

**EVALUATING THE EFFECTS OF SECURITY TOOLS ON DEVELOPER  
PRODUCTIVITY IN DEVSECOPS CONTINUOUS INTEGRATION PIPELINES  
THROUGH AN EMPIRICAL STUDY AT PT XYZ**

By

Ahmad Hafzan  
200001477

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 7 August 2026

### 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.

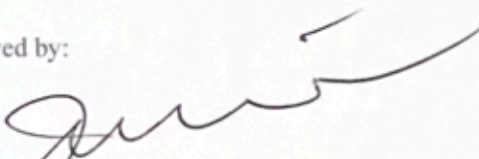
  
Ahmad Hafzan

Student

15/8/26

Date

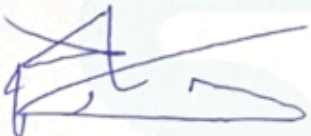
Approved by:

  
Dr. Ir. Mohammad Achmad Amin Soetomo M.Sc

Thesis Advisor

Aug 15<sup>th</sup> 26

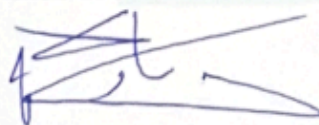
Date

  
Dr. Maulahikmah Galinium S.Kom M.Sc

Thesis Co-Advisor

15.8.2026

Date

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

15.8.2026

Date

Dean of Faculty of Engineering and  
Information Technology

## ABSTRACT

### **EVALUATING THE EFFECTS OF SECURITY TOOLS ON DEVELOPER PRODUCTIVITY IN DEVSECOPS CONTINUOUS INTEGRATION PIPELINES THROUGH AN EMPIRICAL STUDY AT PT XYZ**

By

Ahmad Hafzan

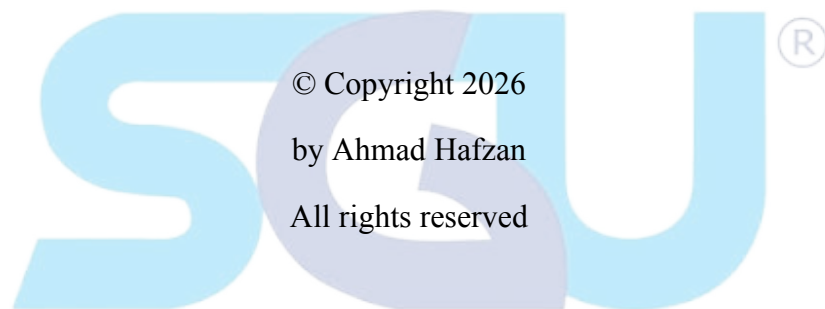
Dr. Ir. Mohammad Achmad Amin Soetomo M.Sc, Advisor

Dr. Maulahikmah Galinium S.Kom M.Sc, Co-Advisor

SWISS GERMAN UNIVERSITY

Organisations delivering software continuously have moved security verification into the Continuous Integration pipeline, where dependency scanning, static analysis and secrets detection now execute on every change. The security case for doing so is settled. The operational case is not, because each control consumes build time, produces findings somebody must judge, and occasionally stops a merge the developer expected to proceed. What that arrangement costs the engineering organisation has not been measured. This interpretive embedded single case study at PT XYZ examines that cost and the conditions under which it is worth paying. Evidence comes from interviews, a focus group discussion, pipeline records and documentary analysis, analysed through hybrid thematic coding with process tracing, cross role comparison and rival explanation testing, then submitted to independent practitioner validation. Productivity is treated through the SPACE framework. Two mechanisms proved decisive. The costly finding is the one that is technically correct and irrelevant to the code under review rather than the false positive, and infrastructure failures presenting identically to security findings erode trust in a control performing exactly as designed. Governance conditions moderated every relationship examined. The study recommends calibrating gates by application criticality and governing secure coding practice explicitly.

*Keywords: DevSecOps, developer productivity, continuous integration, secure coding policy, SPACE framework*



## **DEDICATION**

I dedicate this thesis to God for guidance and blessings throughout my academic journey; to my family for their unwavering love, encouragement and support; to my beloved country, Indonesia, for inspiring me to contribute through knowledge and service; and to Telco Indonesia, my second home, where I have been given valuable opportunities to learn, grow, and develop both professionally and personally.



## ACKNOWLEDGEMENTS

I would like to put on record my thanks to all those who have been part of this thesis and made it what it is; without their help it would not have been done.

