**Proving Compliance in Regulated Environments and Relying on Production Telemetry for ATM Systems: Lessons Learned**

### **Case Study 1: Proving Compliance in Regulated Environments**

Bill Shinn, a principal security solutions architect at Amazon Web Services, discusses the challenges of proving compliance in highly regulated environments, particularly in the context of modern cloud infrastructure and DevOps practices. Traditional audit methods, such as manually sampling server configurations and logs, are not well-suited for dynamic cloud environments where infrastructure is defined as code and servers frequently change due to auto-scaling.

To address this challenge, Shinn advocates for integrating auditors into the control design process using an iterative approach. By assigning a single compliance control per sprint, teams can ensure that necessary audit evidence is readily available when needed. He emphasizes leveraging telemetry systems, such as Splunk or Kibana, to provide auditors with self-service access to real-time compliance data, reducing reliance on static screenshots and CSV files.

Additionally, Shinn stresses the importance of deriving engineering requirements directly from regulatory frameworks like HIPAA. This involves identifying relevant technical safeguards, implementing controls, and ensuring audit evidence aligns with compliance needs. Tools such as AWS CloudWatch can be used to monitor and verify control effectiveness. To further aid organizations in achieving compliance, the DevOps Audit Defense Toolkit offers guidance on designing control environments, mitigating risks, and addressing audit objections.

Traditional audit methods are not effective in cloud-based DevOps environments. Collaboration between auditors, compliance officers, and DevOps teams is crucial for effective compliance. Telemetry systems enable real-time access to audit evidence, improving transparency and efficiency. Compliance requirements should be derived directly from regulatory texts and mapped to engineering controls. Automated monitoring and logging frameworks help link audit evidence to control requirements.

### **Case Study 2: Relying on Production Telemetry for ATM Systems**

Mary Smith, leading a DevOps initiative at a major US financial services organization, highlights the importance of production monitoring in detecting fraud and operational anomalies. She critiques the heavy reliance on code reviews for fraud detection, arguing that production telemetry offers a more effective approach.

She recounts a real-world incident in which a developer planted a backdoor in ATM software, allowing unauthorized cash withdrawals during specific maintenance windows. Despite existing controls, including separation of duties and a formal change approval process, the fraud went undetected through traditional means. Instead, it was discovered through production telemetry when an operations review meeting flagged unscheduled ATM maintenance activities in a particular city.

This case underscores the limitations of static security measures and the need for real-time monitoring to detect suspicious activities. By continuously analyzing operational data, organizations can quickly identify and respond to security threats, reducing the risk of financial losses and operational disruptions.

Code reviews alone are insufficient for detecting fraud and security threats. Real-time production monitoring is essential for identifying suspicious activities. Separation of duties and change approval processes do not guarantee fraud prevention. Regular operational reviews can help uncover anomalies before formal audits occur. A proactive approach to telemetry and monitoring enhances security and fraud detection.

Both case studies illustrate the growing need for modern compliance and security practices that align with DevOps methodologies. Traditional compliance and security measures must evolve to incorporate automation, real-time telemetry, and collaborative approaches that ensure both regulatory adherence and operational security. By leveraging advanced monitoring tools and integrating compliance into the development lifecycle, organizations can maintain compliance and security without hindering innovation.