AKHUWAT COLLEGE KASUR

AFFILIATED WITH

UNIVERSITY OF THE PUNJAB, LAHORE.

FINAL YEAR PROJECT (FYP)

DELIVERABLE-01: SOFTWARE REQUIREMENT SPECIFICATION

PROJECT TITLE

AI-DRIVEN SECURITY MONITORING: ANOMALY DETECTION IN ELK AND WAZUH

BS (IT)

SESSION: 2021-2025

GROUP MEMBERS

Khalid Hussain 058960

Muhammad Osama 058949

SUPERVISED BY:

EBRYX TEAM

&

MR. MUHAMMAD NAEEM AKHTAR

Table of Contents

1. Executive Summary

This document outlines the requirements for an AI-powered anomaly detection system built using Wazuh and the Elastic Stack (Elasticsearch, Logstash, Kibana). The system monitors security logs to identify unusual activities, such as:

- **Anomalous File Creation**: Detecting unauthorized or suspicious file creation in restricted directories.
- **Suspicious Login Attempts**: Identifying too many failed login attempts that may indicate brute-force attacks.

The system will use Artificial Intelligence (AI)/Machine Learning (ML) to automatically detect anomalies, provides real-time alerts, and visualizes data on user-friendly Kibana dashboards for security analysts to investigate and respond effectively.

2. Requirements Analysis

This section details the system's requirements, including user needs, constraints, and key features, based on thorough analysis.

2.1 User Classes and Characteristics

User Class	Characteristics
Security Analysts	Monitor logs, review alerts, investigate incidents, and take corrective actions.
System Administrators	Configure and maintain Wazuh and Elastic Stack components, manage system uptime.
AI/ML Engineers	Develop, train, and optimize AI/ML models for anomaly detection.

2.2 Requirement Identification Techniques

Requirements were gathered using the following methods:

- **Use Case Analysis**: Developed detailed use cases and diagrams to map system interactions and features, ensuring alignment with user needs.
- **Stakeholder Interviews**: Consulted security teams and IT staff to understand practical security challenges and system expectations.
- **Data-Driven Analysis**: Examined real-world security logs to define performance for AI/ML anomaly detection.
- **Literature Review**: Studied research papers on AI-based security systems to adopt best practices and address potential challenges.

3. Functional Requirements

3.1 System Features

The system provides the following core functionalities:

ID	Feature	Description
FR-1	Log Collection	Collects security logs from devices and applications in real-time.
FR-2	AI-Based Anomaly Detection	Uses AI/ML to identify unusual patterns in logs (e.g., anomalies).
FR-3	Alert System	Sends real-time alerts when threats or anomalies are detected.
FR-4	Dashboard Visualization	Displays security data on Kibana dashboards with graphs and filters.
FR-5	Anomalous File Creation Detection	Detects and alerts on unauthorized or suspicious file creation events.
FR-6	Suspicious Login Attempt Detection	Monitors and alerts on too many failed login attempts within a short period.
FR-7	Alert Customization	Allows users to set custom alert thresholds and response actions.
FR-8	Incident Reporting	Enables logging and documentation of incidents for analysis and compliance.

3.2 Detailed Functional Requirements

Identifier	**FR-1**
Title	Log Collection
Requirement	The system shall collect security logs from various devices and applications.
Source	Need for security monitoring from endpoint.
Rationale	Helps detect security threats by analyzing logs in one place.
Business Rule	Alerts should be generated if a file is created in a restricted directory or by an unauthorized user.
Dependencies	None
Priority	High

Identifier	**FR-2**
Title	AI-Based Detection
Requirement	The system shall use AI to detect unusual activities in collected logs.
Source	Requirement for advanced threat detection.
Rationale	Identifies hidden threats not caught by standard rules.
Business Rule	The AI model should analyze logs in real-time and flag unusual patterns.
Dependencies	FR-1 *(Log Collection)*
Priority	High

Identifier	**FR-3**
Title	Alert System
Requirement	The system shall send alerts when a potential security threat is detected.
Source	Requirement for quick threat notification.
Rationale	Enables fast response to potential security issues.
Business Rule	Alerts should be sent via email and displayed on the dashboard.
Dependencies	FR-2 *(AI-Based Detection)*
Priority	High

Identifier	**FR-4**
Title	Dashboard
Requirement	The system shall present security data in a clear and easy-to-understand format
Source	Need for accessible security monitoring.
Rationale	Allows security teams to monitor the system effectively.
Business Rule	The dashboard should display alerts, logs, and system status.
Dependencies	FR-1 *(Log Collection),* FR-3 *(Alert System)*
Priority	High

Identifier	**FR-5**
Title	Anomalous File Creation Detection
Requirement	The system shall detect and alert users about unusual file creation activities based on AI analysis.
Source	Security monitoring needs from Wazuh logs.
Rationale	Helps security analysts detect potential security threats in real time.
Business Rule	Alerts should be generated if a file is created in a restricted directory or by an unauthorized user.
Dependencies	FR-1 *(Log Collection),* FR-2 *(AI-Based Detection)*
Priority	High

