

**THREAT MODELLING APPROACH FOR ENHANCING WEB APPLICATION
SECURITY IN MANUFACTURING PRODUCTION SYSTEMS: A CASE STUDY OF
PT. YH MANUFACTURING**

By

Yastril Ilyas
22551058

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 06 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.


Yastril Ilyas

Student

09/02/2026

Date

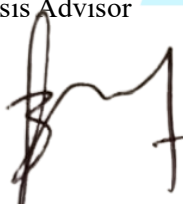
Approved by:



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

Thesis Advisor

15/02/2026

Date
Kalpin Erlangga Silaen, S.Si, M.Kom.

Thesis Co-Advisor

12/02/2026

Date

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

Dean

Date

ABSTRACT

THREAT MODELLING APPROACH FOR WEB APPLICATIONS
PRODUCTION SYSTEM TO ENHANCING SECURITY IN THE MANUFACTURING
INDUSTRY: A CASE STUDY OF PT. YH MANUFACTURING

By

Yastril Ilyas

Dr. Ir. Charles Lim BSc., MSc, Advisor

Kalpin Erlangga Silaen, S.Si,M.Kom, Co-Advisor

SWISS GERMAN UNIVERSITY

The adoption of Industry 4.0 has increased the manufacturing sector's reliance on production web applications, consequently expanding cybersecurity risks. This study aims to develop and validate a risk-based threat modelling approach to enhance the security of production web applications in manufacturing environments. A case study was conducted at PT. YH Manufacturing using an asset-oriented methodology that integrates STRIDE for threat identification, the OWASP Top 10 (2025) for vulnerability classification, and CVSS v4.0 combined with NIST SP 800-30 and business impact mapping for risk assessment. The analysis involved system architecture modelling, data flow diagrams, vulnerability assessment, and expert validation through focus group discussions. The results indicate that several high-severity risks stem not only from technical vulnerabilities but also from weaknesses in system architecture and operational processes, directly affecting the confidentiality, integrity, and availability of production data. This study concludes that integrating threat modelling with business impact-based risk assessment effectively improves risk prioritization, supports targeted mitigation strategies, and strengthens the operational resilience of manufacturing production systems.

Keywords: Threat modelling, Web application security, Industrial cybersecurity, Risk Assessment.

© Copyright 2026

by Yastril Ilyas
All rights reserved



DEDICATION

This thesis is dedicated to PT YH Manufacturing as a contribution to strengthening cybersecurity and industrial resilience, to the academic community for the advancement of knowledge and cybersecurity research, and to Indonesia in support of digital sovereignty and sustainable national progress.



ACKNOWLEDGEMENTS

All praise and gratitude are due to Allah Subhānahu wa Ta‘ālā for His mercy, blessings, and guidance, through which this thesis has been successfully completed.

With sincere humility, the author extends the highest appreciation and gratitude to the Thesis Advisors and all Lecturers for their dedication, guidance, and sincere commitment in imparting knowledge and academic values throughout the research process. Their direction and advice have been a guiding light at every stage of this thesis.

The author also expresses sincere gratitude to PT YH Manufacturing and its entire team for their trust, cooperation, and support, which enabled this research to be conducted in alignment with real-world industrial needs, particularly in strengthening cybersecurity. **As the Prophet Muhammad ﷺ said:**

“The best of people is those who are most beneficial to others.”

(Hadith, Ahmad)

The author would also like to thank colleagues, friends SGU Batch 35, and peers for their support, prayers, and constructive feedback. Every contribution made has been a form of goodness valued in the sight of Allah سبحانه وتعالى. With deep love and respect, the author expresses heartfelt gratitude to beloved family members for their continuous prayers, patience, and sincerity throughout this academic journey, thank my wife support me and my children's. Finally, the author hopes that this research will serve as beneficial knowledge, contribute to the advancement of academic scholarship and cybersecurity practices in the media industry, and become part of a sincere effort to support the well-being of the nation and the state, particularly Indonesia.

