Free PDF 2026 Amazon SCS-C02: High-quality AWS Certified Security - Specialty Study Plan

P.S. Free & New SCS-C02 dumps are available on Google Drive shared by Itcerttest: https://drive.google.com/open?id=1ndios0GpXiNY_GuOQ3lsckiD3A-t2pvX

There are three different versions of our SCS-C02 practice braindumps: the PDF, Software and APP online. If you think the first two formats of SCS-C02 study guide are not suitable for you, you will certainly be satisfied with our online version. It is more convenient for you to study and practice anytime, anywhere. All you need is an internet explorer. This means you can practice for the SCS-C02 Exam with your I-pad or smart-phone. Isn't it wonderful?

Amazon SCS-C02 Exam Syllabus Topics:

Topic	Details
Topic 1	• Data Protection: AWS Security specialists learn to ensure data confidentiality and integrity for data in transit and at rest. Topics include lifecycle management of data at rest, credential protection, and cryptographic key management. These capabilities are central to managing sensitive data securely, reflecting the exam's focus on advanced data protection strategies.
Topic 2	• Identity and Access Management: The topic equips AWS Security specialists with skills to design, implement, and troubleshoot authentication and authorization mechanisms for AWS resources. By emphasizing secure identity management practices, this area addresses foundational competencies required for effective access control, a vital aspect of the certification exam.
Topic 3	• Threat Detection and Incident Response: In this topic, AWS Security specialists gain expertise in crafting incident response plans and detecting security threats and anomalies using AWS services. It delves into effective strategies for responding to compromised resources and workloads, ensuring readiness to manage security incidents. Mastering these concepts is critical for handling scenarios assessed in the SCS-C02 Exam.

>> SCS-C02 Study Plan <<

Amazon SCS-C02 Best Preparation Materials & Reliable SCS-C02 Test Online

We have three versions of SCS-C02 learning materials available, including PDF, Software and APP online. The most popular one is PDF version of SCS-C02 study guide can be printed into papers so that you are able to write some notes or highlight the emphasis. On the other hand, Software version of our SCS-C02 Practice Questions is also welcomed by customers, especially for windows users. As for PPT online version, as long as you download the app into your computer. You can enjoy the nice service from us.

Amazon AWS Certified Security - Specialty Sample Questions (Q222-Q227):

NEW QUESTION # 222
A security engineer configures VPC Flow Logs and the associated IAM role to log all VPC traffic to a log group in Amazon CloudWatch Logs. After a wait of 10 minutes, no logs are appearing in the log group. The security engineer confirms that traffic is being sent to the VPC.
After additional debugging, the security engineer isolates the problem to the role that is associated with the VPC flow logs.
What could be the reason that the logs are not appearing in CloudWatch Logs?

- A. The logs:GetLogEvents permission is not granted in the role.
- B. The security engineer does not have permission to assume the role.
- C. The principal vpc-flow-logs.amazonaws.com does not have permission to assume the role.
- D. The role does not have permission to tag a CloudWatch Logs stream.

Answer: C

NEW QUESTION # 223
A company runs workloads on Amazon EC2 instances. The company needs to continually monitor the EC2 instances for software vulnerabilities and must display the findings in AWS Security Hub. The company must not install agents on the EC2 instances.

- A. Use Security Hub to enable the AWS Foundational Security Best Practices standard. Wait for Security Hub to generate the findings.
- B. Enable Amazon GuardDuty. Initiate on-demand malware scans by using GuardDuty Malware Protection. Enable the integration for GuardDuty in Security Hub.
- C. Enable Amazon Inspector. Set the scan mode to hybrid scanning. Enable the integration for Amazon Inspector in Security Hub.
- D. Use AWS Config managed rules to detect EC2 software vulnerabilities. Ensure that Security Hub has the AWS Config integration enabled.

Answer: C

Explanation:
Comprehensive Detailed Explanation with all AWS Reference
To monitor EC2 instances for software vulnerabilities without installing agents and to display findings in AWS Security Hub, Amazon Inspector is the most appropriate solution.
Amazon Inspector Overview:
Amazon Inspector is a vulnerability management service that automatically scans Amazon EC2 instances and container images in Amazon Elastic Container Registry (ECR) for known vulnerabilities.
It does not require agent installation as it integrates directly with EC2 metadata and uses network-based scanning.
Reference:
Integration with AWS Security Hub:
Enable the integration of Amazon Inspector with Security Hub to ingest and display findings in a centralized dashboard.
Security Hub will show Inspector's findings as part of its comprehensive security overview.
Why Not Other Options?
Option B: Security Hub's AWS Foundational Security Best Practices standard provides a broad set of checks but does not include detailed vulnerability scanning for EC2 instances.
Option C: GuardDuty is focused on detecting security threats and anomalies, not software vulnerabilities.
Option D: AWS Config managed rules provide compliance checks but lack detailed vulnerability scanning.

