SCS-C01 Q&As

AWS Certified Security - Specialty (SCS-C01)

Pass Amazon SCS-C01 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/aws-certified-security-specialty.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A company\\'s application runs on Amazon EC2 and stores data in an Amazon S3 bucket The company wants additional security controls in place to limit the likelihood of accidental exposure of data to external parties Which combination of actions will meet this requirement? (Select THREE.)

A. Encrypt the data in Amazon S3 using server-side encryption with Amazon S3 managed encryption keys (SSE-S3)

B. Encrypt the data in Amazon S3 using server-side encryption with AWS KMS managed encryption keys (SSE-KMS)

C. Create a new Amazon S3 VPC endpoint and modify the VPC\\'s routing tables to use the new endpoint

D. Use the Amazon S3 Block Public Access feature.

E. Configure the bucket policy to allow access from the application instances only

F. Use a NACL to filter traffic to Amazon S3

Correct Answer: BCE

QUESTION 2

A company has multiple AWS accounts that are part of AWS Organizations. The company\\'s Security team wants to ensure that even those Administrators with full access to the company\\'s AWS accounts are unable to access the company\\'s Amazon S3 buckets.

How should this be accomplished?

A. UseSCPs

B. Add a permissions boundary to deny access to Amazon S3 and attach it to all roles

C. Use an S3 bucket policy

D. Create a VPC endpoint for Amazon S3 and deny statements for access to Amazon S3

Correct Answer: A

Reference: https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html

QUESTION 3

A company allows users to download its mobile app onto their phones. The app is MQTT based and connects to AWS IoT Core to subscribe to specific client-related topics.

Recently, the company discovered that some malicious attackers have been trying to get a Trojan horse onto legitimate mobile phones. The Trojan horse poses as the authentic application and uses a client ID with injected special characters to gain access to topics outside the client\\'s privilege scope.

Which combination of actions should the company take to prevent this threat? (Choose two.)

A. In the application, use an IoT thing name as the client ID to connect the device to AWS IoT Core.

B. In the application, add a client ID check. Disconnect from the server if any special character is detected.

C. Apply an AWS IoT Core policy that allows “AWSIoTWirelessDataAccess” with the principal set to “client/${iot:Connection.Thing.ThingName}”.

D. Apply an AWS IoT Core policy to the device to allow “iot:Connect” with the resource set to “client/${iot:ClientId}”.

E. Apply an AWS IoT Core policy to the device to allow “iot:Connect” with the resource set to “client/${iot:Connection.Thing.ThingName}”.

Correct Answer: BE

QUESTION 4

A company deploys an application on AWS. The application recently uploaded confidential data to an Amazon S3 bucket outside the company. The company\\'s security team wants to prevent this scenario from occurring in the future. The company owns 100 different S3 buckets in various AWS accounts and uses AWS Organizations to manage the accounts.

The security team must implement a solution that allows individual teams to create new S3 buckets. The solution must allow applications that are deployed on AWS to access only the S3 buckets that are deployed in the company\\'s organization.

Which solution will meet these requirements?

A. Create an S3 access point in each private subnet. Route all S3 requests to this access point. Create an S3 access point policy that restricts access to specific S3 buckets. Update all S3 access point policies when new S3 buckets are created in the organization.

B. Create an S3 gateway endpoint in each private subnet. Route all S3 requests to this endpoint. Create an S3 gateway endpoint policy that restricts access to specific S3 buckets. Update all S3 gateway endpoint policies when new S3 buckets are created in the organization,

C. Create an S3 interface endpoint in each private subnet. Route all S3 requests to this endpoint. Create an S3 interface endpoint policy that restricts access to specific S3 buckets. Update all S3 interface endpoint policies when new S3 buckets are created in the organization.

D. Create a Gateway Load Balancer endpoint in each private subnet. Route all S3 requests to this endpoint. Create a Gateway Load Balancer endpoint policy that restricts access to specific S3 buckets. Update all Gateway Load Balancer endpoint policies when new S3 buckets are created in the organization.

Correct Answer: C

QUESTION 5

A company hosts multiple externally facing applications, each isolated in its own AWS account The company\\'B Security team has enabled AWS WAF. AWS Config. and Amazon GuardDuty on all accounts. The company\\'s

Operations team has also joined all of the accounts to AWS Organizations and established centralized logging for CloudTrail. AWS Config, and GuardDuty. The company wants the Security team to take a reactive remediation in one account, and automate implementing this remediation as proactive prevention in all the other accounts.

How should the Security team accomplish this?

A. Update the AWS WAF rules in the affected account and use AWS Firewall Manager to push updated AWS WAF rules across all other accounts.

B. Use GuardDuty centralized logging and Amazon SNS to set up alerts to notify all application teams of security incidents.

C. Use GuardDuty alerts to write an AWS Lambda function that updates all accounts by adding additional NACLs on the Amazon EC2 instances to block known malicious IP addresses.

D. Use AWS Shield Advanced to identify threats in each individual account and then apply the account-based protections to all other accounts through Organizations.

Correct Answer: C