Cody Ferre

10/08/2024

CSD380

The case studies that we are looking at are taking an overview of the auditing processes and how important it is to stay within regulations. Our first case study focuses on the problem that auditors are not able to understand the code much less audit someone over the information they are looking at. The main point of this is implementing the standards and programs in order to allow them to look, understand and review the code segments that are being implemented. With the second case study going over the controls that the auditors are using can be automated but by doing dynamic audits where they change controls and the scope of their auditing to allow for further issues to come out even if none are immediately shown.

With the case study of Providing Compliance (2015), starts off with one of the problems being auditors not being properly trained to understand how DevOps work patterns are. His solutions when it came to this was to give them a program that could compile and gather all the data and give them useful information that they could use to handle the audits, this was done using programs like Splunk or Kibana and they would gather the evidence of their audits using screenshots and logs.

Looking at HIPAA requirements shows that Shinn also needed the auditors to have more control and to accomplish this he chose to use a program called AWS CloudWatch. This program allowed them to log the framework while using an audit process called the DevOps Audit Defense Toolkit as guidelines to what they are auditing. These would be the risks, processes, goals and controls within the company, with the main takeaway being that it's important to understand the security controls and how they implemented across the company as too little could mean holes within the security or audit teams and too much could be confining and now follow proper regulations.

The second case study following the audit process is not being good enough to catch all fraud implementations within the code. Saying that while you can look at the code and its implementation to audit it is also important to ensure that the auditors are monitoring the monitoring controls to test and find errors actively rather than passively using an automated system. With this case study the takeaway comes from the dangers of not doing active audits that you also manage the controls and ensure that the code is also being tested and following the proper processes.

The main takeaways from both case studies are to take the time to ensure that our audit teams understand what they are reviewing and gathering evidence for, along with the controls and tools they require to do these audits such as Splunk or Kibana giving them logs and code in a convenient place. The main point being that these tools are needed along with proper training in how to use them, it's necessary to stay within regulations regarding what control aspects they should have to perform those duties. Our second case study focused on the control aspect of auditing as it was showing how we could automate our audit processes, but we could overlook fraud code that could be impactful if we don’t perform active scope audits.

References

Gene Kim, Jez Humble, Patrick Deboid, John Willis, 2016, The DevOps Handbook, <https://dl.faghatketab.ir/Books/Computer/Programming/WebProgramming/The.DevOps.Handbook_faghatketab.ir.pdf>