

**DEVELOPMENT OF AN ADAPTIVE THREAT INTELLIGENCE-LED
RED TEAMING FRAMEWORK FOR INTERNAL TEAMS IN
BANKING SECTOR**

By

Muhammad Arvie Reyhan Nabil
22451065

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 Thesis defense on 04 February, 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.

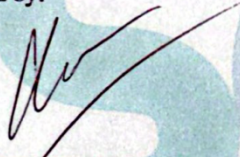


Muhammad Arvie Reyhan Nabil

Student

18 February 2026

Approved by:



Dr. Charles Lim, B.Sc., M.Sc

Thesis Advisor

18 February 2026



Dr. Semi Yulianto, S.E., M.Kom.

Thesis Co-Advisor

18 February 2026

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

Dean of Faculty of Engineering & Information Technology

18 February 2026

ABSTRACT

DEVELOPMENT OF AN ADAPTIVE THREAT INTELLIGENCE-LED RED TEAMING FRAMEWORK FOR INTERNAL TEAMS IN BANKING SECTOR

By

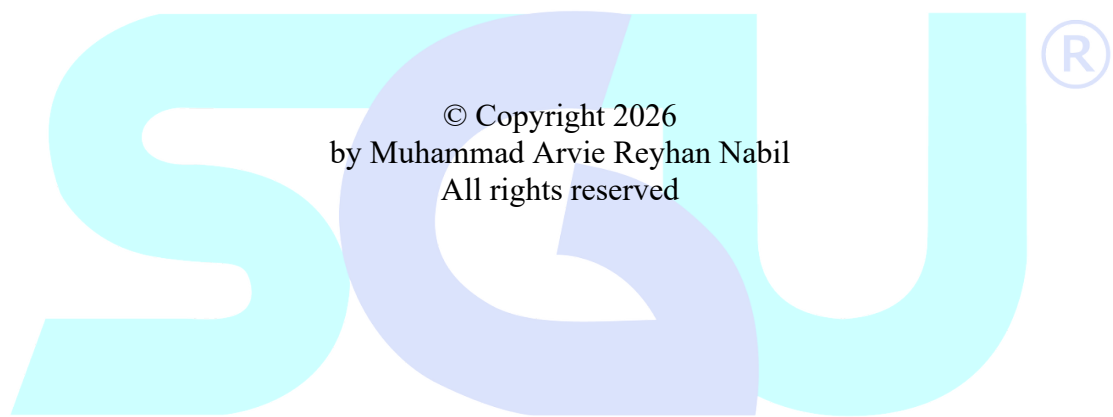
Muhammad Arvie Reyhan Nabil
Dr. Charles Lim, B.Sc., M.Sc, Advisor
Dr. Semi Yulianto, S.E., M.Kom., Co-Advisor

SWISS GERMAN UNIVERSITY

This research addresses the critical operational gap within internal banking Red Teams, which often operate at an 'Initial' maturity level characterized by ad-hoc governance, unsafe Platform, and a reliance on manual execution. The primary objective of this study is to develop an Adaptive Threat Intelligence-Led Red Teaming Framework specifically tailored for internal teams, synthesizing rigorous global standards (TIBER-EU/AASE) with Agile management and "Secure Testing Platform" principles. Adopting the Design Science Research Methodology (DSRM), the study constructed a comprehensive artifact comprising four pillars: Agile Governance, Secure Platform, Unified Execution, and Performance Measurement. The framework's design was evaluated through ex-ante expert validation involving four domain specialists, utilizing Content Validity Ratio (CVR) and thematic analysis. The results demonstrated perfect expert consensus (CVR +1.0) across all evaluation dimensions, confirming the framework's utility in mitigating operational risks such as accidental service disruption. The study concludes that the proposed framework provides a design-validated blueprint for professionalizing internal red teaming, enabling banks to transition from ad-hoc testing to continuous, intelligence-driven cyber resilience operations while maintaining strict regulatory compliance.

Keywords: *Red Teaming, Design Science Research, Threat Intelligence, Banking Cybersecurity, Agile Governance.*

Muhammad Arvie Reyhan Nabil



DEDICATION

I dedicate this work to my family, for their constant encouragement, to my advisors and co-advisor, for their trust and guidance, and to the banking institution that allowed this research to be conducted in service of stronger cyber resilience.



ACKNOWLEDGEMENTS

Alhamdulillah rabbil ‘alamin. All praise is due to Allah Subhanahu wa Ta’ala, who has granted me health, strength, and perseverance throughout this journey. By His mercy and guidance, I was given the opportunity not only to pursue but also to complete my Master’s degree and this thesis.