TABLE OF CONTENTS

	Page
STATEMENT BY THE AUTHOR.....	2
ABSTRACT.....	3
DEDICATION.....	5
ACKNOWLEDGEMENTS.....	6
TABLE OF CONTENTS.....	7
LIST OF FIGURES	13
LIST OF TABLES	15
CHAPTER 1 – INTRODUCTION	18
1.1. Background.....	18
1.2. Research Problem	22
1.3. Research Objective	23
1.4. Research Question	23
1.5. Hypothesis.....	23
1.6. Research Scope and Limitation	24
1.7. Significance of Study.....	24
1.8. Thesis Structure	25
CHAPTER 2 - LITERATURE REVIEW.....	26
2.1. Introduction Industry manufacturing.....	26
2.2. Business Process	26
2.3. Transformation Digital Industry manufacturing.....	28
2.4. Web Application Production System.....	30
2.4.1 Web Application Production.....	31
2.4.2 Web application production system architecture High Level.....	33

2.4.3 Intranet Infrastructure	35
2.4.4 Frontend System	36
2.4.5 Backend System.....	37
2.4.6 API (Application Programming Interface)	38
2.5. Web Application Security Vulnerabilities.....	39
2.5.1 OWASP Top Ten 2021	39
2.5.2 OWASP Top Ten 2025.....	41
2.5.3 Mapping OWASP Top 10 (2021) to OWASP Top 10 (2025).....	45
2.6. Risk	48
2.6.1 Risk Management	48
2.6.2 Risk Assessment	51
2.6.3 Risk Assessment ISO 31000.....	51
2.6.4 Risk Assessment ISO 27005	58
2.6.5 Risk Assessment NIST 800-30	61
2.6.6 COSO Enterprise Risk Management (ERM).....	65
2.6.7 FAIR (Factor Analysis of Information Risk).....	68
2.6.8 Risk Scoring System.....	74
2.6.8.1 Risk Scoring DREAD	74
2.6.8.2 OWASP Risk Rating.....	76
2.6.8.3 Common Vulnerability Scoring System	78
2.6.8.4 Limitations of CVSS as a Risk Metric.....	81
2.6.8.5 CVSS Temporal Metrics and Exploitability	82
2.6.8.6 Integrasi CVSS with EPSS and KEV (Risk Prediction).....	82
2.6.8.9 Business Impact Scoring dalam Risk Calculation	83
2.6.8.10 Modern Risk Calculation Model (CVSS to Risk).....	83

2.6.8.11 Mapping Details Between Risk Models	89
2.7. Threat Modelling	91
2.7.1 Threat Modelling PASTA.....	92
2.7.2 Threat Modelling STRIDE	94
2.7.3 Threat Modelling Attack Tree	96
2.7.4 Threat Modelling “DREAD”	97
2.7.5 Threat Modelling OCTAVE	100
2.7.6 Threat Modelling VAST	102
2.7.7 Threat Modelling LINDDUIN	103
2.8. Data Threat Modelling Approach.....	107
2.8.1 Asset Centric.....	108
2.8.2 Attacker Centric.....	108
2.8.3 Software Centric.	109
2.8.4 Software Centric.	109
2.9. Data Flow Diagram (DFD)	109
2.10. Design Science Research Methodology.....	112
2.10.1 Design framework mapping process using threat modeling.....	114
2.11. Previous Studies.....	115
CHAPTER 3 – RESEARCH METHODS	122
3.1. Research Method	122
3.2. Research Framework	122
3.3. Input & System Context.....	124
3.3.1 Scoping and Preparation	124
3.3.2 Asset Identification.....	125
3.3.3 Boundary and Architecture	125

3.3.4 Data Flow Diagram (DFD)	125
3.4. Threat & Vulnerability Identification	126
3.4.1 Threat Identification (STRIDE).....	126
3.4.2 Vulnerability Assessment	126
3.4.3 Risk Calculation.....	127
3.4.4 Business Risk Assessment	128
3.4.5 Risk Determination	129
3.5 Mitigation Strategy	129
3.6 Research Evaluation.....	130
3.7 Research Validation	131
CHAPTER 4 – RESULT AND DISCUSSION	136
4.1. Introduction.....	136
4.2 Scoping and Preparation	136
4.2.1 Review of Internal Documentation.....	137
4.2.2 Stakeholder Identification.....	138
4.2.3 Alignment with Organizational Objectives	138
4.3 Asset Identification	140
4.3.1 Boundary and Architecture	142
4.3.2 Identification Component and Critical Asset.....	144
4.3.3 Data Flow Diagram (DFD)	148
4.3.4 Data Flow Diagram Process Level 1	150
4.3.5 Data Flow Diagram Process Level 2	155
4.3.5.1 Data Flow Diagram Process User Authentication Service	156
4.3.5.2 Data Flow Diagram Process Production Data Service	161
4.3.5.3 Data Flow Diagram Process Quality Service.....	164

