

# CyberSentry AI

MVP Development Roadmap | 7 Critical Checkpoints

Protecting Kenya's Digital Future with AI-Powered Cybersecurity

# The 21-Day Journey

From Concept to Production-Ready MVP in 3 Weeks, 7 Checkpoints, 21 Days

## Week 1

Foundation & AI Core  
(Checkpoints 1-2)

## Week 2

Automation & Dashboard  
(Checkpoints 3-4)

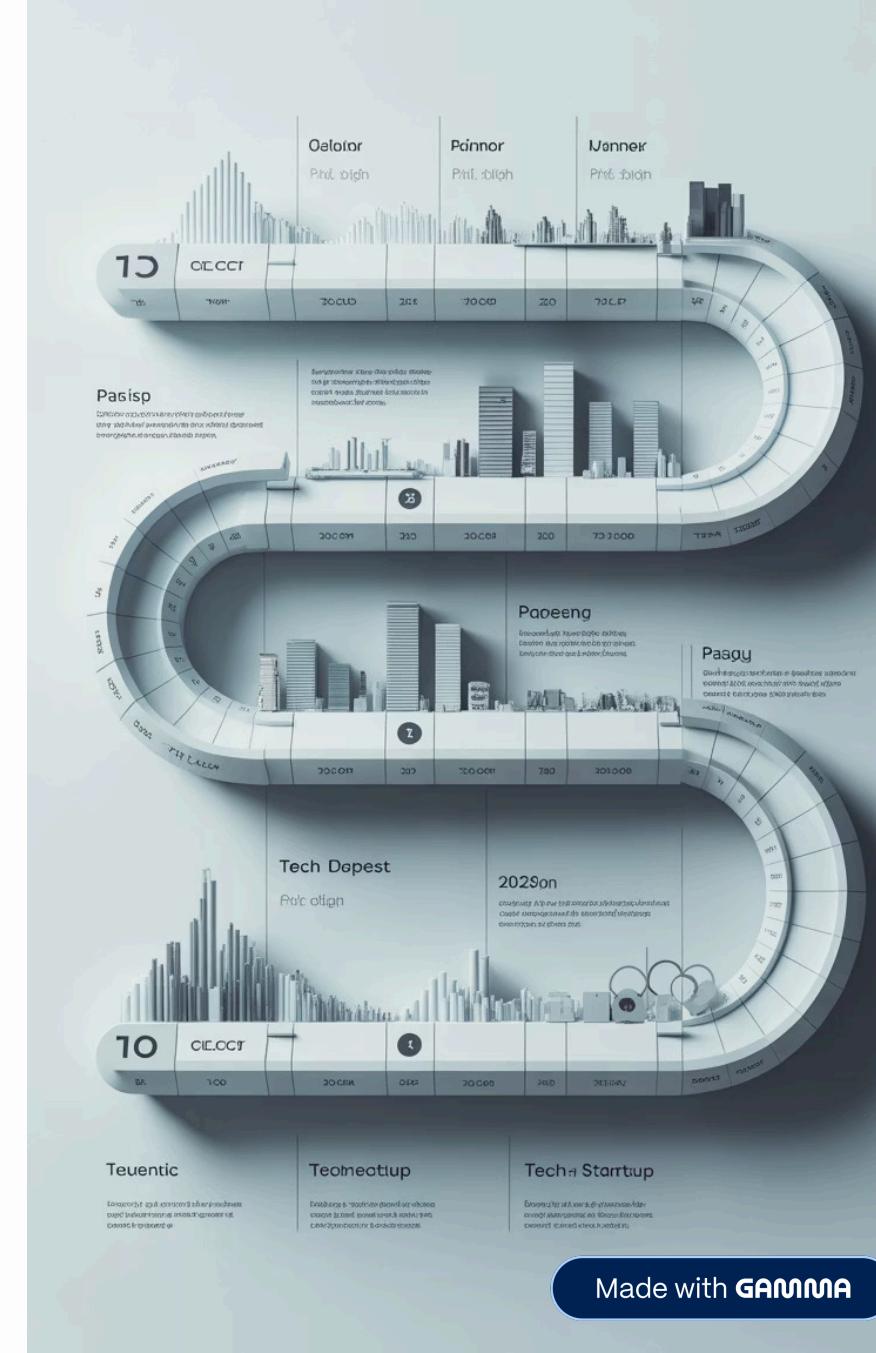
## Week 3

Polish & Deployment  
(Checkpoints 5-6)

## Week 4

Presentation Ready (Checkpoint  
7)

Success Philosophy: Deliver a polished, functional product that demonstrates real value through AI-driven cybersecurity with Kenyan context.



