AWS Security Best Practices

Your To-Do List

Sena Yakut

Identity Access Management Security Best Practices

Your To-Do	Done?	Additional Notes
Always enable MFA.	□	
Use strong password policy for AWS IAM users.	□	
Do not use root account for your daily works.	□	
Do not create your root account access keys.	□	
Use group e-mail address when you're creating a new AWS account.	□	
Audit and monitor your IAM users regularly.	□	
For your IAM policies, roles, think at least privilege principle.	□	
Enable IAM Access Analyzer for every region.	□	
Track your IAM users' behavior with AWS CloudTrail.	□	
Do not use hardcoded AWS credentials. Never. Use IAM roles for accessing.	□	
First disable, after delete your access keys. This is important if you forgot a key that you've used.	□	
Use AWS Organization and SCPs if you have multiple AWS accounts.	□	
If you're using an IDP, think implement SSO to access AWS environment.	□	
If you're using cross account access, add condition for MFA and external IDs.	□	
Use more than one MFA for your root account to use if your device is stolen.	□	

Networking Security Best Practices

Your To-Do	Done?	Additional Notes
Do not open any unused or management ports in your security group.	□	
Review your security group rules regularly.	□	
If you have critical workloads, use NACLs to control your network traffic.	□	
Block malicious IP addresses from NACLs.	□	
Enable VPC flow logs for monitor and analyze your network traffic.	□	
Use AWS Network Firewall when necessary.	□	
Do not configure publicly accessible databases or internal services.	□	
Do not assign public IPs to your internal services.	□	
Always think bastion hosts (jump boxes) or EC2 Connect to connect your instances.	□	
Always think VPN access or AWS Verified access for your internal, dev or test environments.	□	

Data Protection Security Best Practices

Your To-Do	Done?	Additional Notes
For data in rest, always think encrypt something: Your database, your S3 objects, your EBS volume, etc.	□	
Do not encrypt something in production before testing it. It’s critical.	□	
If you do not need, use AWS KMS customer managed keys, not imported keys from yourself.	□	
Use KMS key policies for your encryption keys.	□	
Use key rotation. Always.	□	
For data in transit, always think to use TLS and HTTPs configuration.	□	
For TLS, use latest TLS versions. Do not use SSLv2, SSLv3, TLS 1.0, TLS 1.1.	□	
Always redirect your endpoints from HTTP to HTTPs.	□	
Analyze and determine who should access which data. Implement access control policies based on this.	□	

Logging, Monitoring and Alerting Best Practices

Your To-Do	Done?	Additional Notes
Enable multi regional CloudTrail.	□	
Enable alerts for anomaly detection with CloudWatch rules or other 3rd party solutions.	□	
For the alerts, use the communication channel that you're using: Slack, E-mail, Microsoft Teams, or others.	□	
Create a separate security logging and monitoring AWS account.	□	
Create security monitoring dashboards based on your security needs. Logs are not easy to understand.	□	
Create reasonable alerts for your environment. You do not want to get lots of false positive alarms.	□	
Be automatic. Implement automated remediations based on the alerts.	□	
For the alarms, always ask yourself: "Why is this happening? Is this expected or not?"	□	
For the cost optimization for your logs, use lifecycle policies.	□	
Use CloudWatch logs to detect your anomalies in your environment.	□	

Other AWS Security Best Practices

Your To-Do	Done?	Additional Notes
Enable Amazon GuardDuty in every AWS account.	□	
Enable AWS WAF for your external endpoints.	□	
Enable Amazon Inspector for vulnerability management.	□	
Think about automating security controls, threat analysis, detection, and remediation. Always.	□	
Define your needs, enable AWS security services based on this. You do not want to lot of security services, lot of chaos.	□	
Follow AWS security best practices guide, CIS Benchmarks and other compliance checklists.	□	
Be up to date about new AWS features related to security.	□	