AKHUWAT COLLEGE KASUR

DEPARTMENT OF INFORMATION TECHNOLOGY

SOFTWARE REQUIREMENTS SPECIFICATION (SRS)

AI-DRIVEN SECURITY MONITORING: ANOMALY DETECTION USING ELASTIC STACK & WAZUH

SUPERVISED BY:

EBRYX TEAM

&

MR. MUHAMMAD NAEEM AKHTAR

GROUP MEMBERS:

Khalid Hussain

Muhammad Osama

Table of Contents

1 Executive Summary

This document explains what the AI-powered anomaly detection system will do. The system uses Wazuh and the Elastic Stack to help find unusual activities, like:

- **Anomalous File Creation:** When unauthorized files are created.
- **Suspicious Login Attempts:** When there are too many failed login tries.

The system uses Artificial Intelligence (AI) to automatically detect these unusual behaviors. It also provides real-time security monitoring, sends alerts when something suspicious happens, and shows all the important information on easy to read in Kibana dashboards.

2 Requirements Analysis

This section provides a comprehensive analysis of the system's requirements, including user needs, system constraints, and key functionalities.

2.1 User Classes and Characteristics

User Class	Characteristics
Security Analysts	Monitor logs, respond to alerts, analyze security incidents
System Administrators	Configure and manage Wazuh and Elastic Stack components.
AI/ML Engineers	Train and optimize AI models for anomaly detection.

2.2 Requirement Identifying Technique

The requirements were identified using:

- **Use Case Analysis:** Created detailed use cases and diagrams to understand how the system should work in different situations. This helped map out each feature and its interaction with users.
- **Stakeholder Interviews:** Talked to security teams and IT professionals to learn what they need from the system. These interviews provided valuable insights into real-world security challenges and expectations.
- **Data-Driven Approach:** Analyzed real security log data to set performance goals for the AI model. Using real data ensured that the system's anomaly detection capabilities are practical and effective.
- **Research Papers:** Reviewed existing studies and research papers on AI-based security systems and anomaly detection. This research helped identify best practices, potential challenges, and innovative approaches to improve system design.

3 Functional Requirements

3.1 What the System Will Do

ID	Feature	Description
FR-1	Log Collection	The system will collect security logs.
FR-2	AI-Based Detection	The system will use AI to detect unusual activities.
FR-3	Alert System	It will send alerts when a threat is detected.
FR-4	Dashboard	Security data will be displayed in an easy-to-read format.
FR-5	Anomalous File Creation Detection	The system shall detect and alert users about unauthorized or suspicious file creation.
FR-6	Suspicious Login Attempt Detection	The system shall monitor too many failed login attempts and generate alerts for security teams.
FR-7	Alert Customization	Users shall be able to configure alert and response actions.
FR-8	Incident Reporting	Security analysts shall be able to log incidents and document investigation details.

3.2 Requirement Specification for Anomaly Detection

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	Requirement for tailored 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 should work 99.9% of the time without crashing.
- It should be able to handle high amounts of data without slowing down.
- Backup systems should be in place in case of failure to prevent data loss.

4.2 Ease of Use

- The system should have a simple and user-friendly interface.
- Security alerts should be easy to understand, with clear explanations.
- Users should be able to navigate the system easily without needing special training.

4.3 Speed and Performance

- The system should process security logs within 5 seconds.
- When searching for logs, results should appear within 2 seconds.
- AI detection should be send real-time alerts without delays.

4.4 Security

- The system should protect all data using strong encryption.
- Only authorized users should be able to access sensitive information.
- The system should automatically generate log if any unauthorized access attempts.

4.5 Compatibility

- The system should work on different operating systems like Windows and Linux.
- It should be able to integrate with other security tools and applications.
- It should support different types of log sources without requiring extra configuration.

4.6 Scalability

- The system should handle small and large amounts of security data.
- It should be able to grow as more devices and logs are added over time.
- It should still function well even with a large number of security alerts.

4.7 Maintainability

- The system should be easy to update and improve over time.
- Developers should be able to fix issues quickly without affecting system performance.
- Clear documentation should be provided to help in troubleshooting problems.

5 External Interfaces

5.1 User Interface

- The dashboard will have graphs and filters to help users analyze data.
- Alerts will be sent via email

5.2 Software Interfaces

- The system will work with Wazuh and Elastic Stack.
- AI models will process security logs automatically.

