

**DESIGNING A THREAT MODELING-DRIVEN RISK MANAGEMENT  
FRAMEWORK FOR SECURING PT XYZ'S MEDIA CONTENT  
MANAGEMENT SYSTEM**

By

Nicholaus Ola Malun  
22451020

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 25 August, 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.

Nicholaus Ola Malun

\_\_\_\_\_  
Student

\_\_\_\_\_  
Date

Approved by:

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

\_\_\_\_\_  
Thesis Advisor

\_\_\_\_\_  
Date

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

\_\_\_\_\_  
Thesis Co-Advisor

\_\_\_\_\_  
Date

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

\_\_\_\_\_  
Dean

\_\_\_\_\_  
Date

## ABSTRACT

# DESIGNING A THREAT MODELING-DRIVEN RISK MANAGEMENT FRAMEWORK FOR SECURING PT XYZ'S MEDIA CONTENT MANAGEMENT SYSTEM

By

Nicholaus Ola Malun

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

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

SWISS GERMAN UNIVERSITY

This thesis aims to design a threat modelling driven risk management framework to enhance the security of PT XYZ's Content Management System (CMS), which is critical for safeguarding digital assets and ensuring the integrity of media operations. The research employs a combination of STRIDE and LINDDUN methodologies to systematically identify and classify both security and privacy threats across CMS components. Each identified threat is evaluated using the DREAD scoring model to prioritize risks based on their potential impact, reproducibility, exploitability, affected users, and discoverability. The study also conducts a comprehensive vulnerability analysis and security gap assessment to uncover weaknesses aligned with common threat vectors, including those reflected in the OWASP Top 10. Based on these findings, the research proposes a set of mitigation strategies and security controls aligned with ISO/IEC 27001:2022 to ensure both technical and organizational resilience. The findings reveal that PT XYZ's CMS faces critical risks such as credential reuse, token replay attacks, and unauthorized API access, which require immediate mitigation. The practical implication of this thesis is the development of a tailored risk management model that integrates threat modeling into the software development lifecycle (SDLC), enabling PT XYZ to adopt a proactive and structured approach to CMS security.

*Keywords: CMS, STRIDE, LINDDUN, DREAD ISO 27001:2022, OWASP Top 10.*



## DEDICATION

This work is dedicated to enhancing the cybersecurity of PT XYZ specifically, the media industry more broadly, and contributing to academic knowledge.



## ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to all those who have contributed to the completion of this thesis.

First and foremost, I extend my deepest appreciation to Thesis Advisors and all Teacher, whose guidance, support, and insightful feedback have been invaluable throughout this study. Your expertise and encouragement have greatly enriched this research.

I am also grateful to the team at PT. XYZ for their cooperation and willingness to provide the necessary data and insights. Their involvement has been crucial in grounding this research in real-world applications and challenges.

Special thanks to my colleagues and peers who offered their constructive criticism and support during the research process. Your input has been instrumental in shaping the direction and quality of this work.

I would also like to acknowledge the support of PT. XYZ for providing the resources and environment necessary for conducting this research.

Lastly, my heartfelt thanks go to my family and friends for their unwavering support and understanding throughout this journey. Your encouragement has been a source of motivation and strength.

This research is dedicated to improving cybersecurity practices in the media industry and contributing to academic knowledge in this field.

## TABLE OF CONTENTS

|                                                         | Page |
|---------------------------------------------------------|------|
| STATEMENT BY THE AUTHOR .....                           | 2    |
| ABSTRACT .....                                          | 3    |
| DEDICATION .....                                        | 5    |
| ACKNOWLEDGEMENTS .....                                  | 6    |
| TABLE OF CONTENTS .....                                 | 7    |
| LIST OF FIGURES .....                                   | 12   |
| LIST OF TABLES .....                                    | 13   |
| 1.CHAPTER 1 – INTRODUCTION .....                        | 15   |
| 1.1. Background .....                                   | 15   |
| 1.2. Research Problem .....                             | 20   |
| 1.3. Research Objective.....                            | 21   |
| 1.4. Research Question.....                             | 21   |
| 1.5. Hypothesis.....                                    | 22   |
| 1.6. Research Scope and Limitation.....                 | 22   |
| 1.7. Significance of Study .....                        | 23   |
| 1.8. Thesis Structure .....                             | 24   |
| 2.CHAPTER 2 - LITERATURE REVIEW.....                    | 25   |
| 2.1. Media Industry.....                                | 25   |
| 2.2. Media Technology .....                             | 28   |
| 2.3. Content Management System (CMS).....               | 33   |
| 2.3.1. Design CMS Overview.....                         | 35   |
| 2.3.2. System Design CMS.....                           | 35   |
| 2.3.3. The Role of Infrastructure in CMS Operation..... | 36   |
| 2.3.4. Challenge CMS.....                               | 38   |
| 2.4. Risk Management.....                               | 41   |
| 2.4.1. Risk Management Framework.....                   | 42   |
| 2.4.2. Risk Assessment.....                             | 43   |
| 2.4.3. Threat.....                                      | 45   |

