**Final Year Project Proposal:**

AI-Driven Security Monitoring: Anomaly Detection in ELK and Wazuh

**Project Advisor:**

Muhammad Naeem Akhtar

Department of Information Technology

Akhuwat College University

**Particulars of the students:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr. No** | **Registration#** | **Name in Full** | **Signatures** |
| **1** | **21F-BSIT-28** | Muhammad Osama |  |
| **2** | **21F-BSIT-40** | Khalid Hussain |  |

**Advisor’s Consent :**

I Prof **Muhammad Naeem Akhtar** am willing to guide these students in all phases of above mentioned project as advisor. I have carefully seen the Title and description of the project and believe that it is of an appropriate difficulty level for the number of students named above.

***Signatures and Date***

|  |
| --- |
|  |

**Abstract / Executive Summary**

This project is about creating a system that uses Artificial Intelligence (AI) to detect unusual activities in the Wazuh and ELK (Elastic, Logstash, Kibana) 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 and suggestions on how to handle it. Kibana will be the tool for visualizing and analyzing the data in an easy-to-understand way.

The idea for this project was proposed by the Ebryx Team, who are also supervising and guiding us throughout the development process.

**Introduction and Background**

Organizations increasingly rely on SIEM platforms like Wazuh and ELK to ensure IT security. However, traditional systems often fail to detect complex and novel anomalies in real-time. This project seeks to address this gap by leveraging AI techniques to detect deviations from normal behavior patterns within logs.

This initiative aims to integrate AI algorithms into Wazuh and ELK for real-time anomaly detection, offering a robust and scalable solution for organizations. The proposed system will significantly enhance the detection capabilities for cybersecurity threats and unusual activities.

**Statement of the Problem**

Despite the comprehensive features of Wazuh and ELK, these platforms lack built-in AI capabilities for detecting sophisticated anomalies. Cybersecurity threats are becoming increasingly complex, and traditional rule-based detection methods cannot always identify novel attack patterns or unusual system behavior.

Additionally, organizations face challenges in analyzing large volumes of log data efficiently. This project seeks to answer the question of how to integrate AI into existing systems to detect anomalies effectively and provide actionable insights to mitigate threats.

**Objective(s) / Aim(s) / Target(s)**

1. Develop a system to detect anomalies using AI algorithms integrated with Wazuh and ELK.
2. Provide real-time alerts for detected anomalies, including associated threat levels and mitigation recommendations.
3. Use Kibana for visualization to facilitate user-friendly analysis and exploration.
4. Enhance cybersecurity through proactive detection of unusual activities.

**Completeness Criteria**

The project will be considered complete when the following functionalities are achieved:

1. Log ingestion and storage using ELK.
2. Application of AI algorithms for anomaly detection.
3. Real-time alert generation for anomalies.
4. Visualization of data and insights using Kibana.
5. Comprehensive testing and refinement of the system.

**Challenges**

1. Designing AI models for anomaly detection.
2. Integrating AI with Wazuh and ELK.
3. Ensuring data privacy and security.
4. Efficient processing of large log volumes.
5. Visualizing complex data in an intuitive manner.
6. Learning new technologies and frameworks.

**Use Cases**

1. Anomalous file creation at unusual paths.
2. Suspicious volume of logins to user accounts.

**Knowledge Areas Required**

1. Artificial Intelligence and Machine Learning.
2. Cybersecurity principles.
3. Web engineering and database systems.
4. Data visualization tools (Kibana).
5. Log management systems (ELK, Wazuh).

**Learning Outcomes**

1. Develop expertise in AI algorithms for cybersecurity.
2. Gain practical experience with Wazuh and ELK stacks.
3. Improve knowledge of data visualization and log analysis.
4. Acquire problem-solving skills for real-world cybersecurity challenges.

