

**ENHANCING SECURITY MATURITY THROUGH DEVSECOPS TO
SUPPORT UU PDP: A CASE STUDY OF PT XYZ**

By
Mochammad Nosa Shandy Prastyo
22351021

MASTER'S DEGREE
in
MASTER OF INFORMATION TECHNOLOGY
FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY



SWISS GERMAN UNIVERSITY
The Prominence Tower
Jalan Jalur Sutera Barat No. 15, Alam Sutera
Tangerang, Banten 15143 - Indonesia

Revision after the Thesis Defense on 4 February 2025

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 the thesis.

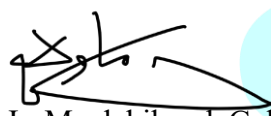

Mochammad Nosa Shandy Prastyo

Student

15 February 2025

Date

Approved by:


Dr. Ir. Maulahikmah Galinium, S.Kom., M.Sc

Thesis Advisor

15 February 2025

Date


Feb 17th, '25

Dr. Ir. Moh. A. Amin Soetomo, S.T., M.Sc.

Thesis Co-Advisor

17 February 2025

Date


Dr. Ir. Maulahikmah Galinium, S.Kom., M.Sc

Dean of Faculty of Engineering and
Information Technology

15 February 2025

Date

ABSTRACT

ENHANCING SECURITY MATURITY THROUGH DEVSECOPS TO SUPPORT UU PDP: A CASE STUDY OF PT XYZ

By

Mochammad Nosa Shandy Prastyo

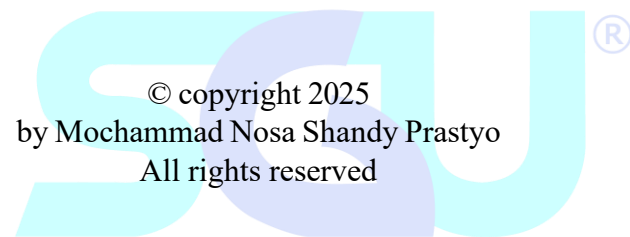
Dr. Ir. Maulahikmah Galinium, S.Kom., M.Sc, Advisor

Dr. Ir. Moh. A. Amin Soetomo, S.T., M.Sc., Co-Advisor

SWISS GERMAN UNIVERSITY

In today's evolving cyber threat landscape, data breaches remain a significant challenge, creating the need for secure applications while maintaining rapid development cycles. The main gap facing PT XYZ is that the product owner ignores security assessments and best practices to meet release deadlines, which results in a vulnerable application. This research explores enhancing security maturity through a DevSecOps approach, with a focus on compliance with UU PDP regulations. By integrating maturity assessments and the maturity models using the SSE-CMM framework into the deployment process, organizations can proactively identify and mitigate vulnerabilities before applications reach production. The study demonstrates that combining maturity assessments with comprehensive security evaluations significantly reduces the risk of data breaches and data protection while supporting agile development. Additionally, the maturity level serves as a measurable indicator of an application's readiness for production. This research contributes valuable insights and practical strategies for organizations aiming to strengthen application security and achieve robust security maturity.

Keywords: DevSecOps, Data Protection, Security Maturity, UU PDP, SSE-CMM.



DEDICATION

I would like to dedicate this research project to my God, my family, my beloved country Indonesia and my second home where I grow in knowledge, Telkom Indonesia.



ACKNOWLEDGEMENT

I would like to express my deepest gratitude to Dr. Ir. Maulahikmah Galinium, S.Kom., M.Scand Mr. Dr. Ir. Moh. A. Amin Soetomo, S.T., M.Sc.as my Thesis advisor, support, advice, and guidance given throughout this research project and the completion of this thesis report. It is because of their priceless contributions that this thesis report and the whole research project can arrive at this point.

I would like to thank my wife, my mom and my son for the countless moral supports throughout my pursue of knowledge in SGU. I can't thank you enough for the time that already taken from you for me to make this thesis done.

I would like to thank all of my direct supervisor, my team at work and my friends especially Batch 33 MIT SGU for their companionship, and to the countless number of people who have helped me throughout this research project, either directly or indirectly.



Table of Contents

	Page
STATEMENT BY THE AUTHOR	1
ABSTRACT	2
DEDICATION	4
ACKNOWLEDGEMENT	5
TABLE OF CONTENTS	9
LIST OF FIGURES	10
LIST OF TABLES	12
1. INTRODUCTION	13
1.1 Background	13
1.2 Research Problem	17
1.3 Research Objective	18
1.4 Research Question	18
1.5 Hypothesis	18
1.6 Scope and Limitation	19
1.7 Significance of Study	19
1.8 Thesis Structure	20
2. LITERATURE REVIEW	21
2.1 PT XYZ	21
2.2 Policy, Law and Regulation	22
2.2.1 Internal Security Policy	23

2.2.2 UU PDP no 27 Tahun 2022	23
2.3 Security Maturity	23
2.3.1 Security Maturity Framework	23
2.3.1.1 Systems Security Engineering Capability Maturity Model (SSE-CMM)	24
2.3.1.2 Federal Information Security Management Framework (NIST)	25
2.3.1.3 Control Objectives for Information and Related Technologies (COBIT)	25
2.4 Information Security Principles	26
2.4.1 Confidentiality	26
2.4.2 Integrity	27
2.4.3 Integrity	28
2.5 DevOps	28
2.6 DevSecOps	29
2.6.1 DevSecOps Culture	30
2.6.2 “Shift Left” of DevSecOps	31
2.6.3 Automated Security Testing Assessment	31
2.6.4 Compliance Automation	32
2.6.5 Security Monitoring	33
2.7 Vulnerability Assessment & Penetration Testing	33
2.7.1 Penetration Testing Strategies	34
2.8 Question Development Framework	35
2.8.1 PICO	36
2.8.2 PEO	36
2.8.3 SPICE	36
2.9 Gap Analysis	36
2.10 Framework Maturity Comparison	38
2.11 Related Works	39
3. RESEARCH METHODS	43
3.1 Research Framework	43
3.2 Literature Review	44

