Assignment 12.2

Bella Apo

Assignment 12.2

CSD380

03/04/2025

Providing Compliance in Regulated Environments

The case study “Providing Compliance in Regulated Environments” discusses the role of a Principal Security Solutions Architect at Amazon in helping large enterprise customers adhere to the relevant laws and regulations. In audit fieldwork, alternative methods of presenting data must be developed to help avoid revealing sensitive configuration details and logs.

To help bridge the gap between auditors and enterprise teams, the security architect encourages collaboration in the control design process. The approach assigns a single control per sprint and ensures that audit evidence is appropriately identified. The method helps to ensure that auditors are receiving the necessary information on demand, helping to improve efficiency, and reducing the burdens of compliance.

In addition, the auditors can retrieve the data from self-service telemetry systems, like Splunk or Kibana. These systems help to eliminate the need to request data samples. This system allows auditors to search for audit evidence within a specific period, which helps increase their transparency while remaining security levels. Proper documentation and visibility of the log destinations are necessities in this approach.

An important aspect of this process is the DevOps Audit Defense Toolkit. This tool serves as an end-to-end narrative that helps to support the audit process for fictitious organizations. The toolkit describes the entity’s organizational goals, business processes, the top risks, and the control environment. It helps management to prove that controls

exist and are effective by detailing how they can be embedded in a deployment process pipeline.

The case study highlights the importance of building thorough documentation to bridge the gap that exists between DevOps practices and the auditor's requirements. It highlights how DevOps can comply with regulations while still working to improve risk assessment and mitigation strategies.

Relying on Production Telemetry for ATM Systems

The case study "Relying on Production Telemetry for ATM Systems" examines the risks of over-reliance on code reviews and their role in detecting fraud within financial institutions. Traditionally, auditors and regulators have depended on code reviews to help identify any potential security threats. But this approach alone has been proven to be inefficient in preventing fraud and other errors. Instead, production monitoring controls, automated testing, and approval workflows should be integrated to mitigate the risks more effectively.

An important aspect of the case study is that a developer, who was a part of the development team, placed a backdoor into an ATM's system's code. This allowed the developer to switch machines into a maintenance mode that allowed them to withdraw cash undetected. Although this breach was identified, and quite quickly, the incident highlighted how detecting insider threats can be nearly impossible. When attacks have the necessary knowledge and access, they can get away with anything.

This case study helps to emphasize that companies place too much trust in code reviews. However, this approach alone is ineffective and leaves vulnerabilities exposed. By integrating telemetry methods, organizations can gain the necessary visibility methods to detect and respond to errors and activities in real time.

Lessons Learned

Both case studies help highlight the need for more dynamic and proactive approaches when dealing with compliance and security monitoring. In regulated environments, adopting iterative control design process and maintaining details documentation is crucial in helping organizations meet their compliance requirements without exposing any sensitive information from clients or the enterprise. Similarly, in financial systems, relying only on code reviews is inadequate for preventing fraud. Organizations should integrate production telemetry, automated testing, and real-time monitoring to help detect and mitigate security threats. These lessons can help organizations to enhance their security, streamline the audit process, and reduce the overall vulnerabilities in both regulatory and operational contexts.

References

Kim, G., Debois, P., Willis, J., & Humble, J. (2016). *The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations*. https://dl.acm.org/citation.cfm?id=3044729