
CONTENTS

APPROVAL	ii
SELF DECLARATION AGAINST PLAGIARISM	iii
ABSTRACT	iv
ABSTRAK	v
DEDICATION	vi
ACKNOWLEDGMENTS	vii
PREFACE	viii
CONTENTS	ix
LIST OF TABLES	xv
LIST OF FIGURES	xvi
LIST OF TERMS	xvii
1 INTRODUCTION	1
1.1 Motivation	1
1.2 Research Problem	2
1.3 Research Objectives	2
1.4 Research Questions	3
1.5 Research Scope	3
1.6 Research Approach	4
1.7 Ethical Considerations	5
1.8 Research Contributions	5
1.9 Thesis Structure	5
2 LITERATURE REVIEW	8
2.1 Introduction	8
2.2 Cybersecurity Threat Landscape in the Public Sector	8
2.3 The Role and Architecture of Security Operations Centers (SOCs)	10
2.4 Modular and Tier-Based Models in Cybersecurity	11
2.5 Cybersecurity Frameworks for Public-Sector SOC's	12
2.6 Design Science Research (DSR) in Cybersecurity and Digital Forensics	14
2.7 Research Gap Identification	15

2.8	Chapter Summary	15
3	RESEARCH METHODOLOGY	17
3.1	Introduction	17
3.2	Research Design and Methodological Approach	17
3.3	DSR Framework and Research Stages	18
3.3.1	Problem Explication	18
3.3.2	Requirement Definition	18
3.3.3	Artefact Design (SOC Model v0.1)	19
3.3.4	Expert Validation (SOC Model v0.2)	19
3.3.5	Demonstration (Use-Case Simulation)	19
3.3.6	Evaluation and Refinement (Final SOC Model v1.0)	19
3.4	Data Collection Methods	20
3.4.1	Systematic Literature Review	21
3.4.2	Expert Interviews	21
3.4.3	Demonstration Observation	21
3.4.4	Evaluation Instruments	21
3.4.5	Instrument Summary	21
3.5	Sampling and Participant Criteria	22
3.5.1	Expert Validation Participants	22
3.5.2	Demonstration and Evaluation Participants	22
3.5.3	Consent and Ethical Compliance	23
3.6	Data Analysis and Model Evaluation Techniques	23
3.6.1	Literature Analysis	23
3.6.2	Expert Feedback Analysis	23
3.6.3	Observational Analysis	24
3.6.4	Evaluation Analysis	24
3.6.5	Triangulation and Rigor	24
3.6.6	Evaluation Metrics for Research Objectives	24
3.7	Ethical Considerations	26
3.7.1	Informed Consent and Voluntariness	26
3.7.2	Confidentiality and Anonymization	26
3.7.3	Use of Institutional Data	26
3.7.4	Ethical Oversight and Integrity	26
3.8	Limitations of the Methodology	27
3.8.1	Limited Sample Size	27
3.8.2	Single Demonstration Context	27
3.8.3	Simulation-Based Evaluation	27
3.8.4	Framework Dependence	27
3.8.5	Researcher Involvement	28

3.9	Chapter Summary	28
4	RESULTS AND ANALYSIS	29
4.1	Introduction	29
4.2	Results of the Problem Explication Stage	29
4.2.1	Cybersecurity Challenges in the Public Sector	30
4.2.2	Limitations of Existing Frameworks and Maturity Models	31
4.2.3	Problem Framing	31
4.3	Results of the Requirements Definition Stage	32
4.3.1	RQ1: Cybersecurity Threat Profiles in Government	32
4.3.1.1	Article Selection and Theme Development for RQ1	33
4.3.1.2	Justification for the Multidimensional Thematic Framework	34
4.3.1.3	Thematic Findings and Interpretation	35
4.3.1.4	Cyber Threat Typologies	35
4.3.1.5	Comparative Analysis with Previous Studies and National Data	39
4.3.1.5.1	Comparison with Humayun et al. (2020)	39
4.3.1.5.2	Alignment with National Data from BSSN	40
4.3.1.5.3	Synthesis	41
4.3.1.6	Institutional and Structural Limitations	42
4.3.1.7	Proposed Mitigation Strategies	43
4.3.1.8	Synthesis for SOC Design	44
4.3.2	RQ2: component for Design of an Effective SOC	45
4.3.2.1	Article Selection and Theme Development for RQ2	45
4.3.2.2	Justification for the Multidimensional Thematic Framework	46
4.3.2.3	Thematic Findings and Interpretation	48
4.3.2.4	Comparative Mapping with Existing SOC Models	53
4.3.2.5	Synthesis of SOC Design component	55
4.4	Artifact Design: Modular and Tier-Based SOC Model v0.1	56
4.4.1	Design Methodology and Rationale	56
4.4.1.1	Threat-to-Module Mapping Based on MITRE ATT&CK	56
4.4.1.1.1	Threat Typology Classification	57
4.4.1.1.2	Mapping to SOC Functional Modules	57
4.4.1.2	SOC Design component and Functional Modules from The- matic Analysis	58
4.4.1.2.1	SOC Design components	58
4.4.1.2.2	SOC Functional Modules	58
4.4.1.2.3	Alignment with NIST Cybersecurity Framework	60
4.4.1.2.4	Design Implication	60

