Omar Johnson

Module 12.2 Assignment

07/25/24

**DevOps and Compliance Audits**

One of the important responsibilities of an organization is to ensure its products comply with the relevant regulations and laws. Bill Shinn, a principal security solutions architect at AWS, notes, however, that compliance auditors are often not trained to use *ideal* methods to perform audits on DevOps teams. Traditionally, auditors ask for samples of servers to check items such as configuration, logs, and more. Although this is okay for physical servers, in more modern DevOps environments, teams are split up between development and deployment, and servers are frequently scaled in and out of the picture. This can make it difficult to take multiple static samples of data for the audit. Shinn describes that a better way to handle this is through telemetry. The DevOps team can work with auditors to determine which data is most essential to the audit and have the data continually sent into telemetry systems. Through the telemetry software, auditors can always view the evidence they need, providing complete “transparency” into operations. Furthermore, Mary Smith from a second case study expresses that code reviews alone are not enough to complete effective audits. Instead, using code reviews in hand with operations reviews (such as those via telemetry) is more effective in discovering vulnerabilities. In her case, “[They] found the fraud even before the scheduled cash audit process, when they reconcile the amount of cash in the ATMs with authorized transactions”.

Both of these cases show how helpful collaboration with regulatory officers can be for DevOps teams. Because standard audits are not well-suited to DevOps environments, practices should be run to ensure the audits cover the full scale of the workflow. As learned, an efficient way to do this is through the use of telemetry systems, where the systems read and store data considered critical to the audits (such as security controls, server logs, permissions, changes, etc.). Auditors can then review the long-term stored data at their disposal. The concept of configured telemetry also provides more flexibility, compared to auditors normally being limited to the currently running or available servers. However, it is important for teams to band with the officers and list which telemetry data is needed so that information is properly captured, ensuring teams are on the right track to compliance. Additionally, there are many resources and tools available for organizations to follow and assure that audit controls are implemented to their full effectiveness.

**References**

Kim, Gene, et al. The DevOps Handbook: How to Create World-Class Agility,

Reliability, & Security in Technology Organizations. 2nd ed., IT Revolution

Press, LLC, 2021.