Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

SCS-C02 MCQs
SCS-C02 TestPrep
SCS-C02 Study Guide
SCS-C02 Practice Test
SCS-C02 Exam Questions

Amazon

SCS-C02

AWS Certified Security - Specialty

Question: 75

A company wants to monitor the deletion of customer managed CMKs A security engineer must create an alarm that will notify the company before a CMK is deleted. The security engineer has configured the integration of IAM CloudTrail with Amazon CloudWatch

What should the security engineer do next to meet this requirement?

A. Use inbound rule 100 to allow traffic on TCP port 443 Use inbound rule 200 to deny traffic on TCP port 3306 Use outbound rule 100 to allow traffic on TCP port 443
B. Use inbound rule 100 to deny traffic on TCP port 3306. Use inbound rule 200 to allow traffic on TCP port range 1024-65535. Use outbound rule 100 to allow traffic on TCP port 443
C. Use inbound rule 100 to allow traffic on TCP port range 1024-65535 Use inbound rule 200 to deny traffic on TCP port 3306 Use outbound rule 100 to allow traffic on TCP port 443
D. Use inbound rule 100 to deny traffic on TCP port 3306 Use inbound rule 200 to allow traffic on TCP port 443 Use outbound rule 100 to allow traffic on TCP port 443

Answer: A

Question: 76

A company is building an application on IAM that will store sensitive Information. The company has a support team with access to the IT infrastructure, including databases. The company's security engineer must introduce measures to protect the sensitive data against any data breach while minimizing management overhead. The credentials must be regularly rotated.

What should the security engineer recommend?

A. Enable Amazon RDS encryption to encrypt the database and snapshots. Enable Amazon Elastic Block Store

(Amazon EBS) encryption on Amazon EC2 instances. Include the database credential in the EC2 user data field. Use an IAM Lambda function to rotate database credentials. Set up TLS for the connection to the database.
B. Install a database on an Amazon EC2 Instance. Enable third-party disk encryption to encrypt the Amazon Elastic Block Store (Amazon EBS) volume. Store the database credentials in IAM CloudHSM with automatic rotation. Set up TLS for the connection to the database.
C. Enable Amazon RDS encryption to encrypt the database and snapshots. Enable Amazon Elastic Block Store (Amazon EBS) encryption on Amazon EC2 instances. Store the database credentials in IAM Secrets Manager with automatic rotation. Set up TLS for the connection to the RDS hosted database.
D. Set up an IAM CloudHSM cluster with IAM Key Management Service (IAM KMS) to store KMS keys. Set up Amazon RDS encryption using IAM KMS to encrypt the database. Store database credentials in the IAM Systems Manager Parameter Store with automatic rotation. Set up TLS for the connection to the RDS hosted database.

Answer: C

Question: 77

A company deployed IAM Organizations to help manage its increasing number of IAM accounts. A security engineer wants to ensure only principals in the Organization structure can access a specic Amazon S3 bucket. The solution must also minimize operational overhead

Which solution will meet these requirements?

A. 1 Put all users into an IAM group with an access policy granting access to the J bucket.
B. Have the account creation trigger an IAM Lambda function that manages the bucket policy, allowing access to accounts listed in the policy only.
C. Add an SCP to the Organizations master account, allowing all principals access to the bucket.
D. Specify the organization ID in the global key condition element of a bucket policy, allowing all principals access.

Answer: D

Question: 78

A company is undergoing a layer 3 and layer 4 DDoS attack on its web servers running on IAM.

Which combination of IAM services and features will provide protection in this scenario? (Select THREE).

A. Amazon Route 53
B. IAM Certificate Manager (ACM)
C. Amazon S3
D. IAM Shield
E. Elastic Load Balancer
F. Amazon Guard Duty

Answer: A,D,E

Question: 79

Your CTO thinks your IAM account was hacked.

What is the only way to know for certain if there was unauthorized access and what they did, assuming your hackers are very sophisticated IAM engineers and doing everything they can to cover their tracks?

A. Use CloudTrail Log File Integrity Validation.

B. Use IAM Config SNS Subscriptions and process events in real time.
C. Use CloudTrail backed up to IAM S3 and Glacier.
D. Use IAM Config Timeline forensics.

