



Advanced Cybersecurity Framework Through Centralized Security Platform

UNDERGRADUATE THESIS

Submitted as one of the requirements to obtain

Sarjana Komputer (S.Kom)

By:

THEODORE BECKHAM

MILANO KOWAAS

001202200020

FACULTY OF COMPUTING

INFORMATION TECHNOLOGY STUDYPROGRAM

CIKARANG

AUGUST, 2025

AI Report

We predict this text is

Human Generated

AI Probability

19%

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.

**Advanced Cybersecurity Framework Through Centralized Security Platform -
7/21/2025**

Theodore_Kowaas_-_Individual_Report.docx

ORIGINALITY REPORT

10%

SIMILARITY INDEX

9%

INTERNET SOURCES

0%

PUBLICATIONS

9%

STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to President University Student Paper	7%
2	repository.president.ac.id Internet Source	1%
3	Submitted to Old Dominion University Student Paper	<1%
4	Submitted to Milton Keynes College Student Paper	<1%
5	etd.aau.edu.et Internet Source	<1%
6	Submitted to Brigham Young University Student Paper	<1%
7	eprints.utar.edu.my Internet Source	<1%
8	Submitted to ESoft Metro Campus, Sri Lanka Student Paper	<1%
9	link.springer.com Internet Source	<1%

ABSTRACT

In the contemporary digital landscape, where cyber threats are constantly evolving, fostering robust security awareness is paramount to organizational resilience. Traditional, fragmented approaches to cybersecurity training often fail to provide timely insights and comprehensive protection. To address this critical gap, we present the Centralized Cybersecurity Framework (CCF), a holistic platform designed to integrate and automate key security awareness initiatives and threat intelligence. The CCF's core functionality focuses on real-time detection and elimination of harmful web links, shielding users from online dangers, malware dissemination, and sophisticated phishing attempts. Complementing this, an integrated security chatbot serves as a real-time advisory tool for staff, delivering immediate guidance on cybersecurity best practices, aiding in the identification of fraudulent messages, and offering crucial assistance during security incidents. By centralizing these functionalities, the CCF not only strengthens an organization's defenses against emergent cyber threats but also cultivates a more knowledgeable and resilient user base, thereby establishing a strong and flexible security ecosystem.

Keywords: Cybersecurity, Phishing Exercise, URL Checker, Network Security

TABLE OF CONTENTS

ABSTRACT	viii
DEDICATION	ix
ACKNOWLEDGMENTS	x
CHAPTER I INTRODUCTION	2
I.1 Background	2
I.2 Problem Formulation	2
I.3 Problem Limitation	3
I.4 Research Objectives	3
I.5 Research Methods	4
CHAPTER II LITERATURE REVIEWS	6
II.1 Phishing Attacks	6
II.2 Tools and Technologies for Security Awareness Tools Feature	6
II.3 Frontend Implementation with React.js	6
II.4 Backend Implementation with Node.js	8
CHAPTER III SYSTEM ANALYST	10
III.1 System Analysis	10
III.2 Product Perspective	11
III.3 Product Function	11
III.4 System Overview	21
CHAPTER IV	24
SYSTEM IMPLEMENTATION AND TESTING	24
III.5 System Interface Implementation	24
III.6 Software Functionality Testing	83
CHAPTER V CONCLUSION	87