4.3.5.4 Data Flow Diagram Process Technical Service.....	166
4.3.5.5 Data Flow Diagram Process Planning Service	169
4.3.5.6 Data Flow Diagram Process Administrator Service	172
4.3.5.7 Data Flow Diagram Process Database Access Service.....	174
4.4 Threat & Vulnerability Identification	176
4.4.1 Mapping Threat STRIDE.....	177
4.4.1.1 Mapping Threat Stride Authentication Service.	177
4.4.1.2 Mapping Threat Stride Production Data Service.	178
4.4.1.3 Mapping Threat STRIDE quality service.	180
4.4.1.4 Mapping Threat STRIDE technical service.....	181
4.4.1.5 Mapping Threat STRIDE Planning service.	183
4.4.1.6 Mapping Threat STRIDE Administration service.....	184
4.4.1.7 Mapping Threat STRIDE Database Access service.	186
4.5 Vulnerability Assessment	190
4.5.1 Security Gap Analysis.....	196
4.6 Risk Calculation.....	200
4.6.1 Business Risk (Business Impat).....	201
4.6.2 Threat Prioritizing.....	211
4.7 Determine Countermeasures.....	223
4.8 Mitigation Strategy	223
4.8.1 Mitigation Strategy Technical Mitigation.....	224
4.8.2 Mitigation Strategy Non-Technical Mitigation	226
4.9 Evaluation	228
4.10 Validation.....	230
4.11 Discussion	233

4.11.1 Discussion of Hypothesis and Evaluate.....	233
CHAPTER 5 – CONCLUSION AND FUTURE WORK	237
5.1 Conclusion	237
5.2 Recommendations.....	238
5.3 Future Works	240
APPENDIX 1 – Vulnerability Scanning.....	242
APPENDIX 2 – Vulnerability Scanning (SonarQube).....	244
APPENDIX 3 – List of Threat Information.....	246
APPENDIX 4 - Table List Web Application – STRIDE Category	246
APPENDIX 5 - Expert Profile and Questionnaire Answer	248
APPENDIX 6: Software Development Expert Questioner Answer [1]	249
APPENDIX 7: Cybersecurity Expert questioner answer [2].....	250
APPENDIX 8: Cybersecurity Expert questioner answer [3].....	251
APPENDIX 9: Cybersecurity Expert questioner answer [4].....	252
APPENDIX 10: Documentation of FGD Process	253
(Developers Application and All Related Division Owner Process).....	253
APPENDIX 11: Documentation of FGD Evaluation with Management	255
APPENDIX 12: Documentation of FGD Validasi with Coordinator Risk.....	256
APPENDIX 13: Documentation of FGD Process	257
(Expert Cybersecurity External)	257
APPENDIX 14: Risk Profile (Risk Calculation).....	260
APPENDIX 15: Budgeting Planning Mitigation Web Application System.....	261
APPENDIX 16: Budget and Cost Benefit Analysis.	262
APPENDIX 17: Roadmap Mitigation Strategy	262
CURRICULUM VITAE	269

