AWS account and uses an Amazon EC2 instance to test application code. The company recently discovered that the instance was compromised and was serving malware. Analysis showed that the instance was compromised 35 days ago. A security engineer must implement a continuous monitoring solution that automatically notifies the security team by email for high severity findings as soon as possible.

Which combination of steps should the security engineer take to meet these requirements? (Select THREE.)

- A. Enable AWS Security Hub in the AWS account.
- B. Create an Amazon Simple Queue Service (Amazon SQS) queue. Subscribe the security team's email distribution list to the queue.
- C. Enable Amazon GuardDuty in the AWS account.
- D. Create an Amazon EventBridge rule for Security Hub findings of high severity. Configure the rule to publish a message to the queue.
- E. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the security team's email distribution list to the topic.
- F. Create an Amazon EventBridge rule for GuardDuty findings of high severity. Configure the rule to publish a message to the topic.

Answer: C,E,F

Explanation:

Amazon GuardDuty provides continuous threat detection for compromised instances by analyzing VPC Flow Logs, DNS logs, and CloudTrail events. According to AWS Certified Security - Specialty guidance, GuardDuty is the fastest service to enable for detecting malware and compromised EC2 instances.

To notify the security team, Amazon SNS provides a native email notification mechanism with minimal setup. Amazon EventBridge integrates directly with GuardDuty findings and can filter based on severity.

Creating an EventBridge rule that matches high severity GuardDuty findings and publishes to SNS ensures immediate notification. Security Hub is not required for this use case and adds additional setup time. Amazon SQS does not support email subscriptions.

Referenced AWS Specialty Documents:

AWS Certified Security - Specialty Official Study Guide

Amazon GuardDuty Findings and Severity

Amazon EventBridge Integration with GuardDuty

NEW QUESTION # 115

A security engineer needs to implement a logging solution that captures detailed information about objects in an Amazon S3 bucket. The solution must include details such as the IAM identity that makes the request and the time the object was accessed. The data must be structured and available in near real time.

Which solution meets these requirements?

- A. Configure AWS Config rules to log access to the objects stored in the S3 bucket.
- B. Enable Amazon S3 server access logging on the S3 bucket. Create a new S3 bucket to store the logs.
Analyze the logs from the logging S3 bucket.
- C. Enable AWS CloudTrail data event logging. Create a new S3 bucket to store the logs. Analyze the logs from the logging S3 bucket.
- D. Enable Amazon Macie to log access to the objects stored in the S3 bucket.

Answer: C

Explanation:

AWS CloudTrail data event logging is the correct solution because it is specifically designed to capture detailed, structured, and near-real-time API activity for Amazon S3 object-level operations. When S3 data events are enabled, CloudTrail records actions such as GetObject, PutObject, and DeleteObject, along with critical context including the IAM principal, source IP address, event time, request parameters, and response elements. These logs are delivered in JSON format, making them highly structured and suitable for security analysis, SIEM integration, and automated detection workflows.

Amazon S3 server access logging (option A) provides basic request-level information but does not include full IAM identity context and is delivered with a significant delay, which does not meet the near-real-time requirement. AWS Config (option C) focuses on resource configuration changes and compliance evaluation; it does not log object-level access events. Amazon Macie (option D) is a data security service that uses machine learning to discover and classify sensitive data in S3 and generate findings for anomalous access patterns, but it is not a comprehensive access logging solution.

AWS Security Specialty documentation clearly states that CloudTrail data events are the authoritative mechanism for auditing S3

object-level access with identity attribution and precise timestamps, making option B the correct and best-practice answer

NEW QUESTION # 116

A company's public website consists of an Application Load Balancer (ALB), a set of Amazon EC2 instances that run a stateless application behind the ALB, and an Amazon DynamoDB table from which the application reads data. The company is concerned about malicious scanning and DDoS attacks. The company wants to impose a restriction in which each client IP address can read the data only 3 times in any 5-minute period.

Which solution will meet this requirement with the LEAST effort?

