Free PDF 2026 Amazon High Hit-Rate SCS-C02: Valid AWS Certified Security - Specialty Test Questions

All customer information to purchase our SCS-C02 guide torrent is confidential to outsides. You needn't worry about your privacy information leaked by our company. People who can contact with your name, e-mail, telephone number are all members of the internal corporate. The privacy information provided by you only can be used in online support services and providing professional staff remote assistance. Our experts check update on the SCS-C02 Exam Questions every day and keep customers informed. If you have any question about our SCS-C02 test guide, you can email or contact us online.

SurePassExams offers accurate and reliable study materials to help you prepare for the Amazon SCS-C02 Exam. They have prepared the best Amazon SCS-C02 Exam Questions that provide authentic and reliable material. With SurePassExams, many candidates have succeeded in passing the Amazon SCS-C02 Exam.

>> Valid SCS-C02 Test Questions <<

Free PDF Quiz 2026 SCS-C02: AWS Certified Security - Specialty – High Pass-Rate Valid Test Questions

SurePassExams has created reliable and up-to-date SCS-C02 Questions that help to pass the exam on the first attempt. The product is easy to use and very simple to understand ensuring it is student-oriented. The AWS Certified Security - Specialty dumps consist of three easy formats; The 3 formats are Desktop-based practice test software, Web-based practice exam, and PDF.

Amazon SCS-C02 Exam Syllabus Topics:

Topic	Details
Topic 1	• Infrastructure Security: Aspiring AWS Security specialists are trained to implement and troubleshoot security controls for edge services, networks, and compute workloads under this topic. Emphasis is placed on ensuring resilience and mitigating risks across AWS infrastructure. This section aligns closely with the exam's focus on safeguarding critical AWS services and environments.
Topic 2	• Threat Detection and Incident Response: In this topic, AWS Security specialists gain expertise in crafting incident response plans and detecting security threats and anomalies using AWS services. It delves into effective strategies for responding to compromised resources and workloads, ensuring readiness to manage security incidents. Mastering these concepts is critical for handling scenarios assessed in the SCS-C02 Exam.

Topic 3	• Data Protection: AWS Security specialists learn to ensure data confidentiality and integrity for data in transit and at rest. Topics include lifecycle management of data at rest, credential protection, and cryptographic key management. These capabilities are central to managing sensitive data securely, reflecting the exam's focus on advanced data protection strategies.

Amazon AWS Certified Security - Specialty Sample Questions (Q234-Q239):

NEW QUESTION # 234

An ecommerce website was down for 1 hour following a DDoS attack Users were unable to connect to the website during the attack period. The ecommerce company's security team is worried about future potential attacks and wants to prepare for such events The company needs to minimize downtime in its response to similar attacks in the future.
Which steps would help achieve this9 (Select TWO)

- A. Set up an Amazon CloudWatch Events rule to monitor the IAM CloudTrail events in real time use IAM Config rules to audit the configuration, and use IAM Systems Manager for remediation.
- B. Use IAM WAF to create rules to respond to such attacks
- C. Use VPC Flow Logs to monitor network: traffic and an IAM Lambda function to automatically block an attacker's IP using security groups.
- D. Subscribe to IAM Shield Advanced and reach out to IAM Support in the event of an attack.
- E. Enable Amazon GuardDuty to automatically monitor for malicious activity and block unauthorized access.

Answer: B,D

Explanation:
Explanation
To minimize downtime in response to DDoS attacks, the company should do the following:
Subscribe to AWS Shield Advanced and reach out to AWS Support in the event of an attack. This provides access to 24x7 support from the AWS DDoS Response Team (DRT), as well as advanced detection and mitigation capabilities for network and application layer attacks.
Use AWS WAF to create rules to respond to such attacks. This allows the company to filter web requests based on IP addresses, headers, body, or URI strings, and block malicious requests before they reach the web applications.

NEW QUESTION # 235

A company wants to know when users make changes to IAM roles in the company's AWS account. The company uses Amazon CloudWatch and AWS CloudTrail in the account. The company has configured a CloudTrail trail to capture read and write API activity for management events. The company has an Amazon Simple Notification Service (Amazon SNS) topic for security notifications.
A security engineer must implement a solution that provides a notification when an IAM role is edited.
Which solution will meet this requirement?

- A. Create an Amazon EventBridge rule that monitors AWS API calls from CloudTrail. Scope the event pattern to monitor changes to IAM roles from the lam.amazonaws.com event source. Set the SNS topic as the target of the EventBridge rule.
- B. Create a new CloudWatch log group. Configure the CloudTrail trail to send events to the new log group. Create a subscription filter that includes an event pattern to monitor changes to IAM roles from the lam.amazonaws.com event source. Set the SNS topic as the target of the subscription filter.
- C. Create a new CloudWatch log group. Configure the CloudTrail trail to send events to the new log group. Set up a CloudWatch metric to monitor changes to IAM roles from the lam.amazonaws.com event source. Create a subscription filter for the log group. Set the SNS topic as the target of the subscription filter.
- D. Enable Amazon Detective. Run a Detective investigation for changes to IAM roles. Create an Amazon EventBridge rule that monitors the results of the Detective investigation. Set the SNS topic as the target of the EventBridge rule.

