MITCHELE JEBET

Cybersecurity Analyst & Security Tool Developer

🖂 jebetmichele@gmail.com | 📍 Nairobi, Kenya

📎 LinkedIn: linkedin.com/in/mitchele-jebet | GitHub: github.com/Girlweb

🌐 Portfolio: mitchele-portfolio.vercel.app

PROFESSIONAL SUMMARY

Technical Cybersecurity Analyst with software development expertise specializing in building security automation tools, AI-powered threat detection systems, and DevSecOps solutions. Combines deep security knowledge with practical coding skills (Python, SQL, Bash) to develop scalable security applications. Proven track record building production-ready security tools including LLM-powered applications, ML-based fraud detection systems, and automated vulnerability scanners. Unique blend of cybersecurity analysis, software engineering, and machine learning enables creation of innovative security solutions rather than just reactive threat response.

TECHNICAL EXPERTISE

Security Development: Security tool development, Automation scripting, DevSecOps pipeline integration, API security, Secure coding practices, Security testing frameworks

Programming & Development: Python (Advanced - 2+ years), SQL, Bash scripting, Git/GitHub, Docker, CI/CD (GitLab CI, Jenkins), RESTful APIs, Web application development (Streamlit, Flask basics)

AI/ML Security Applications: LLM integration (Llama3.3), Machine learning for security (classification, anomaly detection), Prompt engineering, AI model security, Pattern recognition algorithms, Supervised/unsupervised learning

Cybersecurity Tools: Wireshark, Burp Suite, Metasploit, Nmap, Kali Linux, SIEM tools (Wazuh, Splunk), Forensic tools

Security Analysis: Vulnerability assessment, Penetration testing, Threat modeling, Security architecture review, Code security review, Network traffic analysis

Data & Analytics: Pandas, NumPy, Data visualization, Statistical analysis, Log analysis, Threat intelligence analysis

Cloud & Infrastructure: Docker containerization, Infrastructure as Code (Terraform), Cloud security basics, Linux system administration

---

EDUCATION

Bachelor of Electrical Engineering (In Progress) | Kenyatta University, Nairobi

Advanced AI/ML Development Program | Women in Tech Initiative | 2025

Focus: LLM Application Development, ML Model Building, NLP, Feature Engineering, Production Deployment

Professional Cybersecurity Analysis Program | Moringa School | 2025

Focus: Security Tool Development, Threat Detection, DevSecOps, Incident Response

Professional Foundations in Technology | ALX Africa | 2025

PROFESSIONAL PROJECTS & SECURITY TOOL DEVELOPMENT

LinkedIn Post Generator - Production LLM Application | October 2024

Tech Stack: Python, LangChain, Llama3.3 (70B), Groq Cloud API, Streamlit

GitHub: github.com/Girlweb/linkedin-post-generator | Live Demo Available

- Architected and deployed production-ready generative AI application processing 1000+ user requests
- Engineered sophisticated prompt engineering framework ensuring consistent, high-quality LLM outputs with 95% user satisfaction
- Implemented robust API authentication, rate limiting, and error handling for Groq Cloud integration
- Built full-stack web application using Streamlit with real-time inference, input validation, and responsive UI
- Applied security best practices including input sanitization, API key management, and secure credential storage
- Developed modular, maintainable codebase with comprehensive documentation following software engineering standards
- Demonstrated ability to rapidly learn and implement cutting-edge AI technologies in production environment

Key Technical Achievement: Migrated from deprecated model to llama-3.3-70b-versatile, resolved dependency conflicts, implemented CSS fixes - showcasing debugging and problem-solving skills

DevSecOps Security Assessment Platform | 2024 - Ongoing

Tech Stack: Python, Docker, Jenkins, GitLab CI, Terraform, SonarQube

GitHub: github.com/Girlweb/devsecops-pipeline-assessor

- Developing automated security scanner for CI/CD pipelines combining static analysis with ML-based vulnerability detection
- Building pattern recognition algorithms in Python analyzing 10,000+ code commits for security risks and compliance violations
- Implementing containerized testing environments with Docker ensuring reproducible security assessments
- Integrating with GitLab CI and Jenkins for automated security scanning in development workflows
- Applying Infrastructure as Code principles with Terraform for consistent security configuration deployment
- Creating comprehensive security reporting dashboard with risk scoring and remediation tracking

