Mikaela June
CSD 380
Module 12
May 18, 2025

Case Study Analysis: Compliance

Case Study 1: Providing Compliance in Regulated Environments

Main Points

The focus of this case study case was to analyze how a large financial services company successfully integrated compliance requirements into its DevOps processes. Compliance processes are normally manual, slow, and often introduce friction into software delivery pipelines in regulated industries. However, within this case study, this company decided to take a different approach by introducing the following:

- Automated Compliance Controls: Instead of treating compliance as a separate, manual step, the company was able to integrate compliance into their automated CI/CD pipelines.
- Security Embedded in Code: They embedded security policies as code to ensure consistency and reduce the potential risk associated with human error.
- Cross-Functional Collaboration: The organization fostered a culture where developers, operations, and compliance officers worked closely together strengthening their collaboration efforts.

Lessons Learned

- Prioritizing shifting left, or integrating compliance early in the development process, helps to improve both security and efficiency.
- Automation is key to making compliance efficient and repeatable.
- Traceability and visibility through telemetry and logging are essential for satisfying auditors and regulators.

Case Study 2: Relying on Production Telemetry for ATM Systems

Main Points

This case study describes how a major bank improved reliability and security of its ATM network by relying on production telemetry and observability. Some of the key points made by the author were as follows:

- Production Telemetry: The bank implemented real-time telemetry from its ATM systems to monitor behavior, detect issues early, and proactively respond to incidents.
- Fast Feedback Loops: Engineers were alerted to problems immediately, reducing downtime and improving service quality.
- Resilience Engineering: The use of chaos engineering principles allowed the team to understand system vulnerabilities before they were exploited. In the long run this helps businesses be more proactive.

Lessons Learned

- Observability is essential in high-risk systems like ATMs.
- Telemetry provides real-time insights that help with proactive issue resolution.
- Immutable infrastructure and automation improve deployment confidence and reduce human error.
- Learning from production systems through monitoring, logs, and chaos engineering is essential for building resilient services.

Key Takeaways

Both of these case studies demonstrated that:

- DevOps practices are highly beneficial when it comes to regulated and critical environments.
- Cultural changes allow organizations to meet both business goals and regulatory obligations through collaborative efforts.
- Security, compliance, and resilience can be enhanced through automation, collaboration, and telemetry.

These case studies provide valuable evidence that the core DevOps principles, automation, feedback, and continuous learning, can change how regulated enterprises deliver secure, reliable services. By putting these practices into effect, businesses can thrive in the ever-changing technological environment.