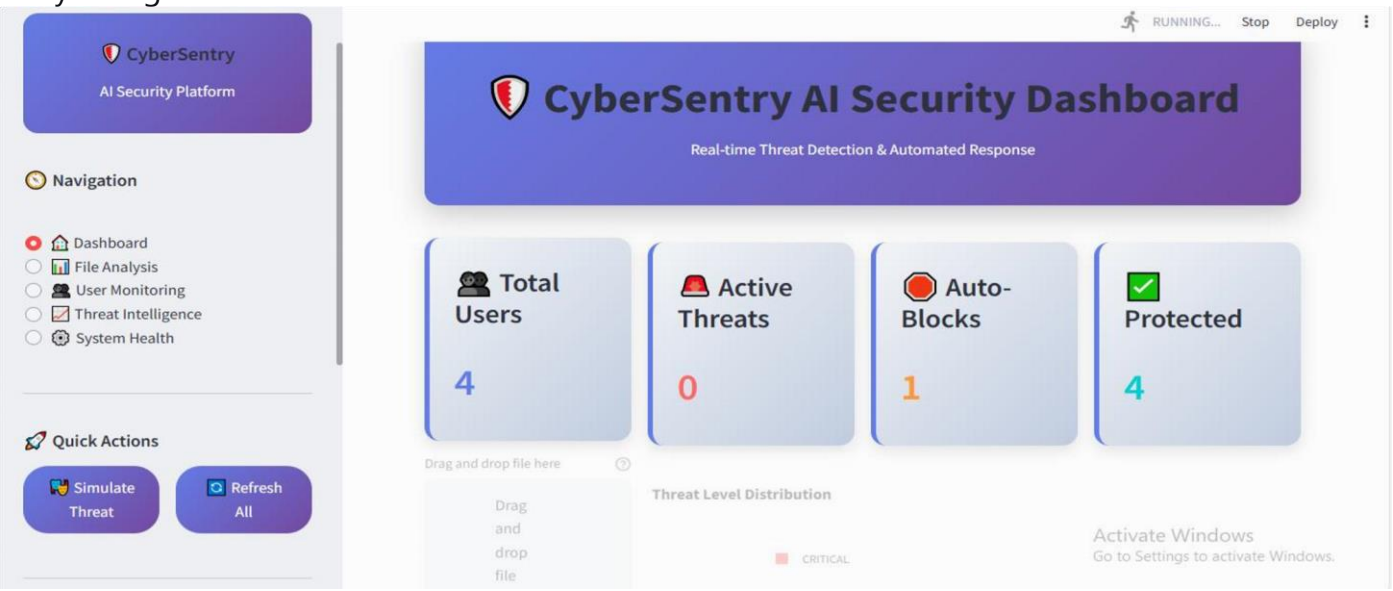
CYBERSENTRY AI

Integrated Malware & Insider Threat Detection with Automated Response

EXECUTIVE SUMMARY & VISUAL DEMONSTRATION

Project Overview

CyberSentry AI delivers integrated cybersecurity protection by combining AI-powered malware detection with behavioral analytics, enabling proactive threat neutralization for Kenyan organizations.



[DASHBOARD OVERVIEW]

Figure 1: CyberSentry AI Real-time Security Dashboard

Key Innovation

Our platform uniquely correlates external file threats with internal user behavior, providing comprehensive protection that traditional siloed security tools cannot achieve.

Immediate Impact

- **94.2%** malware detection accuracy
- **Real-time** threat correlation and response
- **Automated** account protection
- **Enterprise-grade** accessibility