**Nature of the End Product / Research Outcomes**

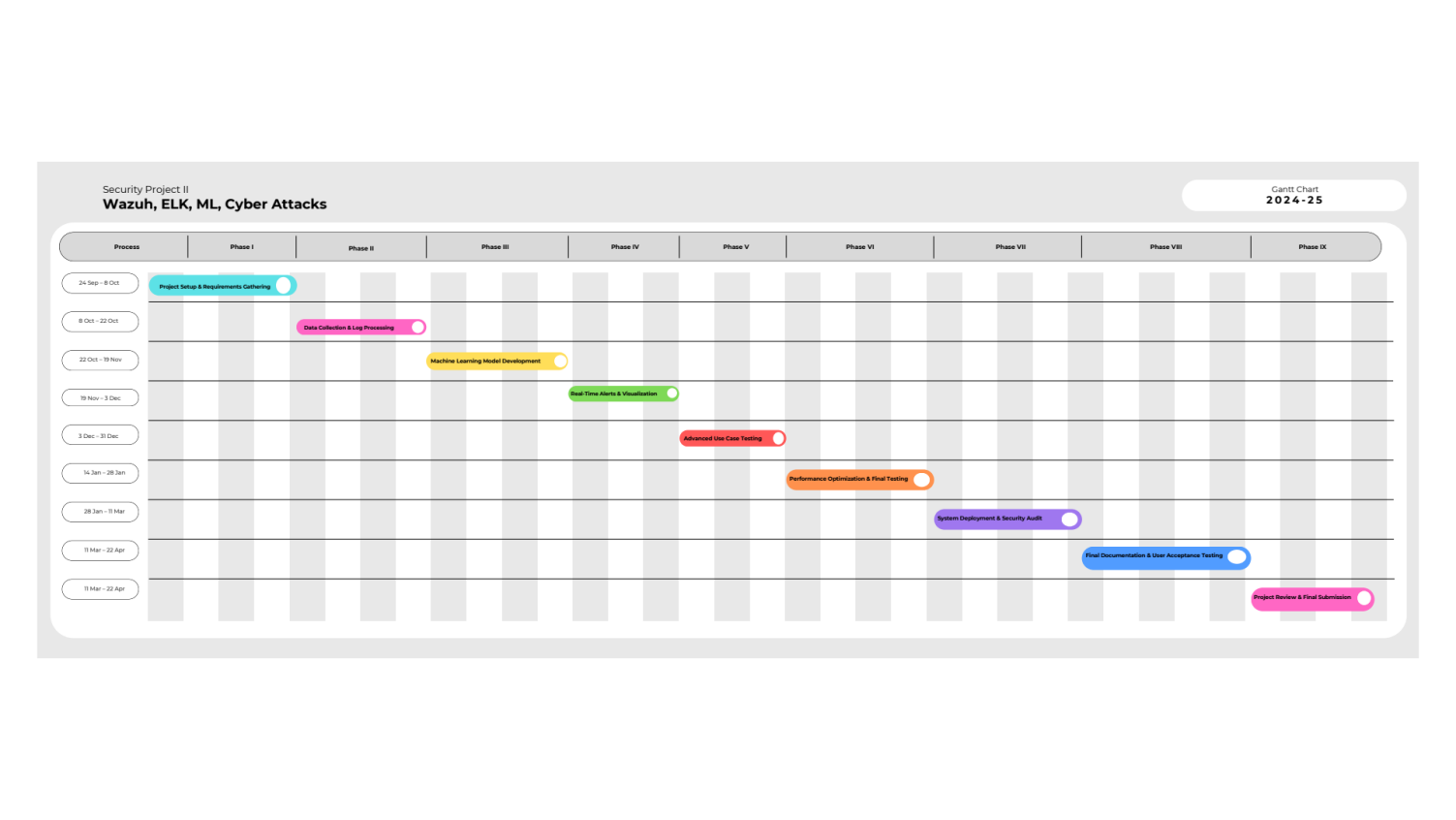
The final product will be a comprehensive anomaly detection system integrated with Wazuh and ELK, featuring:

1. AI-based anomaly detection.
2. Real-time alerts with threat levels.
3. Recommendations for mitigation.
4. Data visualization in Kibana.

**Deliverables / Work Breakdown Structure**

1. Requirement Specifications (10%).
2. System Design (15%).
3. AI Model Development (20%).
4. Backend Integration (20%).
5. Visualization Modules (15%).
6. Testing and Refinement (15%).
7. Documentation and Report (5%).

**Project Plan / Project Schedule / Project Timetable**

The project will commence with requirement analysis and system design, followed by AI model development and backend integration. A detailed Gantt chart will be created to track weekly progress.

**Resources Required**

1. Computers with high computational power.
2. Internet connectivity.
3. Access to Wazuh and ELK environments.

**Bibliography**

1. Elastic Stack Documentation.
2. [Wazuh Documentation.](https://documentation.wazuh.com/current/index.html)
3. Machine Learning in Cybersecurity (Smith et al., 2020).
4. Log Analysis Techniques (Johnson, 2019).
5. AI for Anomaly Detection (Lee et al., 2021).