Testpassport考試指南

品　　質　　更　　高　　服　　務　　更　　好

一年免費更新服務

http://www.testpassport.net

Exam : **SCS-C01**

Title : AWS Certified Security Specialty

Version : DEMO

1. Topic 1, Exam Pool OCT

A company's security team has defined a set of AWS Config rules that must be enforced globally in all AWS accounts the company owns.
What should be done to provide a consolidated compliance overview for the security team?
A. Use AWS Organizations to limit AWS Config rules to the appropriate Regions, and then consolidate the Amazon CloudWatch dashboard into one AWS account.
B. Use AWS Config aggregation to consolidate the views into one AWS account, and provide role access to the security team.
C. Consolidate AWS Config rule results with an AWS Lambda function and push data to Amazon SQS. Use Amazon SNS to consolidate and alert when some metrics are triggered.
D. Use Amazon GuardDuty to load data results from the AWS Config rules compliance status, aggregate GuardDuty findings of all AWS accounts into one AWS account, and provide role access to the security team.
Answer: B

2.A security engineer is designing an incident response plan to address the risk of a compromised Amazon EC2 instance.
The plan must recommend a solution to meet the following requirements:
• A trusted forensic environment must be provisioned
• Automated response processes must be orchestrated
Which AWS services should be included in the plan? {Select TWO)
A. AWS CloudFormation
B. Amazon GuardDuty
C. Amazon Inspector
D. Amazon Macie
E. AWS Step Functions
Answer: A,E

3.A security engineer has been tasked with implementing a solution that allows the company's development team to have interactive command line access to Amazon EC2 Linux instances using the AWS Management Console.
Which steps should the security engineer take to satisfy this requirement while maintaining least privilege?
A. Enable AWS Systems Manager in the AWS Management Console and configure for access to EC2 instances using the default AmazonEC2RoleforSSM role. Install the Systems Manager Agent on all EC2 Linux instances that need interactive access. Configure IAM user policies to allow development team access to the Systems Manager Session Manager and attach to the team's IAM users.
B. Enable console SSH access in the EC2 console. Configure IAM user policies to allow development team access to the AWS Systems Manager Session Manager and attach to the development team's IAM users.
C. Enable AWS Systems Manager in the AWS Management Console and configure to access EC2 instances using the default AmazonEC2RoleforSSM role. Install the Systems Manager Agent on all EC2 Linux instances that need interactive access. Configure a security group that allows SSH port 22 from all

published IP addresses. Configure IAM user policies to allow development team access to the AWS Systems Manager Session Manager and attach to the team's IAM users.
D. Enable AWS Systems Manager in the AWS Management Console and configure to access EC2 instances using the default AmazonEC2RoleforSSM role Install the Systems Manager Agent on all EC2 Linux instances that need interactive access. Configure IAM policies to allow development team access to the EC2 console and attach to the teams IAM users.
Answer: A

4.A large government organization is moving to the cloud and has specific encryption requirements. The first workload to move requires that a customer's data be immediately destroyed when the customer makes that request.
Management has asked the security team to provide a solution that will securely store the data, allow only authorized applications to perform encryption and decryption and allow for immediate destruction of the data
Which solution will meet these requirements?
A. Use AWS Secrets Manager and an AWS SDK to create a unique secret for the customer-specific data
B. Use AWS Key Management Service (AWS KMS) and the AWS Encryption SDK to
generate and store a data encryption key for each customer.
C. Use AWS Key Management Service (AWS KMS) with service-managed keys to generate and store customer-specific data encryption keys
D. Use AWS Key Management Service (AWS KMS) and create an AWS CloudHSM custom key store Use CloudHSM to generate and store a new CMK for each customer.
Answer: A

5.Unapproved changes were previously made to a company's Amazon S3 bucket. A security engineer configured AWS Config to record configuration changes made to the company's S3 buckets. The engineer discovers there are S3 configuration changes being made, but no Amazon SNS notifications are being sent. The engineer has already checked the configuration of the SNS topic and has confirmed the configuration is valid.
Which combination of steps should the security engineer take to resolve the issue? (Select TWO.)
A. Configure the S3 bucket ACLs to allow AWS Config to record changes to the buckets.
B. Configure policies attached to S3 buckets to allow AWS Config to record changes to the buckets.
C. Attach the AmazonS3ReadOnryAccess managed policy to the IAM user.
D. Verify the security engineer's IAM user has an attached policy that allows all AWS Config actions.
E. Assign the AWSConfigRole managed policy to the AWS Config role
Answer: B,E