Ethan Daugherty

09/18/2021

CS-305-H7291

3-2 Journal: Reflection

**Reflection**

As a developer my role in conquering security concerns is to develop programs securely to foster growth and confidence in my product. This involves creating software that protects the information contained within or the data that my software accesses both alone and as a joint with other members involved with a team. Software security doesn’t just fall within the beginning of the life cycle but through out even down the maintaining phase with continuing to maintain software securely, implement updates or patches to fix bugs, and introducing new features and improvements. To implement security into Devops a great way to start is to introduce focus groups and start small, an entire organization doesn’t need to convert all at the same time. Following that with changes in IT and current and future business processes to incorporate security. The plan to secure an entire DevOps Life cycle includes starting with a high-level rapid risk assessment, next plan and secure the DevOps lifecycle tools, then ensure user access keys, privileged service accounts, and APIs are protected properly with privileged account security tools, finally define infrastructure protection access to tools such as with access keys, privileged service accounts, and APIs as these are especially vulnerable to phishing attacks.