|                                                                 |    |
|-----------------------------------------------------------------|----|
| 2.4.4. Vulnerability.....                                       | 46 |
| 2.4.5. Security Gap.....                                        | 47 |
| 2.5. Risk .....                                                 | 48 |
| 2.5.1. Risk Mitigation .....                                    | 50 |
| 2.6. Combine Risk Management and Threat Modeling Framework..... | 52 |
| 2.7. Threat Modeling.....                                       | 54 |
| 2.7.1. Data Flow Diagram.....                                   | 56 |
| 2.7.2. Threat Modeling Approach.....                            | 58 |
| 2.7.2.1. Asset Centric.....                                     | 59 |
| 2.7.2.2. Attacker Centric.....                                  | 59 |
| 2.7.2.3. Software Centric.....                                  | 60 |
| 2.7.2.4. Risk Centric.....                                      | 60 |
| 2.7.3. Threat Modeling Framework.....                           | 60 |
| 2.7.3.1. STRIDE.....                                            | 62 |
| 2.7.3.2. DREAD.....                                             | 63 |
| 2.7.3.3. PASTA.....                                             | 65 |
| 2.7.3.4. Attack tree.....                                       | 67 |
| 2.7.3.5. LINDDUN.....                                           | 68 |
| 2.7.4. Cybersecurity and Privacy Risk Management.....           | 68 |
| 2.7.5. Privacy Threat Modeling and UU PDP.....                  | 70 |
| 2.7.6. Privacy Threat Modeling in CMS.....                      | 72 |
| 2.8. Previous Study.....                                        | 75 |
| 3. CHAPTER 3 – RESEARCH METHODS.....                            | 85 |
| 3.1. Research Design.....                                       | 85 |
| 3.2. Research Framework.....                                    | 86 |
| 3.3.Context Determination.....                                  | 87 |
| 3.3.1. Define the Context.....                                  | 87 |
| 3.4. Data Collection.....                                       | 87 |

|                                                          |     |
|----------------------------------------------------------|-----|
| 3.5. Decompose the Application.....                      | 88  |
| 3.5.1. Identification Asset.....                         | 88  |
| 3.5.2. Data Flow Diagram.....                            | 89  |
| 3.6. Risk Identification.....                            | 89  |
| 3.6.1. Threat Identification.....                        | 89  |
| 3.6.2. Threat Clasification.....                         | 91  |
| 3.6.3.Vulnerability Identification.....                  | 91  |
| 3.6.4.Security Gaps.....                                 | 91  |
| 3.7. Risk Analysis.....                                  | 92  |
| 3.7.1. Threat Analysis.....                              | 92  |
| 3.7.2. Threat Scoring.....                               | 93  |
| 3.7.3. Threat Prioritazion.....                          | 94  |
| 3.9. Determine Countermeasures.....                      | 94  |
| 3.10. Research Evaluation.....                           | 95  |
| 3.11. Research Validation.....                           | 96  |
| 4. CHAPTER 4 – RESULT AND DISCUSSION.....                | 99  |
| 4.1. Introduction.....                                   | 99  |
| 4.2. Preparation Phase.....                              | 99  |
| 4.2.1. Define Objective.....                             | 99  |
| 4.2.1.1 Business Security Goals.....                     | 100 |
| 4.2.1.2. Risk Criteria Stakeholder.....                  | 101 |
| 4.3.Data Collection. ....                                | 103 |
| 4.3.1.Decompose Application.....                         | 104 |
| 4.3.2..Identification Component and Critical Asset.....  | 104 |
| 4.3.3. Data Flow Diagram.....                            | 105 |
| 4.3.3.1.Data Flow News Input Process. ....               | 107 |
| 4.3.3.2.Data Flow Stream News to Platform Proccess. .... | 111 |
| 4.3.4.Entry Point and Trust Level .....                  | 115 |