But my deepest appreciation is reserved for my supervisors. One could not have expected the research to have followed its course or attained the standard it has without them. I am in their debt for the expertise they brought to the table, as well as the patience with which they offered guidance and a fair measure of constructive criticism. For that and for their steady encouragement, I am most grateful.

I must also thank the management and technical staff at PT XYZ for their cooperation. By making the necessary information and resources available, they allowed me to get at the heart of some real-world problems in cybersecurity and software development. In that same vein, I acknowledge PT XYZ for making room to learn and grow professionally and for giving me the means to carry out this study.

To my colleagues and peers: academic support and the quality of our discussions have done much to put the finishing touches on this work. I appreciate the suggestions made which have only served to strengthen the thesis.

On a personal note, I owe a debt of gratitude to my family and friends. Their understanding and the way they have believed in me have been my motivation and strength as I have worked toward this master's degree.

In closing, I hope what is presented here is of use to practitioners and researchers alike, and that it offers some insight into how DevSecOps can be advanced and cybersecurity in the telecom sector improved.

## TABLE OF CONTENTS

|                                                                          | Page |
|--------------------------------------------------------------------------|------|
| LIST OF FIGURES                                                          | 11   |
| LIST OF TABLES                                                           | 12   |
| CHAPTER 1 - INTRODUCTION                                                 | 14   |
| 1.1. Background                                                          | 14   |
| 1.2. Research Problem                                                    | 17   |
| 1.3. Research Objective                                                  | 18   |
| 1.4. Research Question                                                   | 18   |
| 1.5. Hypothesis                                                          | 19   |
| 1.6. Research Scope and Limitation                                       | 20   |
| 1.7. Significance of Study                                               | 21   |
| CHAPTER 2 - LITERATURE REVIEW                                            | 22   |
| 2.1 The Organisational Setting and the Challenge It Presents             | 22   |
| 2.2 Developer Challenges and the Focus of This Study                     | 23   |
| 2.2.1 Signal Quality                                                     | 25   |
| 2.2.2 Feedback Timing                                                    | 25   |
| 2.2.3 Knowledge Asymmetry                                                | 26   |
| 2.2.4 Governance of Scanner Output                                       | 27   |
| 2.3 Purpose and Review Strategy                                          | 29   |
| 2.4 The Evolution of Software Delivery Towards Shared Security Ownership | 30   |
| 2.5 Continuous Integration as the Operational Core of DevSecOps          | 32   |
| 2.5.1 The practice and its documented effects                            | 32   |
| 2.5.2 Shift left and the conditions attached to it                       | 33   |
| 2.6 Security Automation Inside the Continuous Integration Pipeline       | 34   |
| 2.6.1 Control families and their operational signatures                  | 34   |
| 2.6.2 Detection accuracy and the validation burden                       | 36   |
| 2.6.3 Latency, reliability and the cost of blocking                      | 38   |
| 2.6.4 Enforcement policy as a property of the control                    | 39   |
| 2.6.5 What this literature settles and what it leaves open               | 40   |
| 2.7 Developer Productivity and the Measurement Problem                   | 40   |
| 2.7.1 Why output counts were abandoned                                   | 41   |
| 2.7.2 Delivery throughput measures and their boundary                    | 42   |
| 2.7.3 The case for the SPACE framework                                   | 43   |
| 2.7.4 Developer experience as the mechanism beneath the dimensions       | 45   |
| 2.7.5 Productivity measurement in DevSecOps specifically                 | 46   |
| 2.8 The Trade Off Between Security Enforcement and Developer Flow        | 47   |

