Michele Brand

Assignment 12

CSD 380

The two case studies, “Proving Compliance in Regulated Environments” and “Relying on Production Telemetry for ATM Systems,” highlight some of the industry’s auditing practices and fraud detection, respectively. These case studies give a deeper insight into DevOps security environments. Through this essay, I’ll highlight the key points of each case study and the lessons brought up by both of these studies.

In the case study titled “Proving Compliance in Regulated Environments,” the author, Bill Shinn, a security solutions architect at Amazon Web Services, highlights challenges associated with auditing techniques in DevOps. Shinn suggests pushing for a more collaborative auditing technique that would help develop more alternative auditing methods. He also emphasizes using telemetry systems like Splunk or Kibana for self-service auditing. These systems let auditors access real-time data, which in turn improves transparency and visibility into controls.

One key lesson is that collaboration between technical and non-technical teams is crucial for creating effective auditing methods. Using telemetry systems gives auditors real-time data, changing traditional auditing practices in dynamic environments. The study shows that effective auditing in regulated environments requires not just following standards but also a proactive approach to monitoring compliance in real-time.

In “Relying on Production Telemetry for ATM Systems,” author Mary Smith (a pseudonym) highlights the problems with relying only on code reviews for fraud detection. Information security, auditors, and regulators often depend too much on code reviews and ignore production monitoring controls. Smith describes an incident where a developer created a backdoor in ATM code for unauthorized withdrawals, discovered only during regular

operations, not code reviews. This shows the need for robust production monitoring controls to detect and prevent fraud.

The main lesson from this study is that relying too much on code reviews can miss sophisticated fraud techniques. This means robust production monitoring controls are necessary. Effective production telemetry and regular operations reviews are crucial for early fraud detection and mitigation, even in well-structured environments. Smith's study shows that production telemetry can catch anomalies and suspicious activities that static code reviews might miss. Continuous monitoring of the production environment helps detect unusual behavior that could indicate fraud or other malicious activities.

These case studies highlight the need for more collaborative efforts to catch potential security risks in technology. Collaboration, innovative auditing approaches, and strong production monitoring controls are essential strategies for combating fraud and security breaches. Both studies stress that a combination of proactive and reactive measures is essential for maintaining security and compliance in dynamic and complex environments. By using different auditing and monitoring techniques together, organizations can build a strong defense against new threats.

In conclusion, the insights from these case studies show the importance of evolving auditing and monitoring practices to keep up with changes in DevOps and information security. Emphasizing collaboration and using advanced tools like telemetry systems can greatly improve the effectiveness of auditing and fraud detection efforts. As technology continues to change, so must the strategies and tools used to ensure security and compliance.

Sources:

Kim, Gene, et al. *The Devops Handbook: How To Create World-Class Agility, Reliability, And Security In Technology Organizations*. IT Revolution Press ; Distributed by Skillsoft Books, 2017.