AKHUWAT COLLEGE KASUR

AFFILIATED WITH

UNIVERSITY OF THE PUNJAB, LAHORE.

FINAL YEAR PROJECT (FYP)

PROPOSAL DOCUMENT

PROJECT TITLE

"AI-Driven Security Monitoring: Anomaly Detection Using Elastic Stack & Wazuh"

BS (IT)

SESSION: 2021-2025

DEPARTMENT OF INFORMATION TECHNOLOGY

AKHUWAT COLLEGE KASUR.

Table of Contents

1. Introduction

1.1 Project Title

“AI-Driven Security Monitoring: Anomaly Detection using Elastic Stack & Wazuh”

1.2 Project Overview Statement

This project is about creating a system that uses Artificial Intelligence (AI) to detect unusual activities in the Wazuh and Elastic stack Security Suite. These platforms are widely used for managing logs, monitoring file integrity, detecting intrusions, and handling Security Information and Event Management (SIEM).

By adding AI and Machine Learning (ML), the system will improve real-time detection of suspicious behaviors and threats. The system will process logs, show data visually, and use AI to spot anything out of the ordinary. When something unusual is found, it will send alerts with details about the threat level.

Kibana will be the tool for visualizing and analyzing the data in an easy-to-understand way.

1.3 Project Overview Statement Template

Project Title: AI-Driven Security Monitoring: Anomaly Detection using Elastic Stack & Wazuh.

Group Leader: Khalid Hussain

Project Members:

Name	Roll#	Email Address	Signature
Muhammad Osama	058949	osamaacuk.97@gmail.com	
Khalid Hussain	058960	khalidhussain.bsit.auk@gmail.com	

Project Goal: To develop an AI-driven system integrated with Wazuh and elastic stack for real-time anomaly detection, threat alerts, and data visualization.

Objectives:

Sr.#	
1	Integrate AI algorithms with Wazuh and Elastic Stack for anomaly detection.
2	Train AI models to detect odd file creations and too-many logins.
3	Create Kibana dashboards to visualize and explore data easily.
4	Provide real-time alerts with threat levels.
5	Improve security by detecting threats early.

Project Success criteria:

The project will be successful if it can:

- Detect anomalies like anomalous file creation and suspicious login volume with high accuracy.
- Send real-time alerts when unusual activities are found.
- Show clear security insights using Kibana dashboards for easy analysis.
- Work smoothly with Wazuh and the Elastic stack, ensuring reliable performance.
- Improve threat detection by reducing false alarms and identifying real risks.
- Help security teams respond quickly to threats.

Assumptions, Risks, and Obstacles:

- **Assumptions:** We assume the Wazuh and Elastic Stack systems will work well together, there will be enough log data to analyze, AI and machine learning.
- **Risks:** We might face delays due to complex integration, the system's performance could slow down with added processing, there should not be enough logs to train ML model.
- **Obstacles:** Learning AI and machine learning might be challenging, poor data quality could affect model accuracy, and we might have limited resources for training and deploying models

Organization Address: This idea is proposed and supervision by **Ebryx.**

Type of project: ❑ Research ❑ Development	
Target End users: • Financial Institutions • Healthcare Organizations • E-commerce Businesses • Government Agencies • Technology Companies • Educational Institutions • Manufacturing & Industrial Companies	
Development Technology: ❑ Object Oriented ❑ Structured	
Platform: ❑ Web based ❑ Distributed ❑ Desktop based ❑ Setup Configurations ❑ Other_____	
Project Supervisor: Mr. Muhammad Naeem Akhtar	
Approved By:	
Date:	

1.4 Project Goals & Objectives

Goals

- Develop an AI-powered anomaly detection system integrated with Wazuh and Elastic Stack.
- Enhance real-time threat detection and response for cybersecurity teams.
- Provide actionable insights using Kibana analytics and visualization.

Objectives

- Train and deploy ML models to detect anomalies in log data
- Implement real-time alerts for Anomalous File Creation and Suspicious Logins
- Integrate Kibana dashboards for visualizing common anomalies
- Ensure the system processes logs efficiently and scales with data volumes

1.5 High-level system components

- **Collect & Store Logs:** Using Elastic Stack to gather and save logs.
- **ML Model:** Custom machine learning system to detect anomalies.
- **Alerting System:** Real-time alerts via email or integrations (e.g., Slack)
- **Visualization:** Kibana dashboard.
- **User Interface:** Web-based Kibana interface for analysts

1.6 List of optional functional units

- **Integration with External Security Tools** – Allow compatibility with other security platforms (e.g., Splunk, SIEM).
- **Customizable Alert Rules** – Enable users to modify AI detection thresholds based on their security needs.

1.7 Exclusions

- The system will detect anomalies but will not automatically fix security threats.
- It will not support mobile applications, only a web-based Kibana dashboard.

