

Amazon-Web-Services

Exam Questions SCS-C03

AWS Certified Security - Specialty



NEW QUESTION 1

A security team manages a company's AWS Key Management Service (AWS KMS) customer managed keys. Only members of the security team can administer the KMS keys. The company's application team has a software process that needs temporary access to the keys occasionally. The security team needs to provide the application team's software process with access to the keys.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Export the KMS key material to an on-premises hardware security module (HSM). Give the application team access to the key material.
- B. Edit the key policy that grants the security team access to the KMS keys by adding the application team as principal
- C. Revert this change when the application team no longer needs access.
- D. Create a key grant to allow the application team to use the KMS key
- E. Revoke the grant when the application team no longer needs access.
- F. Create a new KMS key by generating key material on premise
- G. Import the key material to AWS KMS whenever the application team needs access
- H. Grant the application team permissions to use the key.

Answer: C

NEW QUESTION 2

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 3

A company's security team wants to receive near-real-time email notifications about AWS abuse reports related to DoS attacks. An Amazon SNS topic already exists and is subscribed to by the security team.

What should the security engineer do next?

- A. Poll Trusted Advisor for abuse notifications by using a Lambda function.
- B. Create an Amazon EventBridge rule that matches AWS Health events for AWS_ABUSE_DOS_REPORT and publishes to SNS.
- C. Poll the AWS Support API for abuse cases by using a Lambda function.
- D. Detect abuse reports by using CloudTrail logs and CloudWatch alarms.

Answer: B

NEW QUESTION 4

A security engineer wants to forward custom application-security logs from an Amazon EC2 instance to Amazon CloudWatch. The security engineer installs the CloudWatch agent on the EC2 instance and adds the path of the logs to the CloudWatch configuration file.

However, CloudWatch does not receive the logs. The security engineer verifies that the awslogs service is running on the EC2 instance.

What should the security engineer do next to resolve the issue?

- A. Add AWS CloudTrail to the trust policy of the EC2 instance
- B. Send the custom logs to CloudTrail instead of CloudWatch.
- C. Add Amazon S3 to the trust policy of the EC2 instance
- D. Configure the application to write the custom logs to an S3 bucket that CloudWatch can use to ingest the logs.
- E. Add Amazon Inspector to the trust policy of the EC2 instance
- F. Use Amazon Inspector instead of the CloudWatch agent to collect the custom logs.
- G. Attach the CloudWatchAgentServerPolicy AWS managed policy to the EC2 instance role.

Answer: D

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 has decided to move its fleet of Linux-based web server instances to an Amazon EC2 Auto Scaling group. Currently, the instances are static and are launched manually. When an administrator needs to view log files, the administrator uses SSH to establish a connection to the instances and retrieves the logs manually.

The company often needs to query the logs to produce results about application sessions and user issues. The company does not want its new automatically scaling architecture to result in the loss of any log files when instances are scaled in.

Which combination of steps should a security engineer take to meet these requirements MOST cost-effectively? (Select TWO.)

- A. Configure a cron job on the instances to forward the log files to Amazon S3 periodically.
- B. Configure AWS Glue and Amazon Athena to query the log files.
- C. Configure the Amazon CloudWatch agent on the instances to forward the logs to Amazon CloudWatch Logs.
- D. Configure Amazon CloudWatch Logs Insights to query the log files.
- E. Configure the instances to write the logs to an Amazon Elastic File System (Amazon EFS) volume.

Answer: CD

NEW QUESTION 7

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 profile.
- C. Configure the policy condition to restrict access based on the s3:ResourceTag/ClientId tag of each invoice.
- 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 bucket.
- H. Embed the keys into the script.
- I. Use the keys to generate the pre-signed URLs.

Answer: B

NEW QUESTION 8

A company uses AWS IAM Identity Center to manage access to its AWS accounts. The accounts are in an organization in AWS Organizations. A security engineer needs to set up delegated administration of IAM Identity Center in the organization's management account.

Which combination of steps should the security engineer perform in IAM Identity Center before configuring delegated administration? (Select THREE.)

- A. Grant least privilege access to the organization's management account.
- B. Create a new IAM Identity Center directory in the organization's management account.
- C. Set up a second AWS Region in the organization's management account.
- D. Create permission sets for use only in the organization's management account.
- E. Create IAM users for use only in the organization's management account.
- F. Create user assignments only in the organization's management account.

