

**IMPROVING SOC DETECTION CAPABILITY USING MITRE ATT&CK
FRAMEWORK AND RISK DRIVEN APPROACH: A CASE STUDY IN XYZ
ORGANIZATION**

By

Adi Nugroho
22351033

MASTER'S DEGREE
in

Magister of Information Technology
Digital Innovation



SWISS GERMAN UNIVERSITY
The Prominence Tower
Jalan Jalur Sutera Barat No. 15, Alam Sutera
Tangerang, Banten 15143 - Indonesia

Januari 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.

Adi Nugroho



Student

20/01/2025

Date

Approved by:

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



Thesis Advisor

20/01/2025

Date

Dr. Ir. Heru P. Ipung, M.Eng.



Thesis Co-Advisor

20/01/2025

Date

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

Dean

Date

Adi Nugroho

ABSTRACT

IMPROVING SOC DETECTION CAPABILITY USING MITRE ATT&CK FRAMEWORK AND RISK DRIVEN APPROACH: A CASE STUDY IN XYZ ORGANIZATION

By

Adi Nugroho

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

Dr. Ir. Heru Purnomo Ipung, M.Eng., Co-Advisor

SWISS GERMAN UNIVERSITY

The Security Operations Center (SOC) is crucial for organizations to ensure operational continuity and security amidst rapidly evolving threats. However, SOC's often develop detection capabilities without a clear direction, which can lead to ineffectiveness. This research aims to create a process model for enhancing SOC detection capabilities, aligning them with organizational goals, relevant risks and adaptive to evolving threat. The study reviews existing detection approaches and employs the MITRE ATT&CK Top 10 framework, and threat intelligent information based on relevant factor to identify pertinent threats. Both hands-off and hands-on methods employed to analyze and validate detection gaps in the SOC. Additionally, the research adopts a case study approach, applying the proposed process model to the XYZ organization. The model was validated through a qualitative approach that included interviews with experts in the SOC field, complemented by surveys to enhance the reliability of the findings. The research findings show that experts agree the proposed process model helps aligns SOC detection capabilities with organizational goals, helps identify relevant threats, and promotes the development of focused SOC detection capabilities.

Keywords: Security Operation Center, SOC, Detection, MITRE ATT&CK

© Copyright 2025
by Adi Nugroho
All rights reserved

DEDICATION

I dedicate this works for the future of the country I loved: Indonesia

ACKNOWLEDGEMENTS

I would like to express my heartfelt gratitude to all those who contributed to the successful completion of this thesis. Their guidance, support, and encouragement have been invaluable throughout this journey. First and foremost, I extend my deepest thanks to my academic advisor, Dr. Ir. Charles Lim, B.Sc, M.Sc. and co-advisor Dr. Ir. Heru Purnomo Ipung, M.Eng. for their unwavering support, insightful guidance, and constructive feedback. Their expertise and encouragement have been instrumental in shaping the direction and quality of my work.

I am also profoundly grateful to the faculty and staff of Swiss German University whose resources, facilities, and expertise have provided a solid foundation for my research. Special thanks to Dr. Eka Budiarto, Pak Putu Indra, for their mentorship and valuable advice.

I wish to acknowledge the contributions of my peers and colleagues (Agung Setiaji, Jodie Prasetyo, Megi Paramitha Putra, Digit Oktavianto, Wahyu Nuryanto, Firza Ramadhan, Sida Nala, Rizky Rionaldo, Khairil), who have offered their perspectives, shared knowledge, and collaborated with me during challenging moments. Your camaraderie and support have enriched my academic experience.

To my family and friends, I owe a debt of gratitude for their unwavering encouragement, patience, and belief in me. Your love and support have been my anchor through the ups and downs of this journey.

This thesis is a culmination of collective efforts, and I am deeply thankful to everyone who played a part in its completion.

