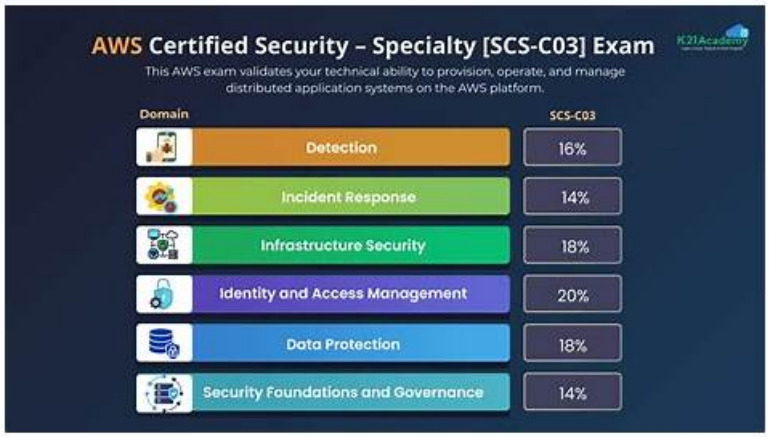
SCS-C03 Exam Forum | New SCS-C03 Exam Review



P.S. Free & New SCS-C03 dumps are available on Google Drive shared by Fast2test: https://drive.google.com/open?id=1I6FhVKqTPUharcrNvxwXOI21_nLM3lxW

Our SCS-C03 exam questions not only includes the examination process, but more importantly, the specific content of the exam. In previous years' examinations, the hit rate of SCS-C03 learning quiz was far ahead in the industry. We know that if you really want to pass the exam, our study materials will definitely help you by improving your hit rate as a development priority. After using SCS-C03 training prep, you will be more calm and it is inevitable that you will get a good result.

Amazon SCS-C03 Exam Syllabus Topics:

Topic	Details
Topic 1	• Incident Response: This domain addresses responding to security incidents through automated and manual strategies, containment, forensic analysis, and recovery procedures to minimize impact and restore operations.
Topic 2	• Identity and Access Management: This domain deals with controlling authentication and authorization through user identity management, role-based access, federation, and implementing least privilege principles.
Topic 3	• Infrastructure Security: This domain focuses on securing AWS infrastructure including networks, compute resources, and edge services through secure architectures, protection mechanisms, and hardened configurations.
Topic 4	• Security Foundations and Governance: This domain addresses foundational security practices including policies, compliance frameworks, risk management, security automation, and audit procedures for AWS environments.

>> SCS-C03 Exam Forum <<

Pass Guaranteed 2026 Amazon Pass-Sure SCS-C03: AWS Certified Security - Specialty Exam Forum

We have a team of rich-experienced IT experts who written the valid Amazon vce braindumps based on the actual questions and checked the updating of SCS-C03 dumps torrent everyday to make sure the success of test preparation. Before you buy our SCS-C03 Exam PDF, you can download the demo of free vce to check the accuracy.

Amazon AWS Certified Security - Specialty Sample Questions (Q41-Q46):

NEW QUESTION # 41
A company recently set up Amazon GuardDuty and is receiving a high number of findings from IP addresses within the company. A security engineer has verified that these IP addresses are trusted and allowed.
Which combination of steps should the security engineer take to configure GuardDuty so that it does not produce findings for these IP addresses? (Select TWO.)

- A. Upload the configuration file to Amazon S3. Add a new trusted IP list to GuardDuty that points to the file.
- B. Create a JSON configuration file that contains the trusted IP addresses.
- C. Upload the configuration file directly to GuardDuty.
- D. Manually copy and paste the configuration file data into the trusted IP list in GuardDuty.
- E. Create a plaintext configuration file that contains the trusted IP addresses.

Answer: A,E

Explanation:
GuardDuty supports "Trusted IP lists" to suppress findings that would otherwise be generated for activity originating from known safe IP addresses (for example, corporate NAT egress IPs, security scanners, or monitoring systems). To use a trusted IP list, you create aplain textfile that contains the IP addresses (typically one per line or in supported list form) and store it inAmazon S3. You then configure GuardDuty to reference that S3 object as a trusted IP list. GuardDuty periodically retrieves the file from S3 and uses it to adjust finding generation accordingly.
That maps directly to Option A (create a plaintext file) and Option D (upload to S3 and create a trusted IP list in GuardDuty pointing to the file).
Options B and E are incorrect because GuardDuty trusted IP lists are not configured by pasting JSON into the console; they are sourced from an S3-hosted text list. Option C is not supported because GuardDuty does not accept direct file uploads into the service as the configuration source; S3 is the expected integration point for IP lists and threat intel lists.

NEW QUESTION # 42
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. Create an Amazon Simple Queue Service (Amazon SQS) queue. Subscribe the security team's email distribution list to the queue.
- B. Create an Amazon EventBridge rule for GuardDuty findings of high severity. Configure the rule to publish a message to the topic.
- C. Enable Amazon GuardDuty in the AWS account.
- D. Create an Amazon EventBridge rule for Security Hub findings of high severity. Configure the rule to publish a message to the queue.
- E. Enable AWS Security Hub in the AWS account.
- F. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the security team's email distribution list to the topic.

