Adam Donner

Web 430

Assignment 9.3

November 6, 2019

Case Study: Providing Compliance in Regulated Environment (2015) & Relying on Production Telemetry for ATM Systems

In today’s world, the need for organizations to protect any sensitive information of their customers is more important than ever. Regulatory compliance in IT is of utmost importance. This can be achieved even when the organization is using DevOps for software delivery.

Bill Shinn is a principal security solutions architect at Amazon Web Services. He is responsible for helping large enterprise customers such as Hearst Media, GE, and Pacific Life, show that they can still comply with any relevant laws and regulations even though they are using public clouds. His goal is to create alternative methods of presenting data that will clearly show auditors that controls are operating and effective. To achieve this goal, his team works closely with auditors in the control design process. A single control is assigned to reach sprint to determine what is needed for audit evidence. Overall this has helped to ensure that the auditors have access to the information they need when the service is in production (Kim, Debois, Willis, Humble, & Allspaw, 2017).

As DevOps is being implemented into more and more IT organizations, the organization needs to understand how compliance controls and security will be impacted. DevOps advocates using automation techniques for continuous delivery. Automation can help organizations stay compliant and even increase their compliance levels. Compliance bottlenecks can be removed early on in the process and bring security, agility, and stability into the software value chain. Automation of processes and testing will help reduce the risk of introducing security flaws (& , 2017). 

The most effective way to achieve this goal is to send all of the data through a telemetry system. By doing this, the auditors can have self-service access to the data and see that the controls are working when it is needed. There is a very high amount of transparency into the works of production through audit logging, chatroom, and deployment pipeline. There needed to be a way to turn all of the data into something that the auditors could recognize. This requires deriving the engineering requirements from the actual regulations (Kim, Debois, Willis, Humble, & Allspaw, 2017).

To make all of this easier, there is a *DevOps Audit Defense Toolkit.* The goal of this is to educate IT managers and practitioners on the audit process so they can demonstrate to the auditors that they have an understanding of what the business risks are and how to properly mitigate those risks. The Toolkit summarizes the techniques to use to mitigate risk as well as provides answers to questions about value creation, compliance, and DevOps (). The Toolkit is intended to be general to all control objectives, contractual obligations, and effective and efficient operations (Kim, Debois, Willis, Humble, & Allspaw, 2017).

Production telemetry is key to understanding how a system is being used in production. It can be used to identify potential problems and will, in-turn, increase security, especially when compliance checks are not enough. An ATM vendor showed how valuable production telemetry is. One of their software developers had out a backdoor into the code. The ATM vendor noticed that their ATMs were being put into maintenance mode at unscheduled times. This allowed for cash to be physically taken out of the machines. Backdoors like the one that was put into the code can be very difficult to detect. Production telemetry allowed for the fraud to be detected and the ATM vendor to be alerted. They were able to resolve the issue before the scheduled cash audit process (Kim, Debois, Willis, Humble, & Allspaw, 2017).

The guiding principals of DevOps, such as automation, telemetry, and validation, provide in-depth audit and change information to satisfy audit and regulatory compliance needs.

References

DevOps Audit Defense Toolkit. (n.d.). Retrieved November 5, 2019, from <https://itrevolution.com/devops-audit-defense-toolkit/>.

How to Ensure Regulatory Compliance in the World of DevOps? (2017, May 18). Retrieved November 5, 2019, from https://www.cigniti.com/blog/ensure-regulatory-compliance-world-devops/.

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. Portland, OR: IT Revolution Press, LLC.