# SCS-C02$^{Q\&As}$

AWS Certified Security - Specialty

## Pass Amazon SCS-C02 Exam with 100% Guarantee

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

**https://www.geekcert.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**

Users report intermittent availability of a web application hosted on IAM. Monitoring systems report an excess of abnormal network traffic followed by high CPU utilization on the application web tier. Which of the following techniques will improve the availability of the application? (Select TWO.)

A. Deploy IAM WAF to block all unsecured web applications from accessing the internet.

B. Deploy an Intrusion Detection/Prevention System (IDS/IPS) to monitor or block unusual incoming network traffic.

C. Configure security groups to allow outgoing network traffic only from hosts that are protected with up-to-date antivirus software.

D. Create Amazon CloudFront distribution and configure IAM WAF rules to protect the web applications from malicious traffic.

E. Use the default Amazon VPC for externakfacing systems to allow IAM to actively block malicious network traffic affecting Amazon EC2 instances.

Correct Answer: BD

**QUESTION 2**

A company needs to improve its ability to identify and prevent IAM policies that grant public access or cross-account access to resources. The company has implemented AWS Organizations and has started using AWS Identity and Access Management Access Analyzer to refine overly broad access to accounts in the organization.

A security engineer must automate a response in the company\\'s organization for any newly created policies that are overly permissive. The automation must remediate external access and must notify the company\\'s security team.

Which combination of steps should the security engineer take to meet these requirements? (Select THREE.)

A. Create an AWS Step Functions state machine that checks the resource type in the finding and adds an explicit Deny statement in the trust policy for the IAM role. Configure the state machine to publish a notification to an Amazon SimpleNotification Service (Amazon SNS) topic.

B. Create an AWS Batch job that forwards any resource type findings to an AWS Lambda function. Configure the Lambda function to add an explicit Deny statement in the trust policy for the IAM role. Configure the AWS Batch job to publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic.

C. In Amazon EventBridge, create an event rule that matches active IAM Access Analyzer findings and invokes AWS Step Functions for resolution.

D. In Amazon CloudWatch, create a metric filter that matches active IAM Access Analyzer findings and invokes AWS Batch for resolution.

E. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the queue to forward a notification to the security team that an external principal has been granted access to the specific IAM role and has been blocked.

F. Create an Amazon Simple Notification Service (Amazon SNS) topic for external or cross-account access notices. Subscribe the security team\\'s email addresses to the topic.

Correct Answer: ACF

To automate a response for any newly created policies that are overly permissive, the security engineer needs to use a combination of services that can monitor, analyze, remediate, and notify the security incidents. Option A is correct because creating an AWS Step Functions state machine that checks the resource type in the finding and adds an explicit Deny statement in the trust policy for the IAM role is a valid way to remediate external access. AWS Step Functions is a service that allows you to coordinate multiple AWS services into serverless workflows. You can use Step Functions to invoke AWS Lambda functions, which can modify the IAM policies programmatically. You can also use Step Functions to publish a notification to an Amazon SNS topic, which can send messages to subscribers such as email addresses. Option B is incorrect because creating an AWS Batch job that forwards any resource type findings to an AWS Lambda function is not a suitable way to automate a response. AWS Batch is a service that enables you to run batch computing workloads on AWS. Batch is designed for large-scale and long-running jobs that can benefit from parallelization and dynamic provisioning of compute resources. Batch is not intended for event-driven and real-time workflows that require immediate response. Option C is correct because creating an Amazon EventBridge event rule that matches active IAM Access Analyzer findings and invokes AWS Step Functions for resolution is a valid way to monitor and analyze the security incidents. Amazon EventBridge is a serverless event bus service that allows you to connect your applications with data from various sources. EventBridge can use rules to match events and route them to targets for processing. You can use EventBridge to invoke AWS Step Functions state machines from the IAM Access Analyzer findings. Option D is incorrect because creating an Amazon CloudWatch metric filter that matches active IAM Access Analyzer findings and invokes AWS Batch for resolution is not a suitable way to monitor and analyze the security incidents. Amazon CloudWatch is a service that provides monitoring and observability for your AWS resources and applications. CloudWatch can collect metrics, logs, and events from various sources and perform actions based on alarms or filters. However, CloudWatch cannot directly invoke AWS Batch jobs from the IAM Access Analyzer findings. You would need to use another service such as EventBridge or SNS to trigger the Batch job. Option E is incorrect because creating an Amazon SQS queue that forwards a notification to the security team that an external principal has been granted access to the specific IAM role and has been blocked is not a valid way to notify the security incidents. Amazon SQS is a fully managed message queue service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS can deliver messages to consumers that poll the queue for messages. However, SQS cannot directly forward a notification to the security team\\'s email addresses. You would need to use another service such as SNS or SES to send email notifications. Option F is correct because creating an Amazon SNS topic for external or cross-account access notices and subscribing the security team\\'s email addresses to the topic is a valid way to notify the security incidents. Amazon SNS is a fully managed messaging service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SNS can deliver messages to a variety of endpoints, such as email, SMS, or HTTP. You can use SNS to send email notifications to the security team when a critical security finding is detected. References: AWS Step Functions AWS Batch Amazon EventBridge Amazon CloudWatch Amazon SQS Amazon SNS