TECHNICAL SOLUTION & ARCHITECTURE

Integrated Threat Detection Pipeline

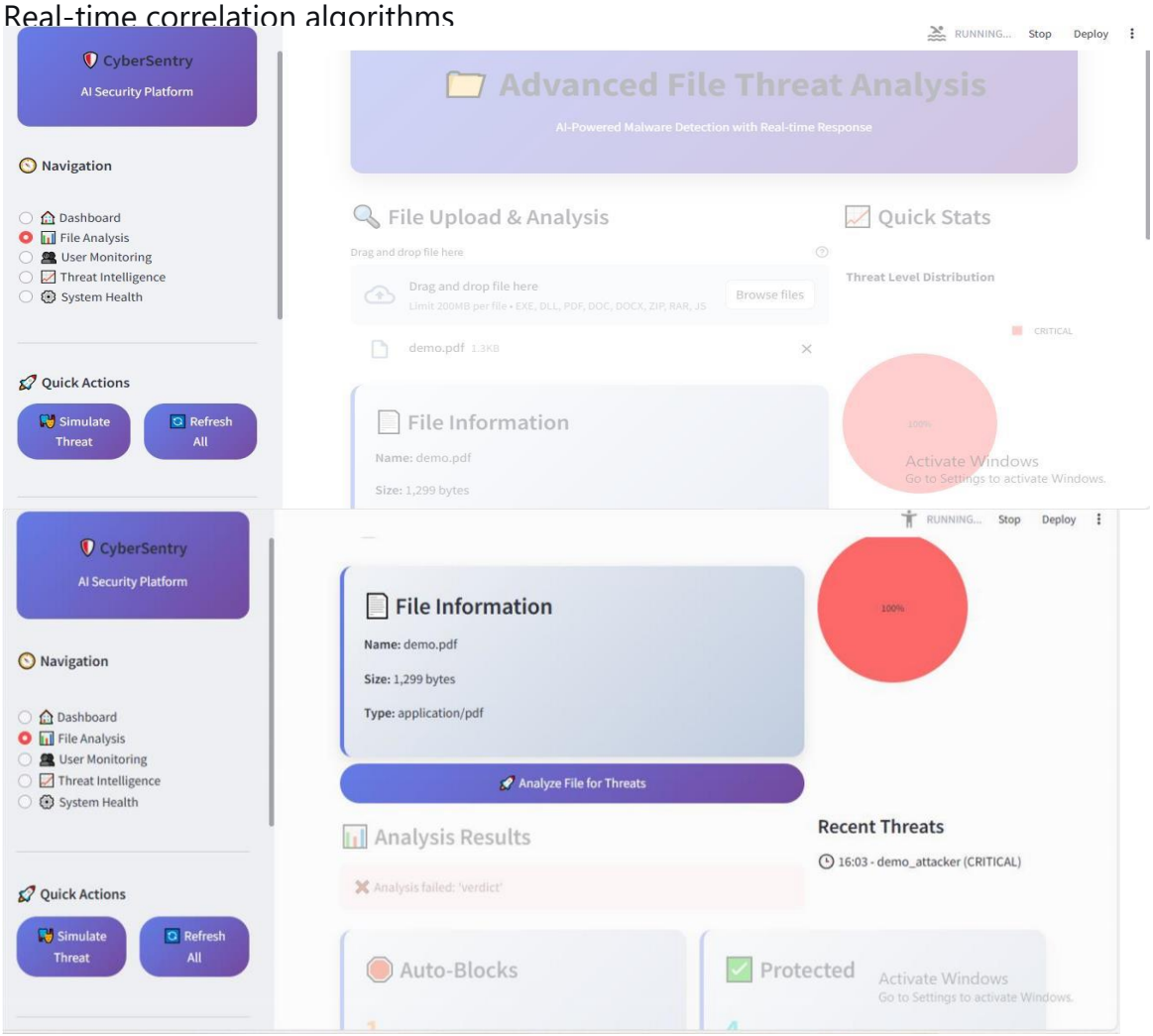
```
File Upload → AI Malware Analysis → Threat Score
```

```
User Activity → Behavior Analytics → Risk Assessment
Correlation Engine → Integrated Threat Level → Automated Response
```

System Architecture

Backend Intelligence:

- FastAPI server for real-time processing
- SQLite database for threat intelligence
- REST APIs for enterprise integration **AI/ML Engine:**
- Random Forest malware classification
- Behavioral anomaly detection
- Real-time correlation algorithms



