Justin Haby

Module 3-2 Journal Reflection

DevSecOps

November 12, 2021

Software Security 21EW2

Professor Donoho

Southern New Hampshire University

**Software Security**

Established companies are more or less regulated, and for developed organizations within highly regulated domains, a structured approach is needed to gauge agile techniques and guarantee compliance with regulatory necessities. Additionally, the less regulated areas have to embrace basic requirements. Unlike small organizations, there is a need to align specific domain units with specific abidance requirements in large domains.

Software developers have a great influence on how the system software will learn and even be maintained. For this reason, system software developers are responsible for designing, identifying, testing, and installing a software system that they have designed for a particular domain from the bottom level. It involves the creation of external and internal programs that enable a firm to run its businesses activities effectively thus can even produce systems that make the organization more productive and marketable (Stol et al., 2020)

According to McGraw (2006), in software development, life cycle security is an essential factor in ensuring the prosperity and functioning of the company’s system software .security should be prioritized right from the point when the project is being designed up to the end. Introducing security into the coding of the software development cycle (SDLC) is very necessary because the implementation of a safe SDLC assists developers in designing software that meets the user’s needs. Additionally, security should be introduced at every stage of software development from initiation up to its layout.

Adding security measures in the organization system software is very important. To transform the DevOps pipeline into a DevSecOps, there are certain measures like using orchestration and leveraging automation. These approaches make auditing simple because they use metadata. The plan in maintaining the life cycle is first by assessing the new release and evaluating the threat model. Additionally, secure the DevOps lifecycle, ensure there are proper security tools, define safety controls, and implement separation of tasks. I support that this plan will be of significant importance to the domains thus recommended in the following of the procedures (Jeganathan, 2021).

**References**

Jeganathan, S. (2021). *Devsecops: A Systematic Approach For Secure Software Development ,*. Retrieved 16 November 2021, from <https://eds-s-ebscohost-com.ezproxy.snhu.edu/eds/pdfviewer/pdfviewer?vid=1&sid=2f97aa4a-7770-4ddf-82f8-ff73279180ea%40redis>

McGraw, G. (2006). Software security. *Building security in*.

Stol, K. J., Schaarschmidt, M., & Goldblit, S. Gamification in Software Engineering: The Mediating Role of Developer Engagement and Job Satisfaction.