Easy Cloud: AWS Security Audit Initial Engagement Questionnaire

Root account/user

- Q: How is the root account/user used currently?

Activate MFA

- Q: Is MFA enforced for every user?

Audit IAM users, Roles, Policies and Organizations

- Q: Can we get an org chart with personnel names, job roles/titles, and department names?
- Q: How do you handle new hires vs senior engineers? Are new hires given full access from day one?
- Q: How are access key pairs handled/stored currently?
- Q: Are you using AWS Roles?
- Q: Are you using the AWS Organizations feature? If so, can you describe how it is being used?

Network Architecture

- Q: What instances are currently running and are you using private and public subnets?
- Q: What are the IP address ranges for each subnet that are being used?

Policy for temporary access

- Q: Do you have a policy for granting temporary access to outside contractors?

Verify key monitoring tools with logging and alarms/notifications

- Q: What monitoring tools with logging are turned on and functional?

Verify how encryption is used, if at all, and identify areas where it may be helpful to turn it on

- Q: Is encryption being used (server-side, client-side, data in-transit, data at rest)?

Discuss threat remediation and incident response plan

- Q: Has your infrastructure been designed for high availability and disaster recovery?
- Q: Assuming you have a disaster recovery plan in place, when is the last time you tested your plan?
- Q: When there is a security incident, do you have a threat remediation plan in place?
- Q: Have you utilized tags to establish clear ownership and governance of key responsibilities?

Discuss any Active Directory integration/federation

- Have you integrated Active Directory with your AWS environment?

Validate backup plan and versioning

- Q: Are snapshots being regularly taken for EBS volumes attached to instances? What is the retention period?
- Q: Are Amazon RDS automated snapshots configured with the appropriate backup retention period?
- Q: Are S3 bucket(s) configured for backup and archive purposes?
- Q: Is an AWS Backup plan being used?

AWS Support Plan

- Do you pay for an AWS Support Plan? If so, which tier?