|                                                                     |    |
|---------------------------------------------------------------------|----|
| 2.9 Thematic Synthesis of the Literature                            | 48 |
| 2.10 Research Gap                                                   | 55 |
| 2.11 Conceptual Framework and Hypotheses                            | 56 |
| 2.12 Positioning of the Contribution                                | 58 |
| CHAPTER 3 - RESEARCH METHODS                                        | 60 |
| 3.1 Research Design and Its Basis                                   | 60 |
| 3.2 Case Boundary and the Normative Layer                           | 61 |
| 3.3 Participant Selection                                           | 64 |
| 3.4 Instrument Development                                          | 66 |
| 3.4.1 How the questions were developed                              | 66 |
| 3.4.2 The semi-structured interview guide                           | 67 |
| 3.4.3 The focus group discussion guide                              | 68 |
| 3.4.4 Keeping interview and focus group evidence distinct           | 68 |
| 3.5 Metrics and Their Operationalisation                            | 70 |
| 3.5.1 Mapping SPACE dimensions to observable measures               | 73 |
| 3.5.2 Assessing secure development practice against NIST SP 800-218 | 74 |
| 3.5.3 Detection accuracy and the false positive analysis procedure  | 77 |
| 3.6 Focus Group Discussion Protocol                                 | 78 |
| 3.7 Data Collection Procedure                                       | 80 |
| 3.7.1 Implementation state at the point of data collection          | 80 |
| 3.8 Analytical Procedure                                            | 82 |
| 3.9 Validity, Reliability and Trustworthiness                       | 84 |
| 3.10 External Validation Procedure                                  | 86 |
| 3.10.1 Selection and independence of validators                     | 86 |
| 3.10.2 What was submitted for review                                | 88 |
| 3.10.3 Review protocol                                              | 88 |
| 3.10.4 Limits of the procedure                                      | 89 |
| 3.11 Alignment Between Method and Findings                          | 89 |
| 3.12 Success Criteria and Evaluation Indicators                     | 91 |
| CHAPTER 4 - RESULT AND DISCUSSION                                   | 94 |
| 4.1 Status and Provenance of the Evidence                           | 94 |
| 4.1.1 What has been collected                                       | 94 |
| 4.1.2 The state of the evidence base                                | 94 |
| 4.1.3 What this chapter therefore demonstrates                      | 95 |
| 4.1.4 How to read the remainder of the chapter                      | 96 |
| 4.2 Basis of Reporting                                              | 96 |
| 4.3 Evidence Base and Participant Context                           | 96 |
| 4.3.1 Composition of the evidence                                   | 96 |

|                                           |                                                           |     |
|-------------------------------------------|-----------------------------------------------------------|-----|
| 4.3.2                                     | Participants                                              | 97  |
| 4.3.3                                     | The unit of analysis in practice                          | 98  |
| 4.3.4                                     | Interview evidence and focus group evidence               | 99  |
| 4.4                                       | Pipeline Behaviour Under Integrated Security Controls     | 101 |
| 4.4.1                                     | Feedback latency and the boundary of the current task     | 102 |
| 4.4.2                                     | Measured change across the two configurations             | 102 |
| 4.4.3                                     | Repeated execution and its sources                        | 104 |
| 4.4.4                                     | Blocking behaviour and lead time                          | 105 |
| 4.4.5                                     | Failure state ambiguity                                   | 106 |
| 4.5                                       | SSDF Gap Assessment                                       | 108 |
| 4.6                                       | Developer Experience of Security Feedback                 | 109 |
| 4.6.1                                     | Accuracy, applicability and the validation episode        | 110 |
| 4.6.2                                     | Feedback specificity and cognitive load                   | 111 |
| 4.6.3                                     | Interruption and the shape of recovery                    | 113 |
| 4.7                                       | Effects Across the SPACE Dimensions                       | 113 |
| 4.7.1                                     | Satisfaction and well being                               | 113 |
| 4.7.2                                     | Performance                                               | 114 |
| 4.7.3                                     | Activity                                                  | 114 |
| 4.7.4                                     | Communication and collaboration                           | 115 |
| 4.7.5                                     | Efficiency and flow                                       | 115 |
| 4.7.6                                     | The dimensional pattern                                   | 116 |
| 4.8                                       | Relative Influence of Controls and Enforcement Decisions  | 118 |
| 4.9                                       | Conditions Governing the Trade Off and Rival Explanations | 120 |
| 4.9.1                                     | Moderating conditions                                     | 120 |
| 4.9.2                                     | Rival explanations                                        | 121 |
| 4.10                                      | Assessment of the Hypotheses                              | 122 |
| 4.11                                      | External Validation Results                               | 123 |
| 4.11.1                                    | Outcome                                                   | 126 |
| 4.11.2                                    | Corrective actions taken                                  | 127 |
| 4.11.3                                    | Corroboration against published findings                  | 128 |
| 4.11.4                                    | Standing of the validation                                | 128 |
| 4.11.5                                    | Outcome against the success criteria                      | 129 |
| 4.12                                      | Discussion interpretation against the reviewed literature | 130 |
| 4.12.1                                    | Interpretation against the reviewed literature            | 130 |
| 4.12.2                                    | The policy gap as a candidate explanation                 | 131 |
| 4.12.3                                    | Answers to the research questions                         | 132 |
| 4.12.4                                    | Limitations bearing on these findings                     | 132 |
| CHAPTER 5 - CONCLUSION AND RECOMMENDATION |                                                           | 134 |