TABLE OF CONTENTS

	Page
DEDICATION	5
ACKNOWLEDGEMENTS	6
TABLE OF CONTENTS	7
LIST OF FIGURES	11
LIST OF TABLES	13
CHAPTER 1 - INTRODUCTION	17
1.1 Background	17
1.2 Research Problem	20
1.3 Research Objectives	23
1.4 Research Questions	24
1.5 Hypothesis	24
1.6 Significance of Study	25
1.7 Scope and Limitations	25
1.8 Thesis Structure	26
CHAPTER 2 - LITERATURE REVIEW	27
2.1 Understanding of Security Operation Center (SOC)	27
2.1.1 Definition	27
2.1.2 SOC Function or Services	28
2.1.3 Challenge Faced by SOC	29
2.1.4 SOC Performance Metrics	31
2.1.5 SOC Success Factor	33
2.2 Alignment SOC with Business	34
2.2.1 COBIT 2019	37
2.3 SOC Detection Capabilities	39
2.3.1 Threat Detection Definition	39
2.3.2 Threat Detection Maturity Framework	40
2.3.3 SOC Threat Detection Capability According to SOC-CMM	46
2.3.4 SOC Threat Detection Capability	48

2.4 Security Operation Center of XYZ's Organization	50
2.4.1 SOC XYZ Organization Detection Capability	52
2.5 Cyber Threat Intelligence	53
2.5.1 Reputation of Cyber Threat Intelligence Information	54
2.5.2 Quality of Cyber Threat Intelligence Information	55
2.5.3 Identify Relevant Cyber Threat Intelligence Information.....	57
2.6 Risk Management	59
2.6.1 NIST Risk Management Framework	60
2.7 MITRE ATT&CK.....	62
2.7.1 Introduction to MITRE ATT&CK Framework	62
2.7.2 MITRE ATT&CK Structure	63
2.7.3 MITRE ATT&CK Framework Implementation in Detection Gap Analysis.....	64
2.7.4 MITRE ATT&CK Top 10	65
2.8 Threat Modeling.....	67
2.8.1 STRIDE.....	67
2.8.2 PASTA (Process for Attack Simulation and Threat Analysis).....	69
2.8.3 Attack Trees	71
2.8.4 Comparison of Threat Modeling Methods.....	72
2.9 Design Interview Question	74
2.10 Process Modelling Success (PMS) Framework.....	75
2.11 Related Works.....	77
2.12 Process Model Proposed Development and Design Rational.....	85
2.13 Comparison Proposed Model with other Detection Strategy Approach.....	113
CHAPTER 3 – RESEARCH METHODS	116
3.1 Introduction.....	116
3.2 Adopted Research Framework.....	116
3.3 Validation and testing of proposed Process Model.....	118
3.3.1 Measuring Success with Process Modelling Success Framework.....	119
3.3.2 Measuring Success with Quantitative Approach	120
3.3.3 Validation Methodology	122
3.3.4 Testing the Proposed Model in XYZ Organization	130
CHAPTER 4 – UNDERSTANDING PROBLEM IN SOC (SECURITY OPERATION CENTER).....	132
4.1 Building Block of SOC.....	132

4.2 Understanding SOC Problems	133
4.3 Method	134
4.3.1 Database	134
4.3.2 Search String	134
4.3.3 Screen and Filtering	135
4.4 Results	136
4.4.1 SOC Problems – People Perspective	136
4.4.2 SOC Problems – Process Perspective	145
4.4.3 SOC Problems – Technology Perspective	164
4.5 Interconnected of SOC Problems and The Importance of SOC Detection Improvement	176
CHAPTER 5 – SOC DESIGN FRAMEWORK, AND COMPLETENESS CRITERIA OF SOC	179
5.1 Background Problem	179
5.2 Objectives	180
5.3 Scope and Limitation	180
5.4 Comparative Study of Existing SOC Design/Building Framework	181
5.4.1 SOC Main Function	189
5.4.2 SOC Maturity Framework Comparison	191
5.5 Design Proposed SOC Completeness Criteria	194
5.5.1 Identification of SOC Problems & Framework Domain	194
5.5.2 Dimension Identification	209
5.5.3 Proposed Completeness Criteria of SOC based on Regulation and Best Practices	215
5.6 Validation of Proposed SOC Completeness Criteria	235
5.6.1 Domain Business & Governance	236
5.6.2 Domain People	241
5.6.3 Domain Process	246
5.6.4 Domain Technology	251
5.7 Relevant Proposed SOC Completeness Criteria to Development of Proposed Process Model	255
5.7.1 Assesment Model and Scoring	255
5.7.2 Self Assesment Results	258
CHAPTER 6 – RESULTS AND DISCUSSION	260
6.1 Process Model Implementation in XYZ Organization	260

