Brittni Ray

CSD 380

Module 12.2

**Case Study Analysis: "Providing Compliance in Regulated Environments" and "Relying on Production Telemetry for ATM Systems"**

**Providing Compliance in Regulated Environments**

**Author’s Main Points**

1. The Challenges in Auditing Modern Environments.
   1. The case study talks about how auditing in our day has become a little more difficult, as relying on screenshots or manual samples are not well suited to dynamic, DevOps-driven environments where code infrastructure is managed and where systems are operating continuously.
2. Iterative Control Design.
   1. Working in collaboration with development teams *and* auditors helps ensure that they are ready for auditing. In this way, real audit evidence that aligns with DevOps workflows can be achieved.
3. Having Centralized Telemetry for Audit Evidence.
   1. Using tools such as the named Splunk and Kibana will help auditors to be able to get the evidence that they need for the audit. This will reduce the need for the manual samples that auditors usually have to rely on.
4. Interpretation of Regulator Requirements.
   1. A lot of compliance requires taking high-level regulations and translating them into measurable engineering requirements. This would involve selecting tools or defining activities for tracking along with using the appropriate controls.
5. DevOps Audit Defense Toolkit.
   1. This toolkit will offer a good framework for helping to design controls and proving compliance through artifacts. In turn, it will also provide an adaptable narrative for various regulatory and operational objectives.

**Lessons Learned**

1. Current auditing processes will need to evolve to match the complexity and speed that exists within a lot of DevOp-type environments. Things like automation can help bridge the gap between the traditional sort of auditing and the quicker, more modern workflows.
2. Strong collaboration between the regulatory officers and technical teams is vital in order to define and implement controls that will meet compliance requirements.
3. Having clear documentation and a centralized framework, such as the DevOps Audit Defense Toolkit, can help improve complicance efforts while also making life easier on auditors.
4. Prioritizing visibility and transparency into production environments will reduce the possibility of errors or security breaches.

**Relying on Production Telementry for ATM Systems**

**Author’s Main Points**

1. Considering the Limitations of Code Reviews.
   1. Conduction *only* code reviews alone is not enough to find when fraud is happening or in preventing any security breaches, especially in the cases where the violators of this are good at what they do.
2. Using Production Telemetry as a Detection Mechanism.
   1. Monitoring production systems continuously will help detect any anomalies in ATM maintenance schedules, which is vital for identifying and stopping fraud more quickly.
3. The Separation of Duties and Change Approval.
   1. Although these are both very great topics to have in the conversation, these sorts of traditional practices may not always be enough to prevent a high-scale or more sophisticated fraught. However, combining these practices with telemetry will help improve the likelihood that a system is at risk.
4. Considering Real-life Incidents.
   1. The author outlines and incident where a backdoor coded into an ATM’s software allowed for unscheduled maintenance mode activations, which also would allow theft. This flaw and fraud had not been detected by code reviews *or* change review processes, but by operational telemetry during a routine review meeting.

**Lessons Learned**

1. Continually monitoring production is vital for detecting anomalies that could reveal fraud or any operational failures. In most cases, this will allow these things to be found before they are found in traditional review processes (code review).
2. Security measures should be more than just change approval and development, including stricter monitoring and automated detection mechanisms.
3. Seeing real-life incidents helps emphasize the importance of having more than a one-note security approach. Which would include integrating automated testing, code reviews, *as well as* telemetry for comprehensive management of risks/vulnerabilities.
4. Having effective production telemetry will allow organizations to quickly identify, single out, and address incidents—which will reduce the likelihood of potential damages or disruptions.
5. Holding operational reviews that are supported by telemetry can be used as a final line of defense against any security breaches—whether they be intended or not.

**Source**

Kim, G., Humble, J., Debois, P., Willis, J., Forsgren, N., & Allspaw, J. (2021). *The devops handbook: How to create world-class agility, reliability, & Security in Technology Organizations*. IT Revolution Press.