|                                                                                 |     |
|---------------------------------------------------------------------------------|-----|
| 5.1 Conclusion                                                                  | 134 |
| 5.2 Recommendation                                                              | 134 |
| 5.2.1 Secure coding governance recommendations                                  | 139 |
| 5.3 Directions for Future Research                                              | 141 |
| 5.4 Mapping of Identified Gaps to Proposed Solutions                            | 141 |
| 5.5 Alignment Between the Study and the Needs of PT XYZ                         | 143 |
| 5.6 Research Roadmap, 2026 to 2030                                              | 145 |
| REFERENCES                                                                      | 147 |
| APPENDICES                                                                      | 154 |
| Appendix A Glossary of Key Terms                                                | 154 |
| Appendix B Semi Structured Interview Guide                                      | 155 |
| Appendix C Focus Group Discussion Protocol                                      | 161 |
| Appendix D SPACE Productivity Measurement Instrument                            | 162 |
| Appendix E Analytical Coding Frame                                              | 169 |
| Appendix F External Validation Record                                           | 171 |
| Appendix G Delivery Flow Comparison Dataset                                     | 172 |
| Appendix H Fieldwork Readiness and Completion Checklist                         | 175 |
| Appendix I Documentary Evidence Register                                        | 177 |
| Appendix J Chain of Evidence Specimen                                           | 179 |
| Appendix K Focus Group Discussion Documentation                                 | 181 |
| Appendix L Short Curricula Vitae of External Validators and Focus Group Experts | 184 |
| CURRICULUM VITAE                                                                | 187 |

## LIST OF FIGURES

|                                                                                                                                                                                                   | Page |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
| Figure 1.1 Delivery flow before and after security integration into the Continuous Integration stage, OWASP (2025) and Souppaya, Scarfone and Dodson (2022)                                       | 16   |
| Figure 1.2 Fishbone Research Problem                                                                                                                                                              | 17   |
| Figure 2.1 Developer challenge conditions arising from automated security scanning in continuous integration and their correspondence to the SPACE productivity dimensions, Forsgren et al., 2021 | 25   |
| Figure 2.2 Conceptual framework in fully specified form, Forsgren et al. (2021) and Noda et al. (2023)                                                                                            | 58   |
| Figure 3.1 Research framework                                                                                                                                                                     | 84   |
| Figure 3.2 Integrated analysis procedure and external validation                                                                                                                                  | 84   |
| Figure 4.1 The security feedback episode as the embedded unit of analysis                                                                                                                         | 99   |
| Figure 4.2 Measured change between Configuration A and Configuration B across latency, cycle, assurance and friction measures                                                                     | 103  |
| Figure 4.3 Directional effect map of control families across the SPACE dimensions                                                                                                                 | 118  |
| Table 4.13 Appointed validators assessed against the competency specification of Table 3.9a                                                                                                       | 124  |
| Figure 5.1 The six layer framework for governing security feedback, with developer attention as the constrained resource                                                                          | 136  |
| Figure B.1 Interview DEV-01                                                                                                                                                                       | 157  |
| Figure B.2 Interview DEV-02                                                                                                                                                                       | 158  |
| Figure B.3 Interview OPS-01                                                                                                                                                                       | 158  |
| Figure B.4 Interview OPS-02                                                                                                                                                                       | 159  |
| Figure B.5 Interview SEC-01                                                                                                                                                                       | 159  |
| Figure B.6 Interview SEC-02                                                                                                                                                                       | 160  |
| Figure B.7 Interview PO-01                                                                                                                                                                        | 160  |
| Figure B.8 Interview PO-02                                                                                                                                                                        | 161  |
| Figure K.1 Focus group discussion session, PT XYZ                                                                                                                                                 | 183  |
| Figure K.2 Priority-ranking exercise                                                                                                                                                              | 184  |

