

**DESIGN FRAMEWORK DNS ATTACK MONITORING AND INCIDENT
ESCALATION ON ENDPOINT SERVER IN EDUCATIONAL INSTITUTION SME
SECTOR**

By

APRIANTO

22451063

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

Januari 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.

Aprianto

Student

Date

Approved by:

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

Thesis Advisor

Date

Kalpin Erlangga S., S.Si, M.Kom, CISSP, CEH, ECIH,
ECSH, CHFI

Thesis Co-Advisor

Date

Dr. Maulah hikmah Galinium,.S.kom, MSc.

Dean

Date

Aprianto

ABSTRACT

DESIGN FRAMEWORK DNS ATTACK MONITORING AND INCIDENT ESCALATION ON ENDPOINT SERVER IN EDUCATIONAL INSTITUTION SME SECTOR

By

Aprianto

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

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

SWISS GERMAN UNIVERSITY

The Small and Medium Enterprise (SME) sector is accelerating digital adoption to remain competitive, but this increases vulnerability to cybercrime. DNS has become an increasingly important attack vector, with significant annual growth in phishing, DNS-deployed malware, DDoS amplification, tunneling and domain hijacking. In the education sector, the AC.ID domain exhibits high vulnerability due to its numerous subdomains, legacy systems and decentralized administration. Many SME institutions lack the security capabilities to communicate and respond effectively.

The purpose of this study, based on the research problem being investigated, involves assessing customers at a university in Makassar who were affected by a web defacement attack. In this case, the research objective focuses on the server endpoint, focusing on how to monitor traffic more effectively and efficiently.

The methodology used in this research is by studying several journal papers related to the threat landscape sector reference, carrying out a risk assessment survey to develop escalation incident rules, the output that will be consolidated is related to monitoring to escalation by the service provider in this DNS attack.

The expected results are a structured DNS-focused monitoring and alerting design for AC.ID web servers, a practical risk-based incident escalation workflow for service providers, and actionable response playbooks covering triage, containment, recovery, and hardening, targeting common AC.ID weaknesses such as outdated web stacks and fragmented server

Aprianto

administration. The thesis is expected to show that DNS-focused monitoring combined with provider-led, risk-based escalation improves detection quality and response consistency for AC.ID SMEs that lack in-house security operations, delivering a deployable SOC service blueprint that can reduce defacement and hijacking impacts, shorten incident handling time, and strengthen continuous monitoring, patch management, and operational governance.

Keywords: SME, DNSMonitoring, DNSattack, Integration with service provider, incident escalation





© Copyright 2026
by Aprianto
All rights reserved

DEDICATION

This work is dedicated to improving the cybersecurity of university at makassar and service provider specifically, the media industry more broadly, and contributing to academic knowledge.



TABLE OF CONTENT

STATEMENT BY THE AUTHOR	2
ABSTRACT	3
DEDICATION	6
TABLE OF CONTENT	7
LIST OF FIGURE	11
CHAPTER 1 – INTRODUCTION	14
1.1. Background.....	15
1.2. Research Problem	19
1.3. Research Questions.....	20
1.4. Research Objectives.....	22
1.5. Scope and Limitations.....	22
1.6. Significance of the Study	23
1.7 Hypothesis.....	24
1.8 Thesis Structure	24
Chapter 2 - LITERATURE REVIEW	26
2.1. Small and Medium Enterprises (SMEs) in the Education Sector	26
2.1.1 Definition and Characteristics of SMEs	26
2.1.2 SMEs in the Education Sector in Indonesia.....	29
2.1.3. IT Infrastructure and Cybersecurity Limitations in Educational SMEs	30
2.2. Overview of Cybersecurity Threats in SMEs	34
2.3. DNS works.....	37
2.3.1. DNS Threat Landscape	38
2.3.2. DNS Cache Poisoning.....	39
2.3.3. DNS Hijacking.....	40
2.3.4. DNS Amplification	41
2.3.5. DDoS on DNS Infrastructure	43
2.3.6. DNS Phising attack and defenses	44
2.3.7. DNS Thunneling	45
2.3.8. Impact of DNS Attacks on Organizational Operations.....	45
2.3.9. Critical Analysis relevance with the study.....	46
2.4. Endpoint Security in SMEs.....	46
2.4.1. Definition of Endpoint Security	46
2.4.2. Common Endpoint Vulnerabilities in SMEs	47