1. I would like to express my deepest gratitude to my parents, Arief Budiman and Shelve Nidya Neyman and to my younger sister, Shafira Arvie Azzahra, for their unconditional love, prayers, and continuous support throughout my studies and the completion of this thesis.
2. My sincere thanks go to my thesis advisor, Dr. Charles Lim, B.Sc., M.Sc, for his invaluable guidance, constructive feedback, and patience in directing this research from its early ideas to its final form.
3. I am also deeply grateful to my co-advisor, Dr. Semi Yulianto, S.E., M.Kom, for his insightful suggestions, encouragement, and support, which have been essential in refining the direction and contribution of this work.
4. I would like to thank all my friends and colleagues in SGU MIT Batch 35 for their camaraderie, discussions, and mutual support during lectures, projects, and long nights of study and writing.
5. I sincerely appreciate the banking institution where I conducted this research for the opportunity, trust, and facilities provided, which enabled the practical realization and relevance of this study.
6. My heartfelt thanks go to all the experts who generously contributed their time and expertise to participate in the framework validation process. Their insights and evaluations were crucial in strengthening the rigor and practicality of the proposed framework.
7. Finally, I would like to extend my deepest appreciation to Nanda Faradilla Putri Fahira, who has always accompanied me, offering unwavering support, patience, and understanding. Her encouragement has been a constant source of motivation throughout this academic journey.

Table of Content

ABSTRACT	3
DEDICATION	5
ACKNOWLEDGEMENTS	6
TABLE OF CONTENT	7
LIST OF FIGURE	9
LIST OF TABLE	10
CHAPTER 1 - INTRODUCTION	12
1.1. BACKGROUND	12
1.2. PROBLEM STATEMENT	14
1.3. RESEARCH QUESTIONS	17
1.4 HYPOTHESIS	18
1.5. RESEARCH OBJECTIVES	19
1.6. SCOPE AND LIMITATIONS	20
1.7. SIGNIFICANCE OF THE STUDY	21
1.8. THESIS STRUCTURE	23
CHAPTER 2 - LITERATURE REVIEW	25
2.1. COMPANY BACKGROUND	25
2.2 COMPANY CHALLENGE	26
2.3 CHALLENGE TO BE SOLVED	28
2.4 PROPOSED APPROACHES AND REQUIREMENTS ANALYSIS	29
2.5 ANALYSIS OF SOLUTION APPROACHES	33
2.6. REVIEW OF PREVIOUS STUDIES	34
2.7. GLOBAL REDTEAMING FRAMEWORK	45
2.8. GAP ANALYSIS DIMENSIONS AND INDICATORS	57
2.9 APPROACH SELECTION FOR FRAMEWORK DIMENSIONS	67
2.10. RESEARCH GAP	90
2.11 MEASUREMENT APPROACHES AND EVALUATION METRICS	104
2.12. FRAMEWORK EVALUATION STRATEGIES	119
2.13 RESEARCH FRAMEWORK DERIVATION PROCESS	140
2.13.1 CONCEPTUAL FOUNDATIONS FOR RESEARCH PHASING	140
2.13.2 ALIGNMENT OF KEY DIMENSIONS WITH THE EMERGENT FOUR-PHASE STRUCTURE	148
2.14 DESIGN SCIENCE RESEARCH FRAMEWORK: ARTIFACT DEVELOPMENT AND VALIDATION	153
CHAPTER 3 -RESEARCH METHODOLOGY	163
3.1. RESEARCH DESIGN	163
3.2. RESEARCH FRAMEWORK	164
3.3. DATA COLLECTION METHODS	171
3.4. DATA ANALYSIS TECHNIQUES	181
3.5. FRAMEWORK ACCEPTANCE CRITERIA AND DECISION FRAMEWORK	186
3.6. REQUIRED MATERIALS AND EQUIPMENT	187
3.7. REQUIRED MATERIALS AND EQUIPMENT	190
CHAPTER 4 – RESULTS AND DISCUSSIONS	192
4.1. PHASE 1 INPUT ANALYSIS AND REQUIREMENTS DEFINITION	192
4.2 PHASE 2 DESIGN PROCESS	207
4.3 PHASE 3 THE ARTIFACT	225
4.4 PHASE 4 VALIDATION RESULTS	242
4.5 FRAMEWORK REFINEMENT AND ACCEPTANCE DETERMINATION	262

4.6 DISCUSSION: VALIDATION IMPLICATIONS AND FRAMEWORK POSITIONING	270
CHAPTER 5 – CONCLUSIONS AND RECOMENDATIONS	276
5.1 CONCLUSION	276
5.2 RECOMMENDATION	278
REFERENCE	283
CURRICULUM VITAE	289
GLOSSARY	290
APPENDIX	293
APPENDIX 1 RISK ASSESSMENT RESULT	293
APPENDIX 2 SEMI-STRUCTURED INTERVIEW GUIDE CISO COMPLIANCE	296
APPENDIX 3 SEMI-STRUCTURED INTERVIEW GUIDE RED TEAM LEAD (INTERNAL) & EXTERNAL RED TEAM CONSULTANT	309
APPENDIX 4 SEMI-STRUCTURED INTERVIEW GUIDE BLUE TEAM LEAD	322
APPENDIX 5 THEMATIC CODEBOOK AND CODING MANUAL	335
APPENDIX 6 QUANTITATIVE ANALYSIS RESULT	353
APPENDIX 7 EXPERT VALIDATION TRANSCRIPT - EXPERT 1	364
APPENDIX 8 EXPERT VALIDATION TRANSCRIPT - EXPERT 2	367
APPENDIX 9 EXPERT VALIDATION TRANSCRIPT - EXPERT 3	370
APPENDIX 10 EXPERT VALIDATION TRANSCRIPT - EXPERT 4	372
APPENDIX 11 SIMULATION ENGAGEMENT OUTPUT	374

