



Integrated Malware Detection and Analysis System for SOC L1 Analysts

UNDERGRADUATE THESIS
Submitted as one of the requirements to obtain
Sarjana Komputer (S.Kom)

By:

Raynald Agner Kale'e
001202200098

FACULTY OF COMPUTER SCIENCE
INFORMATION TECHNOLOGY STUDY PROGRAM
CIKARANG
AUGUST, 2025

Integrated Malware Detection and Analysis System for SOC L1 Analysts

Turnitin Results

CAPSTONE-RAYNALD.docx

ORIGINALITY REPORT

2%

SIMILARITY INDEX

2%

INTERNET SOURCES

2%

PUBLICATIONS

2%

STUDENT PAPERS

PRIMARY SOURCES

1

Submitted to Pontificia Universidad Catolica del Ecuador - PUCE

Student Paper

1%

2

Submitted to Asia Pacific University College of Technology and Innovation (UCTI)

Student Paper

1%

3

Submitted to President University

Student Paper

1%

4

repository.president.ac.id

Internet Source

1%

Exclude quotes On

Exclude bibliography On

Exclude matches

< 1%

GPT-Zero Results

AI Report

We predict this text is

Human Generated

AI Probability

1%

This number is the probability that the document is AI generated, not a percentage of AI text in the document.

Plagiarism



The plagiarism scan was not run for this document. Go to gptzero.me to check for plagiarism.

CAPSTONE-RAYNALD.docx - 8/27/2025

RAYNALD KALEE

Integrated Malware Detection and Analysis System for SOC L1

UNDERGRADUATE THESIS

Submitted as one of the requirements to obtain Sarjana Komputer

By:

RAYNALD AGNER KALEE

001202200098

FACULTY OF COMPUTING INFORMATICS STUDY PROGRAM CIKARANG JULY, 2025

Copyright By

Raynald Agner Kalee

Integrated Malware Detection and Analysis System for SOC L1

ABSTRACT

With the growing sophistication of the cyber threats, the Security Operations Center (SOC) Level 1 (L1) analysts assume a greater role in detection and mitigation of such threats. But manual processes that SOC L1 analysts are currently using to query different sources of threat intelligence, perform malware analysis and create Indicators of Compromise (IOCs) are both error-prone and labor-intensive. This thesis suggests the devising of the system of Integrated Malware Detection and Analysis which is meant to mechanize these processes and make the work of SOC L1 analysts more efficient and precise.

The offered solution accelerates real-time threat intelligence aggregators with several providers like VirusTotal, AbuseIPDB, ThreatFox, etc. and returns AI-driven analysis including automatic malware detection and creation of IOCs. By connecting with Safety Information and Event Administration (SIEM) devices, such as Wazuh, the system can be used to associate threat information, automatically reacting to incidents and effectively managing cases. This saves a lot of time to respond to incidents and also chances of making mistakes.

The system is expected to boost the operational efficiency of the research and apply the unified threat intelligence aggregation, machine-assisted malware analysis, and live incident responders. The study lays out how the system is designed, developed and used, with the aim to stimulate the community in terms of the potential of the system to offer proactive, efficient, and scalable solutions to the problems experienced by SOC L1 analysts in the current cybersecurity environment.

Keywords: Malware Detection, SOC L1 Analysts, Threat Intelligence, Wazuh, SIEM, Cybersecurity automation, Indicators of Compromise (IOCs)

Table of Contents

STATEMENT OF ORIGINALITY	4
SCIENTIFIC PUBLICATION APPROVAL FOR ACADEMIC INTEREST	5
ADVISOR APPROVAL FOR JOURNAL/INSTITUTION'S REPOSITORY	6
SIMILARITY INDEX REPORT	7
ABSTRACT	9
DEDICATION.....	10
ACKNOWLEDGEMENTS	11
Table of Contents.....	12
LIST OF TABLES.....	15
LIST OF FIGURES	16
CHAPTER I INTRODUCTION.....	18
1.1 PROBLEM FORMULATION	18
1. Background of the Problem.....	18
2. Problem Statement.....	19
3. Objective	20
4. Problem from a Customer Perspective.....	20
1.2 PROBLEM CONSTRAINT ANALYSIS.....	20
1. Aspect 1: Data Quality and Availability.....	20
2. Aspect 2: Model Performance	21
3. Aspect 3: Security and Scalability	21
1.3 PROBLEM FUNCTIONAL ANALYSIS.....	21
1.1.1 Functionalities 1: Two-Factor Authentication (2FA).....	21
1.1.2 Functionalities 2: Threat Intelligence Collecting and Reporting	21
1.1.3 Functionalities 3: IoC Scanning and Storage.....	22
1.4 SOLUTION SELECTION	22
1.1.4 Alternative Solution 1: Integrated Web Dashboard	22
1.1.5 Alternative Solution 2: Manual System with Separate Tools.....	22
1.1.6 Solution Selection	22
1.5 SOLUTION USAGE SCENARIOS.....	23
1. Scenario Login with 2FA	23
2. Scenario for Threat Intelligence Collection and Reporting	23