5.3 Hardware Requirements

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

5.4 Communication

- The system will use secure web-based connections

6 Use Case Analyses

6.1 USE CASE 1: Anomalous File Creation Detection

UC Identifier	**UC-1**
Requirements Traceability	FR-5 *(Anomalous File Creation Detection)*
Purpose	Detects and alerts security analysts about unusual file creation activities.
Priority	High
Preconditions	Wazuh is monitoring system logs.
Postconditions	Alerts are generated and logged in the system.
Actors	Security Analysts, System Administrators
Extends	None
Main Success Scenario	• System monitors file creation logs. • AI detects an unusual file creation event. • An alert is generated and sent to security analysts. • Analysts review and take action.
Alternate Flows	If the detected activity is normal, the analyst can mark it as safe.
Exceptions	If the AI model fails, default Wazuh rules will trigger alerts.
Includes	*Log Collection* (FR-1), *AI-Based Detection* (FR-2)

6.2 USE CASE 2: Suspicious Login Attempt Detection

UC Identifier	**UC-2**
Requirements Traceability	FR-6 *(Suspicious Login Attempt Detection)*
Purpose	Identifies and alerts security teams about suspicious login attempts in a short time.
Priority	High
Preconditions	The system is actively collecting authentication logs.
Postconditions	Alerts are triggered if login attempts exceed the defined threshold.
Actors	Security Analysts, System Administrators
Extends	None
Main Success Scenario	• The system records login attempts. • AI detects excessive login attempts from the same user or IP. • An alert is generated and sent to security analysts. • Analysts review and take action if necessary.
Alternate Flows	If the login attempts are valid or authorized the analyst can dismiss the alert.
Exceptions	If network issues prevent data collection, the system logs the failure.
Includes	*Log Collection* (FR-1), *AI-Based Detection* (FR-2)