4.4.1.3	Regulatory and Operational Constraints in Indonesian Government Institutions	60
4.4.2	Structure of SOC Model v0.1	61
4.4.2.1	Modular components	62
4.4.2.2	Capability-Based Tiering	62
4.4.2.3	Standards Alignment	62
4.4.2.4	Implementation Flexibility	62
4.4.2.5	Design Summary	63
4.4.3	Design Principles	63
4.4.3.1	Modularity	64
4.4.3.2	Scalability	64
4.4.3.3	Capability-Based Tiering	64
4.4.3.4	Standards Alignment	64
4.4.3.5	Technology Neutrality	64
4.4.3.6	Delegation and Inter-agency Collaboration	64
4.4.3.7	Proportionality	64
4.4.4	Considerations for Storage and Outsourcing	65
4.4.5	Synthesis and Response to RQ3	65
4.5	Results from Expert Validation and Refinement (SOC Model v0.2)	66
4.5.1	Validation Method and Participants	66
4.5.1.1	Methodology	66
4.5.1.2	Participants	67
4.5.2	Validation Instrument	68
4.5.3	Results and Feedback Summary	69
4.5.3.1	Expert Validation Outcomes	69
4.5.3.2	Qualitative Feedback	71
4.5.4	Implications for Refinement	71
4.5.5	Refinement of SOC Model to Version 0.2	72
4.5.5.1	Functional and Structural Enhancements	72
4.5.5.2	Tier-Based Modular Allocation	74
4.5.5.3	Model Justification and Traceability	75
4.5.5.4	Conclusion of Refinement SOC Model v0.2	75
4.6	Demonstration of the Model in a Simulated Context	76
4.6.1	Demonstration Context	76
4.6.2	Scenario Execution	76
4.6.3	Observational Insights	77
4.7	Evaluation and Finalization: SOC Model v1.0	78
4.7.1	Evaluation Overview	78
4.7.2	Evaluation Instrument	78

4.7.3	Evaluation Result	79
4.7.4	Demonstration and Evaluation Recommendations	80
4.7.5	Limitations of the Validation Scope and Recommendations	80
4.7.6	Finalization: SOC Model v1.0	81
4.7.7	Model Interpretation Guide	83
4.7.8	Justification of Tier Content	84
4.7.9	Implementation Roadmap and Adoption Strategy	88
4.7.9.1	Three-Phase Implementation Stages	88
4.7.9.2	Scalable Adoption Strategy	89
4.7.9.3	Policy and Institutional Enablers	89
4.8	Artifact Evolution from v0.1 to v1.0	89
4.9	Comparative Evaluation of Development and Validation Approaches	91
4.10	Evaluation Metrics Summary by Objective	92
4.11	Chapter Summary	93
5	DISCUSSION	95
5.1	Introduction	95
5.2	Discussion of Key Findings	95
5.2.1	RQ1: Cybersecurity threat profiles most significantly affect govern- ment agencies	95
5.2.2	RQ2: Critical components required to design an Effective SOC	96
5.2.3	RQ3: Proportionate, Modular, and Tiered SOC Model for the In- donesian Government	96
5.3	Integration with Design Science Research (DSR) Methodology	97
5.4	Implications of the Findings	98
5.4.1	Theoretical Implications	98
5.4.2	Practical Implications	99
5.5	Limitations of the Study	99
5.6	Post-Evaluation Expert Feedback (Google Cloud)	100
5.7	Suggestions for Future Research	101
5.8	Chapter Summary	102
6	CONCLUSION	103
6.1	Restating the Purpose of the Study	103
6.2	Summary of Key Research Findings	103
6.3	Contributions of the Study	104
6.4	Significance and Implications	105
6.5	Limitations of the Study	105
6.6	Recommendations for Future Research	106
6.7	Recommendations for Policy and Practice	107

6.8	Final Remarks	107
	BIBLIOGRAPHY	109
	Appendices	126
A	SYSTEMATIC LITERATURE REVIEW MATERIALS	128
A.1	PRISMA Flow Diagram – RQ1	128
A.2	PRISMA Flow Diagram – RQ2	129
A.3	Screening and Selection Summary	129
A.4	Quality Assessment Summary	132
A.4.1	Quality Assessment – RQ1	132
A.4.2	Quality Assessment – RQ2	134
A.5	Final Selected Articles	136
B	CODING FRAMEWORK AND THEMATIC MATRIX	138
B.1	Cyber threat typologies – RQ1	138
B.2	Government Limitations – RQ1	140
B.3	Mitigation Strategy – RQ1	140
B.4	Elemen SOC – RQ2	141
B.5	Modul SOC – RQ2	142
C	EXPERT VALIDATION	143
C.1	Expert Validation Instrument	143
C.2	Expert Validation Metrics	154
C.3	Summary of Expert Validation Participants	154
C.4	Validation Score Results	155
C.5	Thematic Analysis of Expert Feedback	156
D	SOC DEMONSTRATION MATERIALS	159
D.1	Demonstration Case-Study for Tier 1	159
D.2	Observation Form Template	162
D.3	Filled Observation Sheet	166
D.4	Escalation Template and Sample Playbook	170
E	EVALUATION	174
E.1	Evaluation Form Template	174
E.2	Completed Evaluation Form by Government Leader	177
F	POST-EVALUATION INDUSTRY EXPERT FEEDBACK	180
F.1	External Commentary on SOCG v.1.0	180
F.2	SOCG Executive Summary Submitted for Review	182