AWS Certified Security - Specialty (SCS-C02) Practice Questions

Question 1

Scenario: A company's security team needs to centralize security findings from multiple AWS accounts and automate remediation for compromised IAM credentials. Which combination of AWS services should they use?
A. Amazon GuardDuty, AWS Config, and AWS Systems Manager
B. AWS Security Hub, Amazon Detective, and AWS Lambda
C. Amazon Macie, AWS CloudTrail, and Amazon EventBridge
D. AWS Identity and Access Management (IAM), Amazon Inspector, and AWS Step Functions

---

Question 2

Scenario: During a security audit, logs from Amazon VPC Flow Logs and AWS CloudTrail are missing in an S3 bucket. What is the MOST likely cause?
A. The S3 bucket policy denies write access from CloudTrail and VPC Flow Logs.
B. The IAM roles for CloudTrail and VPC Flow Logs lack permissions to publish logs to S3.
C. The S3 bucket is not in the same Region as the CloudTrail trail.
D. The S3 bucket has Object Lock enabled, blocking new log entries.

Question 3

Scenario: A healthcare application stores sensitive patient data in Amazon S3. Regulatory requirements mandate that data cannot be deleted or modified for 7 years. Which AWS features should be implemented?
A. S3 Versioning, S3 Lifecycle policies, and AWS KMS
B. S3 Object Lock in Governance mode, S3 Lifecycle policies, and AWS Backup
C. S3 Block Public Access, S3 Object Lock in Compliance mode, and AWS KMS
D. S3 Server-Side Encryption (SSE-S3), S3 Cross-Region Replication, and AWS Config

---

Question 4

Scenario: A company wants to enforce TLS 1.2 for all API calls to Amazon S3 buckets. How can this be achieved?
A. Configure an S3 bucket policy with a condition to deny requests that do not use TLS 1.2.
B. Enable default encryption on the S3 bucket using AWS KMS and TLS 1.2.
C. Use AWS Certificate Manager (ACM) to issue TLS 1.2 certificates for S3.
D. Configure AWS WAF to block non-TLS 1.2 traffic to S3 buckets.

Question 5

Scenario: A multi-account AWS environment requires centralized governance to prevent root users from creating access keys. Which solution meets this requirement?
A. Use AWS IAM policies to restrict root user actions in each account.
B. Create a Service Control Policy (SCP) in AWS Organizations to deny the `iam:CreateAccessKey`action for root users.
C. Enable AWS Control Tower and configure guardrails to block root user access keys.
D. Use AWS Config to monitor and alert on root user activity.

Question 6

Scenario: A serverless application uses AWS Lambda and Amazon API Gateway. The security team wants to prevent unauthorized API calls and detect anomalous traffic patterns. Which AWS services should be used?
A. AWS WAF, Amazon CloudWatch, and AWS Shield
B. Amazon GuardDuty, AWS Lambda (with custom code), and Amazon CloudWatch
C. Amazon API Gateway Resource Policies, AWS WAF, and Amazon GuardDuty
D. AWS Certificate Manager (ACM), Amazon Inspector, and AWS Config

---

Question 7

Scenario: A company's EC2 instances in a private subnet cannot connect to the internet for software updates. The VPC has a NAT Gateway in a public subnet. Security groups and route tables are correctly configured. What is the MOST likely issue?

A. The NAT Gateway’s security group blocks outbound traffic on port 443.
B. The EC2 instances’ IAM roles lack permissions to access the NAT Gateway.
C. The Network ACL for the private subnet blocks outbound ephemeral ports.
D. The NAT Gateway is not associated with the private subnet’s route table.

Question 8

Scenario: An organization needs to ensure all Amazon RDS instances are encrypted using customer-managed keys (CMKs). Which combination of steps is required?
A. Enable default encryption using AWS KMS CMKs and enforce it via an SCP.
B. Use AWS CloudHSM to generate keys and configure RDS to use them.
C. Enable encryption during RDS instance creation and audit using AWS Config.
D. Create an IAM policy requiring the `kms:Encrypt` action for RDS instances.

