**AWS IAM Access Key Rotator (CIS-Compliant)**

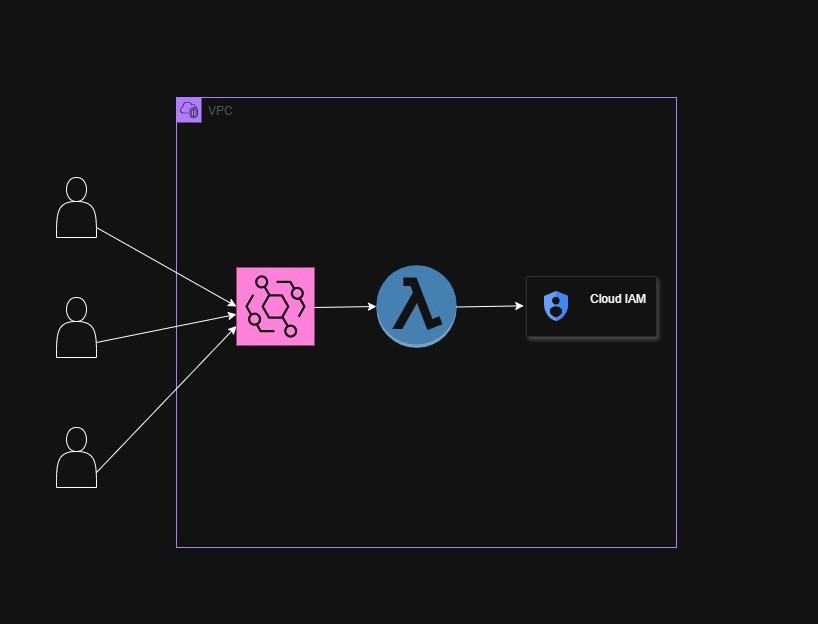
# 1. Index

1. Index  
2. Description  
3. Architecture  
4. Functionality

# 2. Description

This AWS Lambda function enforces CIS AWS Benchmark 1.4 for IAM access keys by rotating keys older than 90 days. It supports dry-run mode for safe testing and skips rotation for whitelisted users. The function runs daily, triggered by Amazon EventBridge, ensuring regular key rotation for enhanced security and compliance.

# 3. Architecture Diagram



1. EventBridge Trigger (rate: 1 day)  
2. Lambda function fetches all IAM users  
3. For each user:  
 a. Skip if whitelisted  
 b. Check access key age  
 c. If age > 90 days:  
 i. Create a new access key  
 ii. Delete the old access key  
 iii. Record in report  
4. Lambda returns a JSON report with details (rotated, skipped, errors)  
5. Logs available in CloudWatch

# 4. Functionality

- ✅ Scans all IAM users daily  
- 🔁 Rotates access keys older than 90 days  
- 🔐 Skips whitelisted users  
- 📄 Returns detailed reports  
- 🧪 Dry-run support for safe testing  
- 📅 Triggered by EventBridge (rate: 1 day)  
- 🪵 Logs actions and errors to CloudWatch