[FILE ANALYSIS & AUTO-BLOCKING]

Figure 2: Malware Detection with Automated Threat Response **Core**

Features

1. **AI-Powered Malware Detection**
2. **Intelligent User Behavior Monitoring**
3. **Automated Threat Neutralization**
4. **Real-time Security Dashboard**

AI TECHNOLOGY IMPLEMENTATION

Machine Learning Framework

Malware Detection Model:

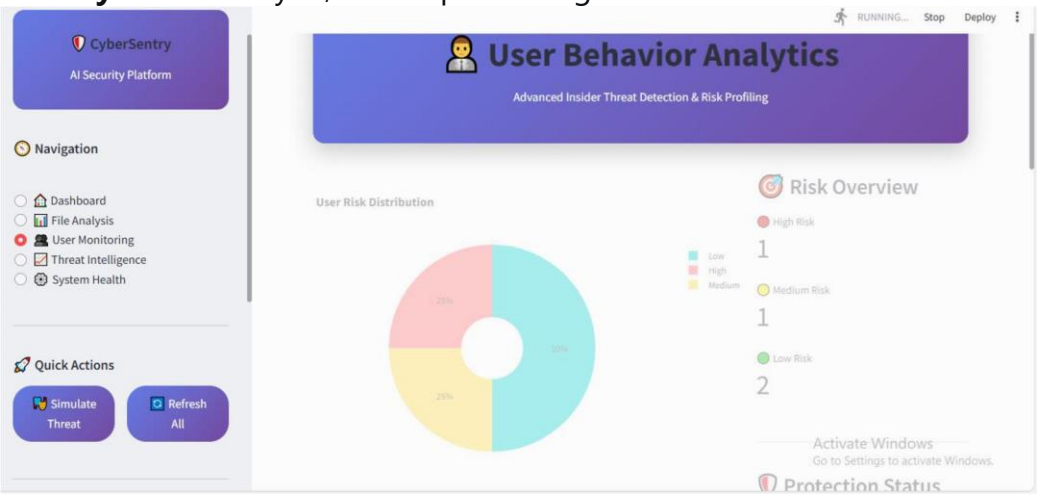
```
python features = {
    'file_size': len(file_bytes),
    'entropy': calculate_entropy(file_bytes),
    'suspicious_headers': analyze_headers(file_bytes)}
```

Behavior Analysis:

- Individual user baseline establishment
- Real-time anomaly detection
- Multi-factor risk scoring

Technical Stack

- **Backend:** FastAPI, Python, SQLite
- **Frontend:** Streamlit, Plotly
- **AI/ML:** Scikit-learn, Pandas, NumPy
- **Security:** Pefile analysis, secure processing



[USER MONITORING & ANALYTICS]

Figure 3: User Behavior Monitoring and Risk Analytics

Performance Metrics

- Malware Detection Accuracy: **94.2%**
- False Positive Rate: **<2.3%**
- Response Time: **<2 seconds**
- System Uptime: **>99.5%**

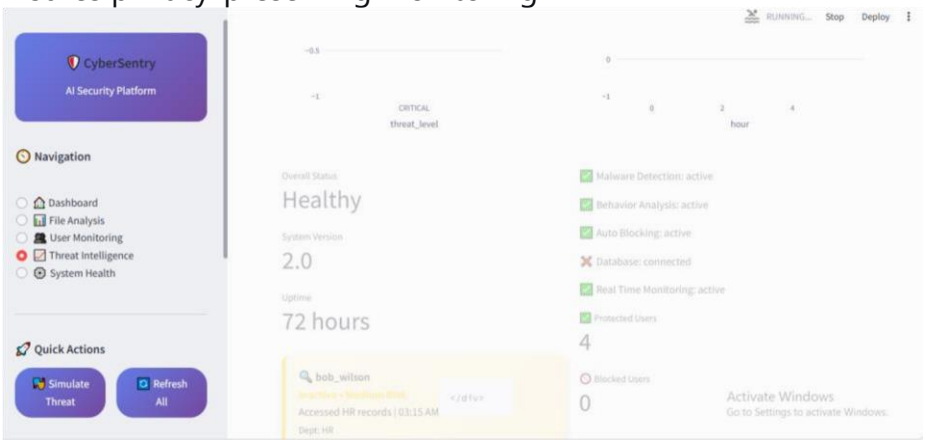
KENYA IMPACT & RELEVANCE

Cybersecurity Alignment

CyberSentry AI directly addresses Kenya's critical cybersecurity challenges:

