A

Seminar Report On

“DevSecOps”

By

SWAPNIL R. LAYARE

71806866B

Under the guidance of

Prof. P.C Shah

DEPARTMENT OF COMPUTER ENGINEERING

Jawahar Education Society’s,

Institute of Technology,Management and

Research,Nashik Survey No. 48, Govardhan,Gangapur Road,

Nashik-422 222 Savitribai Phule Pune University

2020-21

JIT JAWAHAR INSTITUTE OF TECHNOLOGY, NASHIK

Jawahar Education Society's
Institute of Technology,Management & Research,Nashik
Approved by AICTE and DTE,Goverment of Maharashtra, Affiliated to University of Pune

---

CERTIFICATE

This is to certify that **SWAPNIL RAVINDRA LAYARE** from Third Year Computer Engineering has successfully completed his / her seminar work titled **“DEVSECOPS PRACTICES FOR AN AGILE AND SECURE IT SERVICE MANAGEMENT”** at Jawahar Education Society’s, Institute of Technology, Management and Research, Nashik in the partial fulfilment of the Bachelor’s Degree in Engineering.

(P.C Shah)	(Prof.D.B.Sisode)	(Dr.M.V.Bhatkar)
Guide	Head of Department	Principal

Acknowledgment

It is my immense pleasure to work on this seminar " **DEVSECOPS PRACTICES FOR AN AGILE AND SECURE IT SERVICE MANAGEMENT**". It is only the blessing of my divine master which has promptedand mentally equipped me to undergo the study of this seminar.

I would like to thank **Dr. M.V.Bhatkar**, Principal, Jawahar Education of Society's Institute of Technology Management and Research for giving me such an opportunity to develop practical knowledge about subject. I am also thankful to **Prof. D.B.Sisode**, Head of Computer Engineering Department for her valuable encouragement at every phase of my seminar work and completion.

I offer my sincere thanks to my guide **Prof. P.C.Shah**, who very affectionately encour- aged me to work on the subject and gave valuable guidance time to time. While preparingthis seminar I am very much thankful to him.

I am also grateful to entire staff of Computer Engineering Department for their kind co-operation which helped me in successful completion of seminar.

SWAPNIL RAVINDRA LAYARE.

70806866B

Abstract

Without appropriate consideration of security best practices, the continuous delivery of IT services facilitated by DevOps is risky. On the other hand, SecOps offers the possibility to reduce security risks if security is integrated into the continuous delivery pipeline according to best practices. The purpose of this seminar is to investigate how DevSecOps culture can be applied in IT service management.

With proper implementation DevSecOps can boast the securitiy of the IT and management systems

DevOps is a new tendency in business and information technologyalignment. The purpose of DevOps is bridging the gap between the development and operations. Several sources claim that DevOps is a new style of work. Many successful DevOps introduction attempts and also many problems in adoption of this style of work have been discussed. This paper reports on research results in facilitating the adoption of DevOps in small enterprises. The DevOps adoption method and several related to it artefacts are proposed. The proposed method has been tested in a national branch of an international company with an internal IT development team.

Key words: -IT Service Management, DevOps, SecOps, DevSecOps.

