Exam Questions SCS-C03

AWS Certified Security - Specialty

https://www.2passeasy.com/dumps/SCS-C03/

NEW QUESTION 1
A company uses AWS Organizations to manage an organization that consists of three workload OUs: Production, Development, and Testing. The company uses AWS CloudFormation templates to define and deploy workload infrastructure in AWS accounts that are associated with the OUs. Different SCPs are attached to each workload OU.
The company successfully deployed a CloudFormation stack update to workloads in the Development OU and the Testing OU. When the company uses the same CloudFormation template to deploy the stack update in an account in the Production OU, the update fails.
The error message reports insufficient IAM permissions.
What is the FIRST step that a security engineer should take to troubleshoot this issue?

A. Review the AWS CloudTrail logs in the account in the Production O
B. Search for any failed API calls from CloudFormation during the deployment attempt.
C. Remove all the SCPs that are attached to the Production O
D. Rerun the CloudFormation stack update to determine if the SCPs were preventing the CloudFormation API calls.
E. Confirm that the role used by CloudFormation has sufficient permissions to create, update, and delete the resources that are referenced in the CloudFormation template.
F. Make all the SCPs that are attached to the Production OU the same as the SCPs that are attached to the Testing OU.

Answer: A

NEW QUESTION 2
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 identity pools and use AssumeRoleWithWebIdentity to obtain AWS credentials.
C. Integrate with Cognito user pools and use the ID token to obtain AWS credentials.
D. Integrate with Cognito user pools and use the access token to obtain AWS credentials.

Answer: B

NEW QUESTION 3
A company stores sensitive data in an Amazon S3 bucket. The company encrypts the data at rest by using server-side encryption with Amazon S3 managed keys (SSE-S3). A security engineer must prevent any modifications to the data in the S3 bucket.
Which solution will meet this requirement?

A. Configure S3 bucket policies to deny DELETE and PUT object permissions.
B. Configure S3 Object Lock in compliance mode with S3 bucket versioning enabled.
C. Change the encryption on the S3 bucket to use AWS Key Management Service (AWS KMS) customer managed keys.
D. Configure the S3 bucket with multi-factor authentication (MFA) delete protection.

Answer: B

NEW QUESTION 4
A company??s application team needs a new AWS Key Management Service (AWS KMS) customer managed key to use with Amazon S3. The company??s security policy requires separate keys for different AWS services to limit security exposure.
How can a security engineer limit the KMS customer managed key to work with only Amazon S3?

A. Configure the key policy to allow only Amazon S3 to perform the kms:Encrypt action.
B. Configure the key policy to allow KMS actions only when the value for the kms:ViaService condition key matches the Amazon S3 service name.
C. Configure the application??s IAM role policy to allow Amazon S3 to perform the iam:PassRole action.
D. Configure the application??s IAM role policy to allow only S3 operations when the operations are combined with the KMS customer managed key.

Answer: B

NEW QUESTION 5
A company needs to identify the root cause of security findings and investigate IAM roles involved in those findings. The company has enabled VPC Flow Logs, Amazon GuardDuty, and AWS CloudTrail.
Which solution will meet these requirements?

A. Use Amazon Detective to investigate IAM roles and visualize findings.
B. Use Amazon Inspector and CloudWatch dashboards.
C. Export GuardDuty findings to S3 and analyze with Athena.
D. Use Security Hub custom actions to investigate IAM roles.

Answer: A

NEW QUESTION 6
A company runs an application on an Amazon EC2 instance. The application generates invoices and stores them in an Amazon S3 bucket. The instance profile that is attached to the instance has appropriate access to the S3 bucket. The company needs to share each invoice with multiple clients that do not have AWS credentials. Each client must be able to download only the client's own invoices. Clients must download their invoices within 1 hour of invoice creation. Clients must use only temporary credentials to access the company's AWS resources.
Which additional step will meet these requirements?

A. Update the S3 bucket policy to ensure that clients that use pre-signed URLs have the S3:Get* permission and the S3:List* permission to access S3 objects in the bucket.
B. Add a StringEquals condition to the IAM role policy for the EC2 instance profil

C. Configure the policy condition to restrict access based on the s3:ResourceTag/ClientId tag of each invoic
D. Tag each generated invoice with the ID of its corresponding client.
E. Update the script to use AWS Security Token Service (AWS STS) to obtain new credentials each time the script runs by assuming a new role that has S3:GetObject permission
F. Use the credentials to generate the pre-signed URLs.
G. Generate an access key and a secret key for an IAM user that has S3:GetObject permissions on the S3 bucke
H. Embed the keys into the scrip
I. Use the keys to generate the pre-signed URLs.

Answer: B

NEW QUESTION 7
A company needs to deploy AWS CloudFormation templates that configure sensitive database credentials. The company already uses AWS Key Management Service (AWS KMS) and AWS Secrets Manager.
Which solution will meet the requirements?

A. Use a dynamic reference in the CloudFormation template to reference the database credentials in Secrets Manager.
B. Use encrypted parameters in the CloudFormation template.
C. Use SecureString parameters to reference Secrets Manager.
D. Use SecureString parameters encrypted by AWS KMS.

Answer: A

NEW QUESTION 8
A company experienced a security incident caused by a vulnerable container image that was pushed from an external CI/CD pipeline into Amazon ECR.
Which solution will prevent vulnerable images from being pushed?

A. Enable ECR enhanced scanning with Lambda blocking.
B. Use Amazon Inspector with EventBridge and Lambda.
C. Integrate Amazon Inspector into the CI/CD pipeline using SBOM generation and fail the pipeline on critical findings.
D. Enable basic continuous ECR scanning.

Answer: C

NEW QUESTION 9
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 execution role for the Lambda function did not grant permissions to write log data to CloudWatch Logs.
B. The Lambda function was invoked by using Amazon API Gateway, so the logs are not stored in CloudWatch Logs.
C. The execution role for the Lambda function did not grant permissions to write to the Amazon S3 bucket where CloudWatch Logs stores the logs.
D. The version of the Lambda function that was invoked was not current.

Answer: A

NEW QUESTION 10
A company is building a secure solution that relies on an AWS Key Management Service (AWS KMS) customer managed key. The company wants to allow AWS Lambda to use the KMS key. However, the company wants to prevent Amazon EC2 from using the key.
Which solution will meet these requirements?

A. Use IAM explicit deny for EC2 instance profiles and allow for Lambda roles.
B. Use a KMS key policy with kms:ViaService conditions to allow Lambda usage and deny EC2 usage.
C. Use aws:SourceIp and aws:AuthorizedService condition keys in the KMS key policy.
D. Use an SCP to deny EC2 and allow Lambda.

Answer: B

NEW QUESTION 10
A company uses AWS IAM Identity Center with SAML 2.0 federation. The company decides to change its federation source from one identity provider (IdP) to another. The underlying directory for both IdPs is Active Directory.
Which solution will meet this requirement?

A. Disable all existing users and groups within IAM Identity Center that were part of thefederation with the original IdP.
B. Modify the attribute mappings within the IAM Identity Center trust relationship to match information that the new IdP sends.
C. Reconfigure all existing IAM roles in the company's AWS accounts to explicitly trust the new IdP as the principal.
D. Confirm that the Network Time Protocol (NTP) clock skew is correctly set between IAM Identity Center and the new IdP endpoints.

Answer: B

NEW QUESTION 13
A company has several Amazon S3 buckets that do not enforce encryption in transit. A security engineer must implement a solution that enforces encryption in transit for all the company's existing and future S3 buckets.
Which solution will meet these requirements?

A. Enable AWS Confi
B. Create a proactive AWS Config Custom Policy rul

C. Create aGuard clause to evaluate the S3 bucket policies to check for a value of True for the aws:SecureTransport condition ke
D. If the AWS Config rule evaluates to NON_COMPLIANT, block resource creation.
E. Enable AWS Confi
F. Configure the s3-bucket-ssl-requests-only AWS Config managed rule and set the rule trigger type to Hybri
G. Create an AWS Systems Manager Automation runbook that applies a bucket policy to deny requests when the value of the aws:SecureTransport condition key is Fals
H. Configure automatic remediatio
I. Set the runbook as the target of the rule.
J. Enable Amazon Inspecto
K. Create a custom AWS Lambda rul
L. Create a Lambda function that applies a bucket policy to deny requests when the value of the aws:SecureTransport condition key is Fals
M. Set the Lambda function as the target of the rule.
N. Create an AWS CloudTrail trai
O. Enable S3 data events on the trai
P. Create an AWS Lambda function that applies a bucket policy to deny requests when the value of the aws:SecureTransport condition key is Fals
Q. Configure the CloudTrail trail to invoke the Lambda function.

Answer: B

NEW QUESTION 17
A company??s web application runs on Amazon EC2 instances behind an Application Load Balancer (ALB) in an Auto Scaling group. An AWS WAF web ACL is associated with the ALB. Instance logs are lost after reboots. The operations team suspects malicious activity targeting a specific PHP file.
Which set of actions will identify the suspect attacker??s IP address for future occurrences?

A. Configure VPC Flow Logs and search for PHP file activity.
B. Install the CloudWatch agent on the ALB and export application logs.
C. Export ALB access logs to Amazon OpenSearch Service and search them.
D. Configure the web ACL to send logs to Amazon Kinesis Data Firehos
E. Deliver logs to Amazon S3 and query them with Amazon Athena.