Question 9

Scenario: During an incident response, a compromised EC2 instance must be isolated quickly. Which AWS service can automate this process?
A. AWS Systems Manager Run Command
B. AWS Lambda triggered by Amazon GuardDuty findings
C. Amazon Detective to analyze the instance’s network traffic
D. AWS Security Hub to aggregate findings and notify the team

---

Question 10

Scenario: A company wants to audit cross-account access to an S3 bucket. Which AWS service provides detailed information about API calls made by IAM roles from another account?
A. AWS CloudTrail
B. Amazon Macie
C. AWS Config
D. VPC Flow Logs

Question 11

Scenario: A company needs to ensure all API calls to DynamoDB tables are encrypted in transit using TLS 1.2. How can this be enforced?

A. Enable default encryption for DynamoDB using AWS KMS.
B. Apply an IAM policy with a condition to deny requests without TLS 1.2.
C. Configure AWS WAF to block non-TLS 1.2 traffic to DynamoDB.
D. Use AWS Certificate Manager (ACM) to issue TLS 1.2 certificates for DynamoDB.

Question 12

Scenario: A security engineer must centralize logs from multiple AWS services (CloudTrail, VPC Flow Logs, and Lambda) into a single S3 bucket for compliance. Which service can automate this process?
A. Amazon CloudWatch Logs
B. AWS Kinesis Data Firehose
C. AWS Config
D. Amazon EventBridge

Question 13

Scenario: A company wants to prevent IAM users from creating access keys unless MFA is activated. Which IAM policy configuration achieves this?
A. Use an IAM policy with a condition `aws:MultiFactorAuthPresent: "true"`.
B. Enable MFA enforcement in AWS Organizations SCPs.
C. Configure AWS IAM Identity Center (SSO) to require MFA.
D. Use AWS Config to monitor IAM access key creation.

Question 14

Scenario: An organization uses AWS Control Tower. They need to ensure no S3 buckets in any member account are publicly accessible. Which solution should they implement?
A. Use AWS Config rules to detect public S3 buckets.
B. Deploy a Service Control Policy (SCP) denying `s3:PutBucketPublicAccessBlock`.
C. Enable the "Disallow Public S3 Buckets" guardrail in AWS Control Tower.
D. Use AWS Security Hub to aggregate findings from Amazon Macie.

Question 15

Scenario: A Lambda function requires access to a Secrets Manager secret in another AWS account. What is the MOST secure way to grant access?
A. Share the secret using AWS Resource Access Manager (RAM).
B. Create an IAM role in the target account with permissions to access the secret, then assume the role via Lambda.
C. Replicate the secret to the Lambda function's account using cross-region replication.
D. Store the secret in the Lambda function's environment variables.

Question 16

Scenario: A security team needs to analyze historical API activity to identify unauthorized access attempts. Which AWS service provides this capability?
A. Amazon GuardDuty
B. AWS CloudTrail
C. Amazon Inspector
D. AWS Security Hub

Question 17

Scenario: A company's EC2 instances must use only approved AMIs. Which combination of services enforces this?
A. AWS Systems Manager and Amazon Inspector
B. AWS Config and AWS Lambda
C. AWS Service Catalog and IAM policies
D. Amazon CloudWatch and AWS Trusted Advisor

Question 18

Scenario: A financial application requires FIPS 140-2 Level 3 validated encryption for sensitive data. Which AWS service should be used?
A. AWS KMS
B. AWS CloudHSM
C. Amazon S3 Server-Side Encryption (SSE-S3)
D. AWS Secrets Manager

Question 19

Scenario: A company wants to automate the rotation of database credentials stored in AWS Secrets Manager. What is required?
A. Create a Lambda function triggered by CloudWatch Events.
B. Enable automatic rotation in Secrets Manager and ensure the database supports integrated rotation.
C. Use AWS Config to enforce credential rotation every 90 days.
D. Configure an Amazon EventBridge rule to invoke rotation via AWS Step Functions.

Question 20

Scenario: A network engineer needs to ensure all traffic between two VPCs is encrypted. Which solution meets this requirement?
A. Use VPC Peering with TLS-terminating Application Load Balancers.
B. Deploy AWS Site-to-Site VPN between the VPCs.
C. Use VPC endpoints with encryption enabled.
D. Configure AWS Transit Gateway with encryption support.

