Exam Questions SCS-C03

AWS Certified Security - Specialty

https://www.2passeasy.com/dumps/SCS-C03/

NEW QUESTION 1
A company has a large fleet of Amazon Linux 2 Amazon EC2 instances that run an application processing sensitive data. Compliance requirements include no exposed management ports, full session logging, and authentication through AWS IAM Identity Center. DevOps engineers occasionally need access for troubleshooting.
Which solution will provide remote access while meeting these requirements?

A. Grant access to the EC2 serial console and allow IAM role access.
B. Enable EC2 Instance Connect and configure security groups accordingly.
C. Assign an EC2 instance role that allows access to AWS Systems 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 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 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 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 5
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 6
A company experienced a security incident caused by a vulnerable container image that was pushed from an external CI/CD pipeline into Amazon ECR.
Which solution will prevent vulnerable images from being pushed?

A. Enable ECR enhanced scanning with Lambda blocking.

B. Use Amazon Inspector with EventBridge and Lambda.
C. Integrate Amazon Inspector into the CI/CD pipeline using SBOM generation and fail the pipeline on critical findings.
D. Enable basic continuous ECR scanning.

Answer: C

NEW QUESTION 7
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 8
A company needs to build a code-signing solution using an AWS KMS asymmetric key and must store immutable evidence of key creation and usage for compliance and audit purposes.
Which solution meets these requirements?

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

Answer: A

NEW QUESTION 9
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 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 10
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 13
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 18
A security engineer discovers that a company's user passwords have no required minimum length. The company uses the following identity providers (IdPs):
• AWS Identity and Access Management (IAM) federated with on-premises Active Directory
• Amazon Cognito user pools that contain the user database for an AWS Cloud application Which combination of actions should the security engineer take to implement a required minimum password length? (Select TWO.)

A. Update the password length policy in the IAM configuration.
B. Update the password length policy in the Amazon Cognito configuration.
C. Update the password length policy in the on-premises Active Directory configuration.
D. Create an SCP in AWS Organizations to enforce minimum password length.
E. Create an IAM policy with a minimum password length condition.

Answer: BC

NEW QUESTION 20
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 grou
B. Create an IAM user for each consultan
C. Add each user to the grou
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 accoun
G. Define a trust policy that requires MF
H. In the trust policy, specify the company's production account as the principa
I. Attach the trust policy to the role.
J. Create an IAM role in the company??s production accoun
K. Define a trust policy that requires MF
L. In the trust policy, specify the consultant agency's AWS account as the principa
M. Attach the trust policy to the role.

Answer: D

NEW QUESTION 22
CloudFormation stack deployments fail for some users due to permission inconsistencies.
Which combination of steps will ensure consistent deployments MOST securely? (Select THREE.)

A. Create a composite principal service role.
B. Create a service role with cloudformation.amazonaws.com as the principal.
C. Attach scoped policies to the service role.
D. Attach service ARNs in policy resources.
E. Update each stack to use the service role.
F. Allow iam:PassRole to the service role.

Answer: BEF

NEW QUESTION 27
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 32
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 34
Notify when IAM roles are modified.

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

Answer: B

NEW QUESTION 36
A 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 38
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 42
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 44
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 46
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 51
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 52
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 55
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 60

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SCS-C03 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SCS-C03 Product From:

https://www.2passeasy.com/dumps/SCS-C03/

Money Back Guarantee

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