Answer: D

NEW QUESTION 20
A company is planning to deploy a new log analysis environment. The company needs to analyze logs from multiple AWS services in near real time. The solution must provide the ability to search the logs and must send alerts to an existing Amazon Simple Notification
Service (Amazon SNS) topic when specific logs match detection rules. Which solution will meet these requirements?

A. Analyze the logs by using Amazon OpenSearch Servic
B. Search the logs from the OpenSearch AP
C. Use OpenSearch Service Security Analytics to match logs with detection rules and to send alerts to the SNS topic.
D. Analyze the logs by using AWS Security Hu
E. Search the logs from the Findings page in Security Hu
F. Create custom actions to match logs with detection rules and to send alerts to the SNS topic.
G. Analyze the logs by using Amazon CloudWatch Log
H. Use a subscription filter to match logs with detection rules and to send alerts to the SNS topi
I. Search the logs manually by using CloudWatch Logs Insights.
J. Analyze the logs by using Amazon QuickSigh
K. Search the logs by listing the query results in a dashboar
L. Run queries to match logs with detection rules and to send alerts to the SNS topic.

Answer: A

NEW QUESTION 22
A company has an AWS account that hosts a production application. The company receives an email notification that Amazon GuardDuty has detected an Impact:IAMUser/AnomalousBehavior finding in the account. A security engineer needs to run the investigation playbook for this security incident and must collect and analyze the information without affecting the application.
Which solution will meet these requirements MOST quickly?

A. Log in to the AWS account by using read-only credential
B. Review the GuardDuty finding for details about the IAM credentials that were use
C. Use the IAM console to add a DenyAll policy to the IAM principal.
D. Log in to the AWS account by using read-only credential
E. Review the GuardDuty finding to determine which API calls initiated the findin
F. Use Amazon Detective to review the API calls in context.
G. Log in to the AWS account by using administrator credential
H. Review the GuardDuty finding for details about the IAM credentials that were use
I. Use the IAM console to add a DenyAll policy to the IAM principal.
J. Log in to the AWS account by using read-only credential
K. Review the GuardDuty finding to determine which API calls initiated the findin
L. Use AWS CloudTrail Insights and AWS CloudTrail Lake to review the API calls in context.

Answer: B

NEW QUESTION 24
A company is using AWS CloudTrail and Amazon CloudWatch to monitor resources in an AWS account. The company??s developers have been using an IAM role in the account for the last 3 months.
A security engineer needs to refine the customer managed IAM policy attached to the role to ensure that the role provides least privilege access.
Which solution will meet this requirement with the LEAST effort?

A. Implement AWS IAM Access Analyzer policy generation on the role.
B. Implement AWS IAM Access Analyzer policy validation on the role.
C. Search CloudWatch logs to determine the actions the role invoked and to evaluate the permissions.
D. Use AWS Trusted Advisor to compare the policies assigned to the role against AWS best practices.

Answer: A

NEW QUESTION 27
A company has a PHP-based web application that uses Amazon S3 as an object store for user files. The S3 bucket is configured for server-side encryption with Amazon S3 managed keys (SSE-S3). New requirements mandate full control of encryption keys.
Which combination of steps must a security engineer take to meet these requirements? (Select THREE.)

A. Create a new customer managed key in AWS Key Management Service (AWS KMS).
B. Change the SSE-S3 configuration on the S3 bucket to server-side encryption with customer-provided keys (SSE-C).
C. Configure the PHP SDK to use the SSE-S3 key before upload.
D. Create an AWS managed key for Amazon S3 in AWS KMS.
E. Change the SSE-S3 configuration on the S3 bucket to server-side encryption with AWS KMS managed keys (SSE-KMS).
F. Change all the S3 objects in the bucket to use the new encryption key.

Answer: AEF

NEW QUESTION 28
A company is planning to migrate its applications to AWS in a single AWS Region. The company??s applications will use a combination of Amazon EC2 instances, Elastic Load Balancing (ELB) load balancers, and Amazon S3 buckets. The company wants to complete the migration as quickly as possible. All the applications must meet the following requirements:
• Data must be encrypted at rest.
• Data must be encrypted in transit.
• Endpoints must be monitored for anomalous network traffic.
Which combination of steps should a security engineer take to meet these requirements with the LEAST effort? (Select THREE.)