Question 21

Scenario: A security team wants to enforce tagging standards for all EC2 instances. Which service can automatically remediate non-compliant resources?
A. AWS Config with AWS Systems Manager Automation
B. AWS Trusted Advisor with CloudWatch Alarms
C. Amazon Inspector with Lambda functions
D. AWS Security Hub with Amazon EventBridge

Question 22

Scenario: A company's S3 bucket policy allows access only from specific IP ranges. Users report access denied errors when using AWS CLI from approved IPs. What is the MOST likely cause?
A. The bucket has S3 Block Public Access enabled.
B. The IAM user policies lack `s3:GetObject` permissions.

C. The bucket policy uses aws:SourceIp without aws:ViaAWSService for CLI calls.
D. The S3 bucket is configured with a VPC endpoint that restricts access.

Question 23

Scenario: An organization wants to detect unintended resource exposure caused by S3 bucket policies. Which AWS service provides this capability?
A. Amazon Macie
B. AWS IAM Access Analyzer
C. Amazon GuardDuty
D. AWS Security Hub

Question 24

Scenario: A company needs to ensure all EBS volumes are encrypted. Which solution provides the STRONGEST enforcement?
A. Use AWS Config to detect unencrypted EBS volumes.
B. Create an IAM policy denying ec2:RunInstances without encryption parameters.
C. Deploy an SCP denying the creation of unencrypted EBS volumes.
D. Enable default EBS encryption in the AWS account settings.

Question 25

Scenario: A security engineer must investigate unauthorized access to an EC2 instance. Which service provides detailed network traffic analysis?
A. Amazon Detective
B. VPC Flow Logs
C. Amazon GuardDuty
D. AWS CloudTrail

Question 26

Scenario: A company uses AWS Organizations and wants to restrict member accounts from leaving the organization. Which action is required?
A. Configure an SCP denying the organizations:LeaveOrganization action.
B. Use AWS Control Tower to enforce account baselines.

C. Enable IAM permissions boundaries for all IAM users.
D. Use AWS Config to monitor account activity.

Question 27

Scenario: A serverless application uses Amazon API Gateway and Lambda. The security team wants to validate request signatures using HMAC. Which AWS service should be used?
A. AWS WAF
B. AWS KMS
C. Amazon Cognito
D. AWS Secrets Manager

Question 28

Scenario: A company wants to ensure all RDS snapshots are encrypted. Which solution is MOST effective?
A. Enable encryption for RDS instances, which applies to snapshots.
B. Use an SCP to enforce the `rds:EncryptSnapshot` action.
C. Configure AWS Backup to encrypt snapshots with KMS.
D. Apply an IAM policy requiring the `kms:Encrypt` permission for RDS.

Question 29

Scenario: A security team needs to restrict SSH access to EC2 instances to a jump host in a public subnet. Which network configuration achieves this?
A. Configure security groups to allow SSH traffic only from the jump host's private IP.
B. Use AWS Systems Manager Session Manager instead of SSH.
C. Deploy a Network ACL blocking SSH traffic except from the jump host.
D. Enable AWS Shield Advanced for the EC2 instances.

Question 30

Scenario: A company wants to prevent data exfiltration via S3. Which combination of controls is MOST effective?

A. S3 Block Public Access, bucket policies, and Amazon Macie
B. S3 Object Lock, VPC endpoints, and AWS GuardDuty
C. S3 VPC endpoints, bucket policies with `aws:SourceVpc`, and CloudTrail logging
D. S3 encryption using KMS, CloudWatch alarms, and AWS Config rules

Question 31

Scenario: A company uses Amazon S3 for storing audit logs. They need to ensure logs are retained for 10 years and cannot be deleted prematurely. Which AWS features should be implemented?
A. S3 Versioning, S3 Lifecycle policies, and S3 Object Lock in Governance mode
B. S3 Cross-Region Replication, S3 Block Public Access, and AWS Backup
C. S3 Object Lock in Compliance mode, S3 Lifecycle policies, and AWS KMS
D. S3 Server-Side Encryption (SSE-KMS), AWS Config, and Amazon Macie

---

Question 32

Scenario: A security team wants to automate the revocation of temporary credentials if an IAM role is deleted. Which AWS service enables this?
A. AWS Secrets Manager
B. AWS Security Token Service (STS)
C. AWS IAM Access Analyzer
D. AWS Config with custom rules