CONTENTS

LIST OF FIGURES

DevSecOps PRACTICES FOR AN AGILE AND SECURE IT SERVICE MANAGEMENT

INTRODUCTION

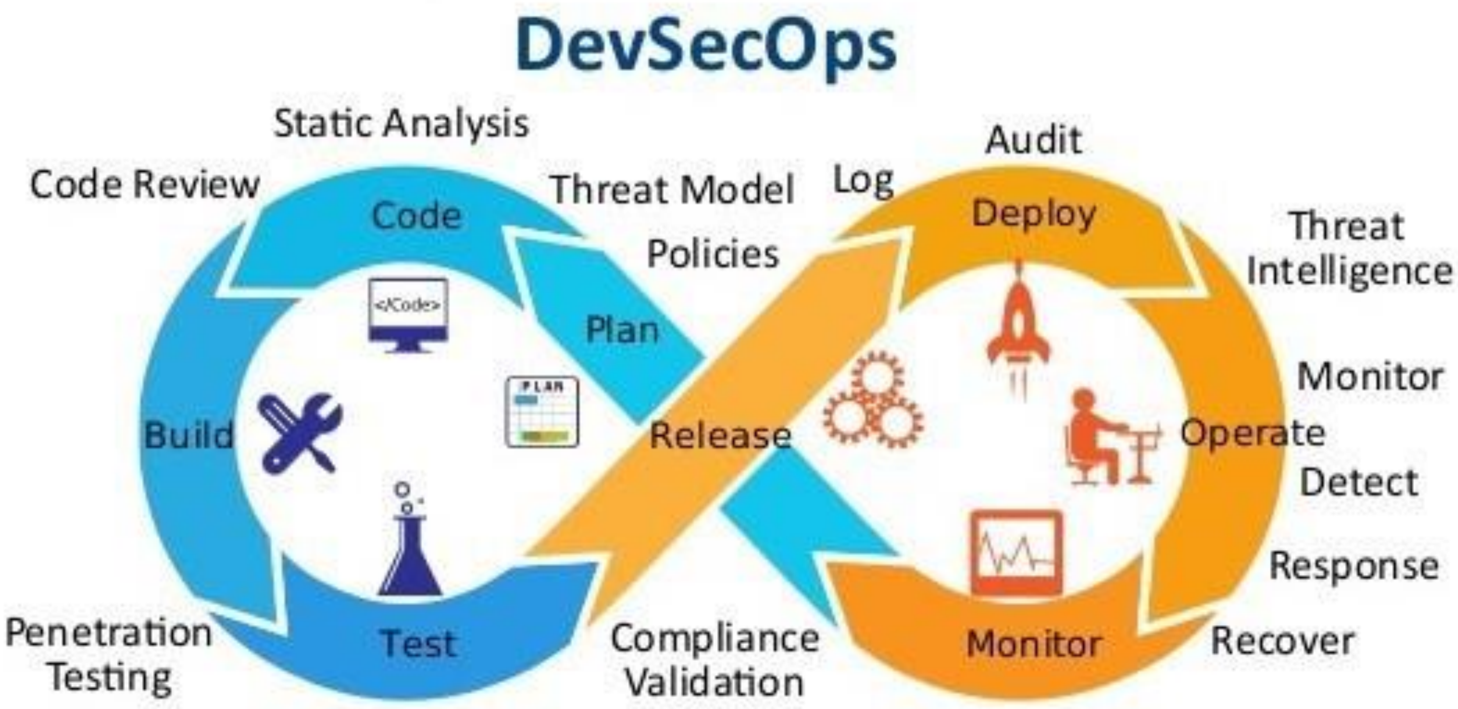
Organizations use information technology (IT) for different objectives. The achievement of most business goals of an organization relies primarily on the competence of IT support. IT service management (ITSM) is the branch of science that is concerned about the implementation and management of quality IT services that meet the needs of the business. IT service professionals achieve IT service management through an appropriate mix of people, processes and IT.

Currently, with improved ITSM processes and the adoption of best practice guides and benchmarks such as ITIL, ISO 20000. Compliance appears to be a need rather than a strategic choice to improve rapidly and easily decisions about IT and business processes. Be more agile allows the business to benefit from a higher growth of Return on Investment ROI and a constant competitive advantage (Nazımoğlu & Özsen, 2010).

Diversification of competition, increased innovation and changing customer needs are driving today's large companies to undertake a digital transformation to remain competitive. In this context, there is no longer any question of being subjected to the "tunnel effect" generated by traditional project management, which, according to the Standish Group, produces applications in which 64% of the functionalities are not or rarely used. These companies need to review their organization to become "agile", i.e. "customer-centric". To do so, they must offer only products that provide added value to their customers and reduce the "time to market" to make these products quickly usable.

As a result, organizations have realized that IT is fundamental to their success (Abdelkebir et al., 2017). Information technology is changing the way organizations operate, business processes, internal and external communication and, most importantly, the way organizations provide services to their customers (Mohamed & Singh, 2012).

Since organizations have started to see the importance of IT, they have begun to implement complex and dynamic IT systems to support their business processes.


DevSecOps
Static Analysis
Code Review
Code
Threat Model
Policies
Plan
Build
Release
Test
Penetration Testing
Compliance Validation
Log
Audit
Deploy
Threat Intelligence
Monitor
Operate
Detect
Response
Recover
Monitor
</Code>
PLAN

LITERATURE REVIEW

In the past, security-related processes were isolated and entrusted to a specific team at the final stage of development. This was not a problem at a time when development cycles lasted months or even years. But those days are over. While an effective DevOps approach ensures fast and frequent development cycles (sometimes a few weeks or days), outdated security practices can negate the benefits of the most effective DevOps projects.

Now, within the collaborative framework of the DevOps model, security is a shared responsibility, integrated from start to finish. This concept is so important that it has given rise to the term "DevSecOps" to emphasize the need to integrate security into DevOps.

