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:

Almendo Gabriel Tetelepta

001202200002

FACULTY OF COMPUTER SCIENCE

INFORMATION TECHNOLOGY STUDY PROGRAM

CIKARANG

AUGUST, 2025

SIMILARITY INDEX REPORT

Casptone Turnitin Check - Almendo

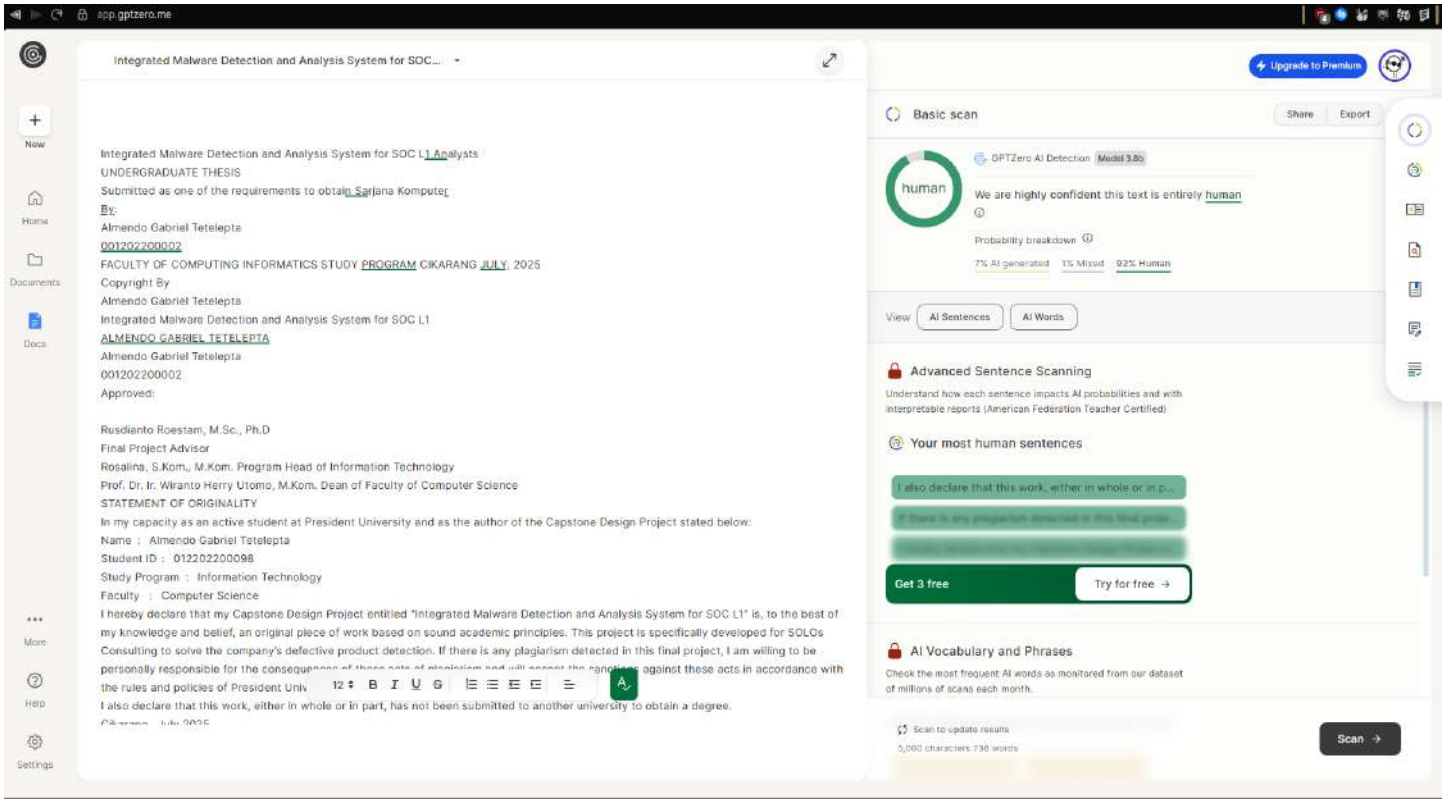
ORIGINALITY REPORT

13%	10%	3%	11%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to President University Student Paper	2%
2	repository.president.ac.id Internet Source	2%
3	Submitted to University of Northampton Student Paper	1%
4	Submitted to City University Student Paper	1%
5	Submitted to University of Petroleum and Energy Studies Student Paper	<1%
6	faculty.washington.edu Internet Source	<1%
7	Submitted to University of Hertfordshire Student Paper	<1%
8	Submitted to University of Central Lancashire Student Paper	<1%
9	Submitted to Bahrain Polytechnic Student Paper	<1%

