100% Pass Quiz 2026 Updated Amazon SCS-C03: AWS Certified Security - Specialty Dump File

Do you still have doubts about the quality of the Amazon SCS-C03 product? No worries. Visit PassLeader and download a free demo of Amazon Certification Exams for your pre-purchase mental satisfaction. Moreover, the Amazon SCS-C03 product of PassLeader is available at an affordable price.

Amazon SCS-C03 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.
Topic 2	• Identity and Access Management: This domain deals with controlling authentication and authorization through user identity management, role-based access, federation, and implementing least privilege principles.
Topic 3	• 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 4	• 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 5	• Data Protection: This domain centers on protecting data at rest and in transit through encryption, key management, data classification, secure storage, and backup mechanisms.

>> SCS-C03 Dump File <<

Quiz Trustable Amazon - SCS-C03 - AWS Certified Security - Specialty Dump File

Preparing for the Amazon SCS-C03 certification exam can be time-consuming and expensive. That's why we guarantee that our customers will pass the AWS Certified Security - Specialty (SCS-C03) exam on the first attempt by using our product. By providing this guarantee, we save our customers both time and money, making our SCS-C03 Practice material a wise investment in their career development.

Amazon AWS Certified Security - Specialty Sample Questions (Q97-Q102):

NEW QUESTION # 97
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. 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.
- B. 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.
- C. 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.
- 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: C

NEW QUESTION # 98
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:
To filter out specific findings, such as those from Amazon Inspector, EventBridge event patterns can be used to selectively route

events. By updating the ProductArn attribute in the event pattern with anything-but for Amazon Inspector's ProductArn (arn:aws:securityhub:us-west-), only findings from other services will trigger the Lambda function. This approach allows the security engineer to filter
2::product/aws/inspector
out unnecessary alerts with minimal operational effort, avoiding the need for additional filtering in Lambda or SNS.

NEW QUESTION # 99
A company detects bot activity targeting Amazon Cognito user pool endpoints. The solution must block malicious requests while maintaining access for legitimate users. Which solution meets these requirements?

- A. Enable Amazon Cognito threat protection.
- B. Monitor requests with CloudWatch.
- C. Restrict access to authenticated users only.
- D. Associate AWS WAF with the Cognito user pool.

Answer: A

Explanation:
Amazon Cognito threat protection is purpose-built to detect and mitigate malicious authentication activity such as credential stuffing and bot traffic. It uses adaptive risk-based analysis without disrupting legitimate users.
AWS WAF cannot be directly associated with Cognito user pools.

NEW QUESTION # 100
A company has a web application that reads from and writes to an Amazon S3 bucket. The company needs to use AWS credentials to authenticate all S3 API calls to the S3 bucket. Which solution will provide the application with AWS credentials to make S3 API calls?

- A. Integrate with Cognito identity pools and use GetId to obtain AWS credentials.
- B. Integrate with Cognito user pools and use the ID token to obtain AWS credentials.
- C. Integrate with Cognito identity pools and use AssumeRoleWithWebIdentity to obtain AWS credentials.
- D. Integrate with Cognito user pools and use the access token to obtain AWS credentials.

Answer: C

Explanation:
Amazon Cognito identity pools are designed to provide temporary AWS credentials for applications by exchanging an authenticated identity token for AWS Security Token Service (STS) credentials. AWS Certified Security - Specialty guidance distinguishes between Cognito user pools (authentication) and identity pools (authorization to AWS resources). A user pool can authenticate a user and issue tokens, but an identity pool is required to obtain AWS credentials that can be used to sign AWS API requests, such as S3 API calls. The correct mechanism is for the application to use AssumeRoleWithWebIdentity through STS (which is the underlying federation method used by identity pools) to receive temporary credentials for an IAM role that grants S3 permissions. GetId alone does not provide credentials; it returns an identity identifier that is used as part of the credential exchange flow. Options C and D are incorrect because user pool tokens are not AWS credentials and cannot directly sign S3 requests. The solution therefore must use identity pools to map users to IAM roles and retrieve temporary credentials, satisfying the requirement for authenticated API calls using short-lived credentials.

NEW QUESTION # 101
A company's security engineer receives an alert that indicates that an unexpected principal is accessing a company-owned Amazon Simple Queue Service (Amazon SQS) queue. All the company's accounts are within an organization in AWS Organizations. The security engineer must implement a mitigation solution that minimizes compliance violations and investment in tools that are outside of AWS. What should the security engineer do to meet these requirements?

- A. Create security groups that only accept inbound traffic from the CIDR blocks of all the VPCs in the organization. Attach the security groups to all the SQS queues in all the VPCs in the organization.
- B. In all the VPCs in the organization, adjust the network ACLs to only accept inbound traffic from the CIDR blocks of all the VPCs in the organization. Attach the network ACLs to all the subnets in all the VPCs in the organization.
- C. Create interface VPC endpoints for Amazon SQS in all the VPCs in the organization. Set the aws:SourceVpce condition

to the VPC endpoint identifier on the SQS policy. Add the aws:PrincipalOrgId condition to the VPC endpoint policy.

- D. Use a cloud access security broker (CASB) to maintain a list of managed resources. Configure the CASB to check the API and console access against that list on a web proxy.

Answer: C

Explanation:
Amazon SQS is an AWS-managed service and does not operate within customer VPCs.
Therefore, security groups and network ACLs cannot be used to control access to SQS, making options A and B invalid.
According to AWS Certified Security - Specialty documentation, the recommended approach to securely access AWS services from within a VPC is through interface VPC endpoints (AWS PrivateLink).
By creating interface VPC endpoints for Amazon SQS, the company ensures that traffic to SQS stays within the AWS network and does not traverse the public internet. Adding an SQS resource policy with the aws:SourceVpce condition restricts access so that only requests originating from the specified VPC endpoint are allowed. Additionally, using the aws:PrincipalOrgId condition ensures that only principals belonging to the same AWS Organization can access the queue.
Option D introduces an external tool, increasing cost and compliance complexity, which directly violates the requirement to minimize investment outside AWS.
AWS documentation clearly identifies VPC endpoints combined with IAM condition keys as a best practice for securing service access in multi-account environments.

NEW QUESTION # 102
.....