Alejandro Quezada

Module 12.2 Assignment: Compliance

Read the case study "Providing Compliance in Regulated Environments" and the case study "Relying on Production Telemetry for ATM Systems" in Chapter 23 of the course textbook. Compose a paper of the author's main points and the lessons learned for both case studies.

The biggest point being pushed in both case studies is telemetry. Now why is that? Telemetry is basically recording data and then that data is sent, “for monitoring and analysis”. There are a number of benefits to having telemetry in place in an organization. You are able to discover threats before it can do any damage, it is possible to monitor resources from a remote location, can determine what might be failing soon, and it offers real time monitoring.

In the first case study the goal is to find a way to show proof that the organization is compliant to the regulations. The issue mentioned is that auditors were trained to deal with physical environments and acquire the data from that. With DevOps, it is difficult to follow the same methods that they have been taught to do. To resolve the issue, telemetry is utilized. With the data being recorded and then is sent to an application, they are able to acquire the data. The neat part mentioned from the case study is that they “search for audit evidence they need for a given time range”, by using the application. They no longer need to ask for screenshots, or samples if telemetry is in place. To find out what data needs to be recorded it is necessary to look into the regulations. Aside from that it also needs to be discussed by the officers and devops. Another helpful tool used is something called the devops audit defense toolkit. The purpose of it is to demonstrate how audits should occur within companies that have devops.

The next case study revolves around ATMs being used fraudulently. “Mary Smith”, had made note that a common problem she has seen is that code reviews are relied on way too much in order to discover any illegal activity. I would agree with that sentiment. We need to take every precaution to make sure everything is secure. Just because everything is secure, does not mean that we should not be using more tools to actively detect any fraudulent activity. We have to use any means necessary to prevent mishaps. In the story shared in the case study the code review was not what detected fraud, but during a meeting by someone with production telemetry. Had that person not noticed it, I believe it would have been till much later before anyone might have discovered it. That shows how important it is to incorporate various other monitoring tools. There is no such thing as being too safe as anything could happen externally, or internally.

Overall, both case studies point that telemetry can do so much more than just recording data and storing it. It allowed one to find fraud due to a backdoor that was implemented by a developer because of the unusual activity occurring. In the other it helped auditors perform audits in companies where their methods would not really work because of devops. Not only is telemetry used in devops, but in other industries such as; medicine and meteorology.

Sources:

Motadata Team (21 Mar 2024) *What is Telemetry?* Motadata <https://www.motadata.com/blog/telemetry/>

Muhammad Raza (14 Oct 2021) *Explained: Monitoring & Telemetry in DevOps* bmc <https://www.bmc.com/blogs/devops-monitoring-telemetry/>

Alexandra (31 May 2024) *What Is Telemetry? How Telemetry Works, Benefits of Telemetry, Challenges, Tutorial, and More* stackify <https://stackify.com/telemetry-tutorial/>

Jeff gallimore (13 Mar 2017) DevOps and Audit Resources <https://itsanicelife.com/2017/03/13/devops-and-audit-resources/>