6.1.1 Understanding Business Context - SOC Alignment with Business Goals	260
6.1.2 Scope and assets definition	274
6.1.3 Risk Identification.....	275
6.1.4 Gap Assessment.....	284
6.1.5 Detection Strategy.....	311
6.1.6 Implement Detection Strategy	313
6.1.7 Testing.....	314
6.2 Validation of Proposed Process Model.....	316
6.2.1 Expert Review Results	316
6.2.2 Survey Results on Proposed Process Model.....	325
6.2.3 User Feedback Results	336
6.3 Discussion	342
6.3.1 Identification of parties involved in the proposed process model	342
6.3.2 Relevant Threat Identification	346
6.3.3 Agility of the proposed Process Model.....	346
6.3.4 Cybersecurity Trend Reports as Baseline Detection	347
6.3.5 Hands-on Gap Analysis Recommendation	348
6.4 Proposed Process Model Improvement	349
CHAPTER 7 – CONCLUSION.....	352
7.1 Conclusion	352
7.2 Future Works and Recommendations	354

LIST OF FIGURES

Figures	Page
Figure 1.1 Top Challenge in SOC (Schulze, 2022)	18
Figure 1.2. Fishbone Diagram of Ineffective SOC	21
Figure 2.1. People, Process, Technology, Governance and Compliance Framework (Vielberth, 2021)	28
Figure 2.2 SOC Value Chain Mapping (Huggins, 2016).....	35
Figure 2.3 Goal Cascading Process in COBIT 2019 (ISACA, 2018b).....	39
Figure 2.4 Detection Maturity Level (Stillions, 2014)	41
Figure 2.5 Maritime Cyber Threats Detection Framework (Potamos and Stavrou, 2022)	42
Figure 2.6. Detection Engineering Phase (Orchilles, 2022)	47
Figure 2.7. MITRE ATT&CK Framework (image source: (Palo Alto Network, 2023))	62
Figure 2.8. Example of Chokepoint T1055 Process Injection (MITRE, 2024b).....	66
Figure 2.9. PASTA Threat Modeling Stages	69
Figure 2.10 Attack Tree Illustrated (Schneier, 1999)	71
Figure 2.11 Process Model Success Framework (Sedera et al., 2002)	76
Figure 2.12. Proposed Model SOC Detection Improvement	88
Figure 2.13. COBIT2019 Goal Cascading Process (Anoruo, 2019).....	90
Figure 2.14 Detection Capability Development Priority based on Kill Chain Phase (Sutherland, 2018).....	108
Figure 3.1. Research Framework of Detection Process Model Development	117
Figure 3.2 Process Modelling Success Measurement Framework (Sedera et al., 2002)	119
Figure 5.1. Interconnected Problem in SOC	196
Figure 5.2. SOC Framework Building Blocks	200
Figure 5.3 Proposed Business & Governance Dimensions	209
Figure 5.4 Proposed of People Dimension	211
Figure 5.5 Proposed of Process Dimension	212
Figure 5.6 Proposed of Technology Dimension	214
Figure 5.7 Capability Level in COBIT2019 (ISACA, 2018b).....	257
Figure 6.1 Process Map of the Relationship between Main, Supporting, and Management Processes	262
Figure 6.2 Mapping Enterprise Goals to Alignment Goals using COBIT2019 Framework	268
Figure 6.3 Asset Decomposition of AP.01 Service and Information Portal Application	276

