



Amazon-Web-Services

Exam Questions SCS-C03

AWS Certified Security - Specialty

NEW QUESTION 1

A company has a large fleet of Amazon Linux 2 Amazon EC2 instances that run an application processing sensitive data. Compliance requirements include no exposed management ports, full session logging, and authentication through AWS IAM Identity Center. DevOps engineers occasionally need access for troubleshooting.

Which solution will provide remote access while meeting these requirements?

- A. Grant access to the EC2 serial console and allow IAM role access.
- B. Enable EC2 Instance Connect and configure security groups accordingly.
- C. Assign an EC2 instance role that allows access to AWS Systems Manager
- D. Create an IAM policy that grants access to Systems Manager Session Manager and assign it to an IAM Identity Center role.
- E. Use Systems Manager Automation to temporarily open remote access ports.

Answer: C

NEW QUESTION 2

A company's security engineer receives an abuse notification from AWS indicating that malware is being hosted from the company's AWS account. The security engineer discovers that an IAM user created a new Amazon S3 bucket without authorization.

Which combination of steps should the security engineer take to MINIMIZE the consequences of this compromise? (Select THREE.)

- A. Encrypt all AWS CloudTrail logs.
- B. Turn on Amazon GuardDuty.
- C. Change the password for all IAM users.
- D. Rotate or delete all AWS access keys.
- E. Take snapshots of all Amazon Elastic Block Store (Amazon EBS) volumes.
- F. Delete any resources that are unrecognized or unauthorized.

Answer: BDF

NEW QUESTION 3

A company is attempting to conduct forensic analysis on an Amazon EC2 instance, but the company is unable to connect to the instance by using AWS Systems Manager Session Manager. The company has installed AWS Systems Manager Agent (SSM Agent) on the EC2 instance.

The EC2 instance is in a subnet in a VPC that does not have an internet gateway attached. The company has associated a security group with the EC2 instance. The security group does not have inbound or outbound rules. The subnet's network ACL allows all inbound and outbound traffic.

Which combination of actions will allow the company to conduct forensic analysis on the EC2 instance without compromising forensic data? (Select THREE.)

- A. Update the EC2 instance security group to add a rule that allows outbound traffic on port 443 for 0.0.0.0/0.
- B. Update the EC2 instance security group to add a rule that allows inbound traffic on port 443 to the VPC's CIDR range.
- C. Create an EC2 key pair
- D. Associate the key pair with the EC2 instance.
- E. Create a VPC interface endpoint for Systems Manager in the VPC where the EC2 instance is located.
- F. Attach a security group to the VPC interface endpoint
- G. Allow inbound traffic on port 443 to the VPC's CIDR range.
- H. Create a VPC interface endpoint for the EC2 instance in the VPC where the EC2 instance is located.

Answer: ADE

NEW QUESTION 4

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 5

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 6

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 7

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 8

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 9

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 needs to build a code-signing solution using an AWS KMS asymmetric key and must store immutable evidence of key creation and usage for compliance and audit purposes. Which solution meets these requirements?

- A. Create an Amazon S3 bucket with S3 Object Lock enabled.
- B. Create an AWS CloudTrail trail with log file validation enabled for KMS events.
- C. Store logs in the bucket and grant auditors access.
- D. Log application events to Amazon CloudWatch Logs and export them.
- E. Capture KMS API calls using EventBridge and store them in DynamoDB.
- F. Track KMS usage with CloudWatch metrics and dashboards.

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 11

A company has security requirements for Amazon Aurora MySQL databases regarding encryption, deletion protection, public access, and audit logging. The company needs continuous monitoring and real-time visibility into compliance status. Which solution will meet these requirements?

- A. Use AWS Audit Manager with a custom framework.
- B. Enable AWS Config and use managed rules to monitor Aurora MySQL compliance.
- C. Use AWS Security Hub configuration policies.
- D. Use EventBridge and Lambda with custom metrics.

Answer: B

NEW QUESTION 16

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 20

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 21

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 Inspector
- 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 24

A company requires a specific software application to be installed on all new and existing Amazon EC2 instances across an AWS Organization. SSM Agent is installed and active. How can the company continuously monitor deployment status of the software application?

- A. Use AWS Config organization-wide with the ec2-managedinstance-applications-required managed rule and specify the application name.

- B. Use approved AMLs rule organization-wide.
- C. Use Distributor package and review output.
- D. Use Systems Manager Application Manager inventory filtering.

Answer: A

NEW QUESTION 27

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. Restrict access to authenticated users only.
- C. Associate AWS WAF with the Cognito user pool.
- D. Monitor requests with CloudWatch.

