SCS-C02 Q&As

AWS Certified Security - Specialty

Pass Amazon SCS-C02 Exam with 100% Guarantee

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

https://www.leads4pass.com/scs-c02.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A company\\'s AWS CloudTrail logs are all centrally stored in an Amazon S3 bucket. The security team controls the company\\'s AWS account. The security team must prevent unauthorized access and tampering of the CloudTrail logs.

Which combination of steps should the security team take? (Choose three.)

A. Configure server-side encryption with AWS KMS managed encryption keys (SSE-KMS)

B. Compress log file with secure gzip.

C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to notify the security team of any modifications on CloudTrail log files.

D. Implement least privilege access to the S3 bucket by configuring a bucket policy.

E. Configure CloudTrail log file integrity validation.

F. Configure Access Analyzer for S3.

Correct Answer: ADE

QUESTION 2

A company is using Amazon Elastic Container Service (Amazon ECS) to deploy an application that deals with sensitive data During a recent security audit, the company identified a security issue in which Amazon RDS credentials were stored with the application code In the company\\'s source code repository

A security engineer needs to develop a solution to ensure that database credentials are stored securely and rotated periodically. The credentials should be accessible to the application only The engineer also needs to prevent database administrators from sharing database credentials as plaintext with other teammates. The solution must also minimize administrate overhead

Which solution meets these requirements?

A. Use the IAM Systems Manager Parameter Store to generate database credentials. Use an IAM profile for ECS tasks to restrict access to database credentials to specific containers only.

B. Use IAM Secrets Manager to store database credentials. Use an IAM inline policy for ECS tasks to restrict access to database credentials to specific containers only.

C. Use the IAM Systems Manager Parameter Store to store database credentials. Use IAM roles for ECS tasks to restrict access to database credentials lo specific containers only

D. Use IAM Secrets Manager to store database credentials. Use IAM roles for ECS tasks to restrict access to database credentials to specific containers only.

Correct Answer: D

To ensure that database credentials are stored securely and rotated periodically, the security engineer should do the following:

Use AWS Secrets Manager to store database credentials. This allows the security engineer to encrypt and manage

secrets centrally, and to configure automatic rotation schedules for them. Use IAM roles for ECS tasks to restrict access to

database credentials to specific containers only. This allows the security engineer to grant fine-grained permissions to ECS tasks based on their roles, and to avoid sharing credentials as plaintext with other teammates.

