3-2 Journal: Reflection

Armon Wilson

SNHU CYB-305

**Reflection**

As a developer, my role in solving security concerns is paramount. It involves understanding potential threats and vulnerabilities at every level of the software stack and throughout the entire development life cycle (Jeganathan, 2019). This means not only writing secure code from the start but also actively participating in security design, threat modeling, and code reviews. It requires a proactive approach to identify and address security risks before they become exploitable vulnerabilities (Jeganathan, 2019).

Security is not confined to a single point in the software stack or development life cycle. It permeates every layer, from the client-side interface to the backend database, and every stage, from planning and design to deployment and maintenance (Jeganathan, 2019). This holistic view of security is essential in the DevSecOps model, where security is integrated into the entire development process rather than being an afterthought.

To transform a DevOps pipeline into a DevSecOps pipeline, security measures must be seamlessly woven into each phase (Jeganathan, 2019). This includes incorporating security into the planning phase through threat modeling and risk assessments, implementing secure coding practices and static analysis tools during development, automating security checks in the build process, and conducting rigorous security testing before deployment. Additionally, continuous monitoring and incident response are crucial to maintain the security posture of the application in the operational phase (Jeganathan, 2019).

Jeganathan (2019) proposes a comprehensive plan to secure the entire DevOps life cycle, encompassing security design and engineering, security testing, security monitoring, and security risk management. This plan is highly recommended as it provides a structured and proactive approach to addressing security concerns. By integrating security practices into every facet of the development process, organizations can significantly reduce the risk of vulnerabilities and ensure the delivery of secure and reliable software applications (Jeganathan, 2019). This approach aligns with the DevSecOps philosophy, where security is a shared responsibility and a continuous concern throughout the software development life cycle.

**References**:

Jeganathan, S. (2019). DevSecOps: A Systemic Approach for Secure Software Development. ISSA Journal, 17(11), 20–27.