3.3	GAP Analyst	45
3.4	Framework Creation	46
3.4.1	Create Maturity Assessment Checklist	46
3.4.2	Assess Existing Product	46
3.4.3	Proposed Framework	47
3.5	Evaluation	47
3.5.1	Narrow Implementation	47
3.5.2	Re-Assess Existing Product	48
3.5.3	Report	48
3.6	Validation	48
4.	RESULTS AND DISCUSSIONS	50
4.1	GAP Analysis	50
4.1.1	FGD Subject Discussion	50
4.1.2	FGD Participants	51
4.1.3	FGD Results	53
4.2	Framework Creation	55
4.2.1	Create Maturity Assessment Checklist	56
4.2.1.1	Data Protection	56
4.2.1.2	Network Segmentation	60
4.2.1.3	OS and Software	61
4.2.1.4	Services Audit	62
4.2.1.5	Endpoint Protection	63
4.2.1.6	Source Code and Credentials Protection	65
4.2.1.7	Secure Code (Scanning and VAPT)	66
4.2.1.8	Multi Factor Authentication	67
4.3	Assess Existing Product	67
4.3.1	Product A	68
4.3.1.1	First Maturity Assessment	68
4.3.2	Product B	69
4.3.2.1	First Maturity Assessment	69
4.4	Proposed DevSecOps Framework	70
4.4.1	Plan	71

4.4.2	Security Assessment	71
4.4.3	Maturity Assessment	72
4.5	Evaluation	74
4.5.1	Narrow Implementation	74
4.5.1.1	Product A	74
4.5.1.2	Product B	75
4.5.1.3	Proactive Monitor	76
4.5.2	Re-Assess Existing Product	76
4.5.2.1	Product A	76
4.5.2.2	Product B	77
4.5.3	Report	78
4.5.3.1	Product A	78
4.5.3.2	Product B	80
4.5.3.3	Proactive Monitor	81
4.6	Validation	84
4.6.1	Participants Selected for the Validation	84
4.6.2	SPICE Framework	84
4.6.3	Validation Result	86
5.	CONCLUSIONS AND RECOMMENDATIONS	90
5.1	Conclusions	90
5.2	Recommendations	90
5.3	Future Works	91
A.	Validation	92
B.	SK Satgas	93
	REFERENCES	102
	GLOSSARY	103

List of Figures

1.1	Internet Use Timeline (emp[2024]	13
1.2	Top OWASP web application security risks based on X-Force penetration testing data. (BM X-Force[2024]	14
1.3	Data Breach Statistics (erry[2019]	15
1.4	Fishbone Research Problem	17
2.1	The CIA triad ensures security and identifies vulnerabilities. (hreatscape[2024]	27
2.2	VAPT is a crucial practice for protecting against cyber threats. (alsariya[2023]	34
3.1	Research Framework	43
4.1	Maturity Assessment Checklist	56
4.2	Proposed DevSecOps Framework	70
4.3	VAPT Steps	72
4.4	Maturity Assessment Flow	73
A.1	Validation Evidence with Akbar	92
A.2	Validation Evidence with Yuga	92

List of Tables

2.1 Levels in Systems Security Engineering Capability Maturity Model (SSE-CMM)	24
2.2 Levels in NIST Cybersecurity Framework (NIST CSF)	25
2.3 Levels in Control Objectives for Information and Related Technologies (COBIT)	26
2.4 Thesis Framework and comparison with other approaches	38
2.5 Thesis Framework and comparison with other approaches	42
4.1 PEO - Question Formation Frameworks	51
4.2 GAP Analysis Results	54
4.3 GAP Analysis Results - Action Plan	55
4.4 Mapping Maturity Assessment Checklist on Data Protection	59
4.5 Mapping Maturity Assessment Checklist on Network Segmentation	61
4.6 Mapping Maturity Assessment Checklist on OS & Software	62
4.7 Mapping Maturity Assessment Checklist on Services Audit	63
4.8 Mapping Maturity Assessment Checklist on Endpoint Protection	65
4.9 Mapping Maturity Assessment Checklist on Source Code & Credentials Protection	66
4.10 Mapping Maturity Assessment Checklist on Secure Code (Scanning and VAPT)	67
4.11 Mapping Maturity Assessment Checklist on Multi Factor Authentication	67
4.12 Product A First Maturity Assessment	68
4.13 Product B First Maturity Assessment	69
4.14 Tools that Support Security Assessment	72
4.15 Maturity Assessment Measure	73
4.16 Product A Second Maturity Assessment	77
4.17 Product B Second Maturity Assessment	77

4.18 Before and After Narrow Implementation	78
4.19 Vulnerability Found By The Severity	80
4.20 Vulnerability Details	81
4.21 Proactive Monitor Results - Vulnerability & Credential Leaks	82
4.22 Vulnerability Found By The Severity Of Proactive Monitor	83
4.23 Timeline To Remediate The Vulnerability	83
4.24 SPICE - Question Formation Frameworks	85
4.25 Mapped Questions	86
4.26 Cross Case Synthesis - Validation	87
4.27 Cross Case Synthesis - Validation	88