- A. Modify the EC2 application to count the source IP address of requests and calculate a rolling 5-minute sum. Return an error message if the count sum is greater than 3.
- **B. Set up AWS WAF in front of the ALB. Create a rule that blocks requests that exceed the limit of 3 requests in any 5-minute period for each IP address.**
- C. Create an AWS Lambda function based on an Amazon CloudWatch request. Configure the Lambda function to count the requests for each IP address in rolling 5-minute intervals and to provide notification if the count exceeds 3.
- D. Add source IP address and request time to the DynamoDB table. Add a 5-minute TTL setting based on request time. Change the read capacity of the DynamoDB table throughput to 3.

Answer: B

Explanation:

This is a classic Layer 7 rate-limiting requirement tied to client IP and a time window, and AWS WAF provides this natively with rate-based rules. Placing AWS WAF in front of the ALB allows the company to count requests per source IP over a rolling window and take action (block, CAPTCHA/challenge, or count depending on configuration) once the threshold is exceeded. This approach mitigates scanning and application-layer request floods early, before requests consume EC2 or DynamoDB capacity, and it requires minimal custom code or operational work.

Options B and C require building and maintaining custom counting logic (either in Lambda or in the application), which increases complexity and risk of errors, and it also introduces operational overhead for scaling state tracking across many IPs. Option D is not appropriate: altering DynamoDB capacity does not enforce "per-IP reads," and storing per-request metadata in the same table is an anti-pattern that increases write load and complexity.

Therefore, using AWS WAF rate-based protection at the ALB is the least-effort, most effective solution.

NEW QUESTION # 117

A company is operating an open-source software platform that is internet facing. The legacy software platform no longer receives security updates. The software platform operates using Amazon Route 53 weighted load balancing to send traffic to two Amazon EC2 instances that connect to an Amazon RDS cluster. A recent report suggests this software platform is vulnerable to SQL injection attacks, with samples of attacks provided. The company's security engineer must secure this system against SQL injection attacks within 24 hours. The solution must involve the least amount of effort and maintain normal operations during implementation. What should the security engineer do to meet these requirements?

- A. Create an Amazon CloudFront distribution specifying one EC2 instance as an origin. Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to the distribution. Test to ensure the vulnerability has been mitigated, then redirect the Route 53 records to point to CloudFront.
- **B. Create an Application Load Balancer with the existing EC2 instances as a target group. Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to the ALB. Test to ensure the vulnerability has been mitigated, then redirect the Route 53 records to point to the ALB. Update security groups on the EC2 instances to prevent direct access from the internet.**
- C. Update the security group that is attached to the EC2 instances, removing access from the internet to the TCP port used by the SQL database. Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to the EC2 instances.
- D. Obtain the latest source code for the platform and make the necessary updates. Test the updated code to ensure that the vulnerability has been mitigated, then deploy the patched version of the platform to the EC2 instances.

Answer: B

Explanation:

AWS WAF provides managed and custom rules that can immediately mitigate common web exploits such as SQL injection without modifying application code. According to AWS Certified Security - Specialty documentation, placing AWS WAF in front of an Application Load Balancer is a recommended rapid-response control for legacy applications with known vulnerabilities.

Creating an ALB in front of the existing EC2 instances allows seamless traffic migration. AWS WAF SQL injection rules can be deployed and tested without downtime. Updating Route 53 to point to the ALB preserves normal operations. Restricting EC2 security groups afterward prevents bypassing the WAF.

Option B introduces CloudFront changes and single-origin testing, increasing complexity. Option C cannot be completed within 24 hours and risks downtime. Option D is invalid because AWS WAF cannot be attached directly to EC2 instances.

NEW QUESTION # 118

An AWS Lambda function was misused to alter data, and a security engineer must identify who invoked the function and what output was produced. The engineer cannot find any logs created by the Lambda function in Amazon CloudWatch Logs. Which of the following explains why the logs are not available?

- A. The version of the Lambda function that was invoked was not current.
- B. The execution role for the Lambda function did not grant permissions to write to the Amazon S3 bucket where CloudWatch Logs stores the logs.
- **C. The execution role for the Lambda function did not grant permissions to write log data to CloudWatch Logs.**
- D. The Lambda function was invoked by using Amazon API Gateway, so the logs are not stored in CloudWatch Logs.

Answer: C

Explanation:

AWS Lambda automatically sends function execution logs to Amazon CloudWatch Logs when logging is enabled in the function code. However, this logging capability depends on the Lambda execution role having the appropriate permissions. According to the AWS Certified Security - Specialty Study Guide, the execution role must include permissions such as `logs:CreateLogGroup`, `logs:CreateLogStream`, and `logs:PutLogEvents`.

