📓 Case Study: Automated Drift Governance for AWS

□ Overview

Before You Solutions designed and implemented **InfraSync – DriftGuard for AWS** to help DevOps teams maintain configuration integrity in complex multi-account environments. The solution continuously scans for drift between Terraform configuration and actual AWS resource states and remediates them automatically.

🧱 Problem

Many organizations rely on Terraform to manage cloud infrastructure. However, manual changes through the AWS Console or CLI can create **configuration drift**, where deployed resources differ from code definitions. This drift leads to:

- Security non-compliance (untracked IAM changes)
- Resource sprawl and unnecessary costs
- Failed CI/CD pipelines due to state mismatches

Existing tools like AWS Config detect configuration differences but lack deep integration with Terraform's state management.

⚙ Solution Implementation

InfraSync was built to close this gap by using AWS native services combined with the Terraform Cloud API.

Architecture Summary:

- **EventBridge:** Captures configuration change events for core services.
- **Lambda Function:** Executes drift detection using live AWS data.
- **Terraform Cloud API:** Compares actual state against stored Terraform plans.
- **Slack Notifications:** Sends alerts with impacted resource details.
- **DynamoDB:** Logs historical drift data for trend analysis.

An **auto-remediation mode** can be enabled to immediately correct drifted resources using the Terraform Cloud API's run/apply endpoint.

📈 Business Impact

Key Results after internal deployment:

- Reduced manual drift reviews by **85%**.
- Improved IaC compliance score from **72%** → **98%**.
- Cut incident resolution time from **2 hours** → **10 minutes**.
- Enabled proactive drift prevention through Slack alerts.

Cost savings:
~$500/month in reduced engineering hours and avoided resource misconfigurations.

🔐 Security and Compliance

- No long-term AWS keys; uses IAM roles and temporary credentials.
- Terraform API tokens stored in AWS Secrets Manager.
- Principle of least privilege enforced for all Lambda functions.
- Drift logs stored with 90-day TTL in DynamoDB for audit compliance.

🧠 Lessons Learned

- Drift detection is most effective when integrated directly into CI/CD pipelines.
- Combining EventBridge events with Terraform Cloud API provides faster remediation than traditional Config Rules.
- Real-time Slack visibility reduces the “silent drift” problem in distributed teams.

🚀 Future Enhancements

- Add AWS Security Hub integration for compliance scoring.
- Expand to Azure and GCP using a unified abstraction layer.
- Enable anomaly detection through Amazon Bedrock for predictive drift analysis.

🏁 Conclusion

InfraSync – DriftGuard for AWS provides an intelligent, IaC-aware solution for drift detection and remediation. It improves reliability, governance, and cost efficiency for any Terraform-driven AWS environment.

Outcome: Continuous alignment between infrastructure code and live environment, faster recovery, and better operational transparency.