Ashley Landin

CSD 380 DevOps

Module 12.2 Assignment

July 28, 2024

Case Studies "Providing Compliance in Regulated Environments" and "Relying on Production Telemetry for ATM Systems"

These case studies engage with the topic of how to connect DevOps with the specific requirements and compliance levels that auditors and compliance officers look for. To have these two areas of the development process become more united, there needed to be changes made to the auditor’s approach to measuring the compliance levels within DevOps practices. There also needed to be changes made to the development teams so that the data required by auditors to analyze would be easier to access and decipher. Through both sectors of the development process applying these specific changes to their existing methods, it has helped them both ensure that systems are compliant with laws and regulations.

One universal idea shared between the two case studies is that the relying on older methods to gauge the compliance of systems is now no longer enough, and it can even lead to vulnerabilities going undetected and causing significant issues later. The case study “Relying on Production Telemetry for ATM Systems” brings up a specific issue in the way auditors traditionally rule compliance levels. “Auditor’s overreliance on code reviews and separation of duties between Dev and Ops can leave vulnerabilities” (). Although code reviews and using separation of duties are good methods to view if a system or application is meeting compliance, it shouldn’t be the only methods that they employ. The case study describes how an issue with ATM machines being put into maintenance mode at times when maintenance was not scheduled for a developer to steal money from these machines was detected and solved through production monitoring controls. This specific issue was able to bypass the code reviews and the separation of duties, so if it weren’t for the additional tools to measure compliance, the issue would have been prolonged. It’s important for DevOps teams to work with the auditors to provide them with additional data that could give more context into their operations.

The second case study “Providing Compliance in Regulated Environments” goes into the tools and habits that can be adopted for the DevOps teams to provide more visibility to auditors as to what is happening within the development process. “Our goal is to create alternative methods of presenting the data that clearly show auditors that our controls are operating and effective.” A couple of alternative methods are described, those being sending all data to telemetry systems, having teams work together with auditors, and using the DevOps Audit Defense Toolkit. The use of telemetry systems provides more autonomy to the auditors. With the development teams sending their data to telemetry systems, the auditors could pull the required data for the compliance audit by accessing those same systems and searching through the data. When development teams work together with auditors, they can get the data necessary for the audit during production by running sprints that provide the specific data. The DevOps Audit Defense Toolkit is a resource used by development teams to educate themselves on the auditing process. This is so that the development teams can then provide the auditors with the necessary information to demonstrate that they are aware of the risks to the organization and that they are actively mitigating those risks within the development process.

As DevOps becomes more universally adopted within the sphere of tech development, it’s becoming increasingly important to bridge the gaps between the development teams and auditors. There are specific methods that have been adopted that facilitate this process, with the development teams either working closely with auditors to design tests to provide the data they need or providing auditors with all their data and allowing them to use self-service methods to pull the data required for the audits. Both the development teams and the auditors must pull away from traditional auditing methods to accommodate the current advancements in technology and methodology.

References:

Kim, G., Humble, J., Debois, P., Willis, J., Forsgren, N., & Allspaw, J. (2021). *The devops*

*handbook: How to create world-class agility, reliability, & Security in Technology Organizations* (Second Edition). IT Revolution Press.