**QUESTION 3**

The Security Engineer is managing a traditional three-tier web application that is running on Amazon EC2 instances. The application has become the target of increasing numbers of malicious attacks from the Internet.

What steps should the Security Engineer take to check for known vulnerabilities and limit the attack surface? (Choose two.)

A. Use IAM Certificate Manager to encrypt all traffic between the client and application servers.

B. Review the application security groups to ensure that only the necessary ports are open.

C. Use Elastic Load Balancing to offload Secure Sockets Layer encryption.

D. Use Amazon Inspector to periodically scan the backend instances.

E. Use IAM Key Management Services to encrypt all the traffic between the client and application servers.

Correct Answer: BD

**QUESTION 4**

A company has decided to migrate sensitive documents from on-premises data centers to Amazon S3. Currently, the hard drives are encrypted to meet a compliance requirement regarding data encryption. The CISO wants to improve security by encrypting each file using a different key instead of a single key. Using a different key would limit the security impact of a single exposed key.

Which of the following requires the LEAST amount of configuration when implementing this approach?

A. Place each file into a different S3 bucket. Set the default encryption of each bucket to use a different IAM KMS customer managed key.

B. Put all the files in the same S3 bucket. Using S3 events as a trigger, write an IAM Lambda function to encrypt each file as it is added using different IAM KMS data keys.

C. Use the S3 encryption client to encrypt each file individually using S3-generated data keys

D. Place all the files in the same S3 bucket. Use server-side encryption with IAM KMS- managed keys (SSE-KMS) to encrypt the data

Correct Answer: D

https://docs.IAM.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3) When you use Server- Side Encryption with Amazon S3-Managed Keys (SSE-S3), each object is encrypted with a unique key. Server-Side Encryption with Customer Master Keys (CMKs) Stored in IAM Key Management Service (SSE-KMS) is similar to SSE-S3, but with some additional benefits and charges for using this service.

When you use SSE-KMS to protect your data without an S3 Bucket Key, Amazon S3 uses an individual IAM KMS data key for every object. It makes a call to IAM KMS every time a request is made against a KMS-encrypted object. https://docs.IAM.amazon.com/AmazonS3/latest/dev/bucket-key.html
https://docs.IAM.amazon.com/kms/latest/developerguide/symmetric-asymmetric.html

**QUESTION 5**

You are responsible to deploying a critical application onto IAM. Part of the requirements for this application is to ensure that the controls set for this application met PCI compliance. Also there is a need to monitor web application logs to identify any malicious activity. Which of the following services can be used to fulfil this requirement. Choose 2 answers from the options given below

A. Amazon Cloudwatch Logs

B. Amazon VPC Flow Logs

C. Amazon IAM Config

D. Amazon Cloudtrail

Correct Answer: AD

The IAM Documentation mentions the following about these services IAM CloudTrail is a service that enables

governance, compliance, operational auditing, and risk auditing of your IAM account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your IAM infrastructure. CloudTrail provides event history of your IAM account activity, including actions taken through the IAM Management Console, IAM SDKs, command line tools, and other IAM services. This event history simplifies security analysis, resource change tracking, and troubleshooting. Option B is incorrect because VPC flow logs can only check for flow to instances in a VPC Option C is incorrect because this can check for configuration changes only For more information on Cloudtrail, please refer to below URL: https://IAM.amazon.com/cloudtrail; You can use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, IAM CloudTrail, Amazon Route 53, and other sources. You can then retrieve the associated log data from CloudWatch Logs. For more information on Cloudwatch logs, please refer to below URL: http://docs.IAM.amazon.com/AmazonCloudWatch/latest/loes/WhatisCloudWatchLoES.html l The correct answers are: Amazon Cloudwatch Logs, Amazon Cloudtrail