# Week 1 - Foundation & AI Intelligence

CHECKPOINTS 1-2

DAYS 1-7

## Checkpoint 1: Foundation

### Days 1-3

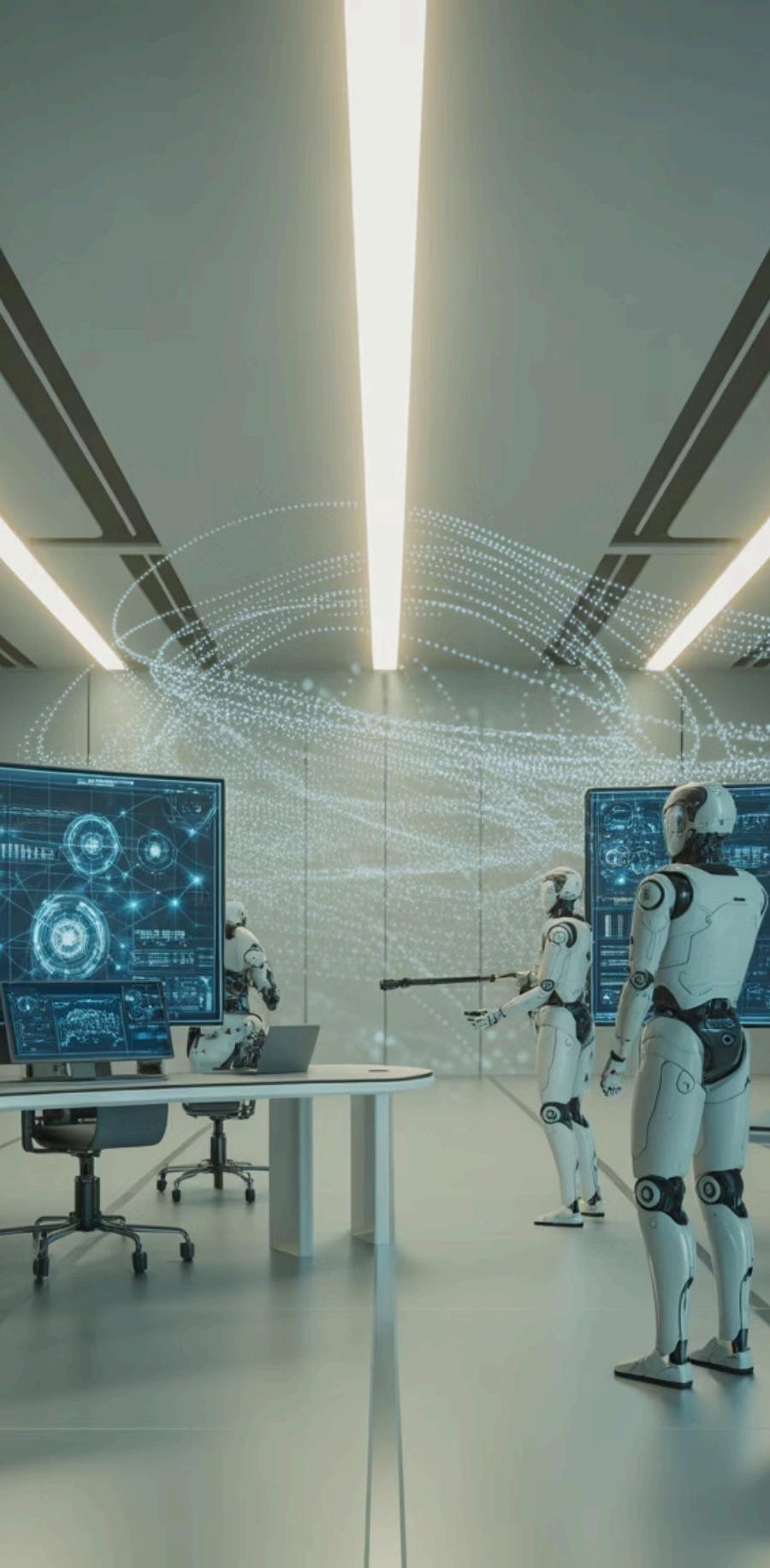
- Complete database schema (5 tables) with PostgreSQL
- Core API endpoints (5+) with Swagger/OpenAPI docs
- JWT authentication system
- Docker Compose for one-command onboarding
- Git workflow and project structure

