MIKE MORETI

CYBERSECURITY ANALYST | SOC SPECIALIST

CONTACT

📞 +254745620302

✉ garisonmike006@gmail.com

Personal Website

https://garisonmike.github.io

📍 Kenya

SKILLS

Technical Skills

- SIEM: Wazuh
- IDS/IPS: Suricata
- Analysis: Wireshark, tcpdump
- OS: Linux/Unix, Windows
- Languages: Python, Java
- Frameworks: Django, Flutter

Security Skills

- Threat Detection & Hunting
- Firewall Management
- Incident Response
- Network Security Monitoring
- Log Analysis & Correlation
- Penetration Testing

LANGUAGES

- ENGLISH
- SWAHILI

SUMMARY

Computer Science student and ALX-certified Cybersecurity Specialist with hands-on expertise in SOC operations and secure backend development. Proven ability to deploy SIEM solutions (Wazuh), analyze network threats (Suricata), and architect secure applications using Django and Flutter. Skilled in bridging offensive and defensive security through threat hunting, penetration testing, and "security-by-design" development practices.

TECHNICAL EXPERIENCE

Cybersecurity & SOC Lab

- Architected and deployed a 3-node **Security Operations Center (SOC)** lab environment using **VirtualBox** to simulate enterprise network attacks and defense.
- Configured a **Wazuh Manager** on Ubuntu live server to monitor Windows 10 and Kali Linux machines, utilizing **Sysmon** and **auditd** for granular endpoint telemetry and log analysis.
- Implemented **Suricata** as a Network Intrusion Detection System (IDS) to identify malicious traffic patterns and practiced threat hunting using SIEM dashboards.
- Conducted controlled red-team simulations (Evil Twin, Wi-Fi deauth, credential harvesting simulations) to analyze WPA2 attack vectors and defensive controls.
- Documented security findings and lab configurations on tiktok.

Security-Focused Software Engineering

- **Data Analysis & Integrity:** Built a **Church Data Analysis** tool using Flutter to process complex datasets while ensuring data privacy and structural integrity.
- **Task Management & Privacy:** Developed a full-stack **Django** application (`taskManagementApp`) with a focus on secure user authentication and data persistence.
- **Secure Mobile/Web Systems:** Engineered multi-platform applications including `CampusRentalFinder` and `getSocial` (Flutter/Django), implementing **Role-Based Access Control (RBAC)** and input validation to prevent common web vulnerabilities (OWASP Top 10).

- **Anonymity & Abuse Prevention:** Developed `anonymous_24hr_post`, a project centered on privacy-focused system architecture and abuse-prevention controls.

EDUCATION

Bachelor of Science in Computer Science

KIRINYAGA UNIVERSITY - KIRINYAGA
2024 - Expected 2028

Focus: **Software Engineering, Cybersecurity, Network Architecture**

Cybersecurity Specialization

ALXAFRICA
21/10/2025 - 28/01/2026

Focus: SOC Operations, Threat Detection, Incident Response

Backend Development Bootcamp

ALXAFRICA
05/05/2025 - 9/12/2025

Focus: Secure API Development, Authentication, Web Security