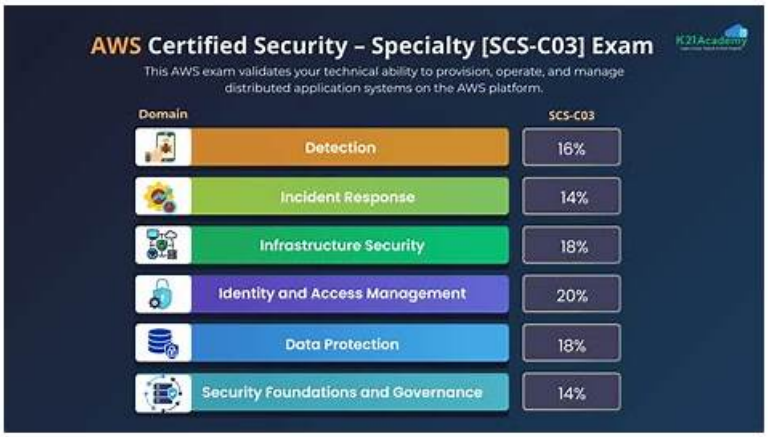
SCS-C03 Valid Exam Notes, SCS-C03 Vce Test Simulator



What's more, part of that Pass4Test SCS-C03 dumps now are free: https://drive.google.com/open?id=1eL3W_01KgxbcfTzspDEoz9RQkyPfP_xZ

In order to meet the different need from our customers, the experts and professors from our company designed three different versions of our SCS-C03 exam questions for our customers to choose, including the PDF version, the online version and the software version. Though the content of these three versions is the same, the displays have their different advantages. With our SCS-C03 Study Materials, you can have different and pleasure study experience as well as pass SCS-C03 exam easily.

Amazon SCS-C03 Exam Syllabus Topics:

Topic	Details
Topic 1	• Detection: This domain covers identifying and monitoring security events, threats, and vulnerabilities in AWS through logging, monitoring, and alerting mechanisms to detect anomalies and unauthorized access.
Topic 2	• 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 3	• Data Protection: This domain centers on protecting data at rest and in transit through encryption, key management, data classification, secure storage, and backup mechanisms.

>> SCS-C03 Valid Exam Notes <<

SCS-C03 Vce Test Simulator - SCS-C03 Exam Study Solutions

Our company has taken a lot of measures to ensure the quality of our SCS-C03 preparation materials. It is really difficult for us to hire a professional team, regularly investigate market conditions, and constantly update our SCS-C03 exam questions. But we persisted for so many years. And our quality of our SCS-C03 study braindumps are praised by all of our worthy customers. And you can always get the most updated and latest SCS-C03 training guide if you buy them.

Amazon AWS Certified Security - Specialty Sample Questions (Q22-Q27):

NEW QUESTION # 22
A company has security requirements for Amazon Aurora MySQL databases regarding encryption, deletion protection, public access, and audit logging. The company needs continuous monitoring and real-time visibility into compliance status.
Which solution will meet these requirements?

- A. Enable AWS Config and use managed rules to monitor Aurora MySQL compliance.
- B. Use AWS Security Hub configuration policies.

- C. Use AWS Audit Manager with a custom framework.
- D. Use EventBridge and Lambda with custom metrics.

Answer: A

Explanation:
AWS Config is the AWS service designed to continuously evaluate resource configurations against defined rules. According to the AWS Certified Security - Specialty Study Guide, AWS Config managed rules exist specifically to check database encryption, public accessibility, deletion protection, and log exports for Amazon RDS and Aurora.
AWS Config provides a real-time compliance timeline and displays the compliance state of each resource against each rule at any point in time. This granular visibility is required to assess ongoing compliance with security policies.
Audit Manager generates reports but does not provide continuous compliance monitoring. Security Hub aggregates findings but does not track configuration drift. EventBridge and Lambda introduce unnecessary complexity.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
AWS Config Managed Rules for RDS
AWS Continuous Compliance Monitoring

NEW QUESTION # 23
A company ' s web application is hosted on Amazon EC2 instances running behind an Application Load Balancer (ALB) in an Auto Scaling group. An AWS WAF web ACL is associated with the ALB. AWS CloudTrail is enabled and stores logs in Amazon S3 and Amazon CloudWatch Logs.
The operations team has observed some EC2 instances reboot at random. After rebooting, all access logs on the instances have been deleted. During an investigation, the operations team found that each reboot happened just after a PHP error occurred on the new-user-creation.php file. The operations team needs to view log information to determine if the company is being attacked.
Which set of actions will identify the suspect attacker ' s IP address for future occurrences?

