Exam Questions SCS-C03

AWS Certified Security - Specialty

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

NEW QUESTION 1
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 2
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 3
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 4
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 5
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 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 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 8
A company is building a secure solution that relies on an AWS Key Management Service (AWS KMS) customer managed key. The company wants to allow AWS Lambda to use the KMS key. However, the company wants to prevent Amazon EC2 from using the key.
Which solution will meet these requirements?

A. Use IAM explicit deny for EC2 instance profiles and allow for Lambda roles.
B. Use a KMS key policy with kms:ViaService conditions to allow Lambda usage and deny EC2 usage.
C. Use aws:SourceIp and aws:AuthorizedService condition keys in the KMS key policy.
D. Use an SCP to deny EC2 and allow Lambda.

Answer: B

NEW QUESTION 9
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 10
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 10
A company has a single AWS account and uses an Amazon EC2 instance to test application code. The company recently discovered that the instance was compromised and was serving malware. Analysis showed that the instance was compromised 35 days ago. A security engineer must implement a continuous monitoring solution that automatically notifies the security team by email for high severity findings as soon as possible.
Which combination of steps should the security engineer take to meet these requirements? (Select THREE.)

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

Answer: BCE

NEW QUESTION 14
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 19
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 23
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 24
A company??s security engineer receives an alert that indicates that an unexpected principal is accessing a company-owned Amazon Simple Queue Service (Amazon SQS) queue. All the company??s accounts are within an organization in AWS Organizations. The security engineer must implement a mitigation solution that minimizes compliance violations and investment in tools outside of AWS.
What should the security engineer do to meet these requirements?

A. Create security groups and attach them to all SQS queues.
B. Modify network ACLs in all VPCs to restrict inbound traffic.
C. Create interface VPC endpoints for Amazon SQ
D. Restrict access using aws:SourceVpce and aws:PrincipalOrgId conditions.
E. Use a third-party cloud access security broker (CASB).

Answer: C

NEW QUESTION 28
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 32
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 33
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 38
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 41
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 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 44
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 47
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 48
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 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 54
.....

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