2.4.3. Relationship Between Endpoint Security and DNS Attacks	47
2.4.4. Endpoint Monitoring Technologies	50
2.5. DNS Attack Monitoring Systems	51
2.5.1. Definition of DNS Monitoring.....	51
2.5.2. Real-Time DNS Monitoring Techniques.....	52
2.5.3. Benefits of Real-Time DNS Monitoring.....	52
2.5.4. DNS Monitoring in Educational Institutions	53
2.6. Incident Response and Escalation.....	55
2.5.1 Incident Response Lifecycle	57
2.5.2 Incident Escalation Model	60
2.4.3. Open-Source DNS Monitoring Tools	65
2.5.3 Role of Service Providers in Incident Escalation	72
2.5.4 Impact of Escalation Procedures on Response Time	74
2.7 Security Operation as a Service (SOC-as-a-Service).....	75
2.7.1 Definition of SOC-as-a-Service	75
2.7.2 Advantages for SMEs	81
2.7.3 SOC-as-a-Service for DNS and Endpoint Monitoring	86
2.7.4 Case Studies of SOC-as-a-Service in SMEs.....	89
2.8. Correlation SME and service provider	93
2.9 Cybersecurity Governance and Regulation in Indonesia.....	94
2.9.1 Role of BSSN in National Cybersecurity	94
2.9.2 DNS Security Regulations in Indonesia	94
2.10 Theoretical Framework.....	96
2.10.1 Cyber Resilience Theory.....	96
2.10.2 Defense in Depth Model	98
2.11. Risk Assessment	102
2.12. Research Design.....	103
2.12.1. Correlation Design research and study research	103
2.13. Review Related Study.....	104
2.14. Related works.....	106
2.14.1 Mapping Research Framework to DSR	113
Chapter 3 - RESEARCH METHODOLOGY.....	123
3.1. Research Framework	123
3.1.1. Research literature review.....	123
3.1.2. Problem Identification	124
3.1.3.Objective	124

3.2. Design and Development.....	124
3.2.1. Design Experimetnal Monitoring system	126
3.2.2. Design Integration method with Service provider	127
3.2.3. Evaluation	128
3.3. Validation.....	128
3.4 Risk Assesment Methodology	128
3.5. Justification for a DNS-Specific Monitoring and Escalation Framework	131
3.6 Research Framework and Metric	134
Chapter 4 – RESULT AND DISCUSSION	138
4.1. Preparation Phase.....	141
4.2.Design & develompent	141
4.3 Evaluation	150
4.5 Incident Response process	151
4.6. Validation AI results	154
4.6.1. LLM Clarification.....	155
4.7. Risk Assessment result	156
4.7.1. Scope Definition	156
4.7.2. Decompose DNS Attack.....	156
4.7.3. Data Flow Diagram (DFD)	156
4.7.4. Threat Identification.....	157
4.7.5. Risk Scoring.....	161
4.8. Research Evaluation.....	161
4.9. Research validation	162
4.10. Research Discussion	162
Chapter 5 - CONCLUSION.....	166
5.1. Summary of Key Findings	166
5.2 Conclusion	167
5.3 Practical Implication	167
5.4 Recommendation	168
5.6. Limitations	168
5.7. Future Research Direction	169
REFERENCES	170
APPENDICES (OPTIONAL).....	178
Appendix A: Curriculum Vitae.....	178
Presales B2B	178
Presales Consultant	178

Presales Consultant	178
Presales Consultant	178
IT Infrastructure	178
Network Engineer	178
Network Engineer	178
Busness Director	180
Allience Busness Head	180
IT Infrastuture Solution Manager	180
Presales Consultant	180
System administrator	181
System administrator	181
Appendix B:	183