Question 33

Scenario: A company's CloudTrail logs show unauthorized API calls from an unknown IP. Which AWS service can automatically block this IP?
A. AWS WAF
B. Amazon GuardDuty
C. AWS Shield
D. Amazon Detective

Question 34

Scenario: A multi-account environment requires centralized monitoring of security findings. Which AWS service aggregates alerts from GuardDuty, Macie, and Inspector?
A. Amazon CloudWatch
B. AWS Security Hub
C. AWS Systems Manager
D. AWS Control Tower

Question 35

Scenario: An EC2 instance in a private subnet must securely access an S3 bucket without internet traffic. Which solution meets this requirement?
A. Use a NAT Gateway in a public subnet.
B. Configure an S3 VPC endpoint with a bucket policy restricting access to the VPC.
C. Enable S3 Block Public Access and IAM instance roles.
D. Deploy a Site-to-Site VPN to the S3 bucket.

Question 36

Scenario: A company wants to enforce MFA for all IAM users accessing the AWS Management Console. Which IAM policy configuration is required?
A. Attach a policy with `"Effect": "Deny"` and `"Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": "false"}}` to all users.
B. Enable the MFA requirement in the IAM account settings.
C. Use AWS Organizations SCPs to enforce MFA.
D. Configure AWS Single Sign-On (SSO) with MFA enabled.

Question 37

Scenario: A security engineer needs to ensure all EBS snapshots are encrypted. Which enforcement method applies to all AWS accounts in an organization?
A. Enable default EBS encryption in each account.
B. Create an AWS Config rule to detect unencrypted snapshots.
C. Deploy an SCP denying the `ec2:CreateSnapshot` action without encryption.
D. Use AWS Backup with KMS encryption for all snapshots.

Question 38

Scenario: A Lambda function processes sensitive data and must use ephemeral encryption keys. Which AWS service should be used?
A. AWS KMS with customer-managed keys (CMKs)
B. AWS CloudHSM
C. AWS Secrets Manager
D. AWS Certificate Manager (ACM)

Question 39

Scenario: A company wants to prevent accidental exposure of Amazon RDS databases to the public internet. Which combination of controls is MOST effective?
A. Security groups, AWS WAF, and Amazon Inspector
B. RDS Publicly Accessible flag set to "No," security groups, and NACLs
C. AWS Config rules, IAM policies, and AWS Shield
D. Amazon Macie, VPC endpoints, and CloudTrail logging

Question 40

Scenario: A security team needs to audit permissions granted to IAM roles over the last 90 days. Which AWS service provides this information?
A. AWS CloudTrail
B. IAM Access Advisor
C. AWS Security Hub
D. Amazon Detective

Answer Key

1. **B**
   Explanation: AWS Security Hub aggregates findings from GuardDuty, Macie, and other services. Lambda can automate remediation (e.g., revoking credentials). Detective is used for root cause analysis but is less focused on automated remediation.

2. **B**
   Explanation: Both CloudTrail and VPC Flow Logs require IAM roles with permissions to write to S3. Bucket policies (A) apply to external access, not service roles.
3. **C**
   Explanation: S3 Object Lock in Compliance mode enforces immutable retention. KMS ensures encryption. Block Public Access is a security best practice but unrelated to retention.
4. **A**
   Explanation: S3 bucket policies can include conditions like `aws:SecureTransport` and `s3:TlsVersion` to enforce TLS 1.2. ACM (C) manages certificates, not protocol enforcement.
5. **B**
   Explanation: SCPs in AWS Organizations apply governance across accounts. IAM policies (A) cannot restrict root users.
6. **C**
   Explanation: API Gateway Resource Policies restrict access, AWS WAF blocks malicious traffic, and GuardDuty detects anomalies.
7. **C**
   Explanation: NAT Gateway requires ephemeral ports (1024-65535) to be open in Network ACLs. Security groups are stateful and likely allow responses.
8. **A**
   Explanation: SCPs can enforce encryption at rest using KMS CMKs. CloudHSM (B) is for FIPS 140-2 Level 3 requirements, not general CMKs.
9. **B**
   Explanation: Lambda can automatically isolate instances (e.g., stop EC2) when triggered by GuardDuty findings.
10. **A**
    Explanation: CloudTrail logs all API calls, including cross-account actions. Macie (B) focuses on data classification, not API auditing.
11. **B**
    Explanation: IAM policies can enforce TLS 1.2 using the `aws:SecureTransport` and `s3:TlsVersion` conditions. KMS (A) encrypts data at rest, not in transit.