The DevSecOps approach involves thinking about the security of the application and infrastructure from the start. It is also advisable to automate some security gateways in order to avoid slowing down DevOps workflows. To achieve these objectives, it is necessary to start by selecting the tools capable of ensuring the continuous integration of security, for example with a common integrated development environment that offers security functions. However, effective DevOps security requires more than just new tools. It is necessary to implement the cultural changes of DevOps within the security teams as soon as possible.

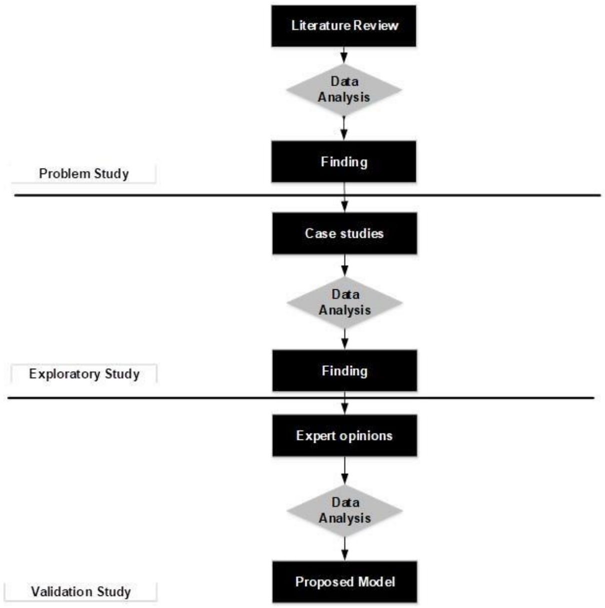
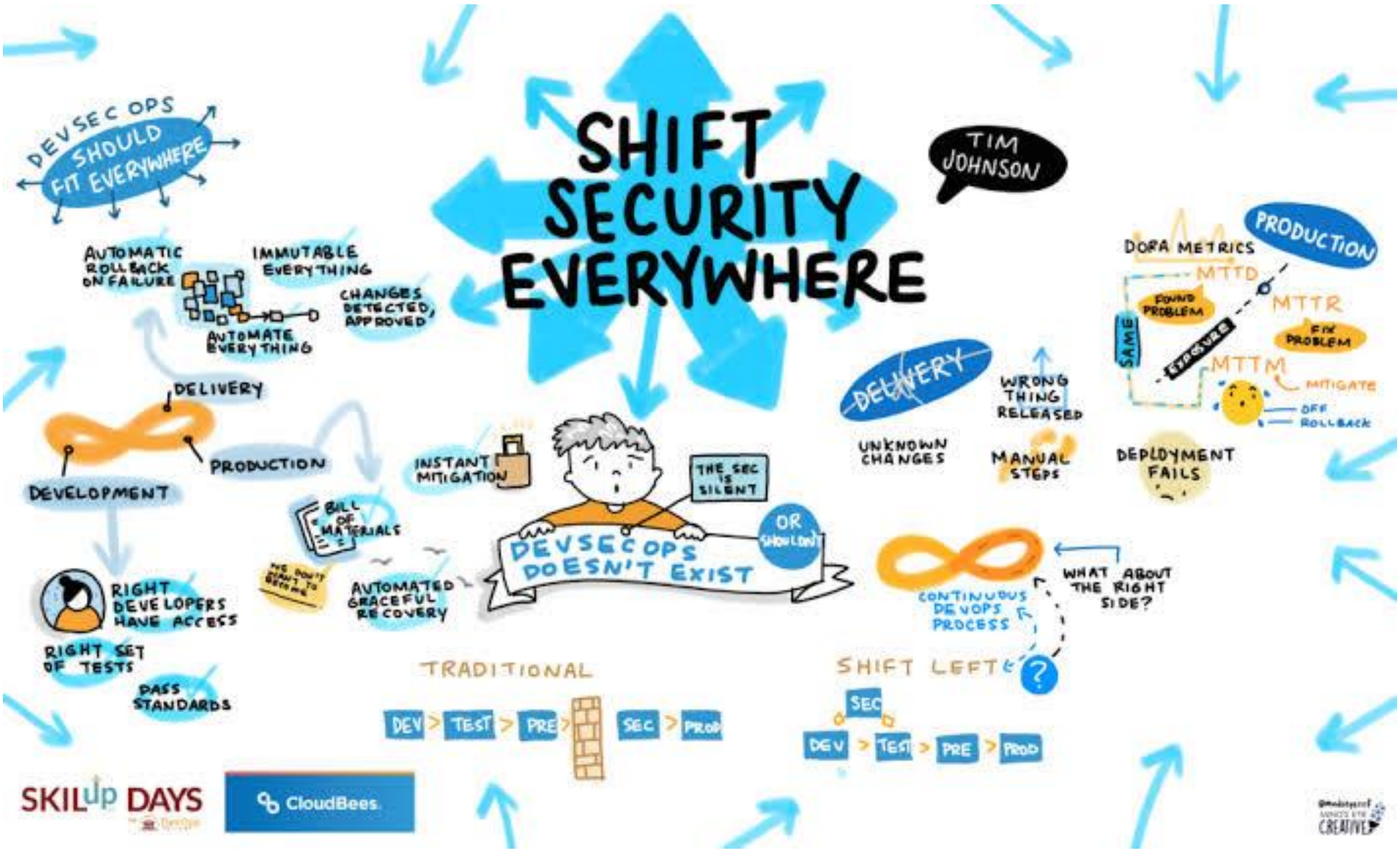