Answer: BDF

NEW QUESTION 9

A company is running its application on AWS. The company has a multi-environment setup, and each environment is isolated in a separate AWS account. The company has an organization in AWS Organizations to manage the accounts. There is a single dedicated security account for the organization. The company must create an inventory of all sensitive data that is stored in Amazon S3 buckets across the organization's accounts. The findings must be visible from a single location. Which solution will meet these requirements?

- A. Set the security account as the delegated administrator for Amazon Macie and AWS Security Hub.
- B. Enable and configure Macie to publish sensitive data findings to Security Hub.
- C. Set the security account as the delegated administrator for AWS Security Hub.
- D. In each account, configure Amazon Inspector to scan the S3 buckets for sensitive data.
- E. Publish sensitive data findings to Security Hub.
- F. In each account, configure Amazon Inspector to scan the S3 buckets for sensitive data.
- G. Enable Amazon Inspector integration with AWS Trusted Advisor.
- H. Publish sensitive data findings to Trusted Advisor.
- I. In each account, enable and configure Amazon Macie to detect sensitive data.
- J. Enable Macie integration with AWS Trusted Advisor.
- K. Publish sensitive data findings to Trusted Advisor.

Answer: A

NEW QUESTION 10

A company uses an organization in AWS Organizations to manage multiple AWS accounts. The company wants to centrally give users the ability to access Amazon Q Developer.

Which solution will meet this requirement?

- A. Enable AWS IAM Identity Center and set up Amazon Q Developer as an AWS managed application.
- B. Enable Amazon Cognito and create a new identity pool for Amazon Q Developer.
- C. Enable Amazon Cognito and set up Amazon Q Developer as an AWS managed application.
- D. Enable AWS IAM Identity Center and create a new identity pool for Amazon Q Developer.

Answer: A

NEW QUESTION 10

A company's data scientists use Amazon SageMaker with datasets stored in Amazon S3. Data older than 45 days must be removed according to policy.

Which action should enforce this policy?

- A. Configure an S3 Lifecycle rule to delete objects after 45 days.
- B. Create a Lambda function triggered on object upload to delete old data.
- C. Create a scheduled Lambda function to delete old objects monthly.
- D. Configure S3 Intelligent-Tiering.

Answer: A

NEW QUESTION 13

A security engineer configured VPC Flow Logs to publish to Amazon CloudWatch Logs. After 10 minutes, no logs appear. The issue is isolated to the IAM role associated with VPC Flow Logs.

What could be the reason?

- A. logs:GetLogEvents is missing.
- B. The engineer cannot assume the role.
- C. The vpc-flow-logs.amazonaws.com principal cannot assume the role.
- D. The role cannot tag the log stream.

Answer: C

NEW QUESTION 15

A company creates AWS Lambda functions from container images that are stored in Amazon Elastic Container Registry (Amazon ECR). The company needs to identify any software vulnerabilities in the container images and any code vulnerabilities in the Lambda functions.

Which solution will meet these requirements?

- A. Enable Amazon GuardDut
- B. Configure Amazon ECR scanning and Lambda code scanning in GuardDuty.
- C. Enable Amazon GuardDut
- D. Configure Runtime Monitoring and Lambda Protection in GuardDuty.
- E. Enable Amazon Inspector
- F. Configure Amazon ECR enhanced scanning and Lambda code scanning in Amazon Inspector.
- G. Enable AWS Security Hu
- H. Configure Runtime Monitoring and Lambda Protection in Security Hub.

Answer: C

NEW QUESTION 17

A consultant agency needs to perform a security audit for a company's production AWS account. Several consultants need access to the account. The consultant agency already has its own AWS account. The company requires multi-factor authentication (MFA) for all access to its production account. The company also forbids the use of long-term credentials.

Which solution will provide the consultant agency with access that meets these requirements?

- A. Create an IAM grou
- B. Create an IAM user for each consultan
- C. Add each user to the grou
- D. Turn on MFA for each consultant.
- E. Configure Amazon Cognito on the company??s production account to authenticate against the consultant agency's identity provider (IdP). Add MFA to a Cognito user pool.
- F. Create an IAM role in the consultant agency's AWS accoun
- G. Define a trust policy that requires MF
- H. In the trust policy, specify the company's production account as the principa
- I. Attach the trust policy to the role.
- J. Create an IAM role in the company??s production accoun
- K. Define a trust policy that requires MF
- L. In the trust policy, specify the consultant agency's AWS account as the principa
- M. Attach the trust policy to the role.

Answer: D

NEW QUESTION 20

A company runs a web application on a fleet of Amazon EC2 instances in an Auto Scaling group. Amazon GuardDuty and AWS Security Hub are enabled. The security engineer needs an automated response to anomalous traffic that follows AWS best practices and minimizes application disruption.

