Jon Green

Module 12.2: Compliance

Both articles discussed the importance of data logging in addition to the actual logging process. The core message from both articles is that there needs to be a solid communication path between devops and the system auditors. Information security is a shared responsibility between all members and logical data collection practices are critical to development. There needs to be a structured process for the sharing of data between the teams. The data logging process should be practical and functional for all teams that are involved. This process will allow the auditors to have full access to the necessary data. The purpose is to reduce the strain on the other cross functional teams due to extensive data submission requests. The goal is for the team to retrieve the data logs as quickly as possible and avoid delaying the submission of data. Another important aspect is to ensure that the data collected is relevant to the event that is being reviewed.

The Proving Compliance in Regulated Environments case study focused on the data logging process and how it should evolve and be tailored toward the current business. In the past, it was up to the auditors to request specific information from the devops teams to complete the review tasks. This process is problematic in modern times considering that most systems are now cloud based. Cloud based technology has changed the landscape in regard to how a team can gain access to stored log data. Advancements in technology have created better collection methods and options such as remote access to the data logs.

The resolution mentioned in the article was to have teams collaborate directly with auditors to assign a control during each sprint of the project. This method provided a simpler option to collect data as the required audit criteria is already built into the sprint. A system was setup to automatically send the logging information to a data storage platform such as Splunk or Kibana. The auditors could then access those platforms as needed to obtain the required data. A key takeaway from the article is that the data collection process needs to be efficient with little to no user impact. Proper tools and shared access need to be provided to all members to provide a seamless experience.

The Relying on Production Telemetry for ATM Systems article discussed how auditors rely too heavily on code reviews to detect fraudulent activities. Code reviews are a great method of identifying issues. However, some things can be resolved by using a little bit of common sense as well as the code review process. In this article, fraud was detected by simply viewing a daily maintenance log for an ATM machine. The ATM machine would go down repeatedly during unscheduled maintenance hours. These events triggered a red flag for the auditing team, which then prompted them to review the ATM logs. The extensive code review process that is normally conducted was unrelated to this situation. Therefore, that security process would not have been beneficial to resolve the issue in a timely manner. In this event, production monitoring in addition to automated testing should have been conducted by the auditors and dev ops team to detect the problem. This is an example of how better communication between the teams is important when attempting to mitigate risk and review data logs.

Sources:

Kim, G., Debois, P., Willis, J., Humble, J., & Allspaw, J. (2017). *The DevOps handbook : how to create world-class agility, reliability, and security in technology organizations*. It Revolution Press, Llc.

‌ Heusser, M. (2019). *4 DevOps communication principles to get teams talking*. Software Quality; TechTarget. https://www.techtarget.com/searchsoftwarequality/tip/4-DevOps-communication-principles-to-get-teams-talking

‌