Proving Compliance in Regulated Environments

By: William Thomason

WEB-430

Assignment 9.3

Proving Compliance in Regulated Environments

This paper will cover the case study in our textbook that talks about how large companies prove their in compliance in regulated environments. Bill Shinn was the person tasked with the responsibilities at principal security solutions architect at Amazon Web Services is to comply with all relevant laws and regulations. Shinn over the years has spent time with over one thousand enterprise customers who have publicly referenced their use of public clouds in highly regulated environments. He found that the auditors have been trained in methods that are not very suitable for DevOps work patterns. This makes it difficult to audit the infrastructure when auto-scaling makes servers appear and disappear; there is no good way to send the auditor a sample. This is also when the deployment pipeline, which is different from the traditional software development process. One group writes the code and the other deploys that code into production. Shinn’s goal was to create alternative methods of presenting the data that clearly shows auditors that their controls are operating and effective.

Shinn has made dedicated teams to help bridge the gap with auditors in the control design process. These teams use an interactive approach by assigning a single control for each sprint to determine what is required to present as audit evidence. This helps ensure that auditors get the right information that is needed when the service is in production, entirely on demand. Shinn ended up sending all data to their telemetry systems and the auditors then can get what they need, completely self-serviced. There is now no need to request data samples instead they log into the system and retrieve the audit evidence they need. With the modern audit logging, chat rooms and deployment pipelines, there is unprecedented visibility and transparency with what is happening in production. This is especially true compared to how operations used to be conducted with lower probability of errors and security flaws being introduced.

Shinn explains in the case study that HIPPA can be tricky to figure out what is required from the actual regulations. HIPPA requirements from an information security standpoint can be found in forty-five CFR Part 160 legislation, Subparts A and C of part 164. When you find technical safeguards and audit controls, you know you are in the right place. There you will find what is required is that we need to determine activities that will be tracked and audited relevant to Patient Healthcare Information, document and implement those controls, select tools, and then finally review and capture the appropriate information.

The DevOps Audit Defense Toolkit is a document that describes how controls could be designed in a deployment pipeline to mitigate the stated risks, and provides examples of control attestations and control artifacts to demonstrate control effectiveness. This document was intended to be general to all control objectives and can be extremely helpful getting you started down the right path. Compliance in Regulated environments is a large undertaking for any company and something that should done the proper way, you customers and your companies vital information must be protected at all times.

References

Goff-Dupont, S. (2018, May 1). DevOps vs. compliance: a guide to having it all. Retrieved from https://www.atlassian.com/blog/devops/how-to-make-compliance-easier-devops

Sadogursky, B. (2018, July 26). DevOps and Compliance: A Match Made in Heaven - DZone DevOps. Retrieved from https://dzone.com/articles/devops-and-compliance-a-match-made-in-heaven