

**AI-ENHANCED THREAT MODELING IN THE DESIGN PHASE OF THE
SOFTWARE DEVELOPMENT LIFE CYCLE: A CASE STUDY AT PT. XYZ**

By
Ricky Fabian Sosiawan
22451006

MASTER'S DEGREE
in

MASTER INFORMATION TECHNOLOGY
DATA SCIENCE AND CYBER SECURITY
FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY



SWISS GERMAN UNIVERSITY
The Prominence Tower
Jalan Jalur Sutera Barat No. 15, Alam Sutera
Tangerang, Banten 15143 - Indonesia
June, 2025
Revision after the Thesis Defense on August 14th 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.

Ricky Fabian Sosiawan

Student

23 August 2025

Approved by:

Dr. Ir. Charles Lim BSc., MSc

Thesis Advisor

23 August 2025

Dr. Ir. Heru Purnomo Ipung, M.Eng

Thesis Co-Advisor

23 August 2025

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

Dean

Ricky Fabian Sosiawan

ABSTRACT

AI-ENHANCED THREAT MODELING IN THE DESIGN PHASE OF THE SOFTWARE DEVELOPMENT LIFE CYCLE: A CASE STUDY AT PT. XYZ

By

Ricky Fabian Sosiawan
Dr. Ir. Charles Lim BSc., MSc, Advisor
Dr. Ir. Heru Purnomo Ipung, M.Eng, Co-Advisor

SWISS GERMAN UNIVERSITY

This thesis presents a qualitative case study on the design and perceived utility of an AI-Enhanced threat modeling approach intended to enhance security during the design phase of the Software Development Life Cycle (SDLC) at PT. XYZ, a financial technology company. Traditional threat modeling processes are often manual and dependent on limited security expertise, creating significant challenges in fast-paced development environments. To address this, this research explores the development of a novel AI tool and seeks to understand the lived experiences and perceptions of its intended users.

Grounded in a constructivist worldview, this study employs a qualitative case study design to conduct an in-depth exploration of the phenomenon within its real-world context.¹ The research involved two key stages: first, the design and development of an AI agent capable of automating threat identification (STRIDE) and risk assessment (DREAD) from design artifacts; and second, a series of semi-structured interviews with software engineers and architects at PT. XYZ.

Thematic analysis of the interview data revealed key insights into the perceived value of the AI-Enhanced framework. Participants highlighted its potential to significantly improve the efficiency and comprehensiveness of threat modeling, viewing it as a

valuable "expert assistant" that could empower development teams. However, they also emphasized the indispensable role of human oversight to ensure contextual accuracy and to build trust in the tool's outputs. This study contributes a rich, contextualized understanding of how AI tools can be integrated into secure software development, providing practical insights for organizations seeking to foster a more proactive security culture.

Keywords: AI-Enhanced, Secure Software Development, Threat Modeling, Design Phase of Software Development Life Cycle, STRIDE, DREAD, Gemini, AI Agent, LLM





DEDICATION

To my beloved wife, daughter, and my entire family. Your unwavering love, endless patience, and constant encouragement were the foundation upon which this work was built. In the spirit of this research, this thesis is also dedicated to all those working to build a more secure digital future for Indonesia.



ACKNOWLEDGEMENTS

I wish to express my deepest and most sincere gratitude to my thesis advisor, Dr. Charles Lim, B.Sc., M.Sc., and my co-advisor, Dr. Ir. Heru Purnomo Ipung, M.Eng. Dr. Lim's expert guidance was the cornerstone of this research, shaping the AI-enhanced framework from its initial concept to its final form. Dr. Ipung's profound expertise in AI was invaluable; his critical questions challenged me to strengthen the technical depth of the AI agent's persona and knowledge base, significantly enhancing the quality of this thesis.

My heartfelt thanks go to the esteemed board of examiners, Dr. Ir. Mohammad Achmad Amin Soetomo, M.Sc., and Dr. Eka Budiarto, ST, M.Sc. Their insightful questions regarding the model's reliability and practical usability pushed me to clarify my findings and strengthen my conclusions. I also extend my appreciation to the entire faculty and staff of the Master of Information Technology program at Swiss German University for fostering an academic environment that encourages innovation and critical thinking.

This research would not have been possible without the generous participation of the experts from PT. XYZ. Their willingness to engage with the AI-generated threat models and provide candid, real-world feedback on its effectiveness, usability, and limitations was the key to validating this framework. Their insights transformed this study from a theoretical exercise into a practical exploration of AI's role in modern software development.