Identifier	**FR-6**
Title	Suspicious Login Attempt Detection
Requirement	The system shall monitor and identify too many failed login attempts from a single user or IP address within a short time frame.
Source	Security policy for monitoring unauthorized access attempts.
Rationale	Prevents brute-force attacks and helps in identifying compromised accounts.
Business Rule	The system should generate alerts if failed login attempts 5 within a minute.
Dependencies	FR-1 *(Log Collection),* FR-3 *(Alert System)*
Priority	High

Identifier	**FR-7**
Title	Alert Customization
Requirement	The system shall allow users to configure alert rules and response actions.
Source	Need for customized security management
Rationale	Enables flexibility in responding to specific threats.
Business Rule	Users should be able to set custom thresholds and choose alert methods.
Dependencies	FR-3 *(Alert System)*
Priority	Low

Identifier	**FR-8**
Title	Incident Reporting
Requirement	The system shall enable security analysts to log incidents and document investigation details.
Source	Need for proper incident management and documentation
Rationale	Supports compliance and helps improve future security practices.
Business Rule	Incident reports should include the incident's date, time, actions taken, and resolution.
Dependencies	FR-4 *(Dashboard)*
Priority	High

4. Non-Functional Requirements

4.1 Reliability

- The system shall achieve 99.9% uptime, excluding planned maintenance.
- It shall handle up to 500 MB of daily logs without performance degradation.
- Automated backups shall prevent data loss in case of failure.

4.2 Speed and Performance

- Security logs shall be processed and indexed within 5 seconds.
- Log search queries shall return results within 2 seconds.
- AI-based alerts shall be generated within 1 second of anomaly detection.

4.3 Compatibility

- The system shall support Windows, Linux, and macOS log sources.
- It shall integrate with third-party tools (e.g., Splunk) via APIs.
- Log formats (e.g., Syslog, JSON) shall be supported without manual configuration.

4.4 Scalability

- The system shall process logs from 10–50 endpoints, with the ability to scale to 100+.
- It shall maintain performance with up to 15 GB of monthly logs.
- Alerts shall remain reliable with up to 100 concurrent notifications.

4.5 Maintainability

- Updates shall be applied without downtime using rolling updates.
- Bugs shall be fixed within 24 hours of detection during development.
- Comprehensive documentation shall guide troubleshooting and maintenance.

5. External Interfaces

5.1 User Interface

- Kibana dashboards shall include:
    - Graphs (e.g., login attempt trends, file creation events).
    - Filters (e.g., by time, IP, user).
    - Tables summarizing alerts and incidents.
- Alerts shall be sent via email with clickable links to dashboard details or shown in dashboard.

5.2 Software Interfaces

- **Wazuh**: Collects and processes logs from endpoints.
- **Elastic Stack**: Stores (Elasticsearch), processes (Filebeat), and visualizes (Kibana) logs.
- **AI/ML Models**: Python-based models (e.g., scikit-learn) analyze logs for anomalies.

5.3 Hardware Requirements

- The system needs at least 8GB RAM and 100GB storage.

5.4 Communication

- The system shall use secure HTTPS/TLS for web-based access to Kibana.
- Log data shall be transmitted via encrypted channels (e.g., Wazuh agent protocols).

6. Use Case Analyses

6.1 Use Case 1: Anomalous File Creation Detection

Field	Details
UC Identifier	UC-1
Requirements Traceability	FR-5 (Anomalous File Creation Detection)
Purpose	Detect and alert on unauthorized file creation in restricted directories.
Priority	High
Preconditions	Wazuh agents are monitoring file system logs.
Postconditions	Alerts are generated and logged for analyst review.
Actors	Security Analysts, System Administrators
Extends	None
Main Success Scenario	**1.** System monitors file creation logs. **2.** AI detects a file created in a restricted path (e.g., /etc). **3.** Alert is sent via email and dashboard. **4.** Analyst investigates and deletes the file if malicious.
Alternate Flows	Analyst marks the file as safe if it's legitimate.
Exceptions	If AI fails, Wazuh's default rules trigger alerts.
Includes	FR-1 (Log Collection), FR-2 (AI-Based Detection), FR-3 (Alert System)

6.2 Use Case 2: Suspicious Login Attempt Detection

Field	Details
UC Identifier	UC-2
Requirements Traceability	FR-6 (Suspicious Login Attempt Detection)
Purpose	Detect and alert on too many failed login attempts.
Priority	High
Preconditions	Authentication logs are being collected.
Postconditions	Alerts are triggered if 5+ failed logins occur within 1 minute.
Actors	Security Analysts, System Administrators
Extends	None
Main Success Scenario	1. System tracks login attempts.2. AI detects 5+ failed logins from an IP.3. Alert is sent via email and dashboard.4. Analyst blocks the IP if suspicious.
Alternate Flows	Analyst dismisses the alert if logins are valid.
Exceptions	Network issues log failures, and alerts are queued.
Includes	FR-1 (Log Collection), FR-2 (AI-Based Detection), FR-3 (Alert System)

7. Use Case Diagram

The use case diagram ***(Figure 01)*** illustrates the interactions between actors (Security Analysts, System Administrators) and use cases (UC-1, UC-2). It shows how analysts monitor alerts and administrators configure the system.

