Jeffrey Reid Module 12.2 March 8, 2025

Compliance

A key thing that both Case Studies bring up is the need to adapt the DevOps process for compliance. The 2015 Case Study on Regulated Environment brings up the need for documentation and the 2013 Case Study on ATMS mentions the importance of alternatives to code reviews. Each Study shows the need to adapt the overall process and expand the data an organization looks out for reviews.

The Regulated Environments Case Study is a key story on the importance of adapting the newer DevOps process to the old audit system. Auditors are traditionally trained to gather samples of servers as well as evidence of various logs. These logs include access control settings, server logs and so forth that show control factors working effectively in a business. For these last things, the process doesn’t change much but for the former, some work needs to be done. The problem with getting samples in the new age of operations is that not all servers are on as auto-scaling shifts resources as it’s needed. Amazon solves this particular problem by using telemetry systems such as Kibana to feed all of their data into. These systems pool all of the necessary logs that both Amazon and an auditor would need, whenever they may need it. This allows an auditor to grab the information as needed without interrupting the production process and keeps up-to-date documentation on hand for anyone.

In addition to helping the auditors gather then necessary compliance information; the data is vital protecting the code infrastructure. Different problems have different solutions and knowing which control is needed to correct said problems is vital. By logging all of the information throughout the development process, all control requirements can be viewed when errors do come up. This speeds up the repair time and doubles as necessary information by auditors. After all, compliance necessitates that proper protections are present to protect all data. Having these logs helps show that in an efficient and less disruptive way to production.

As compared to the first Case Study, the ATM case shows another use for Telemetry data. A key thing auditor’s use in the audit process is code reviews. These break down code to see if fraud can be detected in the business environment. However, fraud is difficult to detect in these situations and other methods need to be deployed. In this particular case study, the use of production monitoring tools was vital in detecting an ATM that was entering maintenance mode at unscheduled times. This helped prevent a major fraud case well before it would have been detected using the standard code review process, if it was even detected. This shows the strong importance of using more than one technique, most especially monitoring and automated testing. These can be used to detected unusual patterns that a simple code screening would completely miss.

Both case studies show the importance of adapting to new problems. Businesses that employ DevOps are best suited to gather data through telemetry throughout the development and production process. This data can be used to better identify and fix problems as well as assist in the work auditors need to do to ensure business compliance. It’s also important to use expanded avenues such as automated testing and production monitoring to cover more ground. Newer attack opportunities require more expansive methods of protecting your business. The best way to do that is Telemetry and proper data monitoring.