## LIST OF TABLES

|                                                                                                                  | <b>Page</b> |
|------------------------------------------------------------------------------------------------------------------|-------------|
| Table 1.1 Structural comparison of delivery flow before and after security integration                           | 16          |
| Table 2.1 Comparison of candidate approaches to securing continuous software delivery                            | 28          |
| Table 2.2 Literature search strategy                                                                             | 30          |
| Table 2.3 Operational signatures of security control families in the Continuous<br>Integration stage             | 35          |
| Table 2.4 Comparison of productivity measurement approaches against the requirements<br>of this study            | 44          |
| Table 2.5 Thematic synthesis of the reviewed literature                                                          | 49          |
| Table 2.6 Critical comparison of the reviewed literature against the design properties<br>required by this study | 52          |
| Table 2.7 Building blocks selected from the critical review and their role in the research<br>framework          | 54          |
| Table 3.1 SSDF practices, expression in the PT XYZ pipeline and productivity relevance                           | 62          |
| Table 3.2 Participant groups and analytical contribution                                                         | 65          |
| Table 3.3 Operationalisation of constructs in the data collection instruments                                    | 69          |
| Table 3.4 Metric operationalisation, showing definition, source, collection and validation                       | 71          |
| Table 3.5 SPACE dimensions mapped to observable measures at PT XYZ                                               | 73          |
| Table 3.6 Binary determination against the nine in-scope SSDF practices                                          | 75          |
| Table 3.7 Observation window are classified into three mutually exclusive categories                             | 78          |
| Table 3.8 Preliminary coding framework                                                                           | 83          |
| Table 3.9 Independent validator profile and basis of independence                                                | 86          |
| Table 3.9a Competencies required of external validators and focus group experts                                  | 87          |
| Table 3.10 External validation protocol                                                                          | 88          |
| Table 3.11 Methodological and analytical alignment matrix                                                        | 90          |
| Table 3.12 Success criteria for the proposed model, with indicators, measurement and<br>thresholds               | 91          |
| Table 4.1 Evidence base and analytical use                                                                       | 97          |
| Table 4.2 Participant profiles                                                                                   | 98          |
| Table 4.3 Evidence established by the semi-structured interviews                                                 | 99          |
| Table 4.4 Evidence established by the focus group discussion                                                     | 100         |
| Table 4.5 Critical incident record CI-01                                                                         | 106         |
| Table 4.6 Critical incident record CI-02                                                                         | 107         |
| Table 4.7 SSDF gap assessment result                                                                             | 108         |
| Table 4.8 Cross role synthesis for accuracy, applicability and trust                                             | 111         |
| Table 4.9 Cross role synthesis for feedback quality and remediation usability                                    | 112         |
| Table 4.10 Directional effects of control families across the SPACE dimensions                                   | 116         |

|                                                                                                              |     |
|--------------------------------------------------------------------------------------------------------------|-----|
| Table 4.11 Relative influence of controls and enforcement decisions                                          | 118 |
| Table 4.12 Assessment of the research hypotheses against the evidence                                        | 122 |
| Table 4.14 External validation outcome                                                                       | 126 |
| Table 4.15 Overall standing of the analysis after external review                                            | 128 |
| Table 4.16 Position against the success criteria of Table 3.12                                               | 129 |
| Table 5.1 Recommendations for PT XYZ with expected productivity effect                                       | 136 |
| Table 5.2 Governance recommendations mapped to SSDF practice groups                                          | 140 |
| Table 5.3 Correspondence between identified gaps, proposed solutions, and their design and evidential status | 142 |
| Table 5.4 Organisational needs at PT XYZ against what the study delivers                                     | 144 |
| Table 5.5 Research roadmap and timeline, 2026 to 2030                                                        | 145 |
| Table A.1 Definition of key terms                                                                            | 154 |
| Table B.1 Interview research guideline mapped to constructs                                                  | 155 |
| Table C.1 Focus group themes and purpose                                                                     | 161 |
| Table D.1 SPACE productivity measurement instrument, full metric set                                         | 163 |
| Table D.2 Interpretation rules applied to the instrument                                                     | 169 |
| Table E.1 Coding frame with definitions and origin                                                           | 169 |
| Table F.1 Validator sign off record                                                                          | 171 |
| Table F.2 Corrective action log                                                                              | 172 |
| Table G.1 Delivery flow comparison, full recorded set                                                        | 173 |
| Table H.1 Fieldwork readiness status                                                                         | 175 |
| Table H.2 Indicative sequence and effort for completion                                                      | 176 |
| Table I.1 Documentary artefacts examined                                                                     | 177 |
| Table I.2 Documentary findings carried into the analysis                                                     | 179 |
| Table J.1 Worked chain of evidence for a single claim                                                        | 179 |
| Table J.2 Chain of evidence status across the principal claims                                               | 180 |
| Table K.1 Focus group session record                                                                         | 181 |
| Table L.1 Short curriculum vitae, Validator V1                                                               | 184 |
| Table L.2 Short curriculum vitae, Validator V2                                                               | 185 |