Javonta Young

Assignment 12

Paper on the case studies

With both of these case studies I feel the main points that need to be addressed with both
are communication between dev and ops, making sure that we keep a log for who needs to
do what and a system that tracks what everyone is doing. Without proper communication a
lot of things fall apart because someone did not get the information that they may have
needed and it throws off the project, or even having split organizations between dev and
ops and things fall short when trying to merge all the work together which creates chaos.
Without proper documentation things can get messy since you do not know who is doing
what and what information is getting stored where. Having tools like Kibana (which they
used in the case study) can not only tell you what has been iterated but also by who and
see the whole project, so you do not have to question where everything is. Having a place
where everything is at makes it easy for anyone to find exactly what they need.

In the first case study, the whole point of it was to show that dev and ops need to
follow the rules and regulations that is provided. Without the proper knowledge on these
rules and regulations puts the organization at risk for not knowing where things are and not
following the security that everyone should be keeping up with. Before they used to have a
system to where it would only take parts of the code and sample it. Where they found it
was problematic is when it would auto-scale and code would disappear and reappear. So,

they saw that it was not beneficial and tried a different approach. The new approach was to be with the auditors so they could see what they needed and also know where to look so information could be readily available. They learned to log into the application that the auditors were using to be able to find what was needed. The whole point of this was to show that people needed to be together to show that they all need each other for things to run smoothly. Without a proper mix of dev and ops things can get hectic like it did for them and things can get lost in miscommunication.

With the second case study, the organization almost got bamboozled by one of their own employees. The employee had put in malicious code for them to have a way to steal money from ATM machines. With the auditors so hyper focused on code reviews they almost overlooked the fact that someone was stealing from them. Having the use of Telemetry would have saved them and would do the job of reviewing whatever code was implemented into the branch versus having someone or a team looking for it. When a human reviews things, it is easy for them to miss stuff like that which creates vulnerabilities within the code. It was only caught by the telemetry systems that were being used when they were in a meeting and noticed the systems of the ATM machines were not in the active mode, they should have been in. The purpose of the case study is to show you that telemetry systems help find vulnerabilities that can happen on the daily from everyone just implementing code into the branch without an automated review with each implementation. With the auditors being so focused only on the reviews they almost got caught slipping.

In conclusion, both of these case studies show that security is our job and no one is safe to just implement what they want. Having telemetry systems and communication is key to successful DevOps.