- A. Configure the ALB to export access logs to an Amazon OpenSearch Service cluster and search for the new-user-creation.php occurrences.
- B. Configure the web ACL to send logs to Amazon Data Firehose, which delivers the logs to an S3 bucket.Use Amazon Athena to query the logs and find the new-user-creation.php occurrences.
- C. Configure VPC Flow Logs on the subnet where the ALB is located and stream the data to CloudWatch. Search for the new-user-creation.php occurrences in CloudWatch.
- D. Configure the CloudWatch agent on the ALB and send application logs to CloudWatch Logs.

Answer: B

Explanation:
AWS WAF logs capturedetailed request-level information, including source IP address, request URI, headers, and rule evaluation results. According to the AWS Certified Security - Specialty documentation, AWS WAF logging is acritical detection controlwhen application-level attacks are suspected, especially when host-based logs are unreliable or can be erased by attackers.
By configuring the AWS WAF web ACL to send logs toAmazon Data Firehose, the company ensures that all future requests are centrally captured and delivered to a durable storage service such as Amazon S3.
UsingAmazon Athena, the security team can query these logs to identify requests targeting specific application paths such as new-user-creation.php and extract the originating client IP addresses.
Option A is incorrect because VPC Flow Logs operate at the network layer and do not capture HTTP request paths. Option B is invalid because ALBs do not support CloudWatch agents. Option C is viable but introduces additional operational complexity and cost, making it less appropriate than the native WAF logging solution.
AWS documentation highlightsAWS WAF logging combined with Athenaas a best practice for forensic analysis and attacker identification.
* AWS Certified Security - Specialty Official Study Guide
* AWS WAF Logging Documentation
* Amazon Athena User Guide
* AWS Detection and Monitoring Best Practices

NEW QUESTION # 24
A company hosts its public website on Amazon EC2 instances behind an Application Load Balancer (ALB). The website is experiencing a global DDoS attack from a specific IoT device brand that uses a unique user agent. A security engineer is creating an AWS WAF web ACL and will associate it with the ALB. Which rule statement will mitigate the current attack and future attacks

from these IoT devices without blocking legitimate customers?

- A. Use an IP set match rule statement.
- B. Use a geographic match rule statement.
- C. Use a rate-based rule statement.
- D. Use a string match rule statement on the user agent.

Answer: D

Explanation:
AWS WAF string match rule statements allow inspection of HTTP headers, including the User- Agent header. According to AWS Certified Security - Specialty guidance, when malicious traffic can be uniquely identified by a consistent request attribute, such as a device-specific user agent, a string match rule provides precise mitigation with minimal false positives.
IP-based blocking is ineffective for globally distributed botnets. Geographic blocking risks denying access to legitimate users. Rate-based rules limit request volume but do not prevent low-and- slow attacks.
By matching the unique IoT device brand in the User-Agent header, the security engineer can block only malicious requests while preserving customer access.

NEW QUESTION # 25
A company runs an application on a fleet of Amazon EC2 instances. The application is accessible to users around the world. The company associates an AWS WAF web ACL with an Application Load Balancer (ALB) that routes traffic to the EC2 instances.
A security engineer is investigating a sudden increase in traffic to the application. The security engineer discovers a significant amount of potentially malicious requests coming from hundreds of IP addresses in two countries. The security engineer wants to quickly limit the potentially malicious requests. The security engineer does not want to prevent legitimate users from accessing the application.
Which solution will meet these requirements?

- A. Add deny rules to the ALB security group that prohibit incoming requests from the IP addresses.
- B. Use AWS WAF to implement a geographical match rule to block all incoming traffic from the two countries.
- C. Use AWS WAF to implement a rate-based rule for all incoming requests.
- D. Edit the ALB security group to include a geographical match rule to block all incoming traffic from the two countries.