FIGURE 1


SHIFT SECURITY EVERYWHERE
TIM JOHNSON
DEVSEC OPS SHOULD FIT EVERYWHERE
AUTOMATIC ROLLBACK ON FAILURE
IMMUTABLE EVERYTHING
CHANGES DETECTED, APPROVED
AUTOMATE EVERYTHING
DELIVERY
PRODUCTION
DEVELOPMENT
RIGHT DEVELOPERS HAVE ACCESS
RIGHT SET OF TESTS
PASS STANDARDS
BILL OF MATERIALS
WE DON'T WANT TO BECOME
AUTOMATED GRACEFUL RECOVERY
INSTANT MITIGATION
THE SEC IS SILENT
DEVSECOPS DOESN'T EXIST
OR SHOULDN'T
TRADITIONAL
DEV > TEST > PRE > SEC > PROD
DELIVERY
UNKNOWN CHANGES
WRONG THING RELEASED
MANUAL STEPS
DEPLOYMENT FAILS
PRODUCTION
DORA METRICS
MTTD
FOUND PROBLEM
MTTR
FIX PROBLEM
SAME
EXPOSURE
MTTM
MITIGATE
OFF
ROLLBACK
CONTINUOUS DEVOPS PROCESS
WHAT ABOUT THE RIGHT SIDE?
SHIFT LEFT
?
SEC
DEV > TEST > PRE > PROD
SKILup DAYS
CloudBees
MINDS EYE CREATIVE

results show empirically that, despite the asserted expertise of the participants, several concepts are indeed used incorrectly because they are misunderstood. The method used in this paper is described in Figure 1.

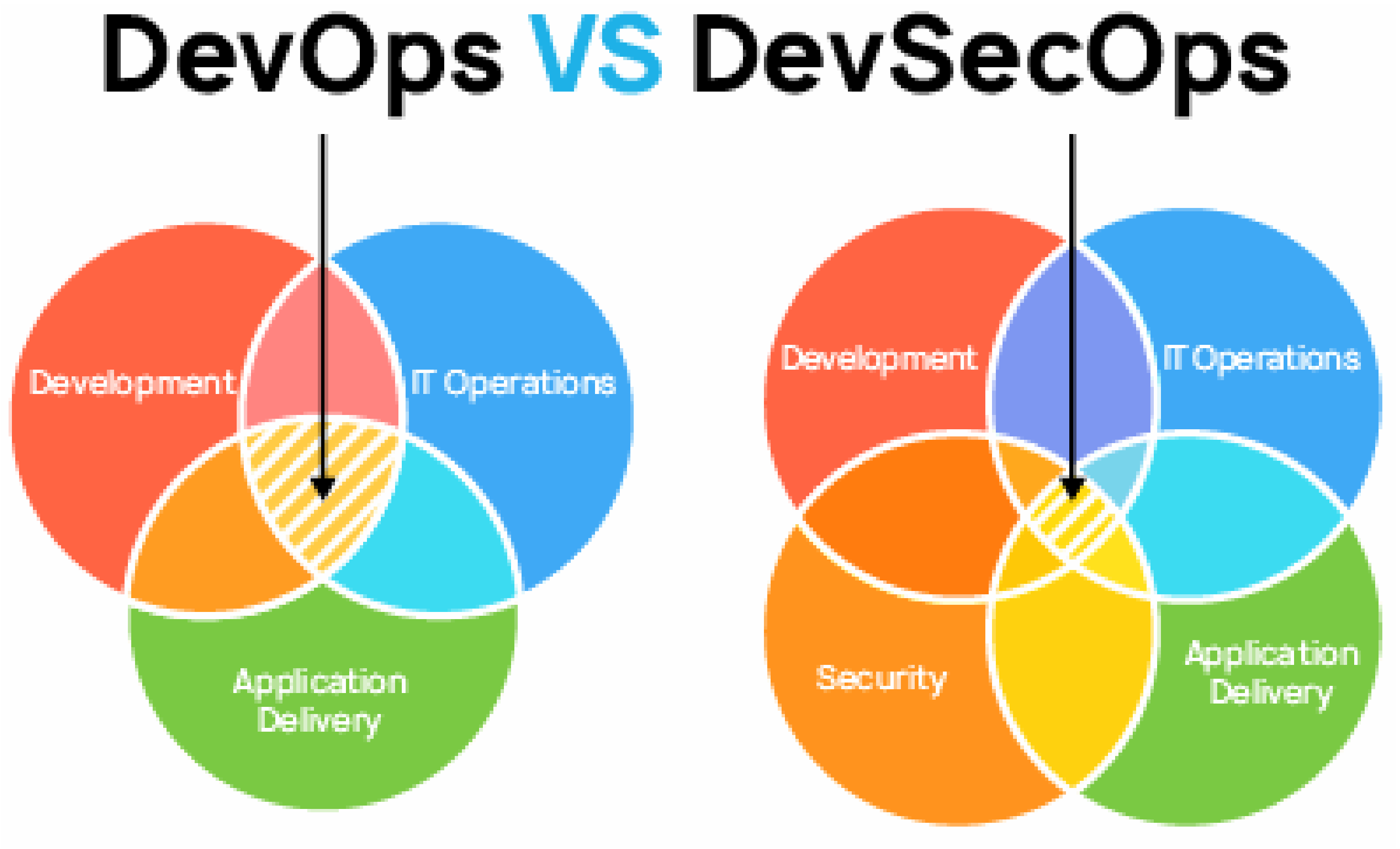
A literature review is a selection of documentation regarding a certain topic that contains information, data, ideas, and evidence to fulfil certain aims or express particular views about the topic. For easier understanding of the peers, as well as to add more scientific rigor to our research, we decided to follow the concept centric approach proposed by Webster and Watson (Webster & Watson, 2002).