Answer: A

NEW QUESTION 28

A company is implementing new compliance requirements to meet customer needs. According to the new requirements, the company must not use any Amazon RDS DB instances or DB clusters that lack encryption of the underlying storage. The company needs a solution that will generate an email alert when an unencrypted DB instance or DB cluster is created. The solution also must terminate the unencrypted DB instance or DB cluster.

Which solution will meet these requirements in the MOST operationally efficient manner?

- A. Create an AWS Config managed rule to detect unencrypted RDS storag
- B. Configure an automatic remediation action to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic that includes an AWS Lambda function and an email delivery target as subscriber
- C. Configure the Lambda function to delete the unencrypted resource.
- D. Create an AWS Config managed rule to detect unencrypted RDS storag
- E. Configure a manual remediation action to invoke an AWS Lambda functio
- F. Configure the Lambda function to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic and to delete the unencrypted resource.
- G. Create an Amazon EventBridge rule that evaluates RDS event patterns and is initiated by the creation of DB instances or DB cluster
- H. Configure the rule to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic that includes an AWS Lambda function and an email delivery target as subscriber
- I. Configure the Lambda function to delete the unencrypted resource.
- J. Create an Amazon EventBridge rule that evaluates RDS event patterns and is initiated by the creation of DB instances or DB cluster
- K. Configure the rule to invoke an AWS Lambda functio
- L. Configure the Lambda function to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic and to delete the unencrypted resource.

Answer: A

NEW QUESTION 31

A company runs a global ecommerce website using Amazon CloudFront. The company must block traffic from specific countries to comply with data regulations. Which solution will meet these requirements MOST cost-effectively?

- A. Use AWS WAF IP match rules.
- B. Use AWS WAF geo match rules.
- C. Use CloudFront geo restriction to deny the countries.
- D. Use geolocation headers in CloudFront.

Answer: C

NEW QUESTION 34

Notify when IAM roles are modified.

- A. Use Amazon Detective.
- B. Use EventBridge with CloudTrail events.
- C. Use CloudWatch metric filters.
- D. Use CloudWatch subscription filters.

Answer: B

NEW QUESTION 36

A security engineer needs to implement a solution to identify any sensitive data that is stored in an Amazon S3 bucket. The solution must report on sensitive data in the S3 bucket by using an existing Amazon Simple Notification Service (Amazon SNS) topic.

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

- A. Enable AWS Confi
- B. Configure AWS Config to monitor for sensitive data in the S3 bucket and to send notifications to the SNS topic.
- C. Create an AWS Lambda function to scan the S3 bucket for sensitive data that matches a patter
- D. Program the Lambda function to send notifications to the SNS topic.
- E. Configure Amazon Macie to use managed data identifiers to identify and categorize sensitive dat
- F. Create an Amazon EventBridge rule to send notifications to the SNS topic.
- G. Enable Amazon GuardDut
- H. Configure AWS CloudTrail S3 data event
- I. Create an Amazon CloudWatch alarm that reacts to GuardDuty findings and sends notifications to the SNS topic.

Answer: C

NEW QUESTION 39

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 41

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 AL
- C. Test to ensure the vulnerability has been mitigated, then redirect the Route 53 records to point to the AL
- 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 origi
- F. Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to the distributio
- 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 databas
- 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 46

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 rul
- E. Associate it with CloudFron
- F. Create a CloudWatch alarm to notify SNS.

Answer: D

NEW QUESTION 50

A company recently experienced a malicious attack on its cloud-based environment. The company successfully contained and eradicated the attack. A security engineer is performing incident response work. The security engineer needs to recover an Amazon RDS database cluster to the last known good version. The database cluster is configured to generate automated backups with a retention period of 14 days. The initial attack occurred 5 days ago at exactly 3:15 PM. Which solution will meet this requirement?

- A. Identify the Regional cluster ARN for the databas
- B. Use the ARN to restore the Regional cluster by using the restore to point in time featur
- C. Set a target time 5 days ago at 3:14 PM.
- D. Identify the Regional cluster ARN for the databas
- E. List snapshots that have been taken of the cluste
- F. Restore the database by using the snapshot that has a creation time that is closest to 5 days ago at 3:14 PM.
- G. List all snapshots that have been taken of all the company's RDS database
- H. Identify the snapshot that was taken closest to 5 days ago at 3:14 PM and restore it.
- I. Identify the Regional cluster ARN for the databas
- J. Use the ARN to restore the Regional cluster by using the restore to point in time featur
- K. Set a target time 14 days ago.

Answer: A

NEW QUESTION 54

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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](#)