Taylor Mommer

Assignment: Compliance

July 19, 2024

Professor Sue Sampson

**Providing Compliance in Regulated Environments**

**Summary of Main Points:**

* **Challenges with Traditional Auditing:** Bill Shinn from Amazon Web Services highlights how traditional audit methods, which rely on sampling servers and reviewing screenshots, are ineffective for cloud-based systems where servers frequently change and are managed through code.
* **Modernizing Evidence Collection:** Shinn suggests using real-time data collection tools like Splunk or Kibana to address this. These tools allow auditors to access the necessary information directly rather than relying on static samples or screenshots.
* **Collaborative Approach:** Shinn recommends involving auditors in the design of controls from the start. This way, the audit evidence needed is built into the system, making the auditing process smoother.
* **Understanding Regulations:** Shinn emphasizes the importance of thoroughly understanding regulations to ensure that technical controls meet legal requirements. This involves interpreting complex legal texts and translating them into actionable technical measures.
* **DevOps Audit Defense Toolkit:** The toolkit offers a structured approach to compliance, outlining how to align organizational goals with control requirements and providing examples of adequate controls and documentation.

**Lessons Learned:**

* **Update Audit Practices:** Traditional audit methods must evolve to suit modern cloud environments. Using real-time data tools can improve compliance verification.
* **Engage Auditors Early:** Working with auditors during the design phase ensures that compliance needs are addressed from the start, making audits more efficient.
* **Translate Regulations into Technical Controls:** A deep understanding of regulations is necessary to design controls that meet legal requirements, making compliance efforts more effective.

**Relying on Production Telemetry for ATM Systems**

**Summary of Main Points:**

* **Effective Use of Telemetry:** Mary Smith, leading the DevOps initiative for a major financial organization, argues that monitoring production systems is crucial for detecting fraud, beyond just relying on code reviews.
* **Real-World Example:** Mary Smith describes a case where a developer inserted a backdoor into ATM software, allowing unauthorized access to cash. The fraud was detected not through code review, but through monitoring systems that flagged unusual ATM activity.
* **Production Monitoring Over Code Reviews:** The case underscores the importance of using production telemetry to detect and respond to fraudulent activities and other issues that might not be caught during code reviews.

**Lessons Learned:**

* **Prioritize Production Monitoring:** Monitoring systems in real-time is essential for catching fraud and other issues that might not be detected through code reviews alone.
* **Proactive in Fraud Detection:** Effective monitoring can identify problems quickly, often before they become significant issues or before scheduled audits occur.