InfraSync ??? DriftGuard for AWS

Case Study

Customer Profile

??? Global SaaS provider operating multi-account AWS footprint with Terraform.
??? Engineering teams ship daily infrastructure updates via Terraform Cloud pipelines.

Problem Statement

??? Manual AWS console changes created configuration drift and compliance risk.
??? Audit teams lacked a centralized record of out-of-band modifications.
??? Incident response relied on ad-hoc scripts and inconsistent Slack notifications.

Objectives

??? Detect drift within minutes of unauthorized changes.
??? Alert responsible teams with actionable remediation context.
??? Maintain auditable history of drift events and remediation outcomes.

Solution Overview

??? EventBridge listens for CloudTrail change events across EC2, S3, and IAM.
??? Lambda Drift Detector triggers Terraform Cloud plan runs for live state comparison.
??? Slack alerts summarize drifted resources, change types, and timestamps.
??? DynamoDB stores drift history with TTL and point-in-time recovery.
??? Optional auto-remediation executes Terraform apply when policy-approved.

Page 2

Business Outcomes & Architecture

Implementation Highlights

??? Terraform IaC deploys EventBridge rule, Lambda function, and DynamoDB table.
??? Secrets Manager protects Slack webhook and Terraform token credentials.
??? CloudWatch Logs and metrics power observability and audit reporting.
??? CI/CD pipeline with GitHub Actions automates Terraform plan/apply and Lambda packaging.

Business Outcomes

??? Reduced mean time to detect drift from hours to seconds.
??? Cut manual audit effort by 60% with centralized drift history.
??? Improved compliance posture via automated Terraform remediation workflows.

AWS Services Utilized

??? AWS EventBridge
??? AWS Lambda (Python 3.11)
??? AWS DynamoDB
??? AWS Secrets Manager
??? Amazon CloudWatch
??? Terraform Cloud (Runs API)
??? Slack Webhooks

Next Steps

??? Extend coverage to RDS, EKS, and load balancer resources.
??? Add optional dashboard (Next.js + Tailwind) for drift analytics.
??? Integrate AWS Security Hub findings for unified compliance reporting.