Free Questions for SCS-C01 by braindumpscollection

Shared by Cole on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

A company has multiple AWS accounts that are part of AW5 Organizations. The company's Security team wants to ensure that even those Administrators with full access to the company's AWS accounts are unable to access the company's Amazon S3 buckets

How should this be accomplished?

Options:

A) UseSCPs

B) Add a permissions boundary to deny access to Amazon S3 and attach it to all roles

C) Use an S3 bucket policy

D) Create a VPC endpoint for Amazon S3 and deny statements for access to Amazon S3

Answer:

A

Question 2

Question Type: MultipleChoice

A company has an AWS account and allows a third-party contractor who uses another AWS account, to assume certain IAM roles. The company wants to ensure that IAM roles can be assumed by the contractor only if the contractor has multi-factor authentication enabled on their IAM user accounts

What should the company do to accomplish this?

A)

Image not found or type unknown

B)

Image not found or type unknown

C)

Image not found or type unknown

D)

Image not found or type unknown

Options:

A) Option A

B) Option B

C) Option C

D) Option D

Answer:

A

Question 3

Question Type: **MultipleChoice**

A company is collecting AWS CloudTrail log data from multiple AWS accounts by managing individual trails in each account and forwarding log data to a centralized Amazon S3 bucket residing in a log archive account. After CloudTrail introduced support for AWS Organizations trails, the company decided to further centralize management and automate deployment of the CloudTrail logging capability across all of its AWS accounts.

The company's security engineer created an AWS Organizations trail in the master account, enabled server-side encryption with AWS KMS managed keys (SSE-KMS) for the log files, and specified the same bucket as the storage location. However, the engineer noticed that logs recorded by the new trail were not delivered to the bucket.

Which factors could cause this issue? (Select TWO.)

Options:

A) The CMK key policy does not allow CloudTrail to make encrypt and decrypt API calls against the key.

B) The CMK key policy does not allow CloudTrail to make GenerateDataKey API calls against the key.

C) The IAM role used by the CloudTrail trail does not have permissions to make PutObject API calls against a folder created for the Organizations trail.

D) The S3 bucket policy does not allow CloudTrail to make PutObject API calls against a folder created for the Organizations trail.

E) The CMK key policy does not allow the IAM role used by the CloudTrail trail to use the key for crypto graphical operations.

Answer:

A, D

Question 4

Question Type: **MultipleChoice**

An company is using AWS Secrets Manager to store secrets that are encrypted using a CMK and are stored in the security account 111122223333. One of the company's production accounts. 444455556666, must to retrieve the secret values from the security account 111122223333. A security engineer needs to apply a policy to the secret in the security account based on least privilege access so the production account can retrieve the secret value only.

Which policy should the security engineer apply?

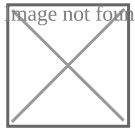

Image not found or type unknown

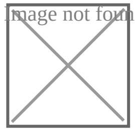

Image not found or type unknown

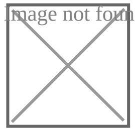

Image not found or type unknown

Options:

A) Option A

B) Option B

C) Option C

D) Option D

Answer:

A

Question 5

Question Type: MultipleChoice

A developer is creating an AWS Lambda function that requires environment variables to store connection information and logging settings. The developer is required to use an AWS KMS Customer Master Key (CMK> supplied by the information security department in order to adhere to company standards for securing Lambda environment variables.

Which of the following are required for this configuration to work? (Select TWO.)

Options:

A) The developer must configure Lambda access to the VPC using the --vpc-config parameter.

B) The Lambda function execution role must have the kms:Decrypt- permission added in the AWS IAM policy.

C) The KMS key policy must allow permissions for the developer to use the KMS key.

D) The AWS IAM policy assigned to the developer must have the kmseGcnerate-DataKcy permission added.

E) The Lambda execution role must have the kms:Encrypt permission added in the AWS IAM policy.

Answer:

B, C

Question 6

Question Type: **MultipleChoice**

A company is using AWS Organizations to manage multiple AWS member accounts. All of these accounts have Amazon GuardDuty enabled in all Regions. The company's AW5 Security Operations Center has a centralized security account for logging and monitoring. One of the member accounts has received an excessively high bill A security engineer discovers that a compromised Amazon EC2 instance is being used to mine crypto currency. The Security Operations Center did not receive a GuardDuty finding in the central security account.

but there was a GuardDuty finding in the account containing the compromised EC2 instance. The security engineer needs to ensure an GuardDuty finding are available in the security account.

What should the security engineer do to resolve this issue?

Options:

A) Set up an Amazon CloudWatch Event rule to forward ail GuardDuty findings to the security account Use an AWS Lambda function as a target to raise findings

B) Set up an Amazon CloudWatch Events rule to forward all GuardDuty findings to the security account Use an AWS Lambda function as a target to raise findings in AWS Security Hub

C) Check that GuardDuty in the security account is able to assume a role in the compromised account using the GuardDuty fast findings permission Schedule an Amazon CloudWatch Events rule and an AWS Lambda function to periodically check for GuardDuty findings

D) Use the aws GuardDuty get-members AWS CLI command m the security account to see if the account is listed Send an invitation from GuardDuty m the security account to GuardDuty in the compromised account Accept the invitation to forward all future GuardDuty findings

Answer:

D

Question 7

Question Type: **MultipleChoice**

A Developer reported that AWS CloudTrail was disabled on their account. A Security Engineer investigated the account and discovered the event was undetected by the current security solution. The Security Engineer must recommend a solution that will detect future changes to the CloudTrail configuration and send alerts when changes occur.

What should the Security Engineer do to meet these requirements?

Options:

A) Use AWS Resource Access Manager (AWS RAM) to monitor the AWS CloudTrail configuration. Send notifications using Amazon SNS.

B) Create an Amazon CloudWatch Events rule to monitor Amazon GuardDuty findings. Send email notifications using Amazon SNS.

C) Update security contact details in AWS account settings for AWS Support to send alerts when suspicious activity is detected.

D) Use Amazon Inspector to automatically detect security issues. Send alerts using Amazon SNS.

Answer:

B

Question 8

Question Type: MultipleChoice

A company uses multiple AWS accounts managed with AWS Organizations Security engineers have created a standard set of security groups for all these accounts. The security policy requires that these security groups be used for all applications and delegates modification authority to the security team only.

A recent security audit found that the security groups are inconsistency implemented across accounts and that unauthorized changes have been made to the security groups. A security engineer needs to recommend a solution to improve consistency and to prevent unauthorized changes in the individual accounts in the future.

Which solution should the security engineer recommend?

Options:

A) Use AWS Resource Access Manager to create shared resources for each requited security group and apply an IAM policy that permits read-only access to the security groups only.

B) Create an AWS CloudFormation template that creates the required security groups Execute the template as part of configuring new accounts Enable Amazon Simple Notification Service (Amazon SNS) notifications when changes occur

C) Use AWS Firewall Manager to create a security group policy, enable the policy feature to identify and revert local changes, and enable automatic remediation

D) Use AWS Control Tower to edit the account factory template to enable the snare security groups option Apply an SCP to the OU or individual accounts that prohibits security group modifications from local account users

Answer:

B

Question 9

Question Type: **MultipleChoice**

A Security Engineer is setting up a new AWS account. The Engineer has been asked to continuously monitor the company's AWS account using automated compliance checks based on AWS best practices and Center for Internet Security (CIS) AWS Foundations Benchmarks

How can the Security Engineer accomplish this using AWS services?

Options:

A) Enable AWS Config and set it to record all resources in all Regions and global resources. Then enable AWS Security Hub and confirm that the CIS AWS Foundations compliance standard is enabled

B) Enable Amazon Inspector and configure it to scan all Regions for the CIS AWS Foundations Benchmarks. Then enable AWS Security Hub and configure it to ingest the
Amazon Inspector findings

C) Enable Amazon Inspector and configure it to scan all Regions for the CIS AWS Foundations Benchmarks. Then enable AWS Shield in all Regions to protect the account from DDoS attacks.

D) Enable AWS Config and set it to record all resources in all Regions and global resources Then enable Amazon Inspector and configure it to enforce CIS AWS Foundations Benchmarks using AWS Config rules.

Answer:

A

Explanation:

https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-standards-cis-config-resources.html

Question 10

Question Type: **MultipleChoice**

A company has several production AWS accounts and a central security AWS account. The security account is used for centralized monitoring and has IAM privileges to all resources in every corporate account. All of the company's Amazon S3 buckets are tagged with a value denoting the data classification of their contents.

A Security Engineer is deploying a monitoring solution in the security account that will enforce bucket policy compliance. The system must monitor S3 buckets in all production accounts and confirm that any policy change is in accordance with the bucket's data classification. If any change is out of compliance; the Security team must be notified quickly.

Which combination of actions would build the required solution? (Choose three.)

Options:

A) Configure Amazon CloudWatch Events in the production accounts to send all S3 events to the security account event bus.

B) Enable Amazon GuardDuty in the security account. and join the production accounts as members.

C) Configure an Amazon CloudWatch Events rule in the security account to detect S3 bucket creation or modification events.

D) Enable AWS Trusted Advisor and activate email notifications for an email address assigned to the security contact.

E) Invoke an AWS Lambda function in the security account to analyze S3 bucket settings in response to S3 events, and send non-compliance notifications to the Security team.

F) Configure event notifications on S3 buckets for PUT; POST, and DELETE events.

Answer:

D, E, F

Question 11

Question Type: MultipleChoice

A company has hundreds of AWS accounts, and a centralized Amazon S3 bucket used to collect AWS CloudTrail for all of these accounts. A security engineer wants to create a solution that will enable the company to run ad hoc queues against its CloudTrail logs dating back 3 years from when the trails were first enabled in the company's AWS account.

How should the company accomplish this with the least amount of administrative overhead?

Options:

A) Run an Amazon EMP cluster that uses a MapReduce job to be examine the CloudTrail trails.

B) Use the events history/feature of the CloudTrail console to query the CloudTrail trails.

C) Write an AWS Lambda function to query the CloudTrail trails Configure the Lambda function to be executed whenever a new file is created in the CloudTrail S3 bucket.

D) Create an Amazon Athena table that tools at the S3 bucket the CloudTrail trails are being written to Use Athena to run queries against the trails.

Answer:

D

Question 12

Question Type: **MultipleChoice**

An application makes calls to AWS services using the AWS SDK. The application runs on Amazon EC2 instances with an associated IAM role. When the application attempts to access an object within an Amazon S3 bucket; the Administrator receives the following error message: HTTP 403: Access Denied.

Which combination of steps should the Administrator take to troubleshoot this issue? (Select three.)

Options:

A) Confirm that the EC2 instance's security group authorizes S3 access.

B) Verify that the KMS key policy allows decrypt access for the KMS key for this IAM principle.

C) Check the S3 bucket policy for statements that deny access to objects.

D) Confirm that the EC2 instance is using the correct key pair.

E) Confirm that the IAM role associated with the EC2 instance has the proper privileges.

F) Confirm that the instance and the S3 bucket are in the same Region.

Answer:

B, C, E