Figure 6.4 Threat Identification of AP.01 Service and Information Portal Application	277
Figure 6.5 TTP Brain Cipher Ransomware (Peris.ai, 2024; SOCRadar, 2024; Vectra, 2024a)	279
Figure 6.6 Network Security Monitoring Detection Coverage.....	289
Figure 6.7 Detetction Capability Gap Analysis on TID.001 – Brain Cipher Ransomware.....	293
Figure 6.8 Detetction Capability Gap Identified on TID.002 – APT Mustang Panda	296
Figure 6.9 Emulation Environment Network Topology	300
Figure 6.10 Brain Cipher Emulation Scenario.....	301
Figure 6.11 Emulation Process of Brain Cipher using Atomic Red Team Tools.....	303
Figure 6.12 Emulation Process of Mustang Panda using Atomic Red Team Tools..	305
Figure 6.13 Security event recorded on the detection system related to TTP T1218.005	309
Figure 6.14 Avctivation of Detection Rules for T1218.005	313
Figure 6.15. Sysmon Configuration in the Windows Machine	314
Figure 6.16 Deetction Results of Retesting on TTP1218.005	315
Figure 6.17 Detection Results of Retesting on TTP1218.005 on Wazuh Detection .	315
Figure 6.18 Type of Respondent Organization.....	325
Figure 6.19 Year of Respondent Experience in SOC	326
Figure 6.20 Improvement of Proposed Process Model according to Expert and User Feedback	350

LIST OF TABLES

Table	Page
Table 2.1. Functional/Services of SOC.....	28
Table 2.2 Maturity Criteria of Process in Threat Detection Maturity Framework (Dost, 2022)	42
Table 2.3 Maturity Criteria of Data, Tools and Category in Threat Detection Maturity Framework (Dost, 2022)	43
Table 2.4 Maturity Criteria of Capabilities Category in Threat Detection Maturity Framework (Dost, 2022)	44
Table 2.5 Maturity Criteria of Coverage Category in Threat Detection Maturity Framework (Dost, 2022)	44
Table 2.6 Maturity Criteria of People Category in Threat Detection Maturity Framework (Dost, 2022)	45
Table 2.7 Detection Capability according to SOC-CMM	48
Table 2.8 Current Detection Capability of XYZ Organization SOC.....	52
Table 2.9 Reputation Criteria of Cyber Threat Intelligence Feeds.....	54
Table 2.10 STRIDE Threat Modeling Description (Naik et al., 2024b, 2024a).....	68
Table 2.11 Comparison of Threat Modeling Methods (Shevchenko et al., 2018b).....	73
Table 2.12. Threat Driven Approach to Cybersecurity (Muckin and Fitch, 2019).....	80
Table 2.13. Comparison of Existing SOC Detection Strategy.....	82
Table 2.14 Scope definition of improving SOC detection.....	91
Table 2.15 Example of Scope definition of improving SOC detection	92
Table 2.16 PASTA Framework adoption in Risk Identification Stage	92
Table 2.17 Assesst/Application Decomposition Process	94
Table 2.18 Example of Asset Decomposition.....	95
Table 2.19 Threat Model Identification Form	95
Table 2.20 Example of Threat Model Identification Form.....	96
Table 2.21 Relevant Threat/Incident to Organization.....	98
Table 2.22 Example Implementation of Identification Relevant Threat/Incident to Organization.....	99
Table 2.23 Identification Risk Relevant to the organization assets	102
Table 2.24 Example of Identification Risk Relevant to the organization assets.....	103
Table 2.25 Mapping Organization Asset Component to MITRE ATT&CK Top 10 Relevant Threat	103
Table 2.26 Illustration of Mapping Organization Asset Component to MITRE ATT&CK Top 10 Relevant Threat	104
Table 2.27. Gap Assessment based on existing technology capability.....	105
Table 2.28 Example of Gap Assessment based on existing technology capability ...	106

