

LIST OF FIGURES

1.1	Thesis Stucture	7
3.1	Six-stage Design Science Research Process Adapted in This Study	20
4.1	SOC artifactEvolution across DSR Stages	29
4.2	PRISMA Flowchart for RQ1 – Cybersecurity Threats in Government	33
4.3	Top Anomalous Threat Behaviors in Indonesian Government Networks (BSSN, 2024)	40
4.4	Top APT and Ransomware Activities in Indonesia (BSSN, 2024)	41
4.5	PRISMA Flow Diagram for Article Selection in RQ2	46
4.6	Radar Chart: SOC Element Coverage Across Models	54
4.7	SOC Model v0.1: Modular Functions Aligned to NIST CSF and Capability Layers	63
4.8	Table of Summary of Expert Participants in SOC Model Validation	68
4.9	Expert Validation Results for SOC Model (19 Indicators)	70
4.10	Refined SOC Model v0.2: Functional Enhancements and New components	73
4.11	Tier-Based Modular Allocation of SOC Functions	75
4.12	SOC Model v1.0: Final structure after validation and evaluation	82
4.13	Tier-Based SOC Modular Allocation in Final Model (v1.0)	83
4.14	SOC artifactEvolution across DSR Stages	90
4.15	Bar chart of Development and Validation Indicators across SOC Models	92
5.1	Refined SOC Model incorporating Basic Forensics capability in Tier 1, based on expert feedback from Google Cloud Security. Optional modules are shaded to reflect adaptive implementation.	101
A.1	PRISMA Flow Diagram for RQ1	128
A.2	PRISMA Flow Diagram for RQ2	129
B.1	Government Limitations Thematic Coding	140
B.2	Mitigation Strategy Thematic Coding	141
B.3	Elemen SOC Thematic Coding	141
B.4	Modul SOC Thematic Coding	142
C.1	Expert Validation Matrix	154
C.2	Summary of Expert Participants	155
C.3	Validation Score Results	156