GPT ZERO


app.gptzero.me
Integrated Malware Detection and Analysis System for SOC...
Upgrade to Premium
New
Home
Documents
Docs
More
Help
Settings
Integrated Malware Detection and Analysis System for SOC L1 Analysts
UNDERGRADUATE THESIS
Submitted as one of the requirements to obtain Sarjana Komputer
By:
Almendo Gabriel Tetelepta
001202200002
FACULTY OF COMPUTING INFORMATICS STUDY PROGRAM CIKARANG JULY, 2025
Copyright By
Almendo Gabriel Tetelepta
Integrated Malware Detection and Analysis System for SOC L1
ALMENDO GABRIEL TETELEPTA
Almendo Gabriel Tetelepta
001202200002
Approved:
Rusdianto Roestam, M.Sc., Ph.D
Final Project Advisor
Rosalina, S.Kom., M.Kom. Program Head of Information Technology
Prof. Dr. Ir. Wiranto Herry Utomo, M.Kom. Dean of Faculty of Computer Science
STATEMENT OF ORIGINALITY
In my capacity as an active student at President University and as the author of the Capstone Design Project stated below:
Name : Almendo Gabriel Tetelepta
Student ID : 012202200098
Study Program : Information Technology
Faculty : Computer Science
I hereby declare that my Capstone Design Project entitled "Integrated Malware Detection and Analysis System for SOC L1" is, to the best of my knowledge and belief, an original piece of work based on sound academic principles. This project is specifically developed for SOLOs Consulting to solve the company's defective product detection. If there is any plagiarism detected in this final project, I am willing to be personally responsible for the consequences of these acts of plagiarism and will accept the sanctions against these acts in accordance with the rules and policies of President Univ
I also declare that this work, either in whole or in part, has not been submitted to another university to obtain a degree.
Basic scan
Share
Export
human
GPTZero AI Detection
We are highly confident this text is entirely human
Probability breakdown
7% AI generated
1% Mixed
92% Human
View
AI Sentences
AI Words
Advanced Sentence Scanning
Understand how each sentence impacts AI probabilities and with interpretable reports (American Federation Teacher Certified)
Your most human sentences
I also declare that this work, either in whole or in p...
Get 3 free
Try for free →
AI Vocabulary and Phrases
Check the most frequent AI words as monitored from our dataset of millions of scans each month.
Scan to update results
5,000 characters 736 words
Scan →

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 labour-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. 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 iii

SCIENTIFIC PUBLICATION APPROVAL FOR ACADEMIC INTEREST iv

ADVISOR APPROVAL FOR JOURNAL/INSTITUTION'S REPOSITORY v

SIMILARITY INDEX REPORT vi

ABSTRACT viii

DEDICATION ix

ACKNOWLEDGEMENTS x

TABLE OF CONTENTS xi

LIST OF TABLES xiii

LIST OF FIGURES xiv

I. INTRODUCTION 1

1.1 Problem Formulation 1

1. Background of the Problem 1

2. Problem Statement 2

3. Objective 2

4. Problem from a Customer Perspective 2

1.2 Problem Constraint Analysis 3

1. Aspect 1: Data Quality and Availability 3

2. Aspect 2: Model Performance 3

3. Aspect 3: Hardware Limitations 4

1.3 Problem Functional Analysis 4

Functionalities 1: Defect Detection Using Computer Vision 4

Functionalities 2: Real Time Defect Detection System 4

Functionalities 3: Data Logging & Reporting 5

1.4 Solution Selection 5

Alternative Solution 1: Convolutional Neural Networks (CNN) 5

Alternative Solution 2: Recurrent Neural Networks (RNN) 6

Solution Selection 6

1.5 Solution Usage Scenarios 7

1. Scenario for Defect Detection Using Computer Vision 7

2. Scenario for Data Logging & Reporting 8

II. SYSTEM ANALYSIS 9

2.1 Existing Business Process 9

2.2 Proposed Business Process 10

2.3 Global Description of the Product 12

1. Main Functionality 12

2. User Characteristics 13

3. Product Development Environment 15

4. Product Operational Environment 16

2.4 Requirement Analysis 17

External Interface 17

Functional Description 17

Data Requirement 22

Functional Requirement 23

Activity Diagram 24

III. DESIGN 31

3.1 Alternative Solution Designs.....31

3.2 Rational/Systematic Design 33

3.3 Hierarchical/Iterative Design 36

IV. IMPLEMENTATION 46

4.1 Functions/Procedure/Class Implementation 47

4.1.1 Add, Remove, Edit Data of Products 47

4.1.2 Capture and Analyze.....49

4.1.3 Store Data 51

4.1.4 Generate Report 53

4.1.5 Monitor Defect Dashboard.....54

4.1.6 Performance Monitoring 55

4.2 UI Implementation and Testing 157

V. CONCLUSION.....159

REFERENCES.....161

APPENDICES.....162

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 129

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

UI Implementation Screenshot 1 157