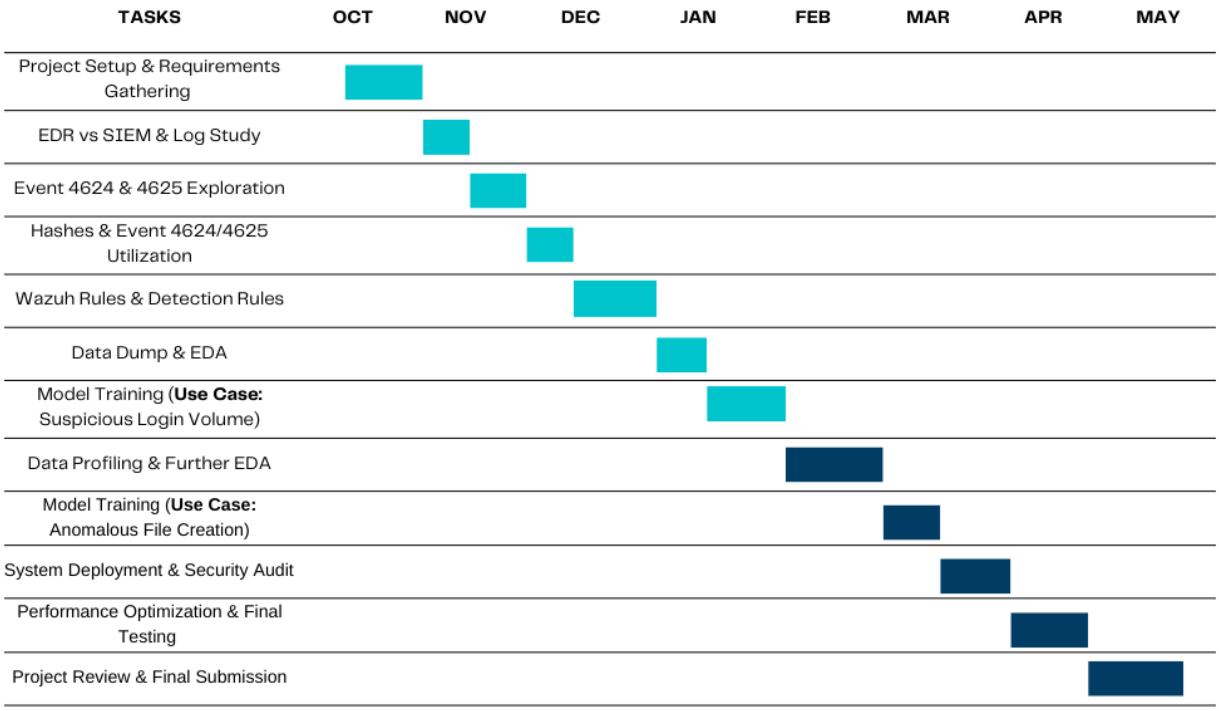
1.8 Application Architecture

The system follows a three-tier architecture:

- **Frontend:** Kibana for interactive data visualization and user dashboards.
- **Backend:** Python-based AI/ML module for log processing, anomaly detection, and alert generation.
- **Database:** Elasticsearch for log storage and fast searching, integrated with Wazuh for security monitoring.

1.9 Gantt Chart

Task	Start Date	End Date	Duration (Days)
Project Setup & Requirements Gathering	17 Oct 2024	31 Oct 2024	15
EDR vs SIEM & Log Study	1 Nov 2024	15 Nov 2024	15
Event 4624 & 4625 Exploration	16 Nov 2024	30 Nov 2024	15
Hashes & Event 4624/4625 Utilization	1 Dec 2024	15 Dec 2024	15
Wazuh Rules & Detection Rules	16 Dec 2024	4 Jan 2025	20
Data Dump & EDA	5 Jan 2025	24 Jan 2025	20
Model Training (Suspicious Login Volume)	25 Jan 2025	15 Feb 2025	22
Data Profiling & Further EDA	16 Feb 2025	5 Mar 2025	18
Model Training (Anomalous File Creation)	6 Mar 2025	26 Mar 2025	21
System Deployment & Security Audit	27 Mar 2025	15 Apr 2025	20
Performance Optimization & Final Testing	16 Apr 2025	5 May 2025	20
Project Review & Final Submission	6 May 2025	31 May 2025	26



1.10 Hardware and Software Specification

Hardware:

- Processor 8GB RAM
- 100GB Storage

Software:

- ELK Stack
- Wazuh
- Python 3.9+ with TensorFlow, scikit-learn
- Kibana
- Filebeat

1.11 Tools and technologies used with reasoning

1. **Elastic Stack & Wazuh** For log management and security monitoring

    - **ELK (Elasticsearch, Logstash, Kibana)** helps collect, store, and analyze logs.
    - **Wazuh** adds security monitoring, helping detect suspicious activities.
    - These tools make it easy to process large amounts of log data and find anomalies.

2. **TensorFlow** For building and training the AI model

    - A powerful open-source machine learning framework.
    - Helps create and train an AI model to detect unusual patterns in data.
    - Supports deep learning techniques, making detection more accurate.

3. **Kibana** For visual analytics and anomaly exploration

    - A dashboard tool that works with Elasticsearch.
    - Helps display logs, trends, and AI-detected anomalies using graphs and charts.
    - Makes it easier to understand and investigate suspicious patterns.

Project Advisor: Mr. Muhammad Naeem Akhtar

Faculty: Department of Information Technology, Akhuwat College Kasur