1.1.7	3. Scenario for IoC Scanning and Storage.....	23
1.1.8	4. Scenario for User Management.....	23
CHAPTER II SYSTEM ANALYSIS.....		25
2.1	Existing Business Process.....	25
2.1.1	2.2 Proposed Business Process	27
2.3	GLOBAL DESCRIPTION OF THE PRODUCT	28
1.	Main Functionality.....	28
2.	User Characteristics	29
2.1.2		30
3.	Product Development Environment Hardware.....	30
4.	Product Operational Environment	31
2.1.3	Software	32
2.4	REQUIREMENT ANALYSIS.....	32
2.1.4	External Interface.....	32
2.1.5	Functional Description.....	32
2.1.6	Use Case : Add, remove, edit data of the user	33
2.1.7	Use Case : Collect and Report Threat Intelligence	34
	Data Requirement	38
	Functional Requirement	39
2.1.8	Activity Diagram	40
CHAPTER III DESIGN		48
2.2	ALTERNATIVE SOLUTION DESIGNS	48
2.3	RATIONAL/SYSTEMATIC DESIGN	52
2.4	HIERARCHICAL/ITERATIVE DESIGN	56
CHAPTER IV IMPLEMENTATION		
2.5	Functions/Procedure/Class implementation.....	63
2.5.1	Login Page.....	64
2.5.2	Login Page 2FA Backend.....	73
2.5.3	Menu Threat Intelligence Front-end	82
2.5.4	Menu Threat Intelligence Back-end.....	99
2.6	UI Implementation and Testing.....	102
CHAPTER V CONCLUSION		105
3	REFERENCES.....	106

4	APPENDICES	107
---	------------------	-----

LIST OF TABLES

1.1 Solution Selection Comparison	7
2.1 User Characteristics	14
2.2 Use Case: Add, Remove, Edit Data	18
2.3 Use Case: Capture and Analyze	19
2.4 Use Case: Store Data	20
2.5 Use Case: Generate Report	20
2.6 Use Case: Monitor Defect Dashboard	21
3.1 Alternative Solution Comparison Table	33
3.2 Quantitative Solution Selection	34

LIST OF FIGURES

2.1 Existing Business Process	10
2.2 Proposed Business Process	12
2.3 Use Case Diagram	18
2.4 Entity Relationship Diagram (ERD)	22
2.5 Context Diagram	23
2.6 Activity Diagram: Add, Remove, Edit Data	24
2.7 Activity Diagram: Capture and Analyze	25
2.8 Activity Diagram: Store Data	26
2.9 Activity Diagram: Generate Report	27
2.10 Activity Diagram: Monitor Defect Dashboard	28
2.11 Data Flow Diagram Level	12
9	
3.1 Block Diagram Level 0	31
3.2 Data Flow Diagram ADPD	36
3.3 Use Case Diagram (Design)	37
3.4 Activity Diagram: Add, Remove, Edit (Design)	38
3.5 Activity Diagram: Capture and Analyze (Design)	39
3.6 Activity Diagram: Store Data (Design)	40
3.7 Activity Diagram: Generate Report (Design)	41
3.8 Activity Diagram: Monitor Defect Dashboard (Design)	42
3.9 Sequence Diagram: Add, Remove, Edit Data	43
3.10 Sequence Diagram: Capture, Analyze, Store, Report, Monitor	44

3.11 Entity Relationship Diagram (Design)	45
4.1 Data Flow Diagram Implementation	46
4.2 UI Implementation Screenshot 1	1