Answer: B,C,F

Explanation:
Amazon GuardDuty provides continuous threat detection for compromised instances by analyzing VPC Flow Logs, DNS logs, and CloudTrail events. According to AWS Certified Security - Specialty guidance, GuardDuty is the fastest service to enable for detecting malware and compromised EC2 instances.
To notify the security team, Amazon SNS provides a native email notification mechanism with minimal setup. Amazon EventBridge integrates directly with GuardDuty findings and can filter based on severity.
Creating an EventBridge rule that matches high severity GuardDuty findings and publishes to SNS ensures immediate notification.
Security Hub is not required for this use case and adds additional setup time. Amazon SQS does not support email subscriptions.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
Amazon GuardDuty Findings and Severity
Amazon EventBridge Integration with GuardDuty

NEW QUESTION # 43
A company is using AWS to run a long-running analysis process on data that is stored in Amazon S3 buckets. The process runs on a fleet of Amazon EC2 instances in an Auto Scaling group. The EC2 instances are deployed in a private subnet that does not have internet access.
The EC2 instances access Amazon S3 through an S3 gateway endpoint that has the default access policy. Each EC2 instance uses an instance profile role that allows s3:GetObject and s3:PutObject only for required S3 buckets.
The company learns that one or more EC2 instances are compromised and are exfiltrating data to an S3 bucket that is outside the company's AWS Organization. The processing job must continue to function.
Which solution will meet these requirements?

- A. Add a network ACL rule to block outbound traffic on port 443.
- B. Update the instance profile role policy to require aws:ResourceOrgId.
- C. Update the policy on the S3 gateway endpoint to allow S3 actions only if aws:ResourceOrgId and aws:PrincipalOrgId match the company's organization.
- D. Apply an SCP that restricts S3 actions using organization condition keys.

Answer: C

Explanation:
Amazon S3 gateway endpoints support endpoint policies that can restrict which S3 resources are accessible through the endpoint.
According to AWS Certified Security - Specialty documentation, endpoint policies are evaluated in addition to IAM policies and are ideal for enforcing data exfiltration controls without breaking legitimate workloads.
By updating the S3 gateway endpoint policy to require both aws:ResourceOrgId and aws:PrincipalOrgId to match the company's AWS Organization, the security engineer ensures that EC2 instances can access only S3 buckets that belong to the organization.
This immediately blocks exfiltration to external S3 buckets while allowing legitimate internal data access to continue uninterrupted.

NEW QUESTION # 44
A company runs a web application on a fleet of Amazon EC2 instances in an Auto Scaling group. Amazon GuardDuty and AWS Security Hub are enabled. The security engineer needs an automated response to anomalous traffic that follows AWS best practices and minimizes application disruption.
Which solution will meet these requirements?

- A. Use Security Hub to update the subnet network ACL to block traffic.
- B. Use EventBridge to invoke a Lambda function that removes the affected instance from the Auto Scaling group and isolates it with a restricted security group.
- C. Send GuardDuty findings to Amazon SNS for email notification.
- D. Use EventBridge to disable the instance profile access keys.

Answer: B

Explanation:
AWS incident response best practices emphasize isolating compromised resources rather than immediately terminating them.
According to AWS Certified Security - Specialty documentation, removing an instance from an Auto Scaling group prevents replacement loops, while applying a restrictive security group isolates the instance for forensic analysis.
Using Amazon EventBridge to trigger an AWS Lambda function enables automated, consistent responses to GuardDuty findings.
This approach minimizes disruption to the application because healthy instances continue serving traffic while the affected instance is isolated.
Disabling credentials or modifying network ACLs can have broader impact on unrelated workloads. SNS notifications alone do not provide response automation.
AWS recommends isolate-and-investigate patterns for EC2 incident response.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
Amazon GuardDuty Automated Responses
AWS Incident Response Playbooks

NEW QUESTION # 45
A company uploads data files as objects into an Amazon S3 bucket. A vendor downloads the objects to perform data processing. A security engineer must implement a solution that prevents objects from residing in the S3 bucket for longer than 72 hours.

- A. Configure S3 Versioning to expire object versions that have been in the bucket for 72 hours.
- B. Generate presigned URLs that expire after 72 hours.
- C. Configure an S3 Lifecycle configuration rule on the bucket to expire objects after 72 hours.
- D. Use the S3 Intelligent-Tiering storage class and configure expiration after 72 hours.

Answer: C

Explanation:
Amazon S3 Lifecycle configuration rules are the native, automated mechanism for managing object retention and deletion. According to AWS Certified Security - Specialty documentation, lifecycle rules can be configured to expire objects based on the number of days since object creation. Once the expiration time is reached, Amazon S3 permanently deletes the objects without manual intervention.
This solution directly enforces a maximum retention period of 72 hours and ensures compliance regardless of whether the vendor downloads the data or not. Lifecycle rules are evaluated continuously by Amazon S3 and do not require scripts, cron jobs, or additional services, making them the most operationally efficient and cost-effective solution.
S3 Versioning controls versions but does not enforce object deletion timelines. S3 Intelligent- Tiering optimizes storage cost but does not delete objects. Presigned URLs only control access duration and do not remove objects from storage.
AWS explicitly recommends lifecycle policies for automated data retention enforcement.

NEW QUESTION # 46
.....

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes

2026 Latest Fast2test SCS-C03 PDF Dumps and SCS-C03 Exam Engine Free Share: https://drive.google.com/open?id=1I6FhVKqTPUharcrNvxwXOI21_nLM3lxW