7 Use Case Diagram

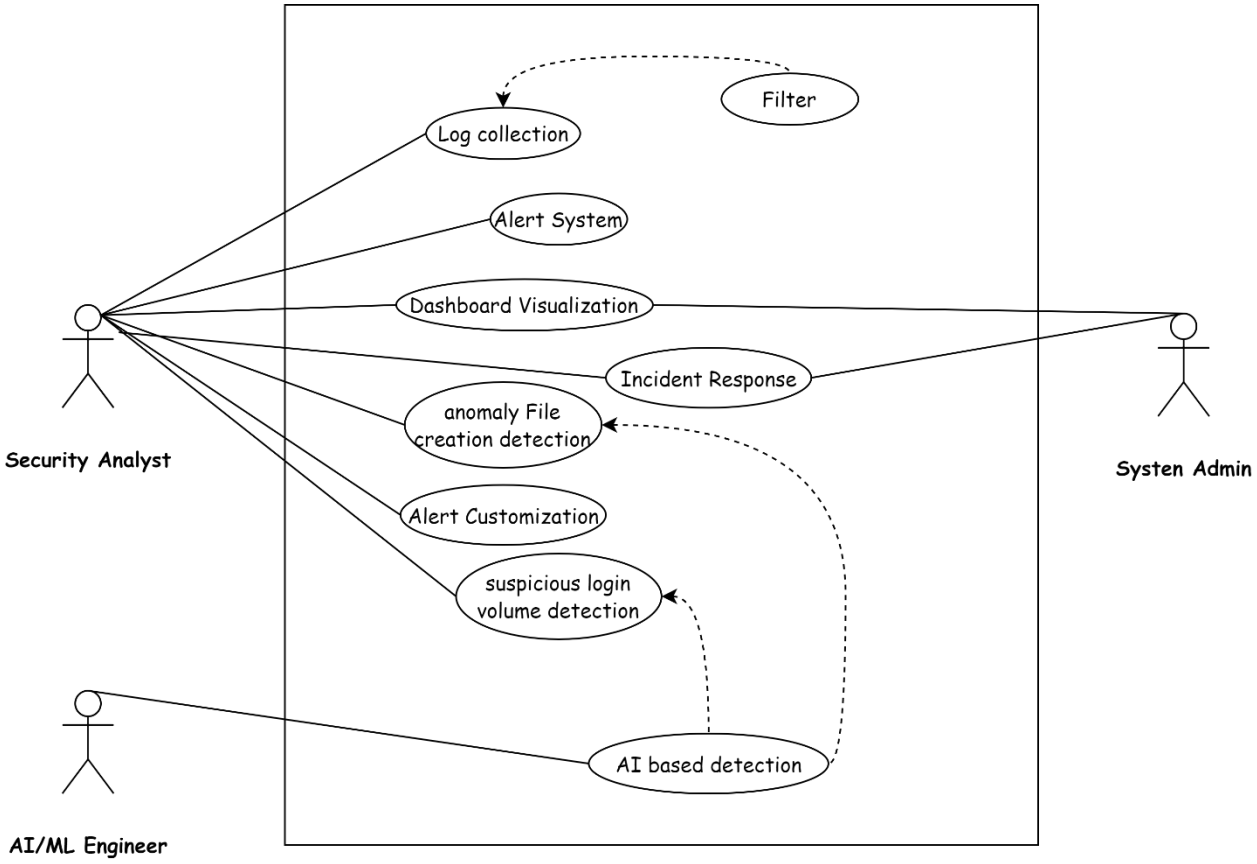

Figure: 01

8 Storyboards

8.1 Anomalous File Creation Detection

1. System continuously monitors file creation activities using Wazuh agents.
2. When an unusual file creation is detected, the system triggers an alert.
3. Alert details are displayed on the Kibana dashboard.
4. The security analyst views the alert information, including file path and creation time.
5. The analyst investigates the source of the file and takes appropriate action, such as deleting the file.

8.2 Suspicious Login Volume Alert

1. System tracks login attempts from all connected devices.
2. If failed login attempts exceed 5 in a minute, the system generates an alert.
3. The Kibana dashboard shows a visual representation of login attempts, highlighting anomalies.
4. The security analyst examines the alert and identifies the suspicious IP address.
5. The analyst blocks the IP address and updates the incident status in the system.

8.3 Incident Reporting and Analysis

1. The security analyst accesses the reporting section in Kibana.
2. The analyst selects report criteria, such as time range and incident types.
3. The system generates a detailed report on security incidents, including graphs and statistics.
4. The analyst downloads the report as a CSV and shares it with the security team.
5. The system stores the report for future analysis and compliance requirements.

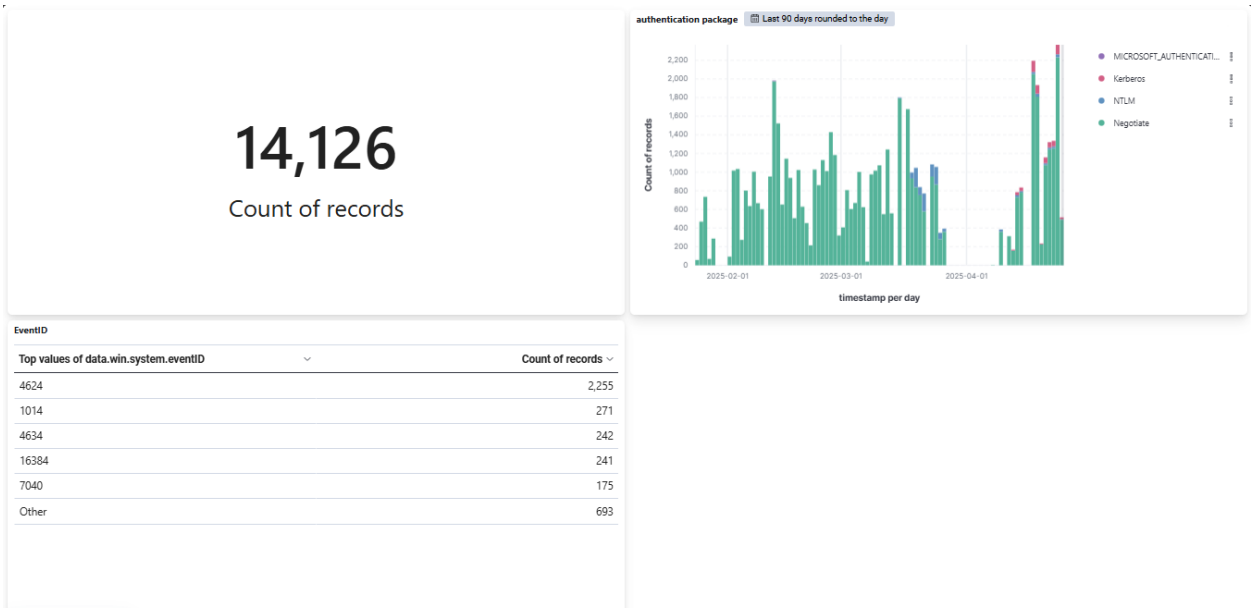

Figure: 04

8 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.