LIST OF FIGURE

Figure	page
FIGURE 1.1 DNS THREAT LANDSCAPE((FOUCHEREAU, 2023)	15
FIGURE 1.2. METHODOLOGY DNS REPORT FINDINGS((FOUCHEREAU, 2023)	16
FIGURE 1.3. WEB HIJACKING BSSN REPORT(BSSN, 2024)	18
FIGURE 1.4.FISHBONE DIAGRAM OF RESEARCH	20
FIGURE 1.5.CENTRAL RESEARCH QUESTIONS(FOUCHEREAU, 2023)	21
FIGURE 2.1.CONCEPTUAL MAP OF FINDINGS(KALLMUENZER ET AL., 2025).....	29
FIGURE 2.2 CONCEPTUAL MAP OF FINDINGS(BSSN, 2024).....	30
FIGURE 2.3.FRAMEWORK VULNERABILITIES, THREATS, COUNTERMEASURES (BWIINO ET AL., 2025)	34
FIGURE 2.4. MULTIDIMENSIONAL CYBERATTACK IMPACT(ARROYABE ET AL., 2024B).....	36
FIGURE 2.5.THREAT LANDSCAPE DNS THREAT(KHORMALI ET AL., 2021).....	38
FIGURE 2.6.HIGH-LEVEL ATTACK DNS CHACE POISONING(ALHARBI ET AL., 2022)	39
FIGURE 2.7.OVERVIEW THREAT MODEL DNS HIJACKING	41
FIGURE 2.8.DNS AMPLIFICATION DRDoS OPERATION PROCESS	42
FIGURE 2.9.A DDOS ATTACK SCENARIO IN CLOUD INFRASTRUCTURE.....	43
FIGURE 2.10.FIVE CATGORIES OF PHISISNG AND NON-PHISING EMAIL AND WEBSITE.....	44
FIGURE 2.11.DNS THUNNELING USED FOR C2 COMMUNICATION.....	45
FIGURE 2.12.PERIMETER AND ENDPOINT SECURITY SOLUTION.....	48
FIGURE 2.13.AGENTLESS EDR DATA COLLECTION. SX REFERS TO AN ENDPOINT SNAPSHOT CAPTURED FOR HOST X.....	49
FIGURE 2.14.MITIGATION DEFENSE MODEL DNS POISONING.....	51
FIGURE 2.15.ARCHITECTURE OBJECTIVE ACHIEVEMENT THE PAPER(OCHAB ET AL., 2024)	53
FIGURE 2.16. ARCHITECTURE DETECTION SYSTEM OF WEB DEFACEMENT BY(PATTIRADJAWANE AND UPUY, 2025).....	54
FIGURE 2.17.RESULTS OF EVALUATION	55
FIGURE 2.18 LLM COMPARATION RESULT(STAMNES KARLSEN ET AL., 2026)	56
FIGURE 2.19.INCIDENT MANAGEMENT PROCESS MODEL FROM ISO 27035:2013.....	57
FIGURE 2.20. DIGITAL FORENSIC AND INCIDENT RESPONE MANAGEMENT	58
FIGURE 2.21. IR LIFE CYCLE IN OPERATION AND MAINTENANCE BY (SUHAIL ET AL., 2025).....	59
FIGURE 2.22. REPORTING DEADLINES FOR ACTIVELY EXPLOITED VULNERABILITIES AND SEVERE, SIGNIFICANT AND BY IMPLICATION, LARGE-SCALE INCIDENTS BY (SUHAIL ET AL., 2025).....	60
FIGURE 2.23. EVENTS SECURITY MANAGEMENT LIFECYCLE BY (ISMAIL ET AL., 2025B)	60
FIGURE 2.24.INCIDENT RESPONSE AND CHANNEL IN CYBER SECURITY BY(EBERT ET AL., 2025)	61
FIGURE 2.25.ISO/IEC 27035-32020 INCIDENT RESPONE OPERATIONAL PROCESS	62
FIGURE 2.26. ENTITY LEVEL SECURITY INCIDENT RESPONE.....	63
FIGURE 2.27.THE FRAMEWORK TRANSLATING INCIDENT RESPONSE INSTRUCTIONS INTO A SYSTEMATIC TECHNICAL FLOW	64
FIGURE 2.28.INSIDEN RESPONE WORKFLOW	64
FIGURE 2.29.OPEN-SOURCE TOOLS	66
FIGURE 2.30. IMPLEMENTED CONSOLIDATE ARCHITECTURE	67

