SCS-C02Q&As

AWS Certified Security - Specialty

Pass Amazon SCS-C02 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/scs-c02.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A company\\'s security engineer wants to receive an email alert whenever Amazon GuardDuty, AWS Identity and Access Management Access Analyzer, or Amazon Made generate a high-severity security finding. The company uses AWS Control Tower to govern all of its accounts. The company also uses AWS Security Hub with all of the AWS service integrations turned on.

Which solution will meet these requirements with the LEAST operational overhead?

A. Set up separate AWS Lambda functions for GuardDuty, 1AM Access Analyzer, and Macie to call each service\\'s public API to retrieve high-severity findings. Use Amazon Simple Notification Service (Amazon SNS) to send the email alerts. Create an Amazon EventBridge rule to invoke the functions on a schedule.

B. Create an Amazon EventBridge rule with a pattern that matches Security Hub findings events with high severity. Configure the rule to send the findings to a target Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the desired email addresses to the SNS topic.

C. Create an Amazon EventBridge rule with a pattern that matches AWS Control Tower events with high severity. Configure the rule to send the findings to a target Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the desired email addresses to the SNS topic.

D. Host an application on Amazon EC2 to call the GuardDuty, 1AM Access Analyzer, and Macie APIs. Within the application, use the Amazon Simple Notification Service (Amazon SNS) API to retrieve high-severity findings and to send the findings to an SNS topic. Subscribe the desired email addresses to the SNS topic.

Correct Answer: B

The AWS documentation states that you can create an Amazon EventBridge rule with a pattern that matches Security Hub findings events with high severity. You can then configure the rule to send the findings to a target Amazon Simple Notification Service (Amazon SNS) topic. You can subscribe the desired email addresses to the SNS topic. This method is the least operational overhead way to meet the requirements. References: : AWS Security Hub User Guide

QUESTION 2

Your development team is using access keys to develop an application that has access to S3 and DynamoDB. A new security policy has outlined that the credentials should not be older than 2 months, and should be rotated. How can you achieve this?

Please select:

A. Use the application to rotate the keys in every 2 months via the SDK

B. Use a script to query the creation date of the keys. If older than 2 months, create new access key and update all applications to use it inactivate the old key and delete it.

C. Delete the user associated with the keys after every 2 months. Then recreate the user again.

D. Delete the IAM Role associated with the keys after every 2 months. Then recreate the IAM Role again.

Correct Answer: B

One can use the CLI command list-access-keys to get the access keys. This command also returns the "CreateDate" of the keys. If the CreateDate is older than 2 months, then the keys can be deleted. The Returns list-access-keys CLI command returns information about the access key IDs associated with the specified IAM user. If there are none, the action returns an empty list Option A is incorrect because you might as use a script for such maintenance activities Option C is incorrect because you would not rotate the users themselves Option D is incorrect because you don\\'t use IAM roles for such a purpose For more information on the CLI command, please refer to the below Link: http://docs.IAM.amazon.com/cli/latest/reference/iam/list-access-keys.htmll The correct answer is: Use a script to query the creation date of the keys. If older than 2 months, create new access key and update all applications to use it inactivate the old key and delete it.

QUESTION 3

A company\\'s public Application Load Balancer (ALB) recently experienced a DDoS attack. To mitigate this issue. the company deployed Amazon CloudFront in front of the ALB so that users would not directly access the Amazon EC2 instances behind the ALB.

The company discovers that some traffic is still coming directly into the ALB and is still being handled by the EC2 instances.

Which combination of steps should the company take to ensure that the EC2 instances will receive traffic only from CloudFront? (Choose two.)

A. Configure CloudFront to add a cache key policy to allow a custom HTTP header that CloudFront sends to the ALB.

B. Configure CloudFront to add a custom: HTTP header to requests that CloudFront sends to the ALB.

C. Configure the ALB to forward only requests that contain the custom HTTP header.

D. Configure the ALB and CloudFront to use the X-Forwarded-For header to check client IP addresses.

E. Configure the ALB and CloudFront to use the same X.509 certificate that is generated by AWS Certificate Manager (ACM).