|                                                                               |     |
|-------------------------------------------------------------------------------|-----|
| 4.4.Risk Identification.....                                                  | 118 |
| 4.4.1.Threat Modeling.....                                                    | 118 |
| 4.4.1.1.Mapping Threat STRIDE Input News Process. ....                        | 119 |
| 4.4.1.2.Mapping Threat STRIDE Stream News to Platform. ....                   | 120 |
| 4.4.2.Privacy Threat Modeling. ....                                           | 122 |
| 4.4.2.1.Mapping Threat LINDDUN Input News Process. ....                       | 123 |
| 4.4.2.2.Mapping Threat LINDDUN Stream News to Platform.....                   | 124 |
| 4.3.Vulnerability Analysis. ....                                              | 125 |
| 4.4.Security Gap Analysis.....                                                | 130 |
| 4.5.Risk Analysis.....                                                        | 136 |
| 4.5.1.Threat Scoring.....                                                     | 137 |
| 4.5.2.Threat Prioritazion .....                                               | 139 |
| 4.6.Determine Countermeasures.....                                            | 141 |
| 4.6.1 Technical Mitigation. ....                                              | 142 |
| 4.6.2 Non Technical Mitigation. ....                                          | 143 |
| 4.7.Research Evaluation.....                                                  | 144 |
| 4.8.Research Validation.....                                                  | 145 |
| 4.9.Research Discussion.....                                                  | 147 |
| 5.CHAPTER 5. CONCLUSION AND RECOMENDATIONS.....                               | 150 |
| 5.1.Conclusion.....                                                           | 150 |
| 5.2.Recomendations.....                                                       | 151 |
| 5.3.Future Works. ....                                                        | 153 |
| 6. REFERENCES.....                                                            | 194 |
| 7.APPENDICES.....                                                             | 155 |
| 8.Appendix 1 : List of Threat Information.....                                | 155 |
| 9.Appendix 2:News Input Threat Detail – STRIDE Category.....                  | 155 |
| 10.Appendix 3:News Input Threat Detail – LINDDUN Category.....                | 163 |
| 11.Appendix 4: News Input Threat Detail – DREAD Scoring.....                  | 166 |
| 12.Appendix 5 : Stream New to Production Threat Detail – STRIDE Category..... | 167 |

|                                                                                |     |
|--------------------------------------------------------------------------------|-----|
| 13.Appendix 6 : Stream New to Production Threat Detail – LINDDUN Category..... | 177 |
| 14.Appendix 7 : Stream News to Production Threat Detail – DREAD Scoring.....   | 181 |
| 15.Appendix 8 : Expert Profile and Questionnaire Answer.....                   | 182 |
| 16.Appendix 9 : Software Development Expert Questionnaire Answer[1].....       | 182 |
| 17.Appendix 10 : Cybersecurity Expert Questionnaire Answer[2].....             | 183 |
| 17.Appendix 11 : Cybersecurity Expert Questionnaire Answer[3].....             | 184 |
| 17.Appendix 12 : Cybersecurity Expert Questionnaire Answer[4].....             | 185 |
| 18.Appendix 13 : Documentation of FGD Process.....                             | 187 |
| 19.Appendix 14 : Documentation of FGD Evaluation with Stakeholder.....         | 187 |
| 20.Appendix 15 : Documentation of Cybersecurity Expert Interview.....          | 188 |
| 21.Appendix 16 : Error log (deactivated service) .....                         | 189 |
| 22.Appendix 17 : Login Failed log.....                                         | 190 |
| 23.Curriculum Vitae.....                                                       | 204 |



