Kendall Taylor

DevOps

Module 12.2 Assignment

March 9th, 2025

Providing Compliance in Regulated Environments

This case study begins with explaining some issues that many organizations have with auditors and proving that they are in compliance with laws and regulations. Among these issues, it states that many auditors are trained in more traditional methods that don't always work with DevOps. The main problem with some of these methods is that it is difficult to sample environments that are always changing or have coded infrastructures. Audits typically require screenshots and files with configuration details.

Bill Shinn wanted to find a simple way for auditors to retrieve information and find proof of compliance. He explained that a good solution for this was to use telemetry systems for auditors to access necessary data. This idea creates a self-serviced approach for auditors to find the information they need and allows for transparency. So major benefits of doing this include minimizing errors and reducing security problems.

Finally, compliance auditors and regulatory officers need to communicate with DevOps and security teams to come up with protocols and methods to reduce, prevent, and fix issues that may occur. They need to discuss possible tools needed and how they plan to document and pass on information to auditors. This will include documentation on audit evidence and how they will prove that controls are there and working.

Lessons Learned:

-Providing evidence for compliance and regulatory audits may be difficult. A plan must be discussed between DevOps teams and compliance officers to ensure necessary information can be safely retrieved.

-Teams should also discuss the best possible ways to prevent and minimize problems, processes, goals, risks, and control environments should be talked about in this discussion as well as plans needed to prove that these controls are working as expected.

-Creating a self-service and on demand system where auditors can retrieve information they need for evidence can help simplify the process and eliminate the need for requesting data samples.

-Utilizing these methods can help to ensure compliance while reducing errors and minimizing security risks.

Relying on Production Telemetry for ATM Systems

This case study explains security officers, regulators, and auditors rely too heavily on code reviews and not enough on monitoring controls. It is believed that these production monitoring systems are needed on top of code reviews and automated testing to ensure issues with fraud and errors can be properly handled and mitigated.

The case study goes on to describe an example where a developer was able to modify the code for the ATM machines, allowing them to switch to maintenance mode and pull out cash at any time. This issue was not caught through a code review, but through an operations meeting. Someone on the team was able to detect that ATMs were going into maintenance mode during unscheduled times. Because of this realization, they found the fraud before the audit process even occurred.

This example shows the need for production telemetry within systems. In this case, it helped detect an issue of fraud far before other processes too place, but was not found during code review. Without proper production monitoring, this issue could have gone on for much longer, resulting in a larger loss for the business.

Lessons Learned:

-Code review can be of great use but should not be the only form of regulating and monitoring

-Production telemetry is necessary to detect unusual activities, data, and behavior. Often the use of telemetry can help detect issues in their early stages.

-Utilizing multiple methods to detect problems can minimize issues and business losses. This can also help ensure that there is a coverage for all types of problems and vulnerabilities.