Rogelio Orozco

Module 12.2

July 24, 2024

CSD 380 – Dev Ops

Case Study Overview: Providing Compliance in Regulated Environments

Bill Shinn, a security solutions architect at Amazon Web Services, helps big companies follow the laws and regulations required in their industries. He has worked with many well-known companies like Hearst Media, GE, Phillips, and Pacific Life, who all use AWS's public cloud services in regulated environments.

One major issue Shinn points out is that traditional audit methods do not fit well with modern DevOps practices. Auditors usually ask for large samples of data and screenshots to check for compliance. For example, an auditor might request evidence from one thousand servers out of ten thousand, which involves taking screenshots of asset management and access control settings. However, this method doesn't work well when servers are constantly changing and managed through code.

To address this, AWS aims to create new ways to present data that clearly show that their controls are effective. Shinn’s teams work closely with auditors during the control design process. Each sprint, they focus on a single control to determine the necessary audit evidence. This approach ensures auditors get the information they need on demand when the service is live.

AWS uses self-service tools like Splunk and Kibana to make this process easier. They send all data to these systems so auditors can access the evidence they need without requesting data samples. Auditors can log into Kibana and search for the necessary audit evidence within a specific time range. This method improves visibility and reduces errors and security issues compared to traditional operations.

Understanding regulations like HIPAA is vital for setting up the right controls. Shinn explains that you need to read the relevant laws to find out what activities need to be tracked and audited. Then, you document and implement the necessary controls, choose the right tools, and gather the appropriate information. This helps compliance officers, security teams, and DevOps teams work together to prevent, detect, and fix problems.

For example, AWS might use CloudWatch to monitor compliance. They can test controls with a single command and ensure logs are sent to a logging framework, linking audit evidence with control requirements.

To help other companies, AWS developed the DevOps Audit Defense Toolkit. This toolkit explains the compliance and audit process for a fictional company. It covers organizational goals, business processes, risks, and control environments. The toolkit includes examples of control attestations and artifacts to show control effectiveness and supports various regulatory requirements.

Case Study Overview: Relying on Production Telemetry for ATM Systems

In the case study "Relying on Production Telemetry for ATM Systems," Mary Smith, who leads the DevOps team at a large financial company, points out a significant issue in how fraud and errors are managed in complex systems. Her insights suggest that while code reviews are important, they are not always enough to catch fraud or errors.

Mary recalls an incident where a developer secretly added a backdoor into the ATM system's code. This backdoor allowed the developer to put ATMs into maintenance mode during off-hours, letting them steal cash without being noticed. The fraud wasn’t detected through code reviews but was discovered thanks to production telemetry—a real-time monitoring system that identified unusual maintenance activity.

The main takeaway from this case study is that relying only on code reviews might not be enough to spot fraud or errors. Code reviews are good for catching mistakes, but they might not reveal intentional wrongdoing, especially if someone has insider knowledge. On the other hand, production monitoring provides real-time insights into how the system is functioning and can detect unusual patterns that code reviews might miss.

Mary stresses that it’s crucial to combine regular operational reviews with strong production monitoring. In her experience, noticing unusual patterns in ATM maintenance helped catch the fraud before a cash audit could find it. This highlights the importance of using both production monitoring and traditional security measures to create a more complete fraud detection system.

The key message is that a mix of different security methods is necessary. While code reviews and automated testing are important, adding continuous production monitoring can help catch both mistakes and fraud. By using this approach, organizations can better protect their systems and improve overall security.

References:

Humphrey, J., Kim, G., & Behr, K. (2016). *The DevOps Handbook: How to create world-class agility, reliability, & security in technology organizations*. IT Revolution Press.