## LIST OF FIGURES

| Figures                                                                  | Page |
|--------------------------------------------------------------------------|------|
| 1.1. Distribution of Industries Attacked by DDoS Attack. (NSFOCUS, 2024) | 16   |
| 1.2. Research Fishbone Diagram.                                          | 20   |
| 2.1. Newsroom 3.0 Model ( Indrati,2018).                                 | 32   |
| 2.2. System Architecture CMS Newsbox                                     | 36   |
| 2.2. Network Architecture CMS Newsbox.                                   | 38   |
| 2.3. NIST SP 800-30 Rev1 Framework.( NIST,2018)                          | 44   |
| 2.4. OWASP Top 10 List 2021.(Tudela et al., 2020)                        | 52   |
| 2.5. Threat Model Process. (Shostack, 2014)                              | 54   |
| 2.6. DREAD Threat Modeling.(Newke et al, 2020)                           | 64   |
| 2.7. PASTA Threat Model.( Ucedaveles et al, 2014 )                       | 66   |
| 2.8. Attack Tree Threat Model example ( Buldas et al,2020)               | 67   |
| 2.9. LINDDUN Steps.( Shotack,2014)                                       | 68   |
| 2.10. Cybersecurity and Privacy Risk Relationship.(NIST,2020)            | 69   |
| 3.1. Research Design.( Hevner et al. (2004)                              | 85   |
| 3.2. Research Framework.                                                 | 86   |
| 4.1. Architecture Diagram of CMS                                         | 103  |
| 4.2. Data Flow Diagram Level 0 CMS                                       | 106  |
| 4.3. Data Flow Diagram Level 1 News Input Process.                       | 107  |
| 4.4. Data Flow Diagram Level 1 Stream News to Platform Process.          | 111  |
| 4.5. Data Flow Diagram Trust Level and Entry Point                       | 116  |
| 4.6. Data Flow Diagram Level 0 for Privacy, News Input and Edit Process. | 122  |
| 4.7. Data Flow Diagram Level 1 for News Input, and Stream to Production. | 123  |

---

**LIST OF TABLES**

| Table                                                                                       | Page |
|---------------------------------------------------------------------------------------------|------|
| 2.1. Comparative mapping RMF to Threat Model.                                               | 53   |
| 2.2. Summary Threat Modeling Step.                                                          | 56   |
| 2.3. Level of Data Flow Diagram. ( Shotack,2014)                                            | 57   |
| 2.4. Comparison Threat Model.( Shotack,2014 )                                               | 61   |
| 2.5. STRIDE Modeling.                                                                       | 63   |
| 2.6. Security Related Threat Modeling Framework for Risk Evaluation.<br>( Erbas,et al,2024) | 71   |
| 2.7. Comparison Table of Threat Modeling Models for Privacy in CMS.                         | 73   |
| 2.8. Security Related Threat Modeling Framework for Risk Evaluation                         | 77   |
| 2.9. Summarizes the comparison of other related studies.                                    | 78   |
| 3.1. Misuse Case Form                                                                       | 90   |
| 3.2. Criteria DREAD of CMS (Security/OSSA Metric)                                           | 93   |
| 3.3. Topic Form for Evaluation Stakeholder PT XYZ                                           | 95   |
| 3.4. Question Form Validation.                                                              | 97   |
| 4.1. Business Security Goals for CMS journalist.                                            | 100  |
| 4.2. Condition Category Current Security of CMS                                             | 101  |
| 4.3. Component CMS                                                                          | 104  |
| 4.4.Mapping Asset Taxonomy News Input Process.                                              | 108  |
| 4.5.Journalist News Input Process.                                                          | 109  |

|                                                                   |     |
|-------------------------------------------------------------------|-----|
| 4.6. News Input Process Detail.                                   | 110 |
| 4.7. List of Assets on Stream News to Platform Process.           | 111 |
| 4.8. Stream News to Production Process.                           | 113 |
| 4.9. Stream News to Platform Process Detail                       | 114 |
| 4.10. Entry Point of CMS                                          | 116 |
| 4.11. Trust Level of CMS                                          | 117 |
| 4.12. RBAC Users of CMS                                           | 117 |
| 4.13. STRIDE Input News Process                                   | 119 |
| 4.14. STRIDE Stream News to Production Process                    | 120 |
| 4.15. DFD Element for Privacy                                     | 122 |
| 4.16. Threat Model News Input to LINDDUN for Input News Process   | 123 |
| 4.17. Threat Model News Input to LINDDUN for Input News Process   | 124 |
| 4.18. Mapping Threat and Vulnerability Input News Process.        | 125 |
| 4.19. Mapping Threat and Vulnerability Stream News to Production. | 127 |
| 4.20. Security Gaps on Input News Process.                        | 130 |
| 4.21. Security Gap on Stream News to Platform Process.            | 132 |
| 4.22. Table Risk Scoring Input News Process.                      | 137 |
| 4.23. Mapping Threat Stream News to Production.                   | 138 |
| 4.24. Threat Prioritization Input News Process                    | 139 |
| 4.25. Threat Prioritization Stream News to Production.            | 140 |
| 4.26. Recommendation Mitigation By OWASP Top 10                   | 142 |
| 4.27. Recommendation Mitigation By ISO 27001:2022                 | 143 |