To obtain an overview of all relevant literature concerning SecDevOps practices, a structured literature review based on the method suggested by Kitchenham et al. (2007) was conducted. This method provides details on search terms and inclusion and exclusion criteria to ensure a consistent and unbiased selection of relevant literature.

According to Kitchenham et al. (2007), the quality of a study refers to the fact that that it minimizes bias and maximizes validity and generalizability. Quality assessment can be used to complete the selection phase by excluding studies that do not meet a certain quality threshold. The quality assessment can also be used to measure and account for the importance of studies.

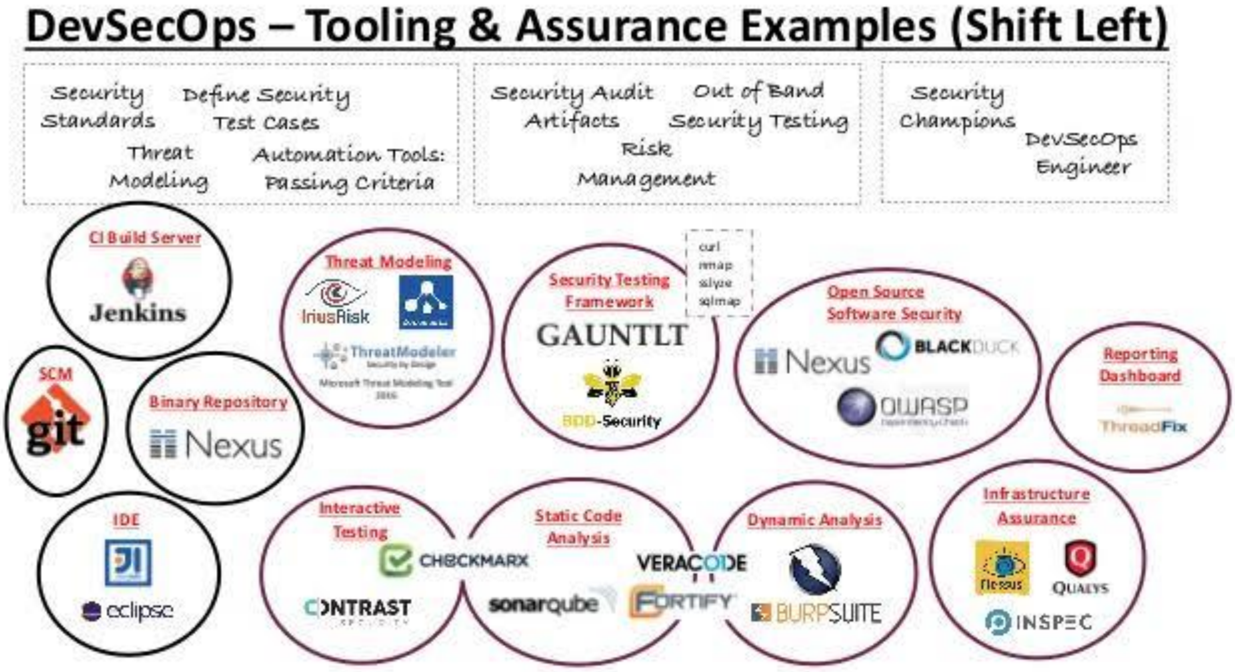
When analyzing the results. In this case, it is used to complete data extraction. Studies with a low score will not be excluded but will be evaluated with regard to their quality score. The quality assessment is done with the help of a checklist. This is in the form of a questionnaire consisting of questions to assess the quality of each primary study according to selected factors. The answers to these questions each have a value that will measure the quality of each study. In the protocol, it is necessary to define the questions and answers constituting the checklist, as well as the choice of an evaluation strategy. This strategy indicates the number of participants in the process, the validation of results, and the resolution of evaluation conflicts, in the case of several evaluators per study. It is also necessary to define, if applied, a minimum score threshold and the fate of primary studies that have not reached it.