Answer: A

Explanation:

The IAM Documentation mentions the following

To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it you can use CloudTrail log file integrity validation. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. You can use the IAM CLI to validate the files in the location where CloudTrail delivered them

Validated log files are invaluable in security and forensic investigations. For example, a validated log file enables you to assert positively that the log file itself has not changed, or that particular user credentials performed specific API activity. The CloudTrail log file integrity validation process also lets you know if a log file has been deleted or changed, or assert positively that no log files were delivered to your account during a given period of time.

Options B.C and D is invalid because you need to check for log File Integrity Validation for cloudtrail logs

For more information on Cloudtrail log file validation, please visit the below URL:

http://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html

The correct answer is: Use CloudTrail Log File Integrity Validation.

omit your Feedback/Queries to our Expert

Question: 80

A company is developing a highly resilient application to be hosted on multiple Amazon EC2 instances. The application will store highly sensitive user data in Amazon RDS tables

The application must

â¢ Include migration to a different IAM Region in the application disaster recovery plan.

â¢ Provide a full audit trail of encryption key administration events

â¢ Allow only company administrators to administer keys.

â¢ Protect data at rest using application layer encryption

A Security Engineer is evaluating options for encryption key management

Why should the Security Engineer choose IAM CloudHSM over IAM KMS for encryption key management in this situation?

A. The key administration event logging generated by CloudHSM is significantly more extensive than IAM KM

B. CloudHSM ensures that only company support staff can administer encryption keys, whereas IAM KMS allows IAM staff to administer keys
C. The ciphertext produced by CloudHSM provides more robust protection against brute force decryption attacks than the ciphertext produced by IAM KMS
D. CloudHSM provides the ability to copy keys to a different Region, whereas IAM KMS does not

Answer: A

Question: 81

A company wants to ensure that its IAM resources can be launched only in the us-east-1 and us-west-2 Regions.

What is the MOST operationally efficient solution that will prevent developers from launching Amazon EC2 instances in other Regions?

A. Enable Amazon GuardDuty in all Regions. Create alerts to detect unauthorized activity outside us-east-1 and us-west-2.
B. Use an organization in IAM Organizations. Attach an SCP that allows all actions when the IAM: Requested Region condition key is either us-east-1 or us-west-2. Delete the FullIAMAccess policy.
C. Provision EC2 resources by using IAM Cloud Formation templates through IAM CodePipeline. Allow only the values of us-east-1 and us-west-2 in the IAM CloudFormation template's parameters.
D. Create an IAM Config rule to prevent unauthorized activity outside us-east-1 and us-west-2.

Answer: B

Question: 82

A company's Security Team received an email notification from the Amazon EC2 Abuse team that one or more of the company's Amazon EC2 instances may have been compromised

Which combination of actions should the Security team take to respond to (be current modem? (Select TWO.)

A. Open a support case with the IAM Security team and ask them to remove the malicious code from the affected instance
B. Respond to the notification and list the actions that have been taken to address the incident
C. Delete all IAM users and resources in the account
D. Detach the internet gateway from the VPC remove aft rules that contain 0.0.0.0V0 from the security groups, and create a NACL rule to deny all traffic Inbound from the internet
E. Delete the identified compromised instances and delete any associated resources that the Security team did not create.

Answer: B,D

Question: 83

A company is using Amazon Macie, AWS Firewall Manager, Amazon Inspector, and AWS Shield Advanced in its AWS account. The company wants to receive alerts if a DDoS attack occurs against the account.

Which solution will meet this requirement?

A. Use Macie to detect an active DDoS event. Create Amazon CloudWatch alarms that respond to Macie findings.
B. Use Amazon Inspector to review resources and to invoke Amazon CloudWatch alarms for any resources that are vulnerable to DDoS attacks.

C. Create an Amazon CloudWatch alarm that monitors Firewall Manager metrics for an active DDoS event.
D. Create an Amazon CloudWatch alarm that monitors Shield Advanced metrics for an active DDoS event.

Answer: D

Explanation:

This answer is correct because AWS Shield Advanced is a service that provides comprehensive protection against DDoS attacks of any size or duration. It also provides metrics and reports on the DDoS attack vectors, duration, and size. You can create an Amazon CloudWatch alarm that monitors Shield Advanced metrics such as DDoSAttackBitsPerSecond, DDoSAttackPacketsPerSecond, and DDoSAttackRequestsPerSecond to receive alerts if a DDoS attack occurs against your account.

