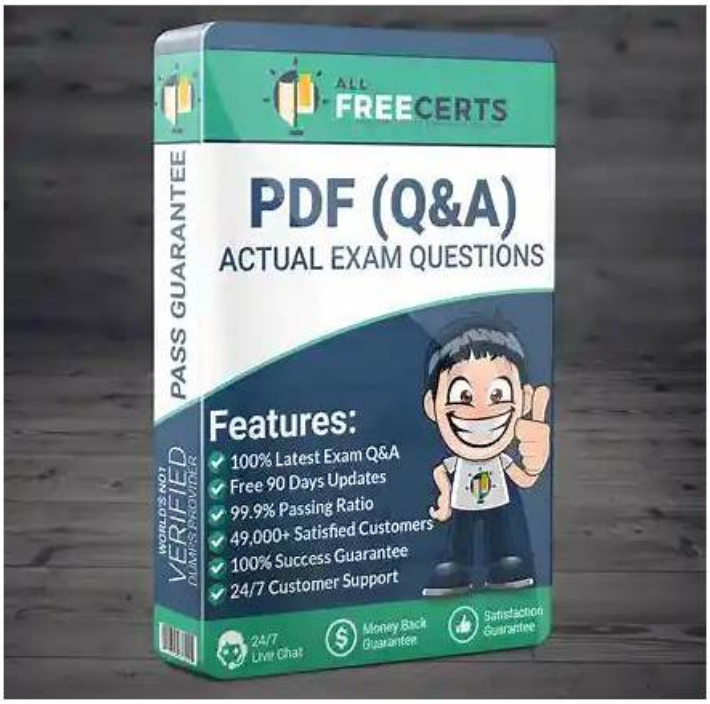
Premium SCS-C03 Exam | SCS-C03 Exam Study Solutions



BraindumpQuiz SCS-C03 Desktop Practice Exam Software: In the Desktop SCS-C03 practice exam software version of SCS-C03 practice test is updated and real. The software is useable on Windows-based computers and laptops. There is a demo of the AWS Certified Security - Specialty (SCS-C03) practice exam which is totally free. Amazon SCS-C03 practice test is very customizable and you can adjust its time and number of questions.

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	• Security Foundations and Governance: This domain addresses foundational security practices including policies, compliance frameworks, risk management, security automation, and audit procedures for AWS environments.
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.

>> Premium SCS-C03 Exam <<

Advantages Of Web-Based Amazon SCS-C03 Practice Tests

Many job-hunters want to gain the competition advantages in the labor market and become the hottest people which the companies rush to get. But if they want to realize that they must boost some valuable SCS-C03 certificate. The SCS-C03 certificate enjoys a high reputation among the labor market circle and is widely recognized as the proof of excellent talents and if you are one of them and you want to pass the SCS-C03 test smoothly you can choose our SCS-C03 practice questions.

Amazon AWS Certified Security - Specialty Sample Questions (Q129-Q134):

NEW QUESTION # 129
A security engineer needs to prepare a company's Amazon EC2 instances for quarantine during a security incident. The AWS Systems Manager Agent (SSM Agent) has been deployed to all EC2 instances. The security engineer has developed a script to install and update forensics tools on the EC2 instances.
Which solution will quarantine EC2 instances during a security incident?

- A. Store the script in Amazon S3 and grant read access to the instance profile.
- B. Configure Systems Manager Session Manager to deny all connection requests from external IP addresses.
- C. Configure IAM permissions for the SSM Agent to run the script as a predefined Systems Manager Run Command document.
- D. Create a rule in AWS Config to track SSM Agent versions.

Answer: C

Explanation:
AWS Systems Manager Run Command enables security engineers toremotely and securely execute scripts on EC2 instanceswithout requiring SSH or inbound network access. According to AWS Certified Security - Specialty incident response guidance, Run Command is a foundational tool forinstance quarantine and forensic preparation.
By configuring IAM permissions that allow the SSM Agent to execute a predefined Run Command document, the security engineer can rapidly deploy forensic tools, disable services, or modify system configurations across affected EC2 instances during an incident. This approach aligns with AWS best practices forcontainment and evidence preservation, while maintaining auditability through Systems Manager logs.
Option A only provides visibility, not quarantine capability. Option B restricts access but does not allow forensic tooling. Option C enables access to the script but does not execute it.
AWS documentation emphasizes thatSystems Manager Run Command is the recommended mechanism for incident response automation and quarantine actionson EC2 instances.
* AWS Certified Security - Specialty Official Study Guide
* AWS Systems Manager Run Command Documentation
* AWS Incident Response Best Practices

NEW QUESTION # 130
A security engineer needs to protect a public web application that runs in a VPC. The VPC hosts the origin for an Amazon CloudFront distribution. The application has experienced multiple layer 7 DDoS attacks. An AWS WAF web ACL is associated with the CloudFront distribution. The web ACL contains one AWS managed rule to protect against known IP addresses that have bad reputations.
The security engineer must configure an automated solution that detects and mitigates layer 7 DDoS attacks in real time with no manual effort.
Which solution will meet these requirements?

- A. Enable AWS Shield Advanced and configure proactive engagement with the AWS DDoS Response Team (DRT).
- B. Add a rate-based rule to the web ACL. Enable AWS Shield Advanced. Enable automatic application layer DDoS mitigation on the CloudFront distribution.
- C. Deploy AWS Network Firewall in the VPC. Create security policies that detect DDoS indicators.
  Create an AWS Lambda function to automatically update the web ACL rules during an attack.
- D. Enable AWS Shield Advanced on the CloudFront distribution. Configure alerts in Amazon CloudWatch for DDoS indicators.