A. Install the Amazon Inspector agent on EC2 instances by using AWS Systems Manager Automation.
B. Enable Amazon GuardDuty in all AWS accounts.
C. Create VPC endpoints for Amazon EC2 and Amazon S3. Update VPC route tables to use only the secure VPC endpoints.
D. Configure AWS Certificate Manager (ACM). Configure the load balancers to use certificates from ACM.
E. Use AWS Key Management Service (AWS KMS) for key managemen
F. Create an S3 bucket policy to deny any PutObject command with a condition for x-amz-meta-side- encryption.
G. Use AWS Key Management Service (AWS KMS) for key managemen
H. Create an S3 bucket policy to deny any PutObject command with a condition for x-amz-server-side- encryption.

Answer: BDF

NEW QUESTION 30
A company has AWS accounts in an organization in AWS Organizations. An Amazon S3 bucket in one account is publicly accessible. A security engineer must remove public access and ensure the bucket cannot be made public again.
Which solution will meet these requirements?

A. Enforce KMS encryption and deny s3:GetObject by SCP.
B. Enable PublicAccessBlock and deny s3:GetObject by SCP.
C. Enable PublicAccessBlock and deny s3:PutPublicAccessBlock by SCP.
D. Enable Object Lock governance and deny s3:PutPublicAccessBlock by SCP.

Answer: C

NEW QUESTION 34
A company needs centralized log monitoring with automatic detection across hundreds of AWS accounts.
Which solution meets these requirements with the LEAST operational effort?

A. Designate a GuardDuty administrator account and enable protections.
B. Centralize CloudWatch logs and use Inspector.
C. Centralize CloudTrail logs and query with Athena.
D. Stream logs to Kinesis and process with Lambda.

Answer: A

NEW QUESTION 39
A company sends Apache logs from EC2 Auto Scaling instances to a CloudWatch Logs log group with 1-year retention. A suspicious IP address appears in logs. A security engineer needs to analyze the past week of logs to count requests from that IP and list requested URLs.
What should the engineer do with the LEAST effort?

A. Export to S3 and use Macie.
B. Stream to OpenSearch and analyze.
C. Use CloudWatch Logs Insights with queries.
D. Export to S3 and use AWS Glue.

Answer: C

NEW QUESTION 44

A company needs a cloud-based, managed desktop solution for its workforce of remote employees. The company wants to ensure that the employees can access the desktops only by using company-provided devices. A security engineer must design a solution that will minimize cost and management overhead.
Which solution will meet these requirements?

A. Deploy a custom virtual desktop infrastructure (VDI) solution with a restriction policy to allow access only from corporate devices.
B. Deploy a fleet of Amazon EC2 instance
C. Assign an instance to each employee with certificate-based device authentication that uses Windows Active Directory.
D. Deploy Amazon WorkSpace
E. Set up a trusted device policy with IP blocking on the authentication gateway by using AWS Identity and Access Management (IAM).
F. Deploy Amazon WorkSpace
G. Create client certificates, and deploy them to trusted device
H. Enable restricted access at the directory level.

Answer: D

NEW QUESTION 48
A company has a web application that reads from and writes to an Amazon S3 bucket. The company needs to authenticate all S3 API calls with AWS credentials.
Which solution will provide the application with AWS credentials?

A. Use Amazon Cognito identity pools and the GetId API.
B. Use Amazon Cognito identity pools and AssumeRoleWithWebIdentity.
C. Use Amazon Cognito user pools with ID tokens.
D. Use Amazon Cognito user pools with access tokens.

Answer: B

NEW QUESTION 53
A company uses AWS Organizations and has an SCP at the root that prevents sharing resources with external accounts. The company now needs to allow only the marketing account to share resources externally while preventing all other accounts from doing so. All accounts are in the same OU.
Which solution will meet these requirements?

A. Create a new SCP in the marketing account to explicitly allow sharing.
B. Edit the existing SCP to add a condition that excludes the marketing account.
C. Edit the SCP to include an Allow statement for the marketing account.
D. Use a permissions boundary in the marketing account.

Answer: B

NEW QUESTION 56
A security engineer needs to control access to data that is encrypted with an AWS Key Management Service (AWS KMS) customer managed key. The security engineer also needs to use additional authenticated data (AAD) to prevent tampering with ciphertext.
Which solution will meet these requirements?

A. Pass the key alias to AWS KMS when calling the Encrypt and Decrypt API actions.
B. Use IAM policies to restrict access to the Encrypt and Decrypt API actions.
C. Use the kms:EncryptionContext condition key when defining IAM policies for the customer managed key.
D. Use key policies to restrict access to the appropriate IAM groups.

Answer: C

NEW QUESTION 58
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SCS-C03 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SCS-C03 Product From:

https://www.2passeasy.com/dumps/SCS-C03/

Money Back Guarantee

SCS-C03 Practice Exam Features:

* SCS-C03 Questions and Answers Updated Frequently

* SCS-C03 Practice Questions Verified by Expert Senior Certified Staff

* SCS-C03 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SCS-C03 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year