Victor Nthuli

victornthuli269@gmail.com | +254724082859 | Nairobi, Kenya | https://www.linkedin.com/in/victor-nthuli

Security Operations Engineer specializing in incident response, threat hunting, and compliance alignment for regulated industries.

Experience

Managing Director — SOCDEV AFRICA

Apr 2025 – Present

Security Operation Center & Development Company. Lead overall company strategy, execution, and growth, combining cybersecurity operations and innovative software solutions. Architected and deployed a full-stack, multi-tenant authentication system with biometric integration and role-based access control. Led threat detection, SIEM integration, and vulnerability assessments for diverse clients across Africa. Fostered a DevSecOps-centered engineering culture with a strong focus on mentorship and open-source contribution.

Security Engineer — Revere Tech

Mar 2026 – Present · Remote

Security engineering support spanning infrastructure hardening, monitoring, and incident response.

Security Consultant — Confidential (Kenyan Government / Defense-sector client)

Apr 2026 – Present

Providing security engineering and operations support for a government client. Scope and technical details withheld due to the sensitivity of the engagement.

Security Operations Engineer — Webmasters K Ltd

May 2023 – Apr 2025

Software Development Company. Conducted web and mobile application security testing and penetration assessments. Oversaw SIEM design, deployment, and integration with IT infrastructure. Led the secure deployment of OpenStack cloud environments and developed internal audit controls. Resigned in April 2025 due to strategic differences on execution timelines and internal alignment.

Technical Intern — Umar Auto Garage

Jul 2022 – Sep 2022

Vehicle System Monitoring and Wiring. Performed diagnostics, maintenance, and engine replacement tasks. Gained foundational understanding of system monitoring and technical operations.

Education

BSc. Applied Computer Technology — United States International University – Africa

2019 – 2023

Concentration: Cybercrime & Forensic IT

KCSE — Light Academy Highschool

2015 – 2018

KCPE — Rockfields Junior School

2007 – 2014

Certifications

• Certified Cyber Security Technician (CCT) (In Progress)

• Getting Started with MITRE ATT&CK; (2024-11-07)

• Burp Suite Basics (2024-10-02)

• Zero to Linux with Hal Pomeranz (2024-09-05)

• Conquering your CISSP (2024-09-04)

• The Illustrated Pentester (2024-08-29)

• Fearless Forensic Shell Fu (2024-08-28)

• New Methods to Attack & Defend Active Directory (2024-08-07)

• Introduction to OSINT (2024-07-19)

• Active Defense & Cyber Deception (2024-07-18)

Skills

Security: Security Monitoring & Incident Response, SIEM Tools & Analytics, Penetration Testing & Exploitation, Linux Systems Security, Cybersecurity Leadership & Training, Threat Intelligence & Reconnaissance Automation, Identity & Access Management, Vulnerability Assessment

Technical: API Security & Design, DevSecOps & Secure CI/CD Pipelines, Cloud Security

Key Projects

RustVault: Self-Hosted Password Vault and Privacy Toolkit (2026)

A password vault and privacy toolkit written in Rust that runs only on your own machine: encrypted vault, recovery key, automatic backups, Firefox hardening and a script-blocking browser extension.

Technologies: Rust, AES-256-GCM, Argon2id, PostgreSQL, SQLite, Firefox WebExtensions, Firejail, Tailscale

Windows Security Setup: Wazuh, Sysmon and Sysinternals in One Command (2025)

A PowerShell script that enrolls a Windows host into Wazuh and installs Sysmon and the Sysinternals Suite in one elevated command.

Technologies: PowerShell, Wazuh, Sysmon, Sysinternals, Windows Server

SOC & SIEM Lab: Wazuh, Graylog, OpenCTI and MISP (2025)

A self-hosted SOC stack: Wazuh for endpoint detection and response, Graylog for log aggregation, OpenCTI with MISP for threat intelligence, and Grafana for unified visualization.

Technologies: Wazuh, Graylog, OpenCTI, MISP, Grafana

Network-Traffic-Monitoring-with-grafana (2025)

This project provides a comprehensive solution for capturing network traffic, processing it with Zeek (formerly Bro), and storing the enriched logs into a MySQL database for further analysis and visualization. It includes scripts and configurations to enhance Zeek's capabilities with GeoIP, ASN data, and JA3/JA4 fingerprinting, enabling detailed network security monitoring and analysis.

Technologies: zeek, shell, python

Security Report Wizard for Grafana (2025)

A FastAPI web wizard that pulls panel data from Grafana dashboards and turns it into spreadsheet reports for stakeholders without dashboard access.

Technologies: Python, FastAPI, