|  |
| --- |
| CS 305 Software Security |
| 3-2 Journal: Reflection |
| Emily Wood |

|  |
| --- |
| emily.wood7@snhu.edu  3-17-2023 |

**What is your role in solving security concerns as a developer? What might solving security concerns as a developer involve?**

Developers should apply secure coding practices, enforce industry standards, train other developers to adopt security principles, conduct peer code reviews, design and develop unit tests, and eliminate the use of vulnerable components from the beginning (Jeganathan, 2019). As a developer, by solving the security concerns, it can mean a significant return on investment for the company. Security breaches can risk clients, developer time, and money.

**Where does security fall within the software stack and development life cycle?**

Security falls within all levels of the development life cycle. From planning, to coding, to building, to testing, to release, to maintenance.

**How might you add security measures to transform a DevOps pipeline into a DevSecOps pipeline?**

Continuous integration can be injected into the DevOps pipeline to turn it into a DevSecOps pipeline. Secure design and engineering, security testing, security monitoring, and security risk management can be included within the DevOps pipeline. Everyone still focuses on the customer. Security is expected to collaborate with the DevOps teams to ensure timely delivery.

**The article suggests creating and following a plan to secure the entire DevOps life cycle. What is included in the suggested plan, and would you recommend following it?**

The plan suggested from the article is as follows: start with a high-level rapid risk assessment. Next, secure a lifecycle tool and ensure all parties have their role-specific access. Next is about applying secure coding practices during development. From then, it is the build stage where modules are checked into the repository. Then the software is tested. After testing, the software is released and deployed. Finally, it is the operate stage, which is not really final and actually a continuous stage. In this stage the software is monitored.

I would recommend following the plan. Applying security to all levels of the DevOps cycle, as suggested, ensures the entire team is trained, security is in the forefront of their mind, and the customer received a secure final product.

**References:**

Jeganathan, S. (2019). DevSecOps: A Systemic Approach for Secure Software Development. *ISSA Journal*, *7*(11), 20–27.