For more information, see Monitoring AWS Shield Advanced with Amazon CloudWatch and AWS Shield Advanced metrics and alarms.

Question: 84

A company is running internal microservices on Amazon Elastic Container Service (Amazon ECS) with the Amazon EC2 launch type. The company is using Amazon Elastic Container Registry (Amazon ECR) private repositories.

A security engineer needs to encrypt the private repositories by using AWS Key Management Service (AWS KMS). The security engineer also needs to analyze the container images for any common vulnerabilities and exposures (CVEs).

Which solution will meet these requirements?

A. Enable KMS encryption on the existing ECR repositories. Install Amazon Inspector Agent from the ECS container instancesâ user data. Run an assessment with the CVE rules.
B. Recreate the ECR repositories with KMS encryption and ECR scanning enabled. Analyze the scan report after the next push of images.
C. Recreate the ECR repositories with KMS encryption and ECR scanning enabled. Install AWS Systems Manager Agent on the ECS container instances. Run an inventory report.
D. Enable KMS encryption on the existing ECR repositories. Use AWS Trusted Advisor to check the ECS container instances and to verily the findings against a list of current CVEs.

Answer: B

Question: 85

A business stores website images in an Amazon S3 bucket. The firm serves the photos to end users through Amazon CloudFront. The firm learned lately that the photographs are being accessible from nations in which it does not have a distribution license.

Which steps should the business take to safeguard the photographs and restrict their distribution? (Select two.)

A. Update the S3 bucket policy to restrict access to a CloudFront origin access identity (OAI).
B. Update the website DNS record to use an Amazon Route 53 geolocation record deny list of countries where the company lacks a license.
C. Add a CloudFront geo restriction deny list of countries where the company lacks a license.
D. Update the S3 bucket policy with a deny list of countries where the company lacks a license.

E. Enable the Restrict Viewer Access option in CloudFront to create a deny list of countries where the company lacks a license.

Answer: A,C

Explanation:

For Enable Geo-Restriction, choose Yes. For Restriction Type, choose Whitelist to allow access to certain countries, or choose Blacklist to block access from certain countries. https://IAM.amazon.com/premiumsupport/knowledge-center/cloudfront-geo-restriction/

Question: 86

A company wants to remove all SSH keys permanently from a specific subset of its Amazon Linux 2 Amazon EC2 instances that are using the same 1AM instance profile However three individuals who have IAM user accounts will need to access these instances by using an SSH session to perform critical duties

How can a security engineer provide the access to meet these requirements?

A. Assign an 1AM policy to the instance profile to allow the EC2 instances to be managed by AWS Systems Manager Provide the 1AM user accounts with permission to use Systems Manager Remove the SSH keys from the EC2 instances Use Systems Manager Inventory to select the EC2 instance and connect
B. Assign an 1AM policy to the 1AM user accounts to provide permission to use AWS Systems Manager Run Command Remove the SSH keys from the EC2 instances Use Run Command to open an SSH connection to the EC2 instance
C. Assign an 1AM policy to the instance profile to allow the EC2 instances to be managed by AWS Systems Manager Provide the 1AM user accounts with permission to use Systems Manager Remove the SSH keys from the EC2 instances Use Systems Manager Session Manager to select the EC2 instance and connect
D. Assign an 1AM policy to the 1AM user accounts to provide permission to use the EC2 service in the AWS Management Console Remove the SSH keys from the EC2 instances Connect to the EC2 instance as the ec2-user through the AWS Management Console's EC2 SSH client method

Answer: C

Explanation:

To provide access to the three individuals who have IAM user accounts to access the Amazon Linux 2 Amazon EC2 instances that are using the same IAM instance profile, the most appropriate solution would be to assign an IAM policy to the instance profile to allow the EC2 instances to be managed by AWS Systems Manager, provide the IAM user accounts with permission to use Systems Manager, remove the SSH keys from the EC2 instances, and use Systems Manager Session Manager to select the EC2 instance and connect.