FIGURE 2.31. SIEM BASED FRAMEWORK FOR SECURITY CONTROL	68
FIGURE 2.32. IDS CLOUD-BASED ARCHITECTURE EVALUATION SETUP	69
FIGURE 2.33. EXPERIMENTAL SETUP DID EVALUATION.....	71
FIGURE 2.34. WORKFLOW TO IMPROVE ORGANIZATIONAL LOGGING MATURITY.....	72
FIGURE 2.35. COMPLIANCE ASSESSMENT SYSTEM ARCHITECTURE MODEL	73
FIGURE 2.36. THE ROLE OF PRODUCT SECURITY IR AT SERVICE PROVIDER	73
FIGURE 2.37. CYBEROWL INCIDENT COMMUNICATION WORKFLOW (NGANGA ET AL., 2025).....	74
FIGURE 2.38. SOC AS A SERVICE MARKET ANALYSIS	76
FIGURE 2.39. TRIAD SECURITY OPERATION	77
FIGURE 2.40.MODEL FOR DEVELOPMENT AND IMPLEMENTATION SOC	78
FIGURE 2.41. KNOWLEDGE TREE OF PEOPLE THEME DEVELOPMENT	79
FIGURE 2.42. SOC DEVELOPMENT PROCESS	80
FIGURE 2.43. SKILL SOC ROLLS	80
FIGURE 2.44. CYBER INFORMATION SOURCES – USED VS PREFERRED.	81
FIGURE 2.45. COMPONENT OF CYBERESP FRAMEWORK AND RELATIONSHIP(CALVO-MANZANO ET AL., 2025).....	83
FIGURE 2.46. METHODOLOGY CLASSIFICATION LITERATURE REVIEW	84
FIGURE 2.47. NIST CSF RESEARCH CLASSIFICATION TOOL (NCRCT).....	85
FIGURE 2.48. NIST CSF FUNCTION- FOCUS OF SMB SECURITY RESEARCH.	86
FIGURE 2.49. BUSINESS MODEL SERVICE PROVIDER TO END USER/CUSTOMER.....	86
FIGURE 2.50. BUSINESS ASSET METHODOLOGY.....	87
FIGURE 2.51. SOC SUSTAINABILITY CHART	89
FIGURE 2.52. THEORETICAL ARCHITECTURE SOC.....	90
FIGURE 2.53. SOC HIGH-LEVEL ARCHITECTURE.....	91
FIGURE 2.54. GRANULAR SOC FUNCTION	92
FIGURE 2.55. STAGE DIAGRAM SOC	93
FIGURE 2.56. SME DIGITAL TRASNFORMATION FRAMEWORK.....	93
FIGURE 2.57. CYBER RESILIENCY ENGINEERING FRAMEWORK(AHN ET AL., 2024)	96
FIGURE 2.58. INFORMATION SECURITY INSPECTION PROCESS (AHN ET AL., 2024)	97
FIGURE 2.59 NIST CSF 2.0 COMPONENTS.....	98
FIGURE 2.60 INCIDENT RESPONSE LIFE CYCLE MODEL BASED ON CSF 2.0 FUNCTIONS(NELSON, 2024)	99
FIGURE 2.61 IR LIFECYLE AND CORRESPONDING NIST CSF 2.0(NELSON, 2024)	100
FIGURE 2.62. FRAMEWORK OF EFFECTIVE CYBERSECURITY IMPLEMENTATION IN LOCAL GOVERNMENT	101
FIGURE 2.63. FRAMEWORK OF EFFECTIVE CYBERSECURITY IMPLEMENTATION IN LOCAL GOVERNMENT	102
FIGURE 2.64. RESEARCH DESIGN.....	103
FIGURE 2.65 FRAMEWORK PROPOSED	111
FIGURE 2.66 INTEGRATION CUSTOMER & MSP	112
FIGURE 3.1 RESEARCH FRAMEWORK PROPOSED	123
FIGURE 3.2. PROPOSED DESIGN INTEGRATION SOLUTION MONITORING AND IR.....	125

