Authorized SCS-C03 Exam Dumps - New SCS-C03 Test Pattern

What's more, part of that FreeCram SCS-C03 dumps now are free: https://drive.google.com/open?id=1ljYQPIvNxtROelyQpXLuNtveW36RiagI

The Amazon SCS-C03 certification exam is one of the top-rated and valuable credentials in the Amazon world. This AWS Certified Security - Specialty SCS-C03 exam questions is designed to validate the candidate's skills and knowledge. With Amazon SCS-C03 exam dumps everyone can upgrade their expertise and knowledge level. By doing this the successful Amazon SCS-C03 Exam candidates can gain several personal and professional benefits in their career and achieve their professional career objectives in a short time period.

Amazon SCS-C03 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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.

>> Authorized SCS-C03 Exam Dumps <<

Free PDF Amazon - Updated Authorized SCS-C03 Exam Dumps

As we all know, SCS-C03 certification is of great significance to highlight your resume, thus helping you achieve success in your workplace. So with our SCS-C03 preparation materials, you are able to pass the exam more easily in the most efficient and productive way and learn how to study with dedication and enthusiasm, which can be a valuable asset in your whole life. There are so many advantages of our SCS-C03 Guide dumps which will let you interested and satisfied.

Amazon AWS Certified Security - Specialty Sample Questions (Q62-Q67):

NEW QUESTION # 62
A company recently experienced a malicious attack on its cloud-based environment. The company successfully contained and

eradicated the attack. A security engineer is performing incident response work.
The security engineer needs to recover an Amazon RDS database cluster to the last known good version. The database cluster is configured to generate automated backups with a retention period of 14 days. The initial attack occurred 5 days ago at exactly 3:15 PM.
Which solution will meet this requirement?

- A. List all snapshots that have been taken of all the company's RDS databases. Identify the snapshot that was taken closest to 5 days ago at 3:14 PM and restore it.
- B. Identify the Regional cluster ARN for the database. List snapshots that have been taken of the cluster. Restore the database by using the snapshot that has a creation time that is closest to 5 days ago at 3:14 PM.
- C. Identify the Regional cluster ARN for the database. Use the ARN to restore the Regional cluster by using the restore to point in time feature. Set a target time 5 days ago at 3:14 PM.
- D. Identify the Regional cluster ARN for the database. Use the ARN to restore the Regional cluster by using the restore to point in time feature. Set a target time 14 days ago.

Answer: C

Explanation:
Amazon RDS supports point-in-time recovery (PITR) using automated backups within the configured retention window. According to the AWS Certified Security - Specialty Study Guide, PITR allows recovery to any second within the retention period, making it the most precise recovery method following a security incident.
By restoring the database cluster to a point just before the attack occurred, such as 3:14 PM, the security engineer ensures that the restored database reflects the last known good state without including malicious changes. This method is more accurate than restoring from snapshots, which are created at fixed intervals and may not align with the exact recovery time.
Options B and C rely on snapshot timing and may reintroduce compromised data. Option D restores to an arbitrary time and does not meet the requirement to recover to the last known good version.
AWS documentation explicitly recommends point-in-time recovery for incident response scenarios that require precise restoration.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
Amazon RDS Automated Backups and PITR
AWS Incident Response and Recovery Guidance

NEW QUESTION # 63
A company needs centralized log monitoring with automatic detection across hundreds of AWS accounts. Which solution meets these requirements with the LEAST operational effort?

- A. Designate a GuardDuty administrator account and enable protections.
- B. Centralize CloudTrail logs and query with Athena.
- C. Centralize CloudWatch logs and use Inspector.
- D. Stream logs to Kinesis and process with Lambda.

Answer: A

Explanation:
Amazon GuardDuty provides fully managed threat detection across accounts when configured with delegated administration. EKS and RDS protections enable workload-aware detection with minimal setup.
Other solutions require custom pipelines and higher operational overhead.

NEW QUESTION # 64
A company must immediately disable compromised IAM users across all AWS accounts and collect all actions performed by the user in the last 7 days. Which solution will meet these requirements?

- A. Remove permission sets and query logs using CloudWatch Logs Insights.
- B. Disable the user in IAM Identity Center and query the organizational event data store.
- C. Disable the IAM user and query CloudTrail logs in Amazon S3 using Athena.
- D. Remove IAM policies and query logs in Security Hub.

Answer: B

Explanation:
AWS IAM Identity Center centrally manages user access across an AWS Organization. Disabling the user in Identity Center immediately revokes access to all AWS accounts. According to AWS Certified Security - Specialty documentation, organizational CloudTrail event data stores provide centralized, queryable access to all events across accounts.
Using CloudTrail Lake enables direct querying of activity without exporting logs. Disabling the user at the Identity Center level ensures full containment.