Correct Answer: BC

To prevent users from directly accessing an Application Load Balancer and allow access only through CloudFront, complete these high-level steps: Configure CloudFront to add a custom HTTP header to requests that it sends to the Application Load Balancer. Configure the Application Load Balancer to only forward requests that contain the custom HTTP header. (Optional) Require HTTPS to improve the security of this solution. https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/restrict-access-to-load-balancer.html

QUESTION 4

A company that operates in a hybrid cloud environment must meet strict compliance requirements. The company wants to create a report that includes evidence from on-premises workloads alongside evidence from AWS resources. A security engineer must implement a solution to collect, review, and manage the evidence to demonstrate compliance with company policy.

Which solution will meet these requirements?

A. Create an assessment in AWS Audit Manager from a prebuilt framework or a custom framework. Upload manual evidence from the on-premises workloads. Add the evidence to the assessment. Generate an assessment report after Audit Manager collects the necessary evidence from the AWS resources.

B. Install the Amazon CloudWatch agent on the on-premises workloads. Use AWS Config to deploy a conformance pack from a sample conformance pack template or a custom YAML template. Generate an assessment report after AWS Config identifies noncompliant workloads and resources.

C. Set up the appropriate security standard in AWS Security Hub. Upload manual evidence from the on-premises workloads. Wait for Security Hub to collect the evidence from the AWS resources. Download the list of controls as a .csv file.

D. Install the Amazon CloudWatch agent on the on-premises workloads. Create a CloudWatch dashboard to monitor the on-premises workloads and the AWS resources. Run a query on the workloads and resources. Download the results.

Correct Answer: C

QUESTION 5

A company has a batch-processing system that uses Amazon S3, Amazon EC2, and AWS Key Management Service (AWS KMS). The system uses two AWS accounts: Account A and Account B.

Account A hosts an S3 bucket that stores the objects that will be processed. The S3 bucket also stores the results of the processing. All the S3 bucket objects are encrypted by a KMS key that is managed in Account A.

Account B hosts a VPC that has a fleet of EC2 instances that access the S3 buck-et in Account A by using statements in the bucket policy. The VPC was created with DNS hostnames enabled and DNS resolution enabled.

A security engineer needs to update the design of the system without changing any of the system\\'s code. No AWS API calls from the batch-processing EC2 in-stances can travel over the internet.

Which combination of steps will meet these requirements? (Select TWO.)

A. In the Account B VPC, create a gateway VPC endpoint for Amazon S3. For the gateway VPC endpoint, create a resource policy that allows the s3:GetObject, s3:ListBucket, s3:PutObject, and s3:PutObjectAcl actions for the S3 bucket.

B. In the Account B VPC, create an interface VPC endpoint for Amazon S3. For the interface VPC endpoint, create a resource policy that allows the s3:GetObject, s3:ListBucket, s3:PutObject, and s3:PutObjectAcl actions for the S3 bucket.

C. In the Account B VPC, create an interface VPC endpoint for AWS KMS. For the interface VPC endpoint, create a resource policy that allows the kms:Encrypt, kms:Decrypt, and kms:GenerateDataKey actions for the KMS key. Ensure that

private DNS is turned on for the endpoint.

D. In the Account B VPC, create an interface VPC endpoint for AWS KMS. For the interface VPC endpoint, create a resource policy that allows the kms:Encrypt, kms:Decrypt, and kms:GenerateDataKey actions for the KMS key. Ensure that private DNS is turned off for the endpoint.

E. In the Account B VPC, verify that the S3 bucket policy allows the s3:PutObjectAcl action for cross-account use. In the Account B VPC, create a gateway VPC endpoint for Amazon S3. For the gateway VPC endpoint, create a resource policy that allows the s3:GetObject, s3:ListBucket, and s3:PutObject actions for the S3 bucket.

Correct Answer: BC

SCS-C02 PDF Dumps SCS-C02 VCE Dumps SCS-C02 Braindumps