List of Figure

Figure 1.1 Fishbone Diagram of Research Problem	17
Figure 2. 1 Yulianto 2025 Research Framework	141
Figure 2.2 Sehgal 2018 Research Framework	142
Figure 2.3 Tuovinen and Frilander 2019 Research Framework	143
Figure 2.4 Azura et al. 2025 Research Framework	144
Figure 2.5 Design Science Research Framework	154
Figure 2.6 Research Framework Mapping to DSRF	161
Figure 3.1 Research Framework	165
Figure 3.2 Research Framework Phase 1	166
Figure 3.3 Research Framework Phase 2	168
Figure 3.4 Research Framework Phase 3	169
Figure 3.5 Research Framework Phase 4	171
Figure 4.1 CTI-to-ATT&CK Translation Workflow	215
Figure 4.2 Secure Testing Platform Architecture - Three-Layer Isolation Model	218
Figure 4.3 Requirements-to-Artifact Traceability Matrix	222

List of Table

Table 1.1 Summary of Risk Assessment	15
Table 2.1 Critical Operational Risks in Internal Red Teaming	27
Table 2.2 Comparative Analysis of Proposed Approaches for Red Team Professionalization	30
Table 2.3 Comparative Analysis of Solution	33
Table 2.4 Previous Research	44
Table 2.5 Global Framework Comparison	54
Table 2.6 Gap Analysis Dimensions and Key Indicators	59
Table 2.7 Journal Mapping of Framework Pillars to Supporting International Literature	60
Table 2.8 Comparative Governance Approach	71
Table 2.9 Comparative Platforms Approach	74
Table 2.10 Comparative Threat Intelligence Approach	79
Table 2.11 Comparative Execution Workflow Approach	83
Table 2.12 Comparative Metrics Approach	87
Table 2.13 Summary of Approach Selection across dimension	88
Table 2.14 Related Works & Proposed Framework	99
Table 2.15 Mapping Global Framework to Dimension	101
Table 2. 16 Summary of Quantitative Metrics	109
Table 2.17 Comparison of Qualitative Methods	114
Table 2.18 Scoring Rubric	123
Table 2. 19 CVR Interpretation	124
Table 2.20 Consensus Decision Rule	125
Table 2.21 Agreement Thresholds (Diamond et al., 2014)	126
Table 2.22 Quantitative acceptance criteria	131
Table 2.23 Research Framework Phases in Analogous Studies	145
Table 2.24 Deriving the Thesis Four Phase Research Framework from Prior Studies	147
Table 2.25 Mapping DSRF to Research Framework	159
Table 3.1 List of Expert	170
Table 3.2 Framework Evaluation Dimensions	178
Table 3.3 Likert Scale Rubric	179
Table 3.4 CVR Threshold	182
Table 3.5 IQR Threshold	183
Table 3.6 Percentage Agreement Threshold	183
Table 3.7 Theme Classification	186
Table 4.1 Red Team Operational Risk Assessment Matrix	193
Table 4. 2 Vulnerability Inventory and Severity Assessment	195
Table 4.3 Operational Gap Analysis	195
Table 4.4 Consolidated Framework Requirements	205
Table 4.5 Framework Deconstruction Matrix	210
Table 4. 6 Governance Synthesis - TIBER Rigor with Agile Management	212
Table 4. 7 Framework Components Integration Matrix	219
Table 4.8 High-Risk Threat Events Mitigation Coverage	223
Table 4.9 Summary of Maturity Level Indicators	238
Table 4.10 Expert Panel Composition	242

Table 4.11 Likert Scale Scores by Evaluation Dimension	243
Table 4.12 Content Validity Ratio (CVR) Results	245
Table 4.13 Consensus Measurement Summary Across Evaluation Dimensions	246
Table 4.14 IQR Interpretation Result	247
Table 4.15 Comprehensive Quantitative Assessment Summary and Threshold Comparison	249
Table 4.16 Identified Themes Summary with Classification and Expert Mention Frequency	250
Table 4.17 Recommended Scalability Adaptation	257
Table 4.18 Pure Red Team Implementation Impact	260
Table 4.19 Tier 1 Assessment Results - Component-Level Content Validity Ratio (CVR)	263
Table 4.20 Tier 2 Assessment Results - Dimension-Level Consensus Measurement	264
Table 4.21 Tier 3 Assessment Results - Thematic Analysis Summary	265
Table 4.22 Comprehensive Framework Acceptance Determination - Three-Tier Synthesis	266
Table 4.23 Validation Results Summary - Three-Tier Assessment Outcomes	268
Table 4.24 Thematic Analysis Outcomes Summary	269