Answer: C

Explanation:
A rate-based rule in AWS WAF is designed to quickly mitigate spikes and potential layer 7 floods bytracking request rates per originating IPand temporarily blocking (or counting/challenging, depending on configuration) IPs that exceed a defined threshold within a 5-minute rolling window. In this scenario, the malicious traffic is distributed acrosshundreds of IPsin two countries, and the application still needs to remain available globally for legitimate users. A rate-based rule provides fast, targeted throttling that reduces abusive request patterns without permanently blocking entire geographies. This aligns with "quickly limit" while minimizing collateral impact.
Blocking both countries with a geo match rule (Option B) would likely block legitimate users located in those countries, which violates the requirement. Security groups (Options C and D) cannot natively enforcegeographicfiltering, and they are not well suited for large, rapidly changing sets of public source IPs at the application layer. Additionally, WAF operates at layer 7 with richer matching (rate limiting, URI/header patterns, bot controls), which is the appropriate control point when the ALB already has a web ACL associated. Therefore, implementing an AWS WAFrate-basedrule is the most effective and least disruptive immediate mitigation.

NEW QUESTION # 26
A company runs several applications on Amazon Elastic Kubernetes Service (Amazon EKS). The company needs a solution to detect any Kubernetes security risks by monitoring Amazon EKS audit logs in addition to operating system, networking, and file events. The solution must send email alerts for any identified risks to a mailing list that is associated with a security team.
Which solution will meet these requirements?

- A. Enable Amazon Inspector container image scanning. Configure Amazon Detective to analyze EKS security logs. Create Amazon CloudWatch log groups for EKS audit logs. Use an AWS Lambda function to process the logs and to send email alerts to the security team.
- B. Install the AWS Systems Manager Agent (SSM Agent) on all EKS nodes. Configure Amazon CloudWatch Logs to collect EKS audit logs. Create an Amazon Simple Notification Service (Amazon SNS) topic and set the security team ' s mailing list as a subscriber. Configure a CloudWatch alarm to publish a message to the SNS topic when new audit logs are

generated.

- C. Deploy AWS Security Hub and enable security standards that contain EKS controls. Create an Amazon Simple Notification Service (Amazon SNS) topic and set the security team's mailing list as a subscriber. Use an Amazon EventBridge rule to send relevant Security Hub events to the SNS topic.
- D. Enable Amazon GuardDuty. Enable EKS Protection and Runtime Monitoring for Amazon EKS in GuardDuty. Create an Amazon Simple Notification Service (Amazon SNS) topic and set the security team ' s mailing list as a subscriber. Use an Amazon EventBridge rule to send relevant GuardDuty events to the SNS topic.

Answer: D

Explanation:
Option C is the best fit because Amazon GuardDuty provides managed threat detection forEKSby analyzingEKS control plane audit logs(EKS Protection) and correlating those signals withruntime telemetry (Runtime Monitoring) that includesprocess/OS activity, network connections, and file activityon the worker nodes. This directly matches the requirement to monitor EKS audit logsin addition tooperating system, networking, and file events to detect Kubernetes security risks.
GuardDuty produces securityfindingsfor suspicious Kubernetes behavior and runtime indicators (for example, unexpected API calls, anomalous container activity, or known malicious behaviors). To notify the security team, anAmazon EventBridgerule can match GuardDuty findings and forward them to anSNS topic. SNS supportsemail subscriptions, so the team's mailing list can receive near-real-time alerts without building a custom log parsing pipeline.
Option A (Security Hub) aggregates findings and maps to controls/standards but does not itself provide the combined audit-log + runtime event detection described. Option B combines unrelated services and still requires custom processing. Option D only alarms on "new audit logs generated," which does not detect
"security risks" and does not include OS/network/file threat detections.

NEW QUESTION # 27
.....

www.prepawaypdf.com □✔□ for ➤ SCS-C03 □ to obtain exam materials for free download □Braindump SCS-C03 Free

- myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, lms.ait.edu.za, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, massageben.com, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free 2026 Amazon SCS-C03 dumps are available on Google Drive shared by Pass4Test: https://drive.google.com/open?id=1eL3W_01KgxbcfTzspDEoz9RQkyPfP_xZ