Which solution will meet these requirements?

- A. Use EventBridge to disable the instance profile access keys.
- B. Use EventBridge to invoke a Lambda function that removes the affected instance from the Auto Scaling group and isolates it with a restricted security group.
- C. Use Security Hub to update the subnet network ACL to block traffic.
- D. Send GuardDuty findings to Amazon SNS for email notification.

Answer: B

NEW QUESTION 24

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 outside of AWS.

What should the security engineer do to meet these requirements?

- A. Create security groups and attach them to all SQS queues.
- B. Modify network ACLs in all VPCs to restrict inbound traffic.

- C. Create interface VPC endpoints for Amazon SQ
- D. Restrict access using aws:SourceVpce and aws:PrincipalOrgId conditions.
- E. Use a third-party cloud access security broker (CASB).

Answer: C

NEW QUESTION 28

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 29

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 30

A company stores infrastructure and application code in web-based, third-party, Git-compatible code repositories outside of AWS. The company wants to give the code repositories the ability to securely authenticate and assume an existing IAM role within the company's AWS account by using OpenID Connect (OIDC). Which solution will meet these requirements?

- A. Create an OIDC identity provider (IdP) by using AWS Identity and Access Management (IAM) federatio
- B. Modify the trust policy of the IAM role to allow the code repositories to assume the IAM role.
- C. Use AWS Identity and Access Management (IAM) Roles Anywhere to create a trust anchor that uses OID
- D. Modify the trust policy of the IAM role to allow the code repositories to assume the IAM role.
- E. Set up an account instance of AWS IAM Identity Cente
- F. Configure access to the code repositories as a customer managed OIDC applicatio
- G. Grant the application access to the IAM role.
- H. Use AWS Resource Access Manager (AWS RAM) to create a new resource share that uses OID
- I. Limit the resource share to the specified code repositorie
- J. Grant the IAM role access to the resource share.

Answer: A

NEW QUESTION 34

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 36

A company is using AWS Organizations with nested OUs to manage AWS accounts. The company has a custom compliance monitoring service for the accounts. The monitoring service runs as an AWS Lambda function and is invoked by Amazon EventBridge Scheduler. The company needs to deploy the monitoring service in all existing and future accounts in the organization. The company must avoid using the organization's management account when the management account is not required. Which solution will meet these requirements?

- A. Create a CloudFormation stack set in the organization's management account and manually add new accounts.
- B. Configure a delegated administrator account for AWS CloudFormation.
- C. Create a CloudFormation StackSet in the delegated administrator account targeting the organization root with automatic deployment enabled.
- D. Use Systems Manager delegated administration and Automation to deploy the Lambda function and schedule.
- E. Create a Systems Manager Automation runbook in the management account and share it to accounts.

Answer: B

NEW QUESTION 38

A company must immediately disable compromised IAM users across all AWS accounts and collect all actions performed by the user in the last 7 days. Which solution will meet these requirements?

- A. Disable the IAM user and query CloudTrail logs in Amazon S3 using Athena.
- B. Remove IAM policies and query logs in Security Hub.
- C. Remove permission sets and query logs using CloudWatch Logs Insights.
- D. Disable the user in IAM Identity Center and query the organizational event data store.

Answer: D

NEW QUESTION 43

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 45

A company runs ECS services behind an internet-facing ALB that is the origin for CloudFront. An AWS WAF web ACL is associated with CloudFront, but clients can bypass it by accessing the ALB directly. Which solution will prevent direct access to the ALB?

- A. Use AWS PrivateLink with the ALB.
- B. Replace the ALB with an internal ALB.
- C. Restrict ALB listener rules to CloudFront IP ranges.
- D. Require a custom header from CloudFront and validate it at the ALB.

Answer: D

NEW QUESTION 49

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. Create an Application Load Balancer with the existing EC2 instances as a target group.
- B. Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to the ALB.
- C. Test to ensure the vulnerability has been mitigated, then redirect the Route 53 records to point to the ALB.
- D. Update security groups on the EC2 instances to prevent direct access from the internet.
- E. Create an Amazon CloudFront distribution specifying one EC2 instance as an origin.
- F. Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to the distribution.
- G. Test to ensure the vulnerability has been mitigated, then redirect the Route 53 records to point to CloudFront.
- H. Obtain the latest source code for the platform and make the necessary update.
- I. Test the updated code to ensure that the vulnerability has been mitigated, then deploy the patched version of the platform to the EC2 instances.
- J. Update the security group that is attached to the EC2 instances, removing access from the internet to the TCP port used by the SQL databases.
- K. Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to the EC2 instances.