If these permissions are missing, Lambda cannot create log groups or streams, and no execution logs will appear in CloudWatch Logs—even though the function was successfully invoked. This is the most common reason Lambda logs are unavailable during forensic investigations.

Option B is incorrect because Lambda logs are stored in CloudWatch Logs regardless of whether the invocation source is API Gateway, EventBridge, or another AWS service. Option C is incorrect because CloudWatch Logs does not require direct S3 permissions from the Lambda execution role. Option D is irrelevant because Lambda versions do not affect logging behavior. AWS documentation emphasizes verifying execution role permissions as a first step when Lambda logs are missing.

Referenced AWS Specialty Documents:

AWS Certified Security - Specialty Official Study Guide

AWS Lambda Execution Roles

Amazon CloudWatch Logs Integration with Lambda

NEW QUESTION # 119

.....

Our SCS-C03 exam materials are so popular and famous in the market according to the advantages of them. Our SCS-C03 study questions not only have three different versions for our customers to choose and enjoy the convenience and pleasure in the varied displays. The most important part is that all content of our SCS-C03 learning braindumps are being sifted with diligent attention and easy to understand for all of our candidates.

Latest SCS-C03 Braindumps: <https://www.pass4leader.com/Amazon/SCS-C03-exam.html>

- Exam SCS-C03 Questions Pdf SCS-C03 Training Tools SCS-C03 Valid Test Duration Easily obtain free download of SCS-C03 by searching on www.prep4away.com SCS-C03 Latest Braindumps Pdf
- Pass-Sure Accurate SCS-C03 Study Material - Pass SCS-C03 Exam Search for SCS-C03 and download exam materials for free through www.pdfvce.com SCS-C03 Exam Actual Tests
- Pdf SCS-C03 Files Best SCS-C03 Vce SCS-C03 Test Answers Search for SCS-C03 and download it for free on www.verifieddumps.com website SCS-C03 Related Exams
- SCS-C03 Latest Braindumps SCS-C03 New Exam Bootcamp SCS-C03 Related Exams Easily obtain free download of **【 SCS-C03 】** by searching on www.pdfvce.com SCS-C03 Test Answers
- High-quality Accurate SCS-C03 Study Material - Passing SCS-C03 Exam is No More a Challenging Task Enter www.dumpsquestion.com and search for SCS-C03 to download for free SCS-C03 Test Answers
- Providing You Pass-Sure Accurate SCS-C03 Study Material with 100% Passing Guarantee Copy URL www.pdfvce.com open and search for SCS-C03 to download for free Best SCS-C03 Vce
- Unique, Full Length Exams - New Amazon SCS-C03 Practice Exam Enter “ www.practicevce.com ” and search for

SCS-C03 ” to download for free SCS-C03 New Study Guide

- Simplified SCS-C03 Guide Torrent Easy to Be Mastered for your exam Search for (SCS-C03) and obtain a free download on 《 www.pdfvce.com 》 Best SCS-C03 Vce
- Simplified SCS-C03 Guide Torrent Easy to Be Mastered for your exam Open www.torrentvce.com enter ⇒ SCS-C03 ⇐ and obtain a free download Exam SCS-C03 Questions Pdf
- SCS-C03 Latest Braindumps SCS-C03 Reliable Exam Cost SCS-C03 New Study Guide Search for ✓ SCS-C03 ✓ and download it for free immediately on ⇒ www.pdfvce.com New SCS-C03 Test Registration
- SCS-C03 Vce Test Simulator Best SCS-C03 Vce → Exam SCS-C03 Questions Pdf Search on (www.examdiscuss.com) for ⇒ SCS-C03 to obtain exam materials for free download Exam SCS-C03 Questions Pdf
- bookmarkity.com, bookmarks4seo.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, hotbookmarkings.com, issuu.com, webookmarks.com, dfsocial.com, tiannajks217910.wikimeglio.com, Disposable vapes

DOWNLOAD the newest Pass4Leader SCS-C03 PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=1kj2vDmelqtzgG-RF8zfEflJ78OtnOJYP>