LIST OF FIGURES

Figures	Page
Figure 1. 1 Cyberattack by Industry in 2023 (Liudmyla Pryimenko, 2024).....	18
Figure 1. 2 Trend Attack by industry manufacturing	19
Figure 1. 3 Top OWASP Web Application Security Risks	19
Figure 1. 4 Risk Assessment (PT YH Manufacturing)	21
Figure 1. 5 Cause and Effect Diagram (Fishbone)	22
Figure 2. 1 Tire-manufacturing-process.....	27
Figure 2. 2 Business Process Raw material (Semi Product).....	28
Figure 2. 3 Dashboard Web Application Production System.....	30
Figure 2. 4 Web Application Production System (Specification).....	32
Figure 2. 5 Web application production system architecture (Generic).....	33
Figure 2. 6 Details Process Web application production system.....	34
Figure 2. 7 Web Application Front End Technology	38
Figure 2. 8 OWASP Top Ten 2021	39
Figure 2. 9 OWASP Top 10 for 2025	42
Figure 2. 10 Evolution of the ranking trends of common security vulnerabilities	43
Figure 2. 11 Organization-Wide Risk Management Approach	49
Figure 2. 12 Risk Management Framework	50
Figure 2. 13 Principles, framework and process	52
Figure 2. 14 Process Framework ISO 31000	53
Figure 2. 15 Information security risk management process	59
Figure 2. 16 Assessment Process NIST 800-30.....	62
Figure 2. 17 COSO Internal Control Framework	66
Figure 2. 18 Risk Management Components	67
Figure 2. 19 The FAIR Framework for Cyber Risk Management	69
Figure 2. 20 The FAIR Model.	69
Figure 2. 21 FAIR-CAM Model	70
Figure 2. 22 FAIR-MAM Model	71

Figure 2. 23 Base, Temporal, and Environmental Scoring Progression.....	79
Figure 2. 24 CVSS Base Score Metrics	79
Figure 2. 25 Threat modelling process	92
Figure 2. 26 Stages Of PASTA Methodology	93
Figure 2. 27 Data Flow Diagram with System Boundaries	95
Figure 2. 28 . Attack tree for an attack analysis Template	97
Figure 2. 29 Threat Modelling DREAD	97
Figure 2. 30 OCTAVE Balances Three Aspects	101
Figure 2. 31 OCTAVE Phases	102
Figure 2. 32 VAST process flow diagram.	103
Figure 2. 33 LINDDUN Methodology Steps.....	104
Figure 2. 34 LINDDUN Mapping Step	104
Figure 2. 35 Research Design Methodology	113
Figure 3. 1 Research Design	122
Figure 3. 2 Research Framework.....	123
Figure 3. 3 Step by step calculation risk to business impact.	128
Figure 3. 4 Risk Profile.....	129
Figure 4. 1 Architecture Diagram of Web Application Production.....	143
Figure 4. 2 Data Flow Diagram Level 0 Web Application.....	149
Figure 4. 3 DFD Level 1 Web Application Production.....	150
Figure 4. 4 Data Flow Diagram Process User Authentication Service.....	156
Figure 4. 5 Data Flow Diagram Process Production Data Service.....	161
Figure 4. 6 Data Flow Diagram Process Quality Service	164
Figure 4. 7 Data Flow Diagram Process Technical Service	166
Figure 4. 8 Data Flow Diagram Process Planning Service.....	169
Figure 4. 9 Data Flow Diagram Process Administrator Service.....	172
Figure 4. 10 Data Flow Diagram Process Database Access Service	174
Figure 4. 11 STRIDE Threats per Process.....	188
Figure 4. 12 Total STRIDE Threat Finding.....	189
Figure 4. 13 Graph of vulnerability Assesment Finding.....	196
Figure 4. 14 Graph Pie Chart Risk Calculation	211

LIST OF TABLES

Table	Page
Table 2. 1 Top Ten critical web application security threats and vulnerabilities	40
Table 2. 2 Predicted OWASP Top 10 (2025)	44
Table 2. 3 Mapping OWASP Top 10 (2021) to OWASP Top 10	45
Table 2. 4 Risk Matrix Company PT YH Manufacturing	57
Table 2. 5 Risk Profile	57
Table 2. 6 NIST SP 800-30 Risk Level Matrix	64
Table 2. 7 Risk Level	64
Table 2. 8 Comparison Risk Assessment Framework	71
Table 2. 9 DREAD Scoring Criteria	74
Table 2. 10 Categorize the risk based on the total score.....	76
Table 2. 11 OWASP Risk Rating	77
Table 2. 12 Impact Factor	77
Table 2. 13 Determining the Severity of the Risk	78
Table 2. 14 CVSS v4.0 Score Classification	81
Table 2. 15 CVSS Temporal Metrics and Exploitability	82
Table 2. 16 CVSS Temporal Metrics to Dynamic Risk.....	84
Table 2. 17 Mapping Details Between Risk Models	89
Table 2. 18 STRIDE Threat Categories (Shevchenko et al., 2018).....	96
Table 2. 19 Common Attacks related to STRIDE	96
Table 2. 20 DREAD Scoring Criteria	98
Table 2. 21 Categorize the risk based on the total score.....	99
Table 2. 22 Key Differences Between OCTAVE and Other Approaches.....	101
Table 2. 23 Comparison Threat Modelling.....	105
Table 2. 24 DFD Components for Threat Modelling	110
Table 2. 25 Explanation of Data Flow Diagram (DFD) Levels.....	110
Table 2. 26 Summarizes the comparison of other related studies.....	118