References: AWS Systems Manager Session Manager - AWS Systems Manager: AWS Systems Manager - AWS Management Console: AWS Identity and Access Management - AWS Management Console: Amazon

Elastic Compute Cloud - Amazon Web Services: Amazon Linux 2 - Amazon Web Services: AWS Systems

Manager - AWS Management Console: AWS Systems Manager - AWS Management Console: AWS Systems Manager - AWS Management Console

Question: 87

A security engineer is using AWS Organizations and wants to optimize SCPs. The security engineer needs to ensure that the SCPs conform to best practices.

Which approach should the security engineer take to meet this requirement?

A. Use AWS IAM Access Analyzer to analyze the policies. View the findings from policy validation checks.
B. Review AWS Trusted Advisor checks for all accounts in the organization.
C. Set up AWS Audit Manager. Run an assessment for all AWS Regions for all accounts.
D. Ensure that Amazon Inspector agents are installed on all Amazon EC2 in-stances in all accounts.

Answer: A

Question: 88

A company's security engineer has been tasked with restricting a contractor's IAM account access to the company's Amazon EC2 console without providing access to any other IAM services The contractors IAM account must not be able to gain access to any other IAM service, even it the IAM account rs assigned additional permissions based on IAM group membership

What should the security engineer do to meet these requirements"

A. Create an mime IAM user policy that allows for Amazon EC2 access for the contractor's IAM user
B. Create an IAM permissions boundary policy that allows Amazon EC2 access Associate the contractor's IAM account with the IAM permissions boundary policy
C. Create an IAM group with an attached policy that allows for Amazon EC2 access Associate the contractor's IAM account with the IAM group
D. Create a IAM role that allows for EC2 and explicitly denies all other services Instruct the contractor to always assume this role

Answer: B

Question: 89

A company is using AWS Organizations to manage multiple accounts. The company needs to allow an IAM user to use a role to access resources that are in another organization's AWS account.

Which combination of steps must the company perform to meet this requirement? (Select TWO.)

A. Create an identity policy that allows the sts: AssumeRole action in the AWS account that contains the resources. Attach the identity policy to the IAM user.
B. Ensure that the sts: AssumeRole action is allowed by the SCPs of the organization that owns the resources that the IAM user needs to access.
C. Create a role in the AWS account that contains the resources. Create an entry in the role's trust policy that allows the IAM user to assume the role. Attach the trust policy to the role.
D. Establish a trust relationship between the IAM user and the AWS account that contains the resources.
E. Create a role in the IAM user's AWS account. Create an identity policy that allows the sts: AssumeRole action. Attach the identity policy to the role.

Answer: A,C

Explanation:

Option A: Create an identity policy that allows the sts:AssumeRole action in the AWS account that contains the resources. Attach the identity policy to the IAM user. This will ensure that the IAM user has the necessary permissions to assume roles in the other account.

Option C: Create a role in the AWS account that contains the resources. Create an entry in the role's trust policy that allows the IAM user to assume the role. Attach the trust policy to the role. This step is necessary to allow the IAM user from the other account to assume the role in this account.

Explanation of other options:

Option B: This option involves Service Control Policies (SCPs), which are used to define the maximum permissions for account members in AWS Organizations. While ensuring the SCPs allow the sts:AssumeRole action might be necessary, it doesn't directly allow cross-account role assumption.

Option D: This option seems too vague and doesn't clearly explain how the trust relationship would be established. Trust relationships are generally established via trust policies, as mentioned in option C.

Option E: This option suggests creating a role in the IAM user's account and attaching a policy allowing sts:AssumeRole to this role. This wouldn't be effective since the role that needs to be assumed would be in the other AWS account that contains the resources, not in the IAM user's own account.

Question: 90

A company's AWS CloudTrail logs are all centrally stored in an Amazon S3 bucket. The security team controls the company's AWS account. The security team must prevent unauthorized access and tampering of the CloudTrail logs.

Which combination of steps should the security team take? (Choose three.)

A. Configure server-side encryption with AWS KMS managed encryption keys (SSE-KMS)
B. Compress log file with secure gzip.
C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to notify the security team of any modifications on CloudTrail log files.
D. Implement least privilege access to the S3 bucket by configuring a bucket policy.
E. Configure CloudTrail log file integrity validation.
F. Configure Access Analyzer for S3.

Answer: A,D,E

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.