FIGURE 3.3. DESIGN DEVELOPING DNS MONITORING.....	126
FIGURE 3.4. FLOW PROCESS THE LOG DATA.....	127
FIGURE 3.5. DESIGN INTEGRATION METHOD WITH SERVICE PROVIDER.....	127
FIGURE 3.6. RESEARCH RISK ASSESMENT METHODOLOGY.....	129
FIGURE 3.7 DNS RULES BASED DETECTION.....	132
FIGURE 3.8 METRIC IPOO SYSTEMATIC FRAMEWORK.....	134
FIGURE 3.9 MAPPING DSR TO RESEARCH FRAMEWORK.....	138
FIGURE 4.1 VIRTUAL-BOX FOR VIRTUAL MACHINE TESTING.....	141
FIGURE 4.2. FLOW PROCESS AUTOMATED LOG COLLECTION.....	142
FIGURE 4.3. STATUS OF WAZUH AGENT AT WEB APP SERVER.....	143
FIGURE 4.4. INSTALL SNORT IN WEB APP SERVER.....	143
FIGURE 4.5. TESTING DNS ATTACK.....	144
FIGURE 4.6 DETECTION DNS ATTACK AT SNORT LOG.....	144
FIGURE 4.7 LOG FOUND FORM SIMULATION ATTACK AT WAZUH SERVER.....	145
FIGURE 4.8. DESIGN SOAR MACHINE DEVELOPMENT.....	146
FIGURE 4.9. RESULT CHAT AI REQUEST.....	147
FIGURE 4.10. DATA DNSCAT2 LOG OUTPUT FROM N8N.....	148
FIGURE 4.11. OUTPUT TICKET FROM ZAMMAD.....	149
FIGURE 4.12. SAMPLE OUTPUT ZAMMAD TICKETING SYSTEM.....	150
FIGURE 4.13. DESIGN INTEGRATION METHOD WITH SERVICE PROVIDER.....	151
FIGURE 4.14. DIAGRAM FLOW COST MODEL AS A SERVICE.....	152
FIGURE 4.15. EXPLAIN THE PROCESS OF POST INCIDENT RESPONSE.....	152
FIGURE 4.16. FORENSIC PHASE 2.....	153
FIGURE 4.17. AI GENERATED VALIDATION PROCESS.....	154
FIGURE 4.18 LLM USED DEEPSEEK V3.2.....	155
FIGURE 4.19. DATA FLOW DIAGRAM DNS SYSTEM AND APPLICATION LAYER.....	157

LIST OF TABLE

Table	Page
TABLE 1.1.CYBER SECURITY MANAGEMENT OF SMES PERCENTAGE(ARROYABE ET AL., 2024C)	18
TABLE 2.1. FACTOR VARIABLE EFFECTING SMES GROWTH(ONGBALI ET AL., 2024)	26
TABLE 2.2. RESULT VARIABLE SCORE(ONGBALI ET AL., 2024)	27
TABLE 2.3 CATEGORIZE CYBER SECURITY CHALLENGES(UNIVERSITY OF GLOUCESTERSHIRE ET AL., 2025)	30
TABLE 2.4 IMPACT OF CYBERCRIME ON SMES(ARROYABE ET AL., 2024B)	35
TABLE 2.5 EXPERIENCE CYBERCRIME IN SMES(ARROYABE ET AL., 2024B)	37
TABLE 2.6 CRITICAL ANALYSIS FOR THIS RESEARCH	46
TABLE 2.7 STUDY RESEARCH PAPER (ALI AND CHEN, 2025)	54
TABLE 2.8 KEY GAPS AI ADOPTION FOR SME(SARKER ET AL., 2026)	56
TABLE 2.9 MAPPING SOC PRODUCT TO SOC COMPONENT	66
TABLE 2.10 EVALUATION SNORT SIGNATURES	70
TABLE 2.11 . EFFICIENCY DID SIGNATURE	70
TABLE 2.12 ANALYSIS STATUS OF AVERAGE RESPONSE AND FAILURE HANDLING.....	75
TABLE 2.13 SOC ARCHITECTURE MODEL AND STRUCTURE (CHAMKAR ET AL., 2024A)	76
TABLE 2.14 BASING REQUIREMENTS PEOPLE, PROCESS AND TECHNOLOGY	77
TABLE 2.15 OVERVIEW CYBER SECURITY FRAMEWORK(CALVO-MANZANO ET AL., 2025)	82
TABLE 2.16 ANALYSIS PROCESSING SYSTEM RECOVERY TIME(AHN ET AL., 2024)	87
TABLE 2.17 RELATED WORKS OF DESIGN SOLUTION	106
TABLE 2.18 MEASURE KEY CRITERIA TO FRAMEWORK	114
TABLE 2.19 MEASUREMENT KEY CRITERIA MAPPING TO NIST CSF 2.0 AND NIST SP800-61r3	116
TABLE 2.20 KEY CIRTERIA MAPPING INTO DSR	118
TABLE 3.1 IMPACT RATING STATEMENT.....	129
TABLE 3.2 RISK VALUE CALCULATION	130
TABLE 3.3 IPOO-BASED EVALUATION METRICS FOR DNS MONITORING AND INCIDENT ESCALATION	136
TABLE 4.1 THREAT ID, THREAT SOURCE AND STRIDE THREAT MODELING.....	157
TABLE 4.2 TASK THREAT RISK ASSESSMENT	159
TABLE 4.3 RISK SCORING OF THREAT IDENTIFICATION	161