

Amazon-Web-Services

Exam Questions SCS-C03

AWS Certified Security - Specialty



NEW QUESTION 1

AWS Config cannot deliver configuration snapshots to Amazon S3. Which TWO actions will remediate this issue?

- A. Verify the S3 bucket policy allows config.amazonaws.com.
- B. Verify the IAM role has s3:GetBucketAcl and s3:PutObject permissions.
- C. Verify the S3 bucket can assume the IAM role.
- D. Verify IAM policy allows AWS Config to write logs.
- E. Modify AWS Config API permissions.

Answer: AB

NEW QUESTION 2

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 3

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 4

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 5

A company hosts its public website on Amazon EC2 instances behind an Application Load Balancer (ALB). The website is experiencing a global DDoS attack from a specific IoT device brand that uses a unique user agent. A security engineer is creating an AWS WAF web ACL and will associate it with the ALB.

Which rule statement will mitigate the current attack and future attacks from these IoT devices without blocking legitimate customers?

- A. Use an IP set match rule statement.
- B. Use a geographic match rule statement.
- C. Use a rate-based rule statement.
- D. Use a string match rule statement on the user agent.

Answer: D

NEW QUESTION 6

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 7

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 8

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 9

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 10

An application is running on an Amazon EC2 instance that has an IAM role attached. The IAM role provides access to an AWS Key Management Service (AWS KMS) customer managed key and an Amazon S3 bucket. The key is used to access 2 TB of sensitive data that is stored in the S3 bucket. A security engineer discovers a potential vulnerability on the EC2 instance that could result in the compromise of the sensitive data. Due to other critical operations, the security engineer cannot immediately shut down the EC2 instance for vulnerability patching.

What is the FASTEST way to prevent the sensitive data from being exposed?

- A. Download the data from the existing S3 bucket to a new EC2 instance.
- B. Then delete the data from the S3 bucket.
- C. Re-encrypt the data with a client-based key.
- D. Upload the data to a new S3 bucket.
- E. Block access to the public range of S3 endpoint IP addresses by using a host-based firewall.
- F. Ensure that internet-bound traffic from the affected EC2 instance is routed through the host-based firewall.
- G. Revoke the IAM role's active session permission.
- H. Update the S3 bucket policy to deny access to the IAM role.
- I. Remove the IAM role from the EC2 instance profile.
- J. Disable the current key.
- K. Create a new KMS key that the IAM role does not have access to, and re-encrypt all the data with the new key.
- L. Schedule the compromised key for deletion.

Answer: C

NEW QUESTION 10

A company has a VPC that has no internet access and has the private DNS hostnames option enabled. An Amazon Aurora database is running inside the VPC. A security engineer wants to use AWS Secrets Manager to automatically rotate the credentials for the Aurora database. The security engineer configures the Secrets

Manager default AWS Lambda rotation function to run inside the same VPC that the Aurora database uses. However, the security engineer determines that the password cannot be rotated properly because the Lambda function cannot communicate with the Secrets Manager endpoint. What is the MOST secure way that the security engineer can give the Lambda function the ability to communicate with the Secrets Manager endpoint?

- A. Add a NAT gateway to the VPC to allow access to the Secrets Manager endpoint.
- B. Add a gateway VPC endpoint to the VPC to allow access to the Secrets Manager endpoint.
- C. Add an interface VPC endpoint to the VPC to allow access to the Secrets Manager endpoint.
- D. Add an internet gateway for the VPC to allow access to the Secrets Manager endpoint.

Answer: C

NEW QUESTION 14

A security engineer has designed a VPC to segment private traffic from public traffic. The VPC includes two Availability Zones. Each Availability Zone contains one public subnet and one private subnet. Three route tables exist: one for the public subnets and one for each private subnet. The security engineer discovers that all four subnets are routing traffic through the internet gateway that is attached to the VPC. Which combination of steps should the security engineer take to remediate this scenario? (Select TWO.)

- A. Verify that a NAT gateway has been provisioned in the public subnet in each Availability Zone.
- B. Verify that a NAT gateway has been provisioned in the private subnet in each Availability Zone.
- C. Modify the route tables for the public subnets to add a local route to the VPC CIDR range.
- D. Modify the route tables for the private subnets to route 0.0.0.0/0 to the NAT gateway in the public subnet of the same Availability Zone.
- E. Modify the route tables for the private subnets to route 0.0.0.0/0 to the internet gateway.

Answer: AD

NEW QUESTION 18

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 21

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 23

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 28

A security administrator is setting up a new AWS account. The security administrator wants to secure the data that a company stores in an Amazon S3 bucket. The security administrator also wants to reduce the chance of unintended data exposure and the potential for misconfiguration of objects that are in the S3 bucket. Which solution will meet these requirements with the LEAST operational overhead?

- A. Configure the S3 Block Public Access feature for the AWS account.
- B. Configure the S3 Block Public Access feature for all objects that are in the bucket.
- C. Deactivate ACLs for objects that are in the bucket.
- D. Use AWS PrivateLink for Amazon S3 to access the bucket.

Answer: A

NEW QUESTION 33

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 34

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 38

A company runs an internet-accessible application on several Amazon EC2 instances that run Windows Server. The company used an instance profile to configure the EC2 instances. A security team currently accesses the VPC that hosts the EC2 instances by using an AWS Site-to-Site VPN tunnel from an on-premises office. The security team issues a policy that requires all external access to the VPC to be blocked in the event of a security incident. However, during an incident, the security team must be able to access the EC2 instances to obtain forensic information on the instances. Which solution will meet these requirements?

- A. Install EC2 Instance Connect on the EC2 instance
- B. Update the IAM policy for the IAM role to grant the required permission
- C. Use the AWS CLI to open a tunnel to connect to the instances.
- D. Install EC2 Instance Connect on the EC2 instance
- E. Configure the instances to permit access to the ec2-instance-connect command use
- F. Use the AWS Management Console to connect to the EC2 instances.
- G. Create an EC2 Instance Connect endpoint in the VP
- H. Configure an appropriate security group to allow access between the EC2 instances and the endpoint
- I. Use the AWS CLI to open a tunnel to connect to the instances.
- J. Create an EC2 Instance Connect endpoint in the VP
- K. Configure an appropriate security group to allow access between the EC2 instances and the endpoint
- L. Use the AWS Management Console to connect to the EC2 instances.

Answer: D

NEW QUESTION 43

A company has a single AWS account and uses an Amazon EC2 instance to test application code. The company recently discovered that the instance was compromised and was serving malware. Analysis showed that the instance was compromised 35 days ago. A security engineer must implement a continuous monitoring solution that automatically notifies the security team by email for high severity findings as soon as possible. Which combination of steps should the security engineer take to meet these requirements? (Select THREE.)

- A. Enable AWS Security Hub in the AWS account.
- B. Enable Amazon GuardDuty in the AWS account.
- C. Create an Amazon Simple Notification Service (Amazon SNS) topic
- D. Subscribe the security team's email distribution list to the topic.
- E. Create an Amazon Simple Queue Service (Amazon SQS) queue
- F. Subscribe the security team's email distribution list to the queue.
- G. Create an Amazon EventBridge rule for GuardDuty findings of high severity
- H. Configure the rule to publish a message to the topic.
- I. Create an Amazon EventBridge rule for Security Hub findings of high severity
- J. Configure the rule to publish a message to the queue.

Answer: BCE

NEW QUESTION 48

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 Config
- B. Create a proactive AWS Config Custom Policy rule
- C. Create a Guard clause to evaluate the S3 bucket policies to check for a value of True for the aws:SecureTransport condition key
- D. If the AWS Config rule evaluates to NON_COMPLIANT, block resource creation.
- E. Enable AWS Config
- F. Configure the s3-bucket-ssl-requests-only AWS Config managed rule and set the rule trigger type to Hybrid
- 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 False
- H. Configure automatic remediation
- I. Set the runbook as the target of the rule.
- J. Enable Amazon Inspector
- K. Create a custom AWS Lambda rule

- 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 trail
- O. Enable S3 data events on the trail
- 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 50

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 group
- B. Create an IAM user for each consultant
- C. Add each user to the group
- 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 account
- G. Define a trust policy that requires MFA
- H. In the trust policy, specify the company's production account as the principal
- I. Attach the trust policy to the role.
- J. Create an IAM role in the company's production account
- K. Define a trust policy that requires MFA
- L. In the trust policy, specify the consultant agency's AWS account as the principal
- M. Attach the trust policy to the role.