In this section, we list the primary practices and benefits of DevOps/SecOps found in the literature.


DevOps VS DevSecOps
Development
IT Operations
Application Delivery
Development
IT Operations
Security
Application Delivery

RESEARCH METHODS

The literature review showed that there is a lack of empirical research on the merging of Devops and Secops practices in IT service management. Although most articles did not perform in-depth analyses of security practices for DevOps, the literature has provided a substantial amount of automated controls and agile development that can be used by organizations to control their IT processes. However, no strategy has been developed to address operations security and integrate it effectively into the day-to-day operations of the IT department. The literature review therefore contributed primarily to assess the current state of research in this area. The empirical component of this research should give a more detailed impression of development practices and integrate security measures into operational processes, and above all give a first insight into DevSecops practices that can be used by companies.



DevSecOps – Tooling & Assurance Examples (Shift Left)

Security Standards
Define Security Test Cases
Threat Modeling
Automation Tools: Passing Criteria

Security Audit Artifacts
Out of Band Security Testing
Risk Management

Security Champions
DevSecOps Engineer

CI Build Server
SCM
Binary Repository
IDE
Threat Modeling
Security Testing Framework
curl
nmap
sslyze
sqlmap
Open Source Software Security
Reporting Dashboard
Interactive Testing
Static Code Analysis
Dynamic Analysis
Infrastructure Assurance

Challenges of DevOps Adoption

Knowledge of potential challenges, derived from available experiences of DevOps adoption, can allow avoiding problems during the adoption process. Even if it is not possible to avoid the problems, this knowledge can help to be more prepared for meeting the challenges. In some cases, the identification of potential challenges can even stop planned adoption processes, if the enterprise decides that it is not possible to overcome the challenges with a reasonable amount of resources.

According to Hamunen DevOps adoption challenges can be grouped in four groups:

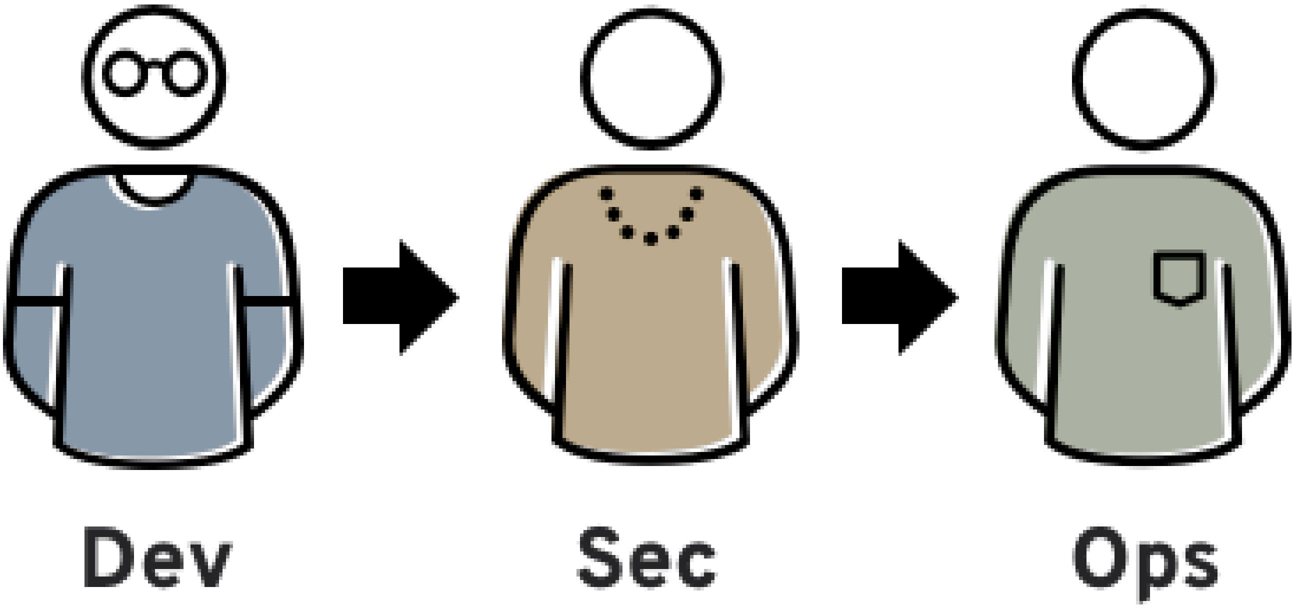
- Lack of awareness
- Lack of support
- Problems linked to the DevOps technological implementation
- Problems with adapting organizational processes to DevOps

Out-side challenges are related to environment, which is around DevOps adoption process, and include the following challenges:

- Wall of confusion based on working in silos, where for each silo (department) there are different goals and minimal information flows between them.
- Speed of innovations based on changes, necessary to be implemented in the systems.
- Complexity of existing environments, where non-production environments do not reflect into production environments, which makes difficult to perform fast root- cause analysis.
- Difficult error prevention and diagnosis process.

In-side challenges include:

- Misunderstanding of DevOps approach and benefits that can be gained from it.
- Perceiving DevOps just as tool implementation, without taking into consideration collaboration, communication and other DevOps culture aspects.
- Difficulties to manage current changes and DevOps adoption, because, usually, there is no option to stop business requests for system development and changes.
- Difficulties to choose the right adoption strategy – whether to choose the Big bang or Step-by-Step based (Phased) approach, as each approach has its pluses and minuses.


Dev
Sec
Ops

CONCLUSION AND FUTURE WORKS

This study aimed to explore the possibilities for companies to manage these IT operations, development and security and increase process control while using DevSecOps without sacrificing too much of the agility and benefits that DevOps offers. Second, it aimed to study how these companies can exploit DevSecOps practices in the management of their IT operations. Demonstrate their internal control to IT auditors.

We conducted two main research questions. The first What DevSecOps practices can be used in IT Service Management. And the second, how can these practices be integrated into effective IT Service Management?

To answer this question, we conducted a literature review to define the most common DevSecOps practices. An exploratory study was then carried out through 5 case studies. The results of this study were evaluated with 18 experts who responded to the case studies.

All respondents were generally positive about the use of DevSecOps, although opinions differed widely on what DevOps is and how it should be handled. It, therefore, seems impossible to develop a framework with which all those involved in DevOps would fully agree. This study provided a comprehensive overview of practices that can be applied in DevSecOps for ITSM. These practices include both traditional practices that can be used in combination with DevOps, as well as security practices integrated into the application development process. The most complicated practices have been classified into several categories: Continuous Vulnerability Assessment and Remediation, the threat intelligence and Feedback Loops between Dev, Sec and Ops.

The validation results of this study with the Delphi method proved the most relevant DevSecOps practices for effective ITSM. The results of this study resulted in a conceptual model of IT Service Management based on DevSecOps practices.

For future work, we are currently working on the validation of this model through the projection of DevSecOps practices on ITSM practices, and more specifically the change management process in organizations.

REFERENCES

Abdelkebir, S., Maleh, Y., & Belaissaoui, M. (2017). An agile framework for its management in organizations: a case study based on DevOps. *Proceedings of the 2Nd International Conference on Computing and Wireless Communication Systems*, 67, 1-8.

Adler, M., & Ziglio, E. (1996). *Gazing into the oracle: The Delphi method and its application to social policy and public health*. Jessica Kingsley Publishers.

Bi, R., Davidson, R., Kam, B., & Smyrnios, K. (2013). Developing organizational agility through it and supply chain capability. *Journal of Global Information Management, 21*(4), 38–55.

Bolger, F., & Wright, G. (1994). Assessing the quality of expert judgment: Issues and analysis. *Decision support systems, 11*(1), 1-24.