Finally, on a personal note, I owe everything to my family. To my wonderful wife and daughter, thank you for your endless patience, love, and understanding through the late nights and long weekends dedicated to this thesis. Your support was my constant motivation. To my entire extended family, thank you for your unwavering encouragement. This achievement is a testament to the foundation you have all provided me, and this work is dedicated to you.

TABLE OF CONTENTS

Content	Page
STATEMENT BY THE AUTHOR.....	2
ABSTRACT.....	3
DEDICATION.....	6
ACKNOWLEDGEMENTS	7
TABLE OF CONTENTS	8
LIST OF FIGURES	10
LIST OF TABLES	11
CHAPTER 1 – INTRODUCTION	12
1.1. BACKGROUND	12
1.2. RESEARCH PROBLEM	13
1.3. RESEARCH OBJECTIVE	16
1.4. RESEARCH QUESTION	16
1.5. HYPOTHESIS.....	17
1.6. RESEARCH SCOPE AND LIMITATION.....	17
1.7. SIGNIFICANCE OF STUDY	18
1.8. THESIS STRUCTURE.....	18
CHAPTER 2 - LITERATURE REVIEW.....	20
2.1 OVERVIEW OF PT. XYZ AND DIGITAL ASSET SECURITY CONTEXT	20
2.2 SECURE SOFTWARE DEVELOPMENT LIFE CYCLE (SDLC).....	21
2.3 THREAT MODELING	25
2.4. STRIDE METHODOLOGY.....	42
2.5 DREAD METHODOLOGY	47
2.6 LARGE LANGUAGE MODELS (LLMs).....	50
2.7 PROMPT ENGINEERING	53
2.8 GEMINI: THE CHOSEN AI PLATFORM	54
2.9 RELATED WORKS.....	59
2.10. FOUNDATIONAL RESEARCH PARADIGMS AND METHODOLOGICAL JUSTIFICATION	70
CHAPTER 3 – RESEARCH METHODS	75
3.1 RESEARCH DESIGN.....	75
3.2 THE AI-ENHANCED FRAMEWORK: THE CASE UNDER STUDY	76
3.3 DATA COLLECTION PROCEDURES	84
3.4 DATA ANALYSIS PROCEDURES	90
3.5 STRATEGIES FOR VALIDATION	91
3.6 SUCCESS CRITERIA FOR FRAMEWORK VALIDATION.....	93

CHAPTER 4 – RESULT AND DISCUSSION	95
4.1 CHAPTER INTRODUCTION	95
4.2 PRESENTATION OF AI-GENERATED ARTIFACTS	95
4.3 FINDINGS: THEMATIC ANALYSIS OF EXPERT INTERVIEWS	96
4.4 DISCUSSION OF FINDINGS	99
4.5 CHAPTER SUMMARY	106
CHAPTER 5 – CONCLUSION AND FUTURE WORK.....	107
5.1 CONCLUSION	107
5.2 STRATEGIC RECOMMENDATIONS FOR PT. XYZ	107
5.3 FUTURE WORK	109
5.4. RESEARCH LIMITATIONS	110
GLOSSARY.....	111
REFERENCES.....	115
APPENDICES	119
APPENDIX 1 – EXPERT INTERVIEW DOCUMENTATION	119
APPENDIX 2 – AI-GENERATED THREAT MODEL REPORTS	122
CURRICULUM VITAE.....	137

LIST OF FIGURES

Figures	Page
Figure 1. 1 Fishbone Diagram - Inadequate Software Design Security Integration	13
Figure 2. 1 Secure SDLC	22
Figure 2. 2 Integrating Security into design phase of SDLC	25
Figure 2. 3 The four-step of threat modelling process.....	27
Figure 2. 4 STRIDE threat categories.....	43
Figure 2. 5 DREAD Threat Prioritization Process.....	48
Figure 2. 6 AI-Enhanced threat modelling	51
Figure 3. 1 Research framework.....	76
Figure 3. 2 Gemini Gems Configuration	78
Figure 3. 3 System instructions.....	79



LIST OF TABLES

Table	Page
Table 2. 1 Comparison of Threat Modeling Methodologies.....	33
Table 2. 2 Comparison Gemini 2.5 Pro without Gems vs Gemini 2.5 Pro with Gems	56
Table 2. 3 Comparison Threat Modeling and LLM approach in design phase of SDLC	63
Table 2. 4 Comparative analysis comparison	72
Table 3. 1 Interview indicators and justification & reference.....	86
Table 4. 1 Traditional vs AI-Enhanced.....	100