QUESTION 3

A company has an organization with SCPs in AWS Organizations. The root SCP for the organization is as follows:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllActions",
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Sid": "DenySES",
            "Effect": "Deny",
            "Action": "ses:*",
            "Resource": "*"
        }
    ]
}
```

The company\\'s developers are members of a group that has an IAM policy that allows access to Amazon Simple Email Service (Amazon SES) by allowing ses:* actions. The account is a child to an OU that has an SCP that allows Amazon SES. The developers are receiving a not-authorized error when they try to access Amazon SES through the AWS Management Console.

Which change must a security engineer implement so that the developers can access Amazon SES?

A. Add a resource policy that allows each member of the group to access Amazon SES.

B. Add a resource policy that allows "Principal": {"AWS": "arn:aws:iam::account-number:group/Dev"}.

C. Remove the AWS Control Tower control (guardrail) that restricts access to Amazon SES.

D. Remove Amazon SES from the root SCP.

Correct Answer: D

The correct answer is D. Remove Amazon SES from the root SCP. This answer is correct because the root SCP is the most restrictive policy that applies to all accounts in the organization. The root SCP explicitly denies access to Amazon

SES by using the NotAction element, which means that any action that is not listed in the element is denied. Therefore, removing Amazon SES from the root SCP will allow the developers to access it, as long as there are no other SCPs or

IAM policies that deny it.

The other options are incorrect because:

A. Adding a resource policy that allows each member of the group to access Amazon SES is not a solution, because resource policies are not supported by Amazon SES. Resource policies are policies that are attached to AWS resources, such as S3 buckets or SNS topics, to control access to those resources. Amazon SES does not have any resources that can have resource policies attached to them. B. Adding a resource policy that allows "Principal": {"AWS": "arn:aws:iam::account-number:group/Dev"} is not a solution, because resource policies do not support IAM groups as principals. Principals are entities that can perform actions on AWS resources, such as IAM users, roles, or AWS accounts. IAM groups are not principals, but collections of IAM users that share the same permissions. C. Removing the AWS Control Tower control (guardrail) that restricts access to Amazon SES is not a solution, because AWS Control Tower does not have any guardrails that restrict access to Amazon SES. Guardrails are high-level rules that govern the overall behavior of an organization\\'s accounts. AWS Control Tower provides a set of predefined guardrails that cover security, compliance, and operations domains.

References:

1: Amazon Simple Email Service endpoints and quotas

2: Resource-based policies and IAM policies

3: Specifying a principal in a policy

4: Policy elements: Principal

5: IAM groups

6: AWS Control Tower guardrails reference

7: AWS Control Tower concepts

8: AWS Control Tower guardrails

QUESTION 4

A company\\'s policy requires that all API keys be encrypted and stored separately from source code in a centralized security account. This security account is managed by the company\\'s security team However, an audit revealed that an API key is steed with the source code of an IAM Lambda function m an IAM CodeCommit repository in the DevOps account

How should the security learn securely store the API key?

A. Create a CodeCommit repository in the security account using IAM Key Management Service (IAM KMS) tor encryption Require the development team to migrate the Lambda source code to this repository

B. Store the API key in an Amazon S3 bucket in the security account using server-side encryption with Amazon S3 managed encryption keys (SSE-S3) to encrypt the key Create a resigned URL tor the S3 key. and specify the URL m a Lambda environmental variable in the IAM CloudFormation template Update the Lambda function code to retrieve the key using the URL and call the API

C. Create a secret in IAM Secrets Manager in the security account to store the API key using IAM Key Management Service (IAM KMS) tor encryption Grant access to the IAM role used by the Lambda function so that the function can retrieve the key from Secrets Manager and call the API

D. Create an encrypted environment variable for the Lambda function to store the API key using IAM Key Management Service (IAM KMS) tor encryption Grant access to the IAM role used by the Lambda function so that the function can decrypt the key at runtime

Correct Answer: C

To securely store the API key, the security team should do the following:

Create a secret in AWS Secrets Manager in the security account to store the API key using AWS Key Management Service (AWS KMS) for encryption. This allows the security team to encrypt and manage the API key centrally, and to

configure automatic rotation schedules for it.

Grant access to the IAM role used by the Lambda function so that the function can retrieve the key from Secrets Manager and call the API. This allows the security team to avoid storing the API key with the source code, and to use IAM

policies to control access to the secret.

QUESTION 5

A company is using AWS to run a long-running analysis process on data that is stored in Amazon S3 buckets. The process runs on a fleet of Amazon EC2 instances that are in an Auto Scaling group. The EC2 instances are deployed in a private subnet Of a VPC that does not have internet access. The EC2 instances and the S3 buckets are in the same AWS account

The EC2 instances access the S3 buckets through an S3 gateway endpoint that has the default access policy. Each EC2 instance is associated With an instance profile role that has a policy that explicitly allows the s3:GetObject action and the s3:PutObject action for only the required S3 buckets.

The company learns that one or more of the EC2 instances are compromised and are exfiltrating data to an S3 bucket that is outside the companys organization in AWS Organizations. A security engtneer must implement a solution to stop this exfiltration of data and to keep the EC2 processing job functional.

Which solution will meet these requirements?

A. Update the policy on the S3 gateway endpoint to allow the S3 actions CY11y if the values of the aws:ResourceOrglD and aws:PrincipalOrglD condition keys match the companys values.

B. Update the policy on the instance profile role to allow the S3 actions only if the value of the aws:ResourceOrgID condition key matches the company\\'s value.

C. Add a network ACL rule to the subnet of the EC2 instances to block outgoing connections on port 443.

D. Apply an SCP on the AWS account to allow the $3 actions only if the values of the aws:ResourceOrgID and aws:PrincipalOrgID condition keys match the company\\'s values.

Correct Answer: D

To stop the data exfiltration from the compromised EC2 instances, the security engineer needs to implement a solution that can deny access to any S3 bucket that is outside the company\\'s organization. The solution should also allow the EC2 instances to access the required S3 buckets within the company\\'s organization for the analysis process. Option A is incorrect because updating the policy on the S3 gateway endpoint will not affect the access to S3 buckets that are outside the company\\'s organization. The S3 gateway endpoint only applies to S3 buckets that are in the same AWS Region as the VPC. The compromised EC2 instances can still access S3 buckets in other Regions or other AWS accounts through the internet gateway or NAT device. Option B is incorrect because updating the policy on the instance profile role will not prevent the compromised EC2 instances from using other credentials or methods to access S3 buckets outside the company\\'s organization. The instance profile role only applies to requests that are made using the credentials of that role. The compromised EC2 instances can still use other IAM users, roles, or access keys to access S3 buckets outside the company\\'s organization. Option C is incorrect because adding a network ACL rule to block outgoing connections on port 443 will also block legitimate connections to S3 buckets within the company\\'s organization. The network ACL rule will prevent the EC2 instances from accessing any S3 bucket through HTTPS, regardless of whether it is inside or outside the company\\'s organization. Option D is correct because applying an SCP on the AWS account will effectively deny access to any S3 bucket that is outside the company\\'s organization. The SCP will apply to all IAM users, roles, and resources in the AWS account, regardless of how they access S3. The SCP will use the aws:ResourceOrgID and aws:PrincipalOrgID condition keys to check whether the S3 bucket and the principal belong to the same organization as the AWS account. If they do not match, the SCP will deny the S3 actions.

References: Using service control policies AWS Organizations service control policy examples