IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 13, April 2025
Impact Factor: 7.67

AI-Powered Devsecops: Embedding Security in CI/CD with Automation and Insight

Mrs. A. Jancy[1], R. Lokeshwaran[2], T. Javith Naseem[3]
Assistant Professor, Department of Information Technology[1]
Students, B.Tech., Final Year, Department of Information Technology[2,3]
Anjalai Ammal Mahalingam Engineering College, Thiruvarur, India

Abstract: *This paper explores the practical implementation of a DevSecOps pipeline enhanced with artificial intelligence (AI) to foster robust security, compliance, and automation across the entire software development lifecycle (SDLC). By merging development, security, and operations into an integrated framework, DevSecOps ensures proactive threat mitigation without hindering development speed. The core objective is to embed security checks directly into development and deployment workflows, leveraging automation tools and AI capabilities for early risk detection and remediation. Key tools such as GitHub Actions, SonarQube, Trivy, OWASP ZAP, and Semantic Kernel, along with Kubernetes and Docker, are utilized for secure CI/CD practices. This AI-empowered pipeline supports advanced features like vulnerability summarization, automated compliance monitoring, and scalable microservice deployments, providing a comprehensive and adaptive solution for modern software teams.*

Keywords: DevSecOps, Secure SDLC, GitHub Actions, OWASP ZAP, Trivy, Docker, Security Automation, AI Security Reporting, CI/CD, Kubernetes

DOI: 10.48175/IJARSCT-26026