12. **B**

    Explanation: Kinesis Data Firehose can stream logs from multiple sources to S3. CloudWatch Logs (A) requires manual subscription.
13. **A**

    Explanation: IAM policies with `aws:MultiFactorAuthPresent` enforce MFA for specific actions. SCPs (B) apply to accounts, not IAM users.
14. **C**

    Explanation: AWS Control Tower guardrails enforce organization-wide rules. SCPs (B) are less targeted than pre-built guardrails.
15. **B**

    Explanation: Cross-account access via IAM roles is secure and follows least privilege. RAM (A) does not share Secrets Manager resources.
16. **B**

    Explanation: CloudTrail logs all API activity, including unauthorized attempts. GuardDuty (A) detects threats but does not log raw API calls.
17. **B**

    Explanation: AWS Config can detect non-compliant AMIs, and Lambda can remediate. Service Catalog (C) manages approved products but does not enforce usage.
18. **B**

    Explanation: AWS CloudHSM meets FIPS 140-2 Level 3 requirements. KMS (A) is Level 2.
19. **B**

    Explanation: Secrets Manager requires database support for integrated rotation. Lambda (A) is manual.
20. **D**

    Explanation: Transit Gateway supports encrypted inter-VPC traffic. VPN (B) encrypts but is for on-premises connectivity.
21. **A**

    Explanation: AWS Config detects non-compliant tags, and Systems Manager Automation remediates them.
22. **B**

    Explanation: Bucket policies allow access, but IAM policies must grant `s3:GetObject`. Block Public Access (A) would block public access, not CLI.
23. **B**

    Explanation: IAM Access Analyzer identifies resource exposure via policies. Macie (A) focuses on data classification.

24. **C**

    Explanation: SCPs enforce encryption across all accounts. Default encryption (D) is account-specific.

25. **A**

    Explanation: Detective analyzes historical data for root cause analysis. VPC Flow Logs (B) show traffic but lack context.

26. **A**

    Explanation: SCPs can block the `organizations:LeaveOrganization` action. Control Tower (B) does not prevent leaving.

27. **B**

    Explanation: AWS KMS can generate HMAC keys for request validation. Secrets Manager (D) stores secrets but does not compute HMAC.

28. **A**

    Explanation: Encrypting RDS instances automatically encrypts snapshots. AWS Backup (C) is manual.

29. **A**

    Explanation: Security groups are stateful and restrict SSH to the jump host's IP. Session Manager (B) avoids SSH but is not network-based.

30. **C**

    Explanation: S3 VPC endpoints keep traffic within the VPC, and `aws:SourceVpc` restricts access. Macie (A) detects data, not exfiltration.

31. **C**

    Explanation: S3 Object Lock in Compliance mode enforces immutability, and lifecycle policies manage retention. KMS ensures encryption.

32. **B**

    Explanation: STS issues temporary credentials tied to IAM roles. Deleting the role invalidates associated credentials.

33. **A**

    Explanation: AWS WAF can block IPs based on rules. GuardDuty (B) detects threats but does not block traffic.

34. **B**

    Explanation: Security Hub aggregates findings from multiple AWS security services.

35. **B**

    Explanation: S3 VPC endpoints allow private subnet access without internet traffic. Bucket policies restrict access to the VPC.

36. **A**
    Explanation: IAM policies with explicit deny conditions enforce MFA. Account settings (B) lack granularity.
37. **C**
    Explanation: SCPs enforce organization-wide encryption rules. AWS Config (B) only detects violations.
38. **A**
    Explanation: KMS CMKs support ephemeral keys via envelope encryption. CloudHSM (B) is for FIPS compliance.
39. **B**
    Explanation: Disabling public access flags and using security groups/NACLs restrict exposure.
40. **B**
    Explanation: IAM Access Advisor shows service permissions granted to roles over time.