Amazon-Web-Services

Exam Questions SCS-C03

AWS Certified Security - Specialty

NEW QUESTION 1
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 2
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 acces
H. Grant the application team permissions to use the key.

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??s application team needs a new AWS Key Management Service (AWS KMS) customer managed key to use with Amazon S3. The company??s security policy requires separate keys for different AWS services to limit security exposure.
How can a security engineer limit the KMS customer managed key to work with only Amazon S3?

A. Configure the key policy to allow only Amazon S3 to perform the kms:Encrypt action.
B. Configure the key policy to allow KMS actions only when the value for the kms:ViaService condition key matches the Amazon S3 service name.
C. Configure the application??s IAM role policy to allow Amazon S3 to perform the iam:PassRole action.
D. Configure the application??s IAM role policy to allow only S3 operations when the operations are combined with the KMS customer managed key.

Answer: B

NEW QUESTION 5
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 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 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 pai
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 endpoin
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 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 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 10
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 10
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 15
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 Hu
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 Hu
D. In each account, configure Amazon Inspector to scan the S3 buckets for sensitive dat
E. Publish sensitive data findings to Security Hub.
F. In each account, configure Amazon Inspector to scan the S3 buckets for sensitive dat
G. Enable Amazon Inspector integration with AWS Trusted Adviso
H. Publish sensitive data findings to Trusted Advisor.
I. In each account, enable and configure Amazon Macie to detect sensitive dat
J. Enable Macie integration with AWS Trusted Adviso
K. Publish sensitive data findings to Trusted Advisor.

Answer: A

NEW QUESTION 17
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 19
A company has an encrypted Amazon Aurora DB cluster in the us-east-1 Region that uses an AWS KMS customer managed key. The company must copy a DB snapshot to the us- west-1 Region but cannot access the encryption key across Regions.
What should the company do to properly encrypt the snapshot in us-west-1?

A. Store the customer managed key in AWS Secrets Manager in us-west-1.
B. Create a new customer managed key in us-west-1 and use it to encrypt the snapshot.
C. Create an IAM policy to allow access to the key in us-east-1 from us-west-1.
D. Create an IAM policy that allows RDS in us-west-1 to access the key in us-east-1.

Answer: B

NEW QUESTION 24
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 25
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 29
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 33
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 36
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 37
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 41
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 Inspecto
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 42
A security engineer needs to prepare Amazon EC2 instances for quarantine during a security incident. AWS Systems Manager Agent (SSM Agent) is installed, and a script exists to install and update forensic tools.
Which solution will quarantine EC2 instances during a security incident?

A. Track SSM Agent versions with AWS Config.
B. Configure Session Manager to deny external connections.
C. Store the script in Amazon S3 and grant read access.
D. Configure IAM permissions for the SSM Agent to run the script as a Systems Manager Run Command document.

Answer: D

NEW QUESTION 44
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 47
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 48
A company has a PHP-based web application that uses Amazon S3 as an object store for user files. The S3 bucket is configured for server-side encryption with Amazon S3 managed keys (SSE-S3). New requirements mandate full control of encryption keys.
Which combination of steps must a security engineer take to meet these requirements? (Select THREE.)

A. Create a new customer managed key in AWS Key Management Service (AWS KMS).
B. Change the SSE-S3 configuration on the S3 bucket to server-side encryption with customer-provided keys (SSE-C).
C. Configure the PHP SDK to use the SSE-S3 key before upload.
D. Create an AWS managed key for Amazon S3 in AWS KMS.
E. Change the SSE-S3 configuration on the S3 bucket to server-side encryption with AWS KMS managed keys (SSE-KMS).
F. Change all the S3 objects in the bucket to use the new encryption key.

Answer: AEF

NEW QUESTION 50
A company is using AWS Organizations with nested OUs to manage AWS accounts. The company has a custom compliance monitoring service for the accounts. The monitoring service runs as an AWS Lambda function and is invoked by Amazon EventBridge Scheduler.
The company needs to deploy the monitoring service in all existing and future accounts in the organization. The company must avoid using the organization's management account when the management account is not required.
Which solution will meet these requirements?

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

Answer: B

NEW QUESTION 52
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 56
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 57
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 61
A company is running a new workload across accounts in an organization in AWS Organizations. All running resources must have a tag of CostCenter, and the tag must have one of three approved values. The company must enforce this policy and must prevent any changes of the CostCenter tag to a non-approved value.
Which solution will meet these requirements?

A. Use AWS Config custom policy rule and an SCP to deny non-approved aws:RequestTag/CostCenter values.
B. Use CloudTrail + EventBridge + Lambda to block creation.
C. Enable tag policies, define allowed values, enforce noncompliant operations, and use an SCP to deny creation when aws:RequestTag/CostCenter is null.
D. Enable tag policies and use EventBridge + Lambda to block changes.

Answer: C

NEW QUESTION 63
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 68
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 69
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 71
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 74
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 78
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 83
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 86
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 89
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 90
.....

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