Answer: A

NEW QUESTION # 236

A security engineer wants to evaluate configuration changes to a specific AWS resource to ensure that the resource meets compliance standards. However, the security engineer is concerned about a situation in which several configuration changes are

made to the resource in quick succession. The security engineer wants to record only the latest configuration of that resource to indicate the cumulative impact of the set of changes.
Which solution will meet this requirement in the MOST operationally efficient way?

- A. Use AWS Config to detect the configuration changes and to record the latest configuration in case of multiple configuration changes.
- B. Use Amazon CloudWatch to detect the configuration changes by filtering API calls to monitor the changes. Use the most recent API call to indicate the cumulative impact of multiple calls.
- C. Use AWS CloudTrail to detect the configuration changes by filtering API calls to monitor the changes. Use the most recent API call to indicate the cumulative impact of multiple calls
- D. Use AWS Cloud Map to detect the configuration changes. Generate a report of configuration changes from AWS Cloud Map to track the latest state by using a sliding time window.

Answer: A

Explanation:
AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. AWS Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations.
To evaluate configuration changes to a specific AWS resource and ensure that it meets compliance standards, the security engineer should use AWS Config to detect the configuration changes and to record the latest configuration in case of multiple configuration changes. This will allow the security engineer to view the current state of the resource and its compliance status, as well as its configuration history and timeline.
AWS Config records configuration changes as ConfigurationItems, which are point-in-time snapshots of the resource's attributes, relationships, and metadata. If multiple configuration changes occur within a short period of time, AWS Config records only the latest ConfigurationItem for that resource. This indicates the cumulative impact of the set of changes on the resource's configuration.
This solution will meet the requirement in the most operationally efficient way, as it leverages AWS Config's features to monitor, record, and evaluate resource configurations without requiring additional tools or services.
The other options are incorrect because they either do not record the latest configuration in case of multiple configuration changes (A, C), or do not use a valid service for evaluating resource configurations (D).
Verified Reference:
https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html
https://docs.aws.amazon.com/config/latest/developerguide/config-item-table.html

NEW QUESTION # 237
A security engineer recently rotated all IAM access keys in an AWS account. The security engineer then configured AWS Config and enabled the following AWS Config managed rules; mfa-enabled-for-iam-console-access, iam-user-mfa-enabled, access-key-rotated, and iam-user-unused-credentials-check.
The security engineer notices that all resources are displaying as noncompliant after the IAM GenerateCredentialReport API operation is invoked.
What could be the reason for the noncompliant status?

- A. The security engineer does not have the GenerateCredentialReport permission.
- B. The security engineer does not have the GetCredentialReport permission.
- C. The AWS Config rules have a MaximumExecutionFrequency value of 24 hours.
- D. The IAM credential report was generated within the past 4 hours.

Answer: C

Explanation:
The correct answer is D. The AWS Config rules have a MaximumExecutionFrequency value of 24 hours.
According to the AWS documentation1, the MaximumExecutionFrequency parameter specifies the maximum frequency with which AWS Config runs evaluations for a rule. For AWS Config managed rules, this value can be one of the following:
* One_Hour
* Three_Hours
* Six_Hours
* Twelve_Hours
* TwentyFour_Hours
If the rule is triggered by configuration changes, it will still run evaluations when AWS Config delivers the configuration snapshot.
However, if the rule is triggered periodically, it will not run evaluations more often than the specified frequency.

In this case, the security engineer enabled four AWS Config managed rules that are triggered periodically.
Therefore, these rules will only run evaluations every 24 hours, regardless of when the IAM credential report is generated. This means that the resources will display as noncompliant until the next evaluation cycle, which could take up to 24 hours after the IAM access keys are rotated.
The other options are incorrect because:
* A. The IAM credential report can be generated at any time, but it will not affect the compliance status of the resources until the next evaluation cycle of the AWS Config rules.
* B. The security engineer was able to invoke the IAM GenerateCredentialReport API operation, which means they have the GenerateCredentialReport permission. This permission is required to generate a credential report that lists all IAM users in an AWS account and their credential status2.
* C. The security engineer does not need the GetCredentialReport permission to enable or evaluate AWS Config rules. This permission is required to retrieve a credential report that was previously generated by using the GenerateCredentialReport operation2.
References:
1: AWS::Config::ConfigRule - AWS CloudFormation 2: IAM: Generate and retrieve IAM credential reports

NEW QUESTION # 238
A company uses identity federation to authenticate users into an identity account (987654321987) where the users assume an IAM role named IdentityRole. The users then assume an IAM role named JobFunctionRole in the target AWS account (123456789123) to perform their job functions.
A user is unable to assume the IAM role in the target account. The policy attached to the role in the identity account is:

What should be done to enable the user to assume the appropriate role in the target account?

- A. Update the IAM policy attached to the role in the identity account to be:

- **B. Update the trust policy on the role in the target account to be:**

- C. Update the trust policy on the role in the identity account to be:

- D. Update the IAM policy attached to the role in the target account to be:

Answer: B

Explanation:
In IAM roles, use the Principal element in the role trust policy to specify who can assume the role.
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_principal.html

NEW QUESTION # 239
......

We have the free demo for the SCS-C02 study guide, it will help you to have a better understanding of the exam dumps, if you decide to buy and pay for it, we will send the downloading link and password to you within 10 minutes, and if you don't receive it, please contact to our service stuff, we will deal with the problem for you immediately. What's more, free update for the SCS-C02 Study Guide for 365 days, and the update version will send to you by email automaticially, therefore you can have the latest information for the AWS Certified Security - Specialty.