Matthew Trembley

1/23/2022

Southern New Hampshire University

CS-305

Journal 3-2: Reflection

My role as a developer for conquering security concerns is just as important as any other. Ranging from the quality of the code I write, to the interfaces I design, to the information I have encrypted, and all things in between; can be the difference between a headlining information scandal, or a successful application. The software I create as a developer, whether it be on my own or with a team of people, needs to protect sensitive information that any user will not want lost to any malicious persons. Security is laced throughout the software development lifecycle. It isn’t just at the implementation phase, as it should be considered in the very beginning. It will even carry on through to maintenance where the program will live on forever – where the program will continuously receive updates, bug fixes, and even improvements to security. To turn a DevOps pipeline into a DevSecOps pipeline, the integration of security would happen from the very beginning until the end. Rather where in traditional DevOps, it would essentially just be thought of during Continuous Integration/Continuous Delivery and improved upon throughout each cycle. The general plan to make a DevOps pipeline into a secure, DevSecOps lifecycle would to start with a risk-assessment and understand what will need to be secured based on the project at hand. After that, the DevOps tools themselves will need to be secured. Once that is done, any accessors, servicing accounts, or API’s need to be protected with the right privileges.