8-9-2021

Embedding Security into DevOps: Investigating DevSecOps in Government Software Development Environment

Gahyun (Susie) Kim
US Air Force, susiekim21@gmail.com

Jiwon Kim
University of Connecticut, jiwon.2.kim@uconn.edu

Jonathan Kim
University of Massachusetts Boston, jonathan.kim@umb.edu

Recommended Citation

Kim, Gahyun (Susie); Kim, Jiwon; and Kim, Jonathan, "Embedding Security into DevOps: Investigating DevSecOps in Government Software Development Environment" (2021). *AMCIS 2021 TREOs*. 32.
https://aisel.aisnet.org/treos_amcis2021/32

Embedding Security into DevOps: Investigating DevSecOps in Government Software Development Environment

TREO Talk Paper

Gahyun (Susie) Kim
US Air Force
susiekim21@gmail.com

Jiwon Kim
University of Connecticut
jiwon.2.kim@uconn.edu

Jonathan Kim
University of Massachusetts Boston
jonathan.kim@umb.edu

Abstract

Security certification is a critical factor for deploying IT systems in the federal government. It is also typically one of the tightest bottlenecks for most government projects. By law, all US federal IT systems must obtain an Authority to Operate (ATO) before operating on government networks. However, obtaining this certification can take federal agencies over two years. This increases not only the expected time and cost for the project but also drastically increases the risk of the deployed solution no longer being relevant for the end-user.

With the recent acceleration of software development and delivery using Agile and DevOps methodologies, it is now even more imperative that the ATO process becomes streamlined to enable secure, continuous delivery. Today, federal agencies are recognizing the value of DevSecOps for obtaining and maintaining the ATO efficiently and many are taking steps toward adopting and practicing it. DevSecOps ensures that quality, security, and repeatability are integrated throughout the software development and delivery lifecycle. Adopting the DevSecOps model has enabled federal agencies to efficiently achieve and maintain an ATO, thereby enabling the secure, continuous delivery of capabilities to users.

Integrating security in DevOps is challenging as traditional security methods are not as agile as DevOps. The movement of DevSecOps has been developed to create and integrate modernized security methods that can keep up with DevOps (Myrbakken and Colomo-Palacios 2017). By embedding security into every software development cycle phase, DevSecOps implements a combination of cultural shifts and technology-enabled practices with the goal of continuously securing development and delivery at speed and scale, even in an environment of high uncertainty. However, there is an academic research gap in the analysis of how organizations adopt DevSecOps practices and achieve success.

With a qualitative study, we provide three best practices. First, security should be included from the start. When organizations build security at project inception, they reduce overall costs and time and can effectively plan strategies for integration security controls at incremental builds. Second, organizations should foster security expertise among the development team. One way to effectively begin disseminating security knowledge to developers is to train a security champion on a team. With security champions, teams are empowered to write secure code and effectively resolve vulnerabilities. Third, organizations should engage in continuous security improvement. One method for continually identifying areas for improvement is retrospectives. Retrospectives include representatives from the development, security, and operations team, thereby including perspectives across functions and fostering continuous cross-team collaboration.

References

Myrbakken, H., and Colomo-Palacios, R. 2017. "Devsecops: A Multivocal Literature Review," *International Conference on Software Process Improvement and Capability Determination*: Springer, pp. 17-29.