NEW QUESTION # 224
A company is implementing new compliance requirements to meet customer needs. According to the new requirements, the company must not use any Amazon RDS DB instances or DB clusters that lack encryption of the underlying storage. The company needs a solution that will generate an email alert when an unencrypted DB instance or DB cluster is created. The solution also must

terminate the unencrypted DB instance or DB cluster.
Which solution will meet these requirements in the MOST operationally efficient manner?

- A. Create an Amazon EventBridge rule that evaluates RDS event patterns and is initiated by the creation of DB instances or DB clusters. Configure the rule to invoke an AWS Lambda function.Configure the Lambda function to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic and to delete the unencrypted resource.
- B. Create an AWS Config managed rule to detect unencrypted RDS storage. Configure a manual remediation action to invoke an AWS Lambda function. Configure the Lambda function to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic and to delete the unencrypted resource.
- C. Create an Amazon EventBridge rule that evaluates RDS event patterns and is initiated by the creation of DB instances or DB clusters. Configure the rule to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic that includes an AWS Lambda function and an email delivery target as subscribers. Configure the Lambda function to delete the unencrypted resource.
- D. Create an AWS Config managed rule to detect unencrypted RDS storage. Configure an automatic remediation action to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic that includes an AWS Lambda function and an email delivery target as subscribers. Configure the Lambda function to delete the unencrypted resource.

Answer: D

Explanation:
Automatic configuration changes -> AWS Config

NEW QUESTION # 225
A Security Engineer is troubleshooting an issue with a company's custom logging application. The application logs are written to an Amazon S3 bucket with event notifications enabled to send events lo an Amazon SNS topic. All logs are encrypted at rest using an IAM KMS CMK. The SNS topic is subscribed to an encrypted Amazon SQS queue. The logging application polls the queue for new messages that contain metadata about the S3 object. The application then reads the content of the object from the S3 bucket for indexing.
The Logging team reported that Amazon CloudWatch metrics for the number of messages sent or received is showing zero. No togs are being received.
What should the Security Engineer do to troubleshoot this issue?
A) Add the following statement to the IAM managed CMKs:
B)
Add the following statement to the CMK key policy:
C)
Add the following statement to the CMK key policy:
D)
Add the following statement to the CMK key policy:

- A. Option B
- B. Option D
- C. Option A
- D. Option C

Answer: B

NEW QUESTION # 226
A company uses a collaboration application. A security engineer needs to configure automated alerts from AWS Security Hub in the us-west-2 Region for the application. The security engineer wants to receive an alert in a channel in the application every time Security Hub receives a new finding.
The security engineer creates an AWS Lambda function to convert the message to the format that the application requires. The Lambda function also sends the message to the application's API. The security engineer configures a corresponding Amazon EventBridge rule that specifies the Lambda function as the target.
After the EventBridge rule is implemented, the channel begins to constantly receive alerts from Security Hub.
Many of the alerts are Amazon Inspector alerts that do not require any action. The security engineer wants to stop the Amazon Inspector alerts.
Which solution will meet this requirement with the LEAST operational effort?

- A. Modify the value of the ProductArn attribute in the event pattern of the EventBridge rule to "anything- but": ["arn:aws:securityhub:us-west-2::product/aws/inspector"].
- B. Create an Amazon Simple Notification Service (Amazon SNS) topic to send messages to the application. Set a filter policy on the topic subscriptions to reject any messages that contain the product /aws/inspector string.
- C. Create a Security Hub custom action that automatically sends findings from all services except Amazon Inspector to the EventBridge event bus.
- D. Update the Lambda function code to find pattern matches of events from Amazon Inspector and to suppress the findings.

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The most operationally efficient solution is to modify the EventBridge rule's event pattern using the anything-but operator on the ProductArn attribute. This effectively filters out all findings generated by Amazon Inspector, allowing all other findings to trigger alerts as intended-without modifying Lambda code or managing additional services like SNS.
This technique aligns with Logging and Monitoring best practices to reduce noise from security alerts and improve response efficiency by filtering at the event rule level.

NEW QUESTION # 227
.....

The more times you choose us, the more discounts you may get. To make your whole experience more comfortable, we also provide considerate whole package services once you make decisions of our SCS-C02 test question. If you have any questions related to our SCS-C02 exam prep, pose them and our employees will help you as soon as possible. It is a mutual benefit job, that is why we put every exam candidates' goal above ours, and it is our sincere hope to make you success by the help of SCS-C02 Guide question and elude any kind of loss of you and harvest success effortlessly.