Bou Ghantous, G., & Gill, A. (2017). DevOps: concepts, practices, tools, benefits and challenges. *Proceedings PACIS2017,* 96.

Cruzes, Daniela S., Jaatun, Martin G., ET Oyetoyan, Tosin DT. D (2018, April). Challenges and approaches of performing canonical action research in software security. *Proceedings of the 5th Annual Symposium and Bootcamp on Hot Topics in the Science of Security,* 1-11.

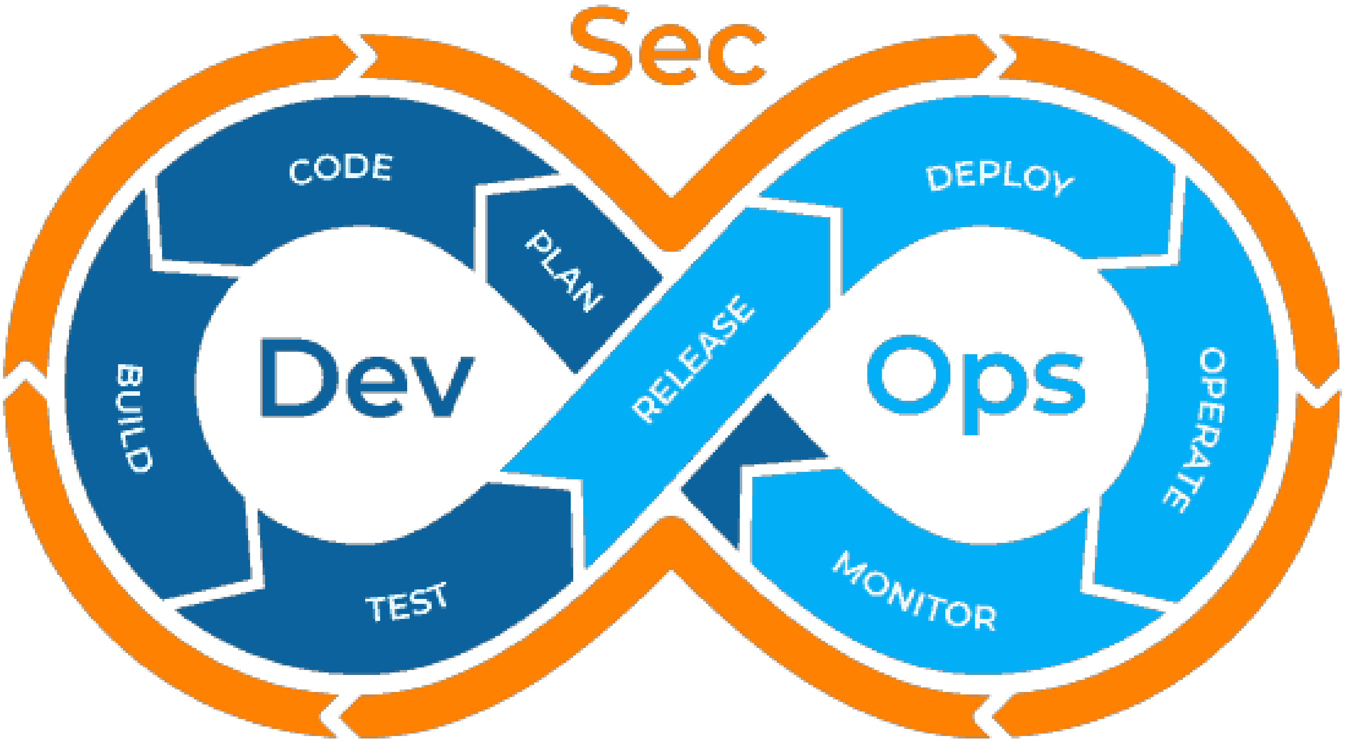
Ebert, C., Gallardo, G., Hernantes, J., & Serrano, N. (2016). DevOps. *IEEE Software, 33*(3), 94-100.

Hsu, T. H. C. (2018). *Hands-On Security in DevOps: Ensure continuous security, deployment, and delivery with DevSecOps.* Packt Publishing Ltd.

Jabbari, R., bin Ali, N., Petersen, K., & Tanveer, B. (2018). Towards a benefits dependency network for DevOps based on a systematic literature review. *Journal of Software: Evolution and Process, 30*(11), e1957.

Kitchenham, B. et Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering*. Rapport technique EBSE 2007-001, Keele University and Durham University Joint Report.

Koopman, M. (2019). *A framework for detecting and preventing security vulnerabilities in continuous integration/continuous delivery pipelines.*



View publication stats