🔷 Day 71 – AWS Security & Compliance Case Studies (30 Q&As)

Section 1: Identity & Access Management (IAM)

Q1. How do you enforce least privilege in AWS?
Answer: Use IAM roles and scoped policies instead of sharing root credentials. Always follow the principle of least privilege with fine-grained permissions.
💡 Tip: Enable MFA for all critical accounts.

Q2. How do you manage temporary access for contractors?
Answer: Use IAM roles with AWS STS to generate short-lived credentials. This ensures contractors only have time-bound, limited access.

AWS Security Token Service (STS) is a web service that enables the creation and provision of temporary, limited-privilege credentials for AWS Identity and Access Management (IAM) users or federated users.

💡 Tip: Automatically expire credentials after the project.

Q3. How to separate permissions for dev, test, and prod?
Answer: Create separate AWS accounts with AWS Organizations and apply Service Control Policies (SCPs). This isolates environments and prevents cross-access.
💡 Tip: Strong isolation prevents accidental prod impact.

Section 2: Encryption & KMS

Q4. How do you encrypt data in S3?
Answer: Enable server-side encryption (SSE-S3 or SSE-KMS) and enforce encryption using bucket policies. This ensures data is always encrypted at rest.
💡 Tip: Default bucket encryption is a must in real-world apps.

Q5. How do you rotate encryption keys?
Answer: Use AWS KMS Customer Managed Keys (CMKs) with automatic yearly rotation. This aligns with compliance and security standards.
💡 Tip: Manual rotation can be done for custom policies.

Q6. How do you secure RDS databases?
Answer: Enable encryption at rest using KMS Key Management Service and enforce TLS/SSL for in-transit data. Combine this with IAM DB authentication for better security.
💡 Tip: Always enforce SSL through parameter groups.

Section 3: Network Security

Q7. Difference between Security Groups and NACLs?
Answer: Security Groups are stateful and work at the instance level. NACLs(Network Access Control List) are stateless and operate at the subnet level. Both are often used together for layered security.
💡 Tip: Always combine SGs + NACLs for maximum protection.

Q8. How to prevent unauthorized public access to EC2?
Answer: Restrict inbound rules to known IPs and avoid 0.0.0.0/0 for sensitive ports. Use Bastion Hosts or SSM Session Manager instead of direct SSH.
💡 Tip: Never leave SSH open to the internet.

Q9. How do you secure a private VPC?
Answer: Place critical workloads in private subnets with NAT Gateway for outbound traffic. Use VPC endpoints for S3/DynamoDB access without internet.
💡 Tip: Reduces attack surface by avoiding public exposure.

Section 4: Web Security (WAF, Shield, GuardDuty)

Q10. How do you protect against SQL injection/XSS?
Answer: Use AWS WAF (AWS WAF (Web Application Firewall)) with managed rules that automatically block malicious patterns. Add custom rules for application-specific threats.
💡 Tip: Always align with OWASP Top 10.

Q11. How do you defend against DDoS attacks?
Answer: Use AWS Shield Advanced along with CloudFront to absorb traffic. Auto Scaling ensures your application survives unexpected surges.
💡 Tip: Combine with Route 53 for global failover.

Q12. How do you detect compromised resources?
Answer: Enable GuardDuty for continuous threat detection and Security Hub for centralized alerts. Route alerts to SNS or EventBridge for quick response.
💡 Tip: Integrate with incident response pipelines.

Section 5: Compliance & Governance

Q13. How do you enforce organization-wide security rules?
Answer: Use AWS Organizations and Service Control Policies (SCPs) to set guardrails. This ensures no account can bypass security rules.
💡 Tip: Centralized governance is key for enterprises.

Q14. How do you ensure compliance with GDPR/PCI/HIPAA?
Answer: Use AWS Artifact for compliance reports, enforce encryption, and IAM least privilege. Design infrastructure according to shared responsibility.
💡 Tip: Mention that AWS is compliant, but customer config matters.

Q15. How do you track all API activity?
Answer: Enable CloudTrail organization-wide logging and store logs securely in S3 with encryption. Use Athena to query activity.
💡 Tip: Retain logs long-term for audits.

Section 6: Monitoring & Auditing

Q16. How do you detect unusual login attempts?
Answer: Use CloudTrail + CloudWatch alarms to flag suspicious logins. Set alerts for logins from unusual geographies or root account usage.
💡 Tip: Force MFA to mitigate risks.

Q17. How do you ensure log integrity?
Answer: Enable CloudTrail log file validation and use S3 versioning. Store logs in Glacier or immutable storage.
💡 Tip: This protects against tampering.

Q18. How to centralize logging across multiple accounts?
Answer: Use centralized logging by sending all CloudTrail/CloudWatch logs to a single S3 bucket in a logging account.
💡 Tip: Use Lake Formation for governance + queries.

Section 7: Disaster Recovery & High Availability

Q19. How do you design a DR plan for a banking app?
Answer: Use Multi-Region Aurora, S3 cross-region replication, and Route 53 failover. Define clear RTO and RPO targets.
💡 Tip: Financial apps need near-zero RPO.

Q20. Difference between Pilot Light and Warm Standby?
Answer: Pilot Light = minimal core infra always running. Warm Standby = scaled-down full copy of production. Multi-Site = full active-active setup.
💡 Tip: Trade-off = cost vs recovery time.

Q21. How to recover from accidental data deletion in S3?
Answer: Enable versioning + MFA delete to prevent permanent loss. Recover files from older versions.
💡 Tip: Always use lifecycle policies for safety.

Section 8: Advanced Security Scenarios

Q22. How do you secure sensitive API endpoints?
Answer: Use API Gateway + WAF for filtering and Cognito for authentication. Add throttling to prevent abuse.
💡 Tip: Rate-limiting is critical.

Q23. How do you protect data in transit across regions?
Answer: Use TLS everywhere and set up AWS PrivateLink or VPN for secure communication. Avoid plain HTTP for inter-region traffic.
💡 Tip: Enforce HTTPS using ACM.

Q24. How do you detect malware in EC2 instances?
Answer: Run Amazon Inspector scans and Systems Manager automation for patching. Use GuardDuty to flag suspicious behavior.
💡 Tip: Continuous scanning is key.

Section 9: Multi-Account Strategy

Q25. How to enforce billing separation for teams?
Answer: Use AWS Organizations with consolidated billing and tagging. Assign budgets per account/project.
💡 Tip: Use Cost Explorer for visibility.

Q26. How to enforce standard security across all accounts?
Answer: Use AWS Control Tower for automated guardrails, SCPs, and centralized policies.
💡 Tip: Ideal for enterprises with multiple accounts.

Q27. How to restrict developers from launching large EC2s?
Answer: Define SCPs that block certain EC2 instance types. Combine with AWS Budgets for alerts.
💡 Tip: Prevents unnecessary costs.

Section 10: Miscellaneous Compliance

Q28. How to meet HIPAA requirements for medical apps?
Answer: Use HIPAA-eligible AWS services, enforce encryption at rest/in-transit, and strict IAM. Sign a BAA with AWS.
💡 Tip: Mention audit trails.

Q29. How do you meet PCI-DSS for credit card processing?
Answer: Use VPC isolation, IAM least privilege, WAF, encryption, and log monitoring.
💡 Tip: Compliance is shared responsibility.

Q30. How to design a secure multi-tenant SaaS on AWS?
Answer: Isolate tenant data using IAM, DynamoDB partitions, and encryption. Apply strict access control per tenant.
💡 Tip: Mention tenant isolation = critical for SaaS.