Sarah Ewing
12/19/2024
Module 12.2 Assignment

Compliance

Proving Compliance in Regulated Environments

This case study talks about how Bill Shinn of Amazon Web Services deals with the challenges of ensuring compliance in highly regulated environments. Shinn discusses auditors' difficulties with traditional auditing methods when dealing with dynamic DevOps environments. He suggests using telemetry systems like Splunk or Kibana for real-time, self-service access to audit evidence. Shinn discusses the importance of collaboration between auditors and DevOps teams to design controls that prevent, detect, and correct problems. The DevOps Audit Defense Toolkit was introduced to help organizations ensure compliance with regulations while using DevOps principles.

There are several lessons we can learn from this case study. First, we learned that thinking outside the box is essential when implementing auditing methods. Because traditional auditing methods don't work well in DevOps environments, telemetry systems can be used for real-time audit evidence. Next, we learned that it's important to collaborate. Auditors and DevOps teams work together to design controls that meet requirements. We also learned that it's important to understand regulations. DevOps teams must be aware of regulations to create controls to meet the requirements. Finally, we learned the importance of effectively using tools. The article talks about how tools like AWS CloudWatch can be used to implement and test controls.

Relying on Production Telemetry for ATM Systems

This case study talks about how Mary Smith, who headed up the DevOps initiative for a large US financial services organization, observed that reliance on code reviews and separation of duties to detect fraud is insufficient. She emphasized the importance of production monitoring controls. Smith shared about an incident where a developer inserted a backdoor in the ATM software, allowing them to withdraw cash from the machines. The fraud was detected because someone noticed unusual maintenance mode activity during a regular operations review meeting. The case study shows that relying on code reviews and separation of duties alone can leave systems vulnerable.

There are lessons that we can learn from this case study as well. First, we learned the importance of production monitoring. Production telemetry can help detect fraud and errors. Next, we learned that code reviews and separation of duties alone will not detect all problems. Malicious actors use techniques that can be missed by only using these practices. Finally, we learned about the importance of regular operations reviews. The case study shows that regularly reviewing systems can help identify unusual activities and potential issues early.