- **Actors**: Security Analyst, System Administrator.
- **Use Cases**: Anomalous File Creation Detection, Suspicious Login Attempt Detection.
- **Relationships**: Analyst interacts with both use cases **,** Administrator configures system settings**.**

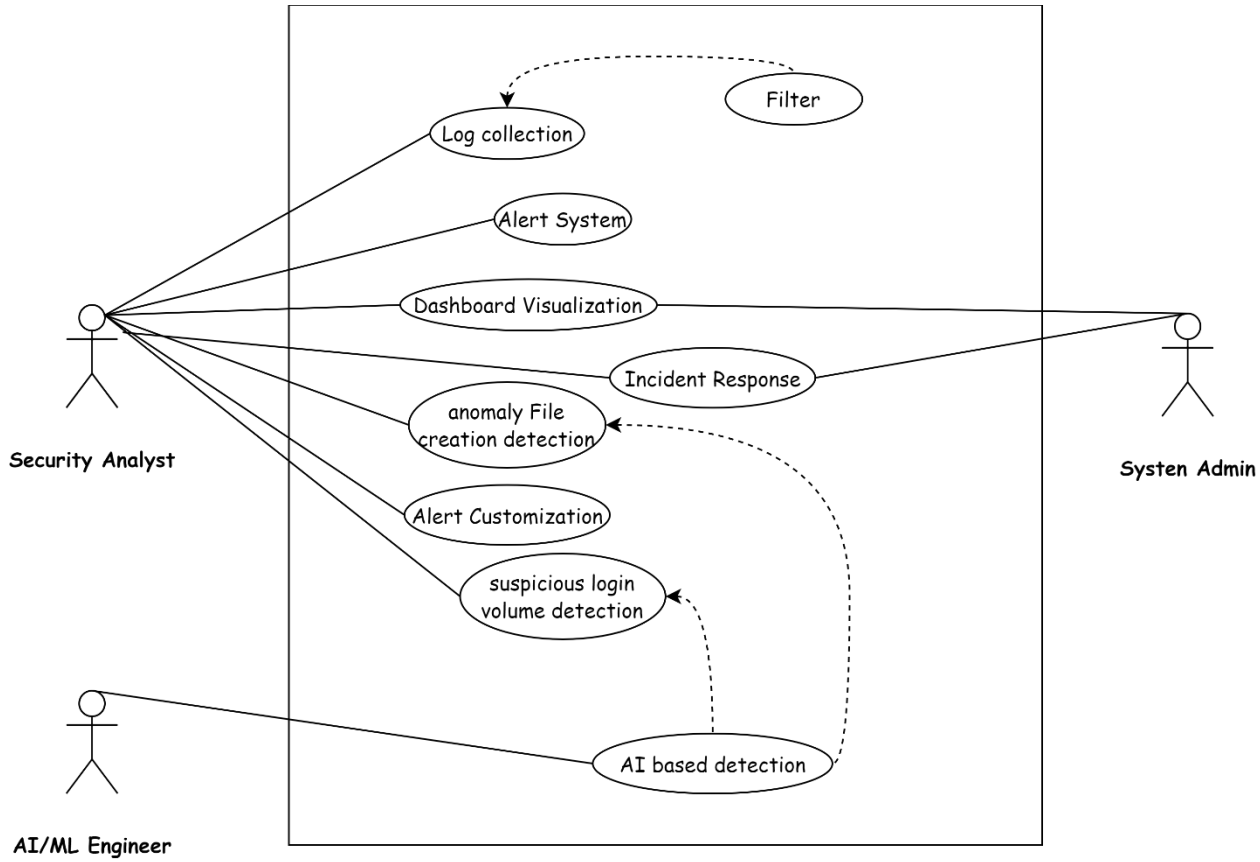

Figure: 01

9. Summary

This document describes an AI-powered anomaly detection system using Wazuh and the Elastic Stack to identify unusual activities, such as *anomalous file creation* and *suspicious login attempts*. The system uses Artificial intelligence for automatic detection, real-time monitoring, and instant alerts, with a clear visualization of data on Kibana dashboards.

Designed for security analysts, system administrators, and AI engineers, it offers features like log collection, customizable alerts, and incident reporting. It supports multiple platforms, scales with growing data, and integrates with other security tools. The system provides clear dashboards and email notifications to keep users informed.

Two key use cases detecting *unusual file creation* and *suspicious logins* demonstrate how it helps security teams respond quickly and effectively

.