Answer: B

Explanation:
Option D is the correct solution because it provides fully automated, real-time detection and mitigation of application-layer (Layer 7) DDoS attacks with no manual intervention. AWS Shield Advanced includes automatic application layer DDoS mitigation when it is enabled for supported resources such as Amazon CloudFront distributions. This feature continuously monitors traffic patterns and, when an attack is detected, automatically deploys AWS WAF rules to mitigate malicious requests.
Adding a rate-based rule to the AWS WAF web ACL further strengthens protection by automatically blocking IP addresses that exceed a defined request threshold, which is a common characteristic of Layer 7 DDoS attacks. This combination aligns directly with AWS best practices for protecting web applications against volumetric and application-layer threats.
Option A only provides alerting and visibility but does not ensure automated mitigation. Option B includes proactive engagement

with the AWS DDoS Response Team, which is valuable for complex or large-scale attacks but still involves human interaction and therefore does not meet the "no manual effort" requirement.
Option C introduces unnecessary complexity and is not recommended for protecting CloudFront-based applications against Layer 7 DDoS attacks.
AWS Security Specialty documentation explicitly recommends AWS Shield Advanced with automatic application layer DDoS mitigation and AWS WAF rate-based rules for fully automated, real-time protection of public web applications.

NEW QUESTION # 131
A security engineer configured VPC Flow Logs to publish to Amazon CloudWatch Logs. After 10 minutes, no logs appear. The issue is isolated to the IAM role associated with VPC Flow Logs.
What could be the reason?

- A. logs:GetLogEvents is missing.
- B. The role cannot tag the log stream.
- C. The engineer cannot assume the role.
- D. The vpc-flow-logs.amazonaws.com principal cannot assume the role.

Answer: D

Explanation:
VPC Flow Logs require an IAM role that CloudWatch Logs can use to publish flow log records. AWS documentation and AWS Certified Security - Specialty materials explain that the VPC Flow Logs service must be able to assume the IAM role through its trust policy. The trust relationship must include the service principal vpc-flow-logs.amazonaws.com. If the trust policy does not allow this principal to assume the role, flow logs cannot be delivered and no records will appear in the CloudWatch Logs log group even when traffic exists. logs:GetLogEvents is not required for delivery; it is used for reading logs. The security engineer's ability to assume the role is not relevant because the service, not the engineer, assumes it. Tagging permissions are not required for basic log delivery. Therefore, the most likely cause is an incorrect trust policy that prevents the VPC Flow Logs service principal from assuming the role.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
Amazon VPC Flow Logs IAM Role Requirements
IAM Trust Policies for AWS Services

NEW QUESTION # 132
A company needs the ability to identify the root cause of security findings in an AWS account. The company has enabled VPC Flow Logs, Amazon GuardDuty, and AWS CloudTrail. The company must investigate any IAM roles that are involved in the security findings and must visualize the findings.
Which solution will meet these requirements?

- A. Enable AWS Security Hub and use custom actions to investigate IAM roles.
- B. Use Amazon Inspector to run investigations on the IAM roles and visualize the findings.
- C. Export GuardDuty findings to Amazon S3 and analyze them with Amazon Athena.
- D. Use Amazon Detective to run investigations on the IAM roles and to visualize the findings.

Answer: D

Explanation:
Amazon Detective is a managed service designed specifically toinvestigate and analyze security findingsby automatically correlating data from Amazon GuardDuty, AWS CloudTrail, and VPC Flow Logs. According to the AWS Certified Security - Specialty Official Study Guide, Detective enables security teams to identify root causes, anomalous behavior, and indicators of compromisethrough interactive visualizations.
Amazon Detective allows investigators to pivot directly toIAM roles, users, and resources that are involved in GuardDuty findings. Detective builds behavior graphs and timelines that show API activity, network traffic, and historical context, making it easier to understand how and why a security incident occurred.
Amazon Inspector (Option B) focuses on vulnerability scanning of compute resources and does not investigate IAM behavior. Option C requires manual analysis and lacks native visualization. AWS Security Hub (Option D) aggregates findings but does not perform root-cause investigation or behavioral analysis.
AWS documentation explicitly states thatAmazon Detective is the recommended service for deep-dive investigations following GuardDuty alerts, especially when IAM roles are involved.

* AWS Certified Security - Specialty Official Study Guide
* Amazon Detective User Guide
* Amazon GuardDuty Integration Documentation

NEW QUESTION # 133
A company runs a public web application on Amazon EKS behind Amazon CloudFront and an Application Load Balancer (ALB). A security engineer must send a notification to an existing Amazon SNS topic when the application receives 10,000 requests from the same end-user IP address within any 5-minute period.
Which solution will meet these requirements?

- A. Configure an AWS WAF web ACL with a rate-based rule. Associate it with CloudFront. Create a CloudWatch alarm to notify SNS.
- B. Configure CloudFront standard logging and CloudWatch Logs metric filters.
- C. Configure VPC Flow Logs and CloudWatch Logs metric filters.
- D. Configure an AWS WAF web ACL with an ASN match rule and CloudWatch alarms.

Answer: A

Explanation:
AWS WAF rate-based rules are designed specifically to track the number of requests from a single IP address over a configurable time window. According to AWS Certified Security - Specialty guidance, rate-based rules integrate natively with CloudFront and emit CloudWatch metrics that can trigger alarms.
CloudFront logs and VPC Flow Logs are not real-time detection tools. ASN match rules do not count request rates.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
AWS WAF Rate-Based Rules
CloudFront and AWS WAF Integration

NEW QUESTION # 134
.....

- SCS-C03 New Test Camp ✌ SCS-C03 Reliable Test Dumps □ SCS-C03 Certification □ Search for 《 SCS-C03 》 and easily obtain a free download on □ www.testkingpass.com □ □SCS-C03 Mock Test
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes