AWS Certified Security – Specialty (SCS-C02)

Interview Prep Guide

Prepared for GoHackersCloud Students

Created: September 20, 2025

Top 25 AWS Security – Specialty Interview Questions

1. Explain the AWS Shared Responsibility Model from a security perspective.

   AWS secures the infrastructure, customers secure workloads, IAM, data, applications.

2. What are IAM best practices for security?

   Least privilege, roles over keys, MFA, password policies, IAM Access Analyzer, SCPs.

3. How do you protect data at rest in AWS?

   Use SSE-S3, SSE-KMS, client-side encryption, EBS/RDS encryption, KMS key rotation.

4. How do you protect data in transit?

   Use TLS/SSL, enforce HTTPS, ACM certificates, VPN/Direct Connect with encryption.

5. What is AWS KMS and how is it used?

   Key Management Service for creating/managing CMKs, integrates with S3, EBS, RDS, Lambda.

6. Difference between KMS and CloudHSM.

   KMS = managed keys, CloudHSM = dedicated hardware for compliance, more control.

7. How do you detect suspicious activity in AWS?

   Use GuardDuty, CloudTrail, Security Hub, CloudWatch alarms, VPC flow logs.

8. What is Amazon Macie?

   Data classification service to detect PII in S3, integrates with Security Hub.

9. How do you manage secrets in AWS?

   Use Secrets Manager or SSM Parameter Store with KMS encryption, rotation policies.

10. What is AWS Shield and WAF?

    Shield = DDoS protection (Standard/Advanced). WAF = web application firewall with rules for SQLi/XSS.

11. How do you secure an S3 bucket?

    Block public access, bucket policies, IAM policies, SSE, logging, Macie, Config rules.

12. Explain VPC security controls.

    Security groups, NACLs, VPC endpoints, private subnets, flow logs, Transit Gateway.

13. What is the difference between Inspector and GuardDuty?

    Inspector = vulnerability scanning. GuardDuty = threat detection from logs/events.

14. How to secure APIs on AWS?

    Use API Gateway with Cognito, IAM auth, WAF, throttling, usage plans, logging.

15. How do you implement compliance frameworks in AWS?

    Use AWS Artifact, Config rules, Audit Manager, Security Hub controls, encryption policies.

16. What is AWS Organizations SCP and why use it?

    Service Control Policies restrict services/actions across accounts, enforce compliance.

17. Explain centralized logging in AWS.

    Aggregate CloudTrail, VPC flow logs, and CloudWatch logs into central S3, use Athena/SIEM for analysis.

18. What is Certificate Manager?

    Provision/manage SSL/TLS certs for ELB, CloudFront, API Gateway.

19. How do you secure cross-account access?

    Use IAM roles with trust, SCPs, resource-based policies, no long-term keys.

20. How to implement monitoring & alerting?

GuardDuty findings, CloudWatch alarms, Security Hub dashboards, automated remediation with Lambda.

21. What is Detective?

Investigative service to analyze CloudTrail, VPC flow logs, GuardDuty findings.

22. Explain Incident Response in AWS.

Prepare runbooks, isolate compromised resources, analyze with logs, rotate keys, use forensic snapshots.

23. What is Nitro Enclaves?

EC2 feature for creating isolated compute environments for highly sensitive data.

24. How to secure containers in AWS?

ECR image scanning, IAM roles for tasks, least privilege, encrypt secrets, GuardDuty EKS findings.

25. Walk me through designing a secure architecture for a fintech app.

Multi-AZ VPC, private subnets, ALB with WAF, Shield Advanced, RDS encrypted, KMS keys, centralized logging, GuardDuty, Macie, Config rules.

How to leverage GoHackersCloud certifications for Security success

1) Follow GoHackersCloud Security Path

Focus on IAM, KMS, GuardDuty, WAF, Shield labs.

2) Highlight Security Labs

Showcase S3 security, centralized logging, incident response labs.

3) STAR Stories

Use security incidents from labs to structure interview answers.

4) Portfolio

Include cert badges, diagrams of secure architectures, GitHub with IaC templates.

5) Continuous Learning

Stay updated on AWS security services, reference GoHackersCloud mentorship.

4-Week Prep Plan (GoHackersCloud Security Path)

Week 1 — Identity & Access

IAM, SCPs, KMS basics, complete GoHackersCloud IAM labs.

Week 2 — Data Protection & Logging

S3 security, CloudTrail, Config, Macie labs.

Week 3 — Threat Detection & Response

GuardDuty, Inspector, Security Hub, incident response labs.

Week 4 — Mock Interviews

Security scenario drills, compliance Qs, portfolio polish.

Resume / LinkedIn tips

• Place Security certification & GoHackersCloud badge near top. • Highlight security projects (logging, incident response). • Add GitHub IaC templates and diagrams.

Good luck — use GoHackersCloud labs, practice tests, and mentorship to showcase AWS security expertise.