Technical Impact: Automated manual security review process saving 15+ hours weekly, identified 50+ security issues before production

AI-Powered Fraud Detection & Anomaly Detection System | 2024

Tech Stack: Python, Scikit-learn, Pandas, NumPy, Feature Engineering, Statistical Modeling

GitHub: github.com/Girlweb/ai-data-annotation-tool

- Engineered ML-based fraud detection system achieving 99% accuracy in identifying anomalous patterns across 50,000+ transactions

- Built supervised learning pipeline training Random Forest and XGBoost classifiers on historical fraud data
- Developed 25+ engineered features from raw data including temporal patterns, transaction velocity, behavioral signatures
- Implemented data preprocessing pipeline handling missing data, outlier detection, and feature scaling
- Created automated alerting system generating structured reports in JSON/CSV for security operations integration
- Applied cross-validation and hyperparameter tuning achieving 40% reduction in false positive rate

Technical Innovation: Combined traditional rule-based fraud detection with ML ensemble methods for superior accuracy

Network Security & IoT Forensics Investigation Tool | 2024

Tech Stack: Python, Wireshark, Protocol Analysis, Network Security, Forensic Documentation

- Developed automated network traffic analysis tool for IoT device security assessment and protocol vulnerability detection
- Built Python scripts processing 100,000+ network packets identifying MQTT protocol weaknesses and unencrypted communications
- Implemented systematic evidence collection and chain-of-custody documentation following forensic best practices
- Created threat modeling framework identifying 12 critical vulnerabilities including authentication bypass mechanisms
- Generated automated security reports with CVSS scoring, risk prioritization, and technical

remediation guidance

Technical Achievement: Reduced manual packet analysis time from 8 hours to 45 minutes through Python automation

Security Challenge Platform Achievements | TryHackMe & HackTheBox | 2023 - Present

- Ranked Top 15% of TryHackMe users (50+ completed challenges) - Certificate: THM-850TRUZ5A3
- Specialized in: Web application security, network penetration testing, privilege escalation, binary exploitation
- Developed Python automation scripts for common security testing tasks reducing engagement time by 60%
- Practiced secure coding review, vulnerability analysis, and exploit development in controlled environments
- Created detailed technical write-ups documenting attack chains, proof-of-concepts, and remediation strategies

---

CERTIFICATIONS & PROFESSIONAL DEVELOPMENT

Cisco Certified Network Associate (CCNA) | Cisco Networking Academy | 2023

ArcX Cyber Threat Intelligence (CTI) Specialist | ArcX | 2024

TryHackMe Pre-Security Learning Path | Certificate: THM-850TRUZ5A3 | 2024

Cisco Endpoint Security Badge | Cisco Networking Academy | 2024

TECHNICAL COMPETENCIES SUMMARY

Development: Python (Advanced), SQL, Bash, Git, Docker, CI/CD, APIs, Web development

AI/ML: LLMs (Llama3.3), LangChain, Scikit-learn, Feature engineering, Model deployment

Security: Penetration testing, Vulnerability assessment, Security automation, DevSecOps, Forensics

Tools: Wireshark, Burp Suite, Metasploit, Nmap, Kali Linux, Splunk, Jenkins, GitLab

Systems: Linux administration, Network security, Cloud security, Infrastructure as Code

---

KEY DIFFERENTIATORS

Technical Depth: Not just a security analyst - builds production security tools and applications from scratch using Python, ML frameworks, and modern development practices

AI/ML Security Expertise: Rare combination of cybersecurity knowledge with practical AI/ML development experience enabling creation of intelligent security solutions

DevSecOps Mindset: Understands both security requirements and software development lifecycle, builds security into development process rather than bolt-on afterwards

Proven Builder: GitHub portfolio demonstrates ability to deliver complete, functional security applications - not just theoretical knowledge

Problem-Solving Approach: Automates repetitive security tasks through code, builds tools that scale, applies data-driven approaches to threat detection

Quick Learner: Rapidly masters new technologies (LLMs, cloud platforms, security tools) and applies them to solve real security challenges

---

PROFESSIONAL AVAILABILITY

Open to remote, hybrid, and on-site opportunities.

Available for immediate or flexible start dates.

Location: Nairobi, Kenya | Work Authorization: Kenyan Citizen

Languages: English (Fluent), Swahili (Native)

REFERENCES

Professional references available upon request