NEW QUESTION # 65
A security engineer is troubleshooting an AWS Lambda function that is namedMyLambdaFunction. The function is encountering an error when the function attempts to read the objects in an Amazon S3 bucket that is namedDOC-EXAMPLE-BUCKET. The S3 bucket has the following bucket policy:

```
{
" Effect " : " Allow " ,
" Principal " : { " Service " : " lambda.amazonaws.com " },
" Action " : " s3:GetObject " ,
" Resource " : " arn:aws:s3:::DOC-EXAMPLE-BUCKET " ,
" Condition " : {
" ArnLike " : {
" aws:SourceArn " : " arn:aws:lambda:::function:MyLambdaFunction "
}
}
}
```

Which change should the security engineer make to the policy to ensure that the Lambda function can read the bucket objects?

- A. Change the Resource element to " arn:aws:lambda:::function:MyLambdaFunction " . Change the Principal element to the following:{ " Service " : " s3.amazonaws.com " }
- B. Change the Action element to the following:[" s3:GetObject* " , " s3:GetBucket* "]
- C. Change the Resource element to " arn:aws:s3:::DOC-EXAMPLE-BUCKET/* " .
- D. Remove the Condition element. Change the Principal element to the following:{ " AWS " : " arn:aws: lambda:::function:MyLambdaFunction " }

Answer: C

Explanation:
The policy currently grants s3:GetObject but targets thebucket ARN(arn:aws:s3:::DOC-EXAMPLE- BUCKET). For Amazon S3, object-level actions such asGetObjectmust referenceobject ARNs, not the bucket ARN. The correct resource pattern is the bucket ARNwith /*appended (for example, arn:aws:s3:::DOC- EXAMPLE-BUCKET/*) so the permission applies to objects within the bucket. Without this, S3 evaluates the request against a resource that does not match the requested object, resulting in an access denial even though the action appears correct.
The other options do not address the root cause. Expanding actions (Option B) is unnecessary and overly permissive, and it still would not fix the incorrect resource ARN for object reads. Changing principals or removing conditions (Option A) is not required just to allow reads-Lambda typically accesses S3 using the function'sexecution role, and bucket policies are commonly used for cross-account or service-based access control, but the immediate failure here is the mismatch between s3:GetObject and the bucket-only resource.
Option D is invalid because it inverts principal/service usage and sets an incorrect resource type for S3 authorization.

NEW QUESTION # 66
A company creates AWS Lambda functions from container images that are stored in Amazon Elastic Container Registry (Amazon ECR). The company needs to identify any software vulnerabilities in the container images and any code vulnerabilities in the Lambda functions.
Which solution will meet these requirements?

- A. Enable Amazon GuardDuty. Configure Runtime Monitoring and Lambda Protection in GuardDuty.
- B. Enable Amazon GuardDuty. Configure Amazon ECR scanning and Lambda code scanning in GuardDuty.
- C. Enable Amazon Inspector. Configure Amazon ECR enhanced scanning and Lambda code scanning in Amazon Inspector.
- D. Enable AWS Security Hub. Configure Runtime Monitoring and Lambda Protection in Security Hub.

Answer: C

Explanation:
Amazon Inspector is the AWS service designed specifically for vulnerability management across compute workloads, including Amazon ECR container images and AWS Lambda functions.
According to the AWS Certified Security - Specialty documentation, Amazon Inspector provides automated vulnerability assessments for container images stored in ECR by performing enhanced image scanning that identifies common vulnerabilities and exposures (CVEs) in operating systems and application dependencies.
Inspector also supports Lambda code scanning to analyze function packages and container- based Lambda images for known software vulnerabilities. Findings include severity ratings and remediation guidance, allowing security teams to identify and prioritize risks efficiently.
Amazon GuardDuty focuses on threat detection using behavioral analysis and does not perform static vulnerability scanning of container images or Lambda code. AWS Security Hub aggregates findings from other services but does not perform scanning itself.
AWS best practices recommend Amazon Inspector for vulnerability detection in container images and serverless workloads.

NEW QUESTION # 67
.....

The three versions of our SCS-C03 training materials each have its own advantage. On the one hand, the software version can simulate the real SCS-C03 examination for all of the users in windows operation system. By actually simulating the real test environment. On the other hand, if you choose to use the software version, you can download our SCS-C03 Exam Prep only for Windows system. We strongly believe that the software version of our SCS-C03 study materials will be of great importance for you to prepare for the exam and all of the employees in our company wish you early success.