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 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 4
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 5
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 6
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 instanc
B. Send the custom logs to CloudTrail instead of CloudWatch.

C. Add Amazon S3 to the trust policy of the EC2 instanc
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 instanc
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 7
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 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
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 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 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 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 endpoin
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 endpoin
L. Use the AWS Management Console to connect to the EC2 instances.

Answer: D

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 17
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 21
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 25
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 27
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 29
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 33
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 37
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 40
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 42
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 stor
B. Implement CloudTrail Lake dashboards to visualize and query the results.
C. Use the CloudTrail Event History feature in the AWS Management Consol
D. Visualize and query the results in the console.
E. Send the CloudTrail logs to an Amazon S3 bucke
F. Provision a persistent Amazon EMR cluster that has access to the S3 bucke
G. Enable S3 Object Lock on the S3 bucke
H. Use Apache Spark to perform querie
I. Use Amazon QuickSight for visualizations.
J. Send the CloudTrail logs to a log group in Amazon CloudWatch Log
K. Set the CloudWatch Logs stream to send the data to an Amazon OpenSearch Service domai
L. Enable cold storage for the OpenSearch Service domai
M. Use OpenSearch Dashboards for visualizations and queries.

Answer: A

NEW QUESTION 46
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 47
A company uploads data files as objects into an Amazon S3 bucket. A vendor downloads the objects to perform data processing.
A security engineer must implement a solution that prevents objects from residing in the S3 bucket for longer than 72 hours.

A. Configure S3 Versioning to expire object versions that have been in the bucket for 72 hours.
B. Configure an S3 Lifecycle configuration rule on the bucket to expire objects after 72 hours.
C. Use the S3 Intelligent-Tiering storage class and configure expiration after 72 hours.
D. Generate presigned URLs that expire after 72 hours.

Answer: B

NEW QUESTION 48
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 assigne
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 se
D. Create a second permission set that includes the removed polic
E. Apply the permission sets separately to the user.
F. Evaluate the logic of the AWS managed policy and the customer managed polic
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 53
A company must inventory sensitive data across all Amazon S3 buckets in all accounts from a single security account.

A. Delegate Amazon Macie and Security Hub administration.
B. Use Amazon Inspector with Security Hub.
C. Use Inspector with Trusted Advisor.
D. Use Macie with Trusted Advisor.

Answer: A

NEW QUESTION 56
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 60
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 62
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 66
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 instanc
C. Install diagnostic tools on the instance for investigatio
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 rul
F. Replace the security group with a new security group that allows connections only from a diagnostics security grou
G. Update the outbound network ACL for the us-east-1b subnet to remove the deny all rul
H. Launch a new EC2 instance that has diagnostic tool
I. Assign the new security group to the new EC2 instanc
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 terminatio
L. Terminate the instanc
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 instanc
P. Attach the AWS WAF web ACL to the instance to mitigate the attac
Q. Log in to the instance and install diagnostic tools to investigate the instance.

Answer: C

NEW QUESTION 70
.....

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