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 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 Manage
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 3
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 4
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 5
A company??s developers are using AWS Lambda function URLs to invoke functions directly. The company must ensure that developers cannot configure or deploy unauthenticated functions inproduction accounts. The company wants to meet this requirement by using AWS Organizations. The solution must not require additional work for the developers.
Which solution will meet these requirements?

A. Require the developers to configure all function URLs to support cross-origin resource sharing (CORS) when the functions are called from a different domain.
B. Use an AWS WAF delegated administrator account to view and block unauthenticated access to function URLs in production accounts, based on the OU of accounts that are using the functions.
C. Use SCPs to allow all lambda:CreateFunctionUrlConfig and lambda:UpdateFunctionUrlConfig actions that have a lambda:FunctionUrlAuthType condition key value of AWS_IAM.
D. Use SCPs to deny all lambda:CreateFunctionUrlConfig and lambda:UpdateFunctionUrlConfig actions that have a lambda:FunctionUrlAuthType condition key value of NONE.

Answer: D

NEW QUESTION 6
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 7
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 8
A company wants to establish separate AWS Key Management Service (AWS KMS) keys to use for different AWS services. The company??s security engineer created a key policy to allow the infrastructure deployment team to create encrypted Amazon Elastic Block Store (Amazon EBS) volumes by assuming the InfrastructureDeployment IAM role. The security engineer recently discovered that IAM roles other than the InfrastructureDeployment role used this key for other services.
Which change to the policy should the security engineer make to resolve these issues?

A. In the statement block that contains the Sid "Allow use of the key", under the "Condition" block, change StringEquals to StringLike.
B. In the policy document, remove the statement block that contains the Sid "Enable IAM User Permissions". Add key management policies to the KMS policy.
C. In the statement block that contains the Sid "Allow use of the key", under the "Condition" block, change the kms:ViaService value to ec2.us-east-1.amazonaws.com.
D. In the policy document, add a new statement block that grants the kms:Disable* permission to the security engineer's IAM role.

Answer: C

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

Answer: B

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

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

Answer: B

NEW QUESTION 13
A company 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 14
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 18
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 21
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 26
A company is using AWS CloudTrail and Amazon CloudWatch to monitor resources in an AWS account. The company??s developers have been using an IAM role in the account for the last 3 months.
A security engineer needs to refine the customer managed IAM policy attached to the role to ensure that the role provides least privilege access.
Which solution will meet this requirement with the LEAST effort?

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

Answer: A

NEW QUESTION 27
A company 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 32
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 35
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 37
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 41
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 45
A company needs a cloud-based, managed desktop solution for its workforce of remote employees. The company wants to ensure that the employees can access the desktops only by using company-provided devices. A security engineer must design a solution that will minimize cost and management overhead.
Which solution will meet these requirements?

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

Answer: D

NEW QUESTION 50
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 51
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 grou
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 56
A security engineer is designing a solution that will provide end-to-end encryption between clients and Docker containers running in Amazon Elastic Container Service (Amazon ECS). This solution must also handle volatile traffic patterns.
Which solution would have the MOST scalability and LOWEST latency?

A. Configure a Network Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers.
B. Configure an Application Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers.
C. Configure a Network Load Balancer with a TCP listener to pass through TLS traffic to the containers.
D. Configure Amazon Route 53 to use multivalue answer routing to send traffic to the containers.

Answer: C

NEW QUESTION 58
A company has a web application that reads from and writes to an Amazon S3 bucket. The company needs to authenticate all S3 API calls with AWS credentials.
Which solution will provide the application with AWS credentials?

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

Answer: B

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

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

D. Use key policies to restrict access to the appropriate IAM groups.

Answer: C

NEW QUESTION 65
.....

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