**Using Telemetry for Compliance Auditing**

Samuel Litton

Bellevue University

CSD380-A348

Professor Darren Osier

July 24, 2024

**Using Telemetry for Compliance Auditing**

DevOps strategies provide a great many benefits, but it also brings some challenges. One such challenge is the gap of knowledge between DevOps and auditing officers. We can look at two case studies to help us better understand this problem and how to handle it within the DevOps environment.

The first case study is Proving Compliance in Regulated Environments (Kim et al., 2021). This study follows Bill Shinn, a principal security solutions architect at AWS, and his experience with proving compliance to laws and regulations in a cloud environment. He found that the typical auditor’s methodology just doesn’t fit with DevOps. Companies must be able to provide proof that their controls are operating and effective, but in a cloud environment that isn’t so simple. However, Shinn states that the solution is using telemetry and giving access to that data to the auditors.

The second case study is Relying on Production Telemetry for ATM Systems (Kim et al., 2021). This study follows an unnamed banking and financial services organization in the US. They found that security auditors were heavily relying on code reviews to detect fraud. They suggest that automated testing, code reviews, and approvals should be used alongside production monitoring controls to better detect fraud. This method detected an instance of fraud much earlier than the cash audit process.

The findings of both case studies point to the same solution, telemetry. With telemetry, teams can not only prove compliance with laws and regulations, but they can also predict and catch instances of fraud. On top of this, systems using telemetry can actually provide a better solution to these issues than the traditional methodologies.

For proving compliance, teams do not have to take time to find and provide all data and samples to the auditor. This is because they can simply give the auditor access to their telemetry system and data. With a tool such as Splunk or Kibana, the auditor can login remotely and instantly, without interrupting the workflow of the company. The team simply needs to set up the telemetry system and make sure that the data is presentable to the auditor. Or they could simply automate the audit process to perform continuous compliance checks.

For fraud prevention, a team can set up a telemetry system to monitor data such as network traffic, server logs, and user behavior. The team could then integrate a fraud detection algorithm or use a tool such as ChaosSearch. With these tools, teams can automatically predict, alert, or even potentially block fraudulent transactions. This automated process could catch fraudulent activity much faster than scheduled audits.

While DevOps may present some challenges, it also provides elegant solutions to those challenges that oftentimes outperform the traditional methodologies. The two case studies presented above prove this. They also show us that telemetry is a powerful tool that should be used to automate compliance checks and continuously watch for and block fraud.

References

Bunting, D. (2024, June 19). 5 Ways to Use Log Analytics and Telemetry Data for Fraud Prevention. *ChaosSearch*. <https://www.chaossearch.io/blog/log-analytics-and-telemetry-data>

Csw. (2024, January 21). *7 Telemetry techniques to enhance cloud security*. CloudSecurityWeb. <https://cloudsecurityweb.com/articles/2024/01/21/7-telemetry-techniques-to-enhance-cloud-security/>

Kim, G., Debois, P., Humble, J., Willis, J., & Forsgren, N. (2021). *The DEVOPS Handbook: How to Create World-Class Agility, Reliability, & Security in Technology Organizations*. It Revolution Press.