

**SECURING SOFTWARE DELIVERY: DEVSECOPS CI/CD PIPELINE
DESIGN, IMPLEMENTATION, AND ASSESSMENT FOR VEHICLE
MANUFACTURING**

By

Rehmia Eunike Gracia Meliala

12002007

BACHELOR'S DEGREE

in

INFORMATION TECHNOLOGY
ENGINEERING AND INFORMATION TECHNOLOGY



SWISS GERMAN UNIVERSITY
The Prominence Tower Alam Sutera
Tangerang 15143
Indonesia

June 2024

Revision after the Thesis Defense on 3rd July 2024

STATEMENT BY THE AUTHOR

I hereby declare that this submission is my own work and to the best of my knowledge, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in this thesis.

Rehmia Eunike Gracia Meliala



17/07/24

Student

Date

Approved by:

Dr. Charles Lim



17/07/24

Thesis Advisor

Date

Ilia Budnikov



17/07/24

Thesis Co-Advisor

Date

Dr. Maulahikmah Galinium

Dean

Date

ABSTRACT

DEVSECOPS: A CONCEPT OF INTEGRATING SECURITY TESTS IN CI/CD-PIPELINES IN VEHICLE MANUFACTURING INDUSTRY

By

Rehmia Eunike Gracia Meliala

Dr. Charles Lim, Advisor

Ilia Budnikov, Co-Advisor

SWISS GERMAN UNIVERSITY

Security is critical in software development, especially with today's demands for rapid software release. Integrating security into the early stages of development is essential because it allows vulnerabilities to be discovered and addressed early, saving significant time and reducing the costs associated with fixing security issues later in the development cycle. However, most industry practices often overlook this aspect and are typically subjective and ad hoc. This study aims to provide a systematically developed blueprint for integrating security testing into the CI/CD pipeline, specifically for a vehicle manufacturing company. Data was gathered from a systematic literature review, a market study, and a case study to develop the concept. This research proposed a DevSecOps CI/CD Pipeline toolchain that is designed in a systematic way, combining academic insights and industry practices to identify integration points and security testing activities at each step of the CI/CD pipeline within the company where this research was conducted. The proposed toolchain is then made into an architecture then validated through a prototype that is implemented.

Keywords: DevSecOps, CI/CD Pipeline, Security Testing, Continuous Integration and Continuous Deployment (CI/CD), Continuous Integration, Security in Software Development

© Copyright 2024
By Rehmia Eunike Gracia Meliala
All rights reserved

DEDICATION

*To the company where I conducted my thesis and the remarkable team there,
for providing the resources, guidance, and support necessary for the completion of this
thesis.*

Your contribution has been invaluable.

ACKNOWLEDGEMENT

Here, I wish to thank those who have advised me during my thesis: Dr. Ir. Charles Lim, who provided me with his extensive academic knowledge; Mr. Ilia Budnikov, who supported me on a day-to-day basis; and Mr. Stefan Wenker who offered me the opportunity to undertake this research.

I would also like to thank my friends who have been on this learning journey with me. I extend my gratitude to all the lecturers who have guided me over the past four years, especially, Dr. Maulahikmah Galinium, Dipl.-Inf. I Eng Kho, and Associate Professor James Purnama. Your guidance and support have been invaluable.

Most importantly, I wish to express my deepest gratitude to my parents for their unwavering support, love, and encouragement throughout this journey. To my late mother, whose memory continues to inspire me, and to my father, whose belief in me has been my greatest motivation.

TABLE OF CONTENTS

STATEMENT BY THE AUTHOR	2
ABSTRACT	3
DEDICATION	5
ACKNOWLEDGEMENT	6
CONTENTS	9
LIST OF FIGURES	10
LIST OF TABLES	11
1 INTRODUCTION	12
1.1 Research Background	12
1.2 Research Problem	14
1.3 Research Objectives	15
1.4 Research Questions	16
1.5 Hypotheses	16
1.6 Significance of Study	16
1.7 Research Scope	17
1.8 Research Limitations	17
1.9 Thesis Structure	17
2 THEORETICAL FOUNDATIONS AND RELATED WORKS	19
2.1 Manufacturing Company	19
2.1.1 Company Profile	20
2.1.2 Current Business Technical Challenges	21
2.1.3 Specific Challenges	21
2.2 DevOps	21
2.2.1 People:	22
2.2.2 Process:	23
2.2.3 Technology:	24

2.3	DevSecOps	24
2.3.1	Current State of DevSecOps	25
2.3.2	Benefits	26
2.3.3	Challenges	27
2.4	CI/CD Pipeline	28
2.4.1	CI/CD Pipeline Stages	29
2.4.2	Security Testing in CI/CD Pipelines	31
2.4.2.1	SAST	32
2.4.2.2	DAST	32
2.4.3	Common Tools	32
2.5	Industry Study	33
2.5.1	Literature Review	33
2.5.2	Market Study	34
2.6	Related Works	34
3	RESEARCH METHODOLOGY	45
3.1	Overview of the Research Method	45
3.2	State of the Art Literature Review:	46
3.2.1	Planning the Review	46
3.2.1.1	Identify the Need for a Review:	46
3.2.1.2	Define the Research Questions:	46
3.2.2	Develop a Review Protocol:	47
3.2.3	Performing the Review	47
3.2.3.1	Identify Research:	48
3.2.3.2	Selection of Primary Studies:	48
3.2.3.3	Data Extraction and Monitoring:	48
3.2.4	Step 3: Reporting the Review	48
3.2.4.1	Write the Report:	48
3.2.4.2	Discuss the Findings:	48
3.3	Market Study:	49
3.4	Interview Case Study:	49
3.5	CI/CD Pipeline Implementation	51
3.6	Pipeline Validation	52
3.7	CI/CD Pipeline Assessment	52

4	Experimental Results	53
4.1	Systematic Literature Review	53
4.2	Interview-Based Case Study	60
4.3	Market Study	62
4.4	CI/CD Pipeline Architecture Design	72
4.5	CI/CD Pipeline Architecture Implementation	76
4.6	CI/CD Pipeline Architecture Validation	77
4.7	CI/CD Pipeline Architecture Evaluation	78
4.8	Summary of Results	80
5	Conclusion and Recommendation	81
5.1	Conclusion	81
5.2	Future Works	82
	GLOSSARY	83
	REFERENCES	97
	APPENDICES	63
A	Interview Questions	98
A.1	Appendix	98
	CURRICULUM VITAE	99

List of Figures

2.1 Basic Stages of a CI/CD Pipeline 30

3.1 The general research flow. 45

4.1 Architecture Concept for the CI/CD Pipeline 72

4.2 Snippet for gitlab-ci.yml file. 76

4.3 Physical Model (Instance) of the Designed Pipeline 77

4.4 Simulation Result of the Implemented Architecture 78

4.5 Email Notifying Critical Vulnerabilities 78

List of Tables

2.1 Summary of Related Works 39

2.2 Summary of This Research Compared to Other 43

4.1 RQ 1 Result 53

4.2 RQ 2 Result 55

4.3 RQ 3 Result 57

4.4 CI/CD Pipeline Workflow Based on the Interview 62