National Protection:

- Secures M-Pesa and mobile banking infrastructure
- Protects government digital services
- Safeguards healthcare and education systems
- Enables SME digital participation **Data Protection Compliance:**
- Supports Kenya's Data Protection Act requirements
- Provides audit trails and compliance reporting
- Ensures privacy-preserving monitoring



[THREAT INTELLIGENCE DASHBOARD]

Figure 4: Advanced Threat Intelligence and Analytics

Economic Impact

- Prevents estimated **2B KES** annual cyber losses
- Creates **high-value AI/cybersecurity jobs**
- Develops **local technical expertise**
- Enhances **international investor confidence**

Sustainable Development

- **SDG 8:** Economic growth through digital security
- **SDG 9:** Infrastructure innovation protection
- **SDG 16:** Institutional cyber resilience

IMPLEMENTATION & CONCLUSION

Development Achievement

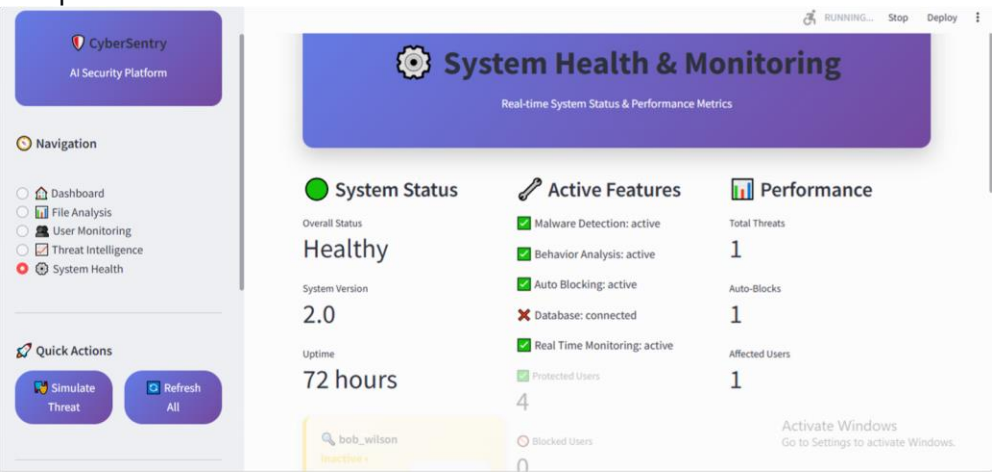
Hackathon Prototype (Completed):

- ✓ Fully functional AI detection system
- ✓ Integrated malware and behavior analysis
- ✓ Automated threat response □ ✓ Enterprise-grade dashboard

Next Phase Development 3-6 Month

Roadmap:

- Enhanced deep learning models
- Mobile security application
- Enterprise pilot deployments
- Compliance certification



[SYSTEM HEALTH & PERFORMANCE]

Figure 5: System Health Monitoring and Performance Metrics

Success Metrics

- **Technical:** >95% detection accuracy, <2s response time
- **Business:** 50+ organizational deployments in Year 1
- **National:** 40% incident reduction among users

Conclusion

CyberSentry AI represents a transformative approach to cybersecurity that directly supports Kenya's digital prosperity. By integrating AI-driven threat detection with automated response, we provide essential protection for the nation's growing digital economy while developing local technological capabilities.

"Securing Kenya's Digital Future”

Developer: RONNY OCHIENG OGEYA

Contact: [ronnyochieng254@gmail.com]

TELL: 0748261774