Answer: A

NEW QUESTION 52

A company that uses AWS Organizations is using AWS IAM Identity Center to administer access to AWS accounts. A security engineer is creating a custom permission set in IAM Identity Center. The company will use the permission set across multiple accounts. An AWS managed policy and a customer managed policy are attached to the permission set. The security engineer has full administrative permissions and is operating in the management account. When the security engineer attempts to assign the permission set to an IAM Identity Center user who has access to multiple accounts, the assignment fails. What should the security engineer do to resolve this failure?

- A. Create the customer managed policy in every account where the permission set is assigned.
- B. Give the customer managed policy the same name and same permissions in each account.
- C. Remove either the AWS managed policy or the customer managed policy from the permission set.
- D. Create a second permission set that includes the removed policy.
- E. Apply the permission sets separately to the user.
- F. Evaluate the logic of the AWS managed policy and the customer managed policy.
- G. Resolve any policy conflicts in the permission set before deployment.

- H. Do not add the new permission set to the use
- I. Instead, edit the user's existing permission set to include the AWS managed policy and the customer managed policy.

Answer: A

NEW QUESTION 55

A company runs a public web application on Amazon EKS behind Amazon CloudFront and an Application Load Balancer (ALB). A security engineer must send a notification to an existing Amazon SNS topic when the application receives 10,000 requests from the same end-user IP address within any 5-minute period. Which solution will meet these requirements?

- A. Configure CloudFront standard logging and CloudWatch Logs metric filters.
- B. Configure VPC Flow Logs and CloudWatch Logs metric filters.
- C. Configure an AWS WAF web ACL with an ASN match rule and CloudWatch alarms.
- D. Configure an AWS WAF web ACL with a rate-based rule.
- E. Associate it with CloudFront.
- F. Create a CloudWatch alarm to notify SNS.

Answer: D

NEW QUESTION 59

A company needs to detect unauthenticated access to its Amazon Elastic Kubernetes Service (Amazon EKS) clusters. The solution must require no additional configuration of the existing EKS deployment.

Which solution will meet these requirements with the LEAST operational effort?

- A. Install a third-party security add-on.
- B. Enable AWS Security Hub and monitor Kubernetes findings.
- C. Monitor CloudWatch Container Insights metrics for EKS.
- D. Enable Amazon GuardDuty and use EKS Audit Log Monitoring.

Answer: D

NEW QUESTION 61

A security engineer receives a notice about suspicious activity from a Linux-based Amazon EC2 instance that uses Amazon Elastic Block Store (Amazon EBS)-based storage. The instance is making connections to known malicious addresses. The instance is in a development account within a VPC that is in the us-east-1 Region. The VPC contains an internet gateway and has a subnet in us-east-1a and us-east-1b. Each subnet is associated with a route table that uses the internet gateway as a default route. Each subnet also uses the default network ACL. The suspicious EC2 instance runs within the us-east-1b subnet. During an initial investigation, a security engineer discovers that the suspicious instance is the only instance that runs in the subnet.

Which response will immediately mitigate the attack and help investigate the root cause?

- A. Log in to the suspicious instance and use the netstat command to identify remote connection
- B. Use the IP addresses from these remote connections to create deny rules in the security group of the instance
- C. Install diagnostic tools on the instance for investigation
- D. Update the outbound network ACL for the subnet in us-east-1b to explicitly deny all connections as the first rule during the investigation of the instance.
- E. Update the outbound network ACL for the subnet in us-east-1b to explicitly deny all connections as the first rule
- F. Replace the security group with a new security group that allows connections only from a diagnostics security group
- G. Update the outbound network ACL for the us-east-1b subnet to remove the deny all rule
- H. Launch a new EC2 instance that has diagnostic tool
- I. Assign the new security group to the new EC2 instance
- J. Use the new EC2 instance to investigate the suspicious instance.
- K. Ensure that the Amazon Elastic Block Store (Amazon EBS) volumes that are attached to the suspicious EC2 instance will not delete upon termination
- L. Terminate the instance
- M. Launch a new EC2 instance in us-east-1a that has diagnostic tool
- N. Mount the EBS volumes from the terminated instance for investigation.
- O. Create an AWS WAF web ACL that denies traffic to and from the suspicious instance
- P. Attach the AWS WAF web ACL to the instance to mitigate the attack
- Q. Log in to the instance and install diagnostic tools to investigate the instance.

Answer: C

NEW QUESTION 63

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The SCS-C03 Practice Test Here](#)