## Checkpoint 2: AI Intelligence

### Days 4-7

- Malware detection model (>90% accuracy)
- File upload & analysis API (<3s processing)
- Feature extraction pipeline + behavioral analytics
- User risk scoring (0-100)
- Archive/ZIP/RAR, PDF, Office macros, image steganography detection

**Success Criteria:** Database operational | 5+ APIs tested | Auth working | Docker builds | Model >90% accurate | Multi-format file analysis working



# Week 2 - Multi-Agent Automation System

CHECKPOINT 3

DAYS 8-10

Goal: Intelligent, Autonomous Threat Response



SENTRY Agent

Alert coordinator and prioritization



Hunter Agent

Proactive threat hunting in user directories



Responder Agent

Autonomous incident response and quarantine

Threat Correlation

Severity classification (4 levels),  
automated response with  
account suspension, email/SMS  
notifications, full audit trail

Kenyan-Specific

M-PESA fraud pattern detection  
and SIM swap attack  
identification

# Week 2 - Dashboard Foundation

CHECKPOINT 4

DAYS 11-14

Goal: Real-Time Security Command Center



## Core Features

Main overview with metrics and 5+ interactive charts, real-time threat feed (30s auto-refresh), user management and file analysis interfaces, agent activity log, <2s load time



## Kenyan Context

Kenyan threat landscape visualization, Swahili language toggle (Tishio/Threat, Hatari/Danger, Salama/Safe), mobile-responsive design verified on actual devices

**Success Criteria:** Dashboard loads <2s | Real-time updates | Charts render correctly | Responsive design | Agents visible | Swahili elements present

# Week 3 - Demo Excellence

CHECKPOINT 5

DAYS 15-17

Goal: Compelling Storytelling Through Data

## Demo Data

- 100+ realistic demo users
- 50+ threat incidents (varied severity)
- Three scripted hero scenarios with narrative arcs

## Polish & Features

- Professional UI/UX (colors, animations, smooth transitions)
- Admin features complete
- Settings & configuration page
- 2-3 minute demo video as live backup
- Offline Docker container for laptop-local fallback

### M-PESA Fraud

Transaction fraud detection story

### Malware Attack

Multi-stage attack response

1

2

3

SIM Swap

Incident timeline visualization

# Week 3 - Cloud Deployment

CHECKPOINT 6

DAYS 18-19

Goal: Secure, Scalable Production Environment

## Deployment Stack

Railway or Render hosting, GitHub Actions CI/CD pipeline, environment secrets management, security hardening with headers and penetration testing, backend deployed with HTTPS, dashboard deployed and connected

## Performance Targets

Load testing passed for 50+ concurrent users, <2s response time, zero security vulnerabilities

**Success Criteria:** Public URL accessible | HTTPS enabled | No vulnerabilities | <2s response | CI/CD operational

# Week 4 - Presentation Arsenal

CHECKPOINT 7

DAYS 20-21

Goal: Winning Presentation Package

## Core Deliverables

- 3-4 demo scenarios prepared and rehearsed
- Pitch deck complete (10-12 slides)
- Demo video recorded (2-3 min)
- One-pager for judges
- 5+ presentation rehearsals
- Q&A responses prepared
- Multiple backup plans

## Strategic Additions

- "Why Kenya" slide: Market validation, local impact, opportunity size
- Agent architecture diagram: Multi-agent system vision
- Competitor matrix: Global vs local solutions comparison
- 30-second elevator pitch: For spontaneous opportunities
- Live demo + video side-by-side for seamless switching

# Technical Excellence Summary

## What Makes CyberSentry AI Unique



### AI Capabilities

90% malware detection accuracy, <3s file analysis (archives, PDFs, Office docs, images), multi-agent autonomous response system, behavioral analytics and risk scoring



### Kenyan-First Features

M-PESA fraud pattern detection, SIM swap attack identification, Swahili language support, local cybercrime landscape integration



### Performance Metrics

<2s dashboard load time, 50+ concurrent user support, real-time threat correlation, automated response within seconds



### Deployment Ready

Docker containerized, CI/CD automated, cloud deployed with HTTPS, offline demo capability

# Ready to Protect Kenya's Digital Future

21

Days to MVP

From concept to production-ready

7

Critical Checkpoints

Structured development milestones

3

AI Agents

Autonomous threat response system

90%

Detection Accuracy

Malware identification rate

CyberSentry AI combines world-class AI technology with deep understanding of Kenya's unique cybersecurity challenges. Our multi-agent system, Kenyan-first features, and production-ready deployment make us the definitive solution for protecting Kenya's digital future.