Implementing DevSecOps Pipeline for an Enterprise Organization

Nilima Chavan¹, Nikita Bharambe², Srushti Deshmukh³, Dipali Ahire⁴, Prof. A. R. Jain⁵

Students, Department of Information Technology¹²³⁴
Guide, Department of Information Technology⁵

Pune Vidyarthi Griha’s College of Engineering & S. S. Dhamankar Institute of Management, Nashik, India

Abstract: DevSecOps is an organizational software engineering culture and practice that aims at unifying software development (Dev), security (Sec) and operations (Ops). DevSecOps is an extension of DevOps, which is considered as a means to intertwine development, operation and security. The main characteristic of DevSecOps is to improve customer outcomes and mission value by automating, monitoring, and applying security at all phases of the software lifecycle: plan, develop, build, test, release, deliver, deploy, operate, and monitor. Continuous practices, i.e., continuous integration, delivery, and deployment, are the software development industry practices that enable organizations to frequently and reliably release new features and products. DevSecOps means thinking about application and infrastructure security from the start. With the increasing interest in the literature on continuous practices, it is important to systematically review and synthesize the approaches, tools, challenges, and practices reported for adopting and implementing continuous practices. This paper aimed at systematically reviewing the state of the art of continuous practices to classify approaches and tools, identify challenges and practices in this regard, and identify the gaps for future research. We used the systematic literature review method for reviewing the peer reviewed papers on continuous practices published between 2004 and June 1, 2016. We applied the thematic analysis method for analysing the data extracted from reviewing 69 papers selected using predefined criteria. Conclusion: Although DevSecOps is getting increasing attention by industry, it is still in its infancy and needs to be promoted by both academia and industry.

Keywords: Container Orchestration and Resource Management Platform; DevSecOps; CI/CD Pipelines; Infrastructure as Code; Policy as Code; Observability As Code; GitOps; Workflow Models.

REFERENCES