Table 2.29 Proposed Process Model Activity Mapping	110
Table 2.30 Comparison of Proposed Model to Develop SOC Detection Capability with other approach.....	114
Table 3.1. Knowledge Resources Nomination Worksheet	123
Table 3.2 Mapping of Aspect PMS Framework to Item Questions.....	126
Table 3.3. Success Criteria of Proposed Process Model.....	129
Table 4.1 Topics Identified in SOC Domain according to (Vielberth et al., 2020)...	133
Table 4.2 Search queries employed to conduct paper/journal searches on databases	134
Table 4.3 Screen and Filtering Protocol	135
Table 4.4 SOC Problem – People Perspective.....	136
Table 4.5 SOC Problem in People Perspective Mapping to Topics in People Domain	139
Table 4.6 SOC Analyst Metric (Enoch Agyepong et al., 2020; Chamkar et al., 2023; Forsberg and Frantti, 2023).....	140
Table 4.7 SOC Problem in Process Domain According to Several Studies	147
Table 4.8 SOC Problem Identification According to Several Studies.....	148
Table 4.9 SOC Problem in Technology Domain According to Several Studies	164
Table 4.10 SOC Problem in Technology Domain – Related to Detection Technology Porblem.....	167
Table 4.11 Technology Selection Problem – SOC Problem in Technology Domain	172
Table 4.12 Operational Problem of SOC Technology – SOC Problem in Technology Domain.....	173
Table 4.13 Data Source Quality Problem – SOC Problem in Technology Domain..	175
Table 5.1. Existing SOC Framework Comparison	182
Table 5.2. SOC Main Function according To Existing Framework	190
Table 5.3. Comparison of Domain and Aspects of SOC-CMM (Van Os, 2016) vs SOC-MF.....	192
Table 5.4. List of Identified SOC Problem	194
Table 5.5. SOC Framework Component based on Existing Framework.....	198
Table 5.6 Proposed SOC Framework Component – Business & Governance Domain	202
Table 5.7 Proposed SOC Framework Component – People Domain.....	203
Table 5.8 Proposed SOC Framework Component – Process Domain.....	204
Table 5.9 Proposed SOC Framework Component – Technology Domain.....	206
Table 5.10 SOC completeness Criteria Component (Domain and Dimension)	208
Table 5.11 Completeness Criteria related to SOC in the Business and Governance Domain according Regulation, Standard and Best Practices.....	217
Table 5.12 Completeness Criteria related to SOC in the People Domain according Regulationns, Standard and Best Practices	220
Table 5.13 Completeness Criteria related to SOC in the Process Domain according Regulations, Standard and Best Practices	225
Table 5.14 Completeness Criteria related to SOC in the Technology Domain according Regulationns, Standard and Best Practices	231
Table 5.15 Expert Profile Involved in The Validation Process	235
Table 5.16 Aspect to be Considered in Planning, Strategy & Governance Dimension according to Expert Review	239

Table 5.17 Aspect to be Considered in Measurement & Evaluation Dimension according to Expert Review	240
Table 5.18 Aspect to be Considered in Human Resource Management Dimension according to Expert Review	241
Table 5.19 Aspect to be Considered in SOC Role and Responsibility Dimension according to Expert Review	243
Table 5.20 Aspect to be Considered in Career Progression Dimension according to Expert Review	243
Table 5.21 Aspect to be Considered in Knowledge Management Dimension according to Expert Review	245
Table 5.22 Aspect to be Considered in SOC Analyst Performance Evaluation Dimension according to Expert Review	246
Table 5.23 Aspect to be Considered in Event Log Collection and Management Dimension according to Expert Review	247
Table 5.24 Aspect to be Considered in Event Monitoring and Analysis Dimension according to Expert Review	248
Table 5.25 Aspect to be Considered in Incident Management Dimension according to Expert Review	249
Table 5.26 Aspect to be Considered in Detection Engineering and Validation Dimension according to Expert Review	250
Table 5.27 Aspect to be Considered in Reporting, Visualization and Communication Dimension according to Expert Review	251
Table 5.28 Aspect to be Considered in Core Component Technology Dimension according to Expert Review	252
Table 5.29 Aspect to be Considered in Supporting Technology Dimension according to Expert Review	253
Table 5.30 Aspect to be Considered in Operation Dimension according to Expert Review	254
Table 5.31 Detection Engineering and Validation Dimension in Process Domain ...	256
Table 5.32 Self Assessment of Detection Engineering and Validation of SOC XYZ Organization	258
Table 6.1 Stakeholder Identification of XYZ Organization	264
Table 6.2 Stakeholders Needs Identification	265
Table 6.3 XYZ Organization Mission & Strategic Mapping to Enterprise Goals based on COBIT 2019	266
Table 6.4 Enterprises Goals to Alignment Goals Result	268
Table 6.5 Alignment Goals Identification	269
Table 6.6 Risk Impact Criteria	270
Table 6.7 Risk Probability Criteria	270
Table 6.8 Risk Analysis Matrix of XYZ Organization	271
Table 6.9 Risk Value Range	271
Table 6.10 Identification Adversarial Risk to XYZ Organization	273
Table 6.11 Scope Definition in SOC Detection Improvement Process	274
Table 6.12 Asset Decomposition of XYZ Organization	276
Table 6.13 Identification of Possible Threat Scenario based on Threat Identification using STRIDE-LM	278