Table 3. 1 Research Evaluation.....	130
Table 3. 2 Validation Research Framework	133
Table 4. 1 Assessment Scope	136
Table 4. 2 Internal Documentation Reviewed	137
Table 4. 3 Stakeholder Groups and Roles.....	138
Table 4. 4 Alignment with Organizational Objectives (with CIA & ISO 27001)	138
Table 4. 5 Asset Identification.....	140
Table 4. 6 Component Web Application System.....	145
Table 4. 7 user access matrix.....	149
Table 4. 8 Process Specification DFD Level 1.....	151
Table 4. 9 asset for the Production Web Application System.	152
Table 4. 10 User Authentication Service	156
Table 4. 11 Process User Authentication Service.....	158
Table 4. 12 Component IDs for User Authentication Service	159
Table 4. 13 user authentication process Details.....	160
Table 4. 14 Production Data Service Process	161
Table 4. 15 Component IDs for Production Data Service	162
Table 4. 16 Production Data Service Process Details.....	162
Table 4. 17 Quality Service Process	164
Table 4. 18 Component IDs for Quality Service	165
Table 4. 19 Quality Service Process Details.....	165
Table 4. 20 Technical Update & Service Processes.....	166
Table 4. 21 Component for Technical Update & Service.....	167
Table 4. 22 Technical Update & Service Process Details.....	168
Table 4. 23 Planning Service Process Decomposition.....	169
Table 4. 24 Components Involved in Planning Service.....	170
Table 4. 25 Planning Service Process Details.....	170
Table 4. 26 Administration & System Setting Service Processes	172
Table 4. 27 Component for Administration.....	173
Table 4. 28 Administration & System Setting Service Process Details	173
Table 4. 29 Database Access Service Processes.....	174

Table 4. 30 Component for Database Access Service	175
Table 4. 31 Database Access Service Process Details	176
Table 4. 32 STRIDE Authentication Service Process	177
Table 4. 33 STRIDE Production Data Service Process	179
Table 4. 34 STRIDE Quality Data Service Process.....	180
Table 4. 35 STRIDE Technical Data Service Process	181
Table 4. 36 STRIDE Threat Mapping for Planning Service.....	183
Table 4. 37 STRIDE Administration Data Service.....	184
Table 4. 38 STRIDE Database Access service	186
Table 4. 39 Summary Count of STRIDE Threats per Process	188
Table 4. 40 Summary of Total STRIDE Threats	189
Table 4. 41 Mapping Threat and Vulnerability User Authentication Service	190
Table 4. 42 Mapping Threat and Vulnerability Production Data Service	191
Table 4. 43 Mapping Threat and Vulnerability Quality Service.....	192
Table 4. 44 Mapping Threat and Vulnerability Technical Update & Service	193
Table 4. 45 Mapping Threat and Vulnerability Planning Service	193
Table 4. 46 Mapping Threat and Vulnerability Administration & System Setting	194
Table 4. 47 Mapping Threat and Vulnerability Database Access Service.....	195
Table 4. 48 Security Gap Analysis Web Application Production	196
Table 4. 49 Risk Calculation Business Impact	201
Table 4. 50 Threat Prioritization User Authentication Service.....	212
Table 4. 51 Threat Prioritization Production Data Service.....	213
Table 4. 52 Threat Prioritization Quality Service.....	215
Table 4. 53 Threat Prioritization Technical Update & Service.....	216
Table 4. 54 Threat Prioritization Planning Service.....	218
Table 4. 55 Threat Prioritization Administration & System Setting	219
Table 4. 56 Threat Prioritization Database Access Service	221
Table 4. 57 Mitigation Strategy Technical Mitigation.....	224
Table 4. 58 Mitigation Strategy Non-Technical Mitigation	226