Answer: D

NEW QUESTION 53

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 Firehose
- E. Deliver logs to Amazon S3 and query them with Amazon Athena.

Answer: D

NEW QUESTION 54

A company uses AWS to run a web application that manages ticket sales in several countries. The company recently migrated the application to an architecture that includes Amazon API Gateway, AWS Lambda, and Amazon Aurora Serverless. The company needs the application to comply with Payment Card Industry Data Security Standard (PCI DSS) v4.0. A security engineer must generate a report that shows the effectiveness of the PCI DSS v4.0 controls that apply to the application. The company's compliance team must be able to add manual evidence to the report.

Which solution will meet these requirements?

- A. Enable AWS Trusted Advisor
- B. Configure all the Trusted Advisor checks
- C. Manually map the checks against the PCI DSS v4.0 standard to generate the report.
- D. Enable and configure AWS Config
- E. Deploy the Operational Best Practices for PCI DSS conformance pack in AWS Config
- F. Use AWS Config to generate the report.
- G. Enable AWS Security Hub
- H. Enable the Security Hub PCI DSS security standard
- I. Use the AWS Management Console to download the report from the security standard.
- J. Create an AWS Audit Manager assessment that uses the AWS managed PCI DSS v4.0 standard framework
- K. Add all evidence to the assessment
- L. Generate the report in Audit Manager for download.

Answer: D

NEW QUESTION 57

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 59

A company is running an application in the eu-west-1 Region. The application uses an AWS Key Management Service (AWS KMS) customer managed key to encrypt sensitive data. The company plans to deploy the application in the eu-north-1 Region. A security engineer needs to implement a key management solution for the application deployment in the new Region. The security engineer must minimize changes to the application code. Which change should the security engineer make to the AWS KMS configuration to meet these requirements?

- A. Update the key policies in eu-west-1. Point the application in eu-north-1 to use the same customer managed key as the application in eu-west-1.
- B. Allocate a new customer managed key to eu-north-1 to be used by the application that is deployed in that Region.
- C. Allocate a new customer managed key to eu-north-1. Create the same alias name for both key
- D. Configure the application deployment to use the key alias.
- E. Allocate a new customer managed key to eu-north-1. Create an alias for eu--1. Change the application code to point to the alias for eu--1.

Answer: C

NEW QUESTION 63

A company needs to scan all AWS Lambda functions for code vulnerabilities.

- A. Use Amazon Macie.
- B. Enable Amazon Inspector Lambda scanning.
- C. Use GuardDuty and Security Hub.
- D. Use GuardDuty Lambda Protection.

Answer: B

NEW QUESTION 64

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 69

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 73

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 78

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 80

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 85

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 86

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 90

A company must capture AWS CloudTrail data events and must retain the logs for 7 years. The logs must be immutable and must be available to be searched by complex queries. The company also needs to visualize the data from the logs. Which solution will meet these requirements MOST cost-effectively?

- A. Create a CloudTrail Lake data store
- B. Implement CloudTrail Lake dashboards to visualize and query the results.
- C. Use the CloudTrail Event History feature in the AWS Management Console
- D. Visualize and query the results in the console.
- E. Send the CloudTrail logs to an Amazon S3 bucket
- F. Provision a persistent Amazon EMR cluster that has access to the S3 bucket
- G. Enable S3 Object Lock on the S3 bucket
- H. Use Apache Spark to perform queries
- I. Use Amazon QuickSight for visualizations.
- J. Send the CloudTrail logs to a log group in Amazon CloudWatch Logs
- K. Set the CloudWatch Logs stream to send the data to an Amazon OpenSearch Service domain
- L. Enable cold storage for the OpenSearch Service domain
- M. Use OpenSearch Dashboards for visualizations and queries.

Answer: A

NEW QUESTION 91

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 Config
- 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 pattern
- 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 data
- F. Create an Amazon EventBridge rule to send notifications to the SNS topic.
- G. Enable Amazon GuardDuty
- 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 93

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 94

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 98

.....

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](#)