# AI-Driven Network Detection and Response (NDR) System for Cybersecurity in Kenya

## 1. History and Context

Artificial Intelligence (AI) has evolved from simple rule-based systems to advanced machine learning models capable of autonomous decision-making. In cybersecurity, AI’s role has grown critical — helping detect, predict, and mitigate cyber threats faster than human analysts can. Kenya’s rapid digital transformation, fueled by mobile banking, government digitization, and cloud adoption, has unfortunately come with a rise in cyberattacks. The 2024 Cybersecurity Report by KE-CIRT noted over 400 million cyber threat attempts in Kenya alone.

## 2. Problem Statement

Kenyan organizations face increasing cyber threats — phishing, ransomware, insider data leaks, and DDoS attacks — often going undetected until after damage occurs. Current security systems rely heavily on human monitoring or rule-based intrusion detection systems that fail against evolving threats. Small and mid-sized businesses lack automated, intelligent defense tools that adapt in real time.

## 3. Proposed Solution

The proposed solution is an **AI-driven Network Detection and Response (NDR) system** that monitors real-time traffic data, detects anomalies, and classifies threats automatically. The system uses Go-based agents to capture network packets, send structured data to an AI backend (built with FastAPI + scikit-learn), which classifies events as normal, low, or critical threats. High-severity alerts trigger notifications to IT managers while all events are logged for analysis.

## 4. System Overview

1. **Network Agent (Go)**: Captures and sends network flow data in JSON format. 2. **AI Inference API (FastAPI + ML Model)**: Validates input and classifies it using a trained model. 3. **Database Layer (PostgreSQL)**: Stores logs, threat levels, and system metrics. 4. **Alert Engine**: Sends notifications via email/SMS/webhooks for high-severity alerts. 5. **Dashboard (Vue.js)**: Visualizes network patterns, threat statistics, and activity timelines.

## 5. Behind the Scenes

The Go agent uses packet sniffing libraries to capture TCP/UDP headers and metadata, batching them periodically to the backend API. The AI model, trained on historical datasets, uses statistical and machine learning techniques (e.g., RandomForest, IsolationForest) to classify the likelihood of malicious behavior. Over time, it learns patterns specific to the organization's environment.

## 6. Business Model

The system operates under a SaaS (Software as a Service) model, offering three tiers: - **Basic**: For small organizations; limited to traffic logging and anomaly alerts. - **Pro**: Includes AI threat classification and dashboard analytics. - **Enterprise**: Adds integrations, incident response automation, and 24/7 monitoring support.

## 7. Market and Competitors

Global players like Darktrace, Vectra AI, and Cisco Secure dominate the NDR market. However, they are costly and often inaccessible to African SMEs. Our localized system offers affordability, real-time performance, and adaptability to Kenyan infrastructure realities, such as mixed on-premise and mobile networks.

## 8. Future Plans

1. Integrate large language models (LLMs) for intelligent report generation and contextual threat summaries. 2. Build a federated learning module so the AI can learn across multiple institutions without exposing sensitive data. 3. Expand into regional markets across East Africa with cybersecurity compliance features.

## 9. Challenges

1. Access to high-quality labeled network data for training. 2. Balancing accuracy with real-time performance. 3. Resistance to AI adoption due to trust issues and limited awareness. 4. Infrastructure differences in rural vs. urban deployments.

## 10. Cost Summary

- Development (AI, backend, frontend): KES 2.5M - Cloud Infrastructure & APIs: KES 800,000 annually - Marketing & Compliance: KES 500,000 - Total Estimated Initial Investment: ~KES 3.8M

## 11. Tools Summary

- **Go** – Lightweight network packet capture agent. - **FastAPI** – Backend for AI inference and APIs. - **Scikit-learn** – Machine learning model for threat classification. - **PostgreSQL** – Data storage. - **Docker** – Deployment and scalability. - **Vue.js** – User dashboard. - **Prometheus + Grafana** – Metrics and performance monitoring.