Table 6.14 TTP Brain Cipher Ransomware (Peris.ai, 2024; SOCRadar, 2024; Vectra, 2024a)	280
Table 6.15 TTP Mustang Panda (MITRE ATT&CK, 2021; Nurfauzi, 2022).....	281
Table 6.16 Threat and History of Incident Relevant to XYZ Organization	281
Table 6.17 Risk Identification of Asset Component.....	282
Table 6.18 Identification of MITRE ATT&CK 10 Relevant to XYZ Organization .	283
Table 6.19 Relevant MITRE ATT&CK Top 10 to Web Application Server Assets	284
Table 6.20 XYZ Organization Web Firewall Detection Coverage (Exabeam, 2024)	285
Table 6.21 XYZ Organization Firewall Detection Coverage (Black Cell, 2023; Exabeam, 2024)	286
Table 6.22 MITRE ATT&CK Coverage Endpoint Detection Response of XYZ Organization.....	286
Table 6.23 Network Detection Response MITRE ATT&CK Coverage	287
Table 6.24 Detection Coverage of Detection Technology against TID.001 – Brain Cipher Ransomware	292
Table 6.25 Detection Coverage of Detection Technology against TID.002 – Mustang Panda	295
Table 6.26 Detection Coverage of Relevant Threat.....	297
Table 6.27 MITRE ATT&CK Top 10 Technique	297
Table 6.28 Detection Coverage Summary	298
Table 6.29 Brain Cipher Ransomware Emulation Scenario	302
Table 6.30 Brain Cipher Threat Emulation Result	304
Table 6.31 Mustang Panda Ransomware Emulation Scenario	306
Table 6.32 Emulation Scenario and Emulation Result for APT Mustang Panda	309
Table 6.33 MITRE ATT&CK Top 10 Relevant to Asset Within Scope	310
Table 6.34 Emulation Result for MITRE ATT&CK Top 10 Relevant to Asset	310
Table 6.35 Detetcion Gap Identified from Emulation Process	312
Table 6.36 Detection Coverage of Relevant Threat based on Hands-on	313
Table 6.37 Detection Rules based on Source Process Creation using mshta.exe and Command Execute using mshta.exe	313
Table 6.38 Summary of SOC Expert Profile involved in the Validation Process	316
Table 6.39 Summary of Survey Results of Expert Opinion on Proposed Process Model	326
Table 6.40 Summary of Survey Results of Expert Opinion on Proposed Process Model based on Process Model Success Framework	331
Table 6.41 Results of Expert Opinion on Proposed Process Model based on Process Model Success Framework	335
Table 6.42 Estimated time required to run the proposed process based on user feedback	339
Table 6.43 Identification of Relevant Stakeholder involved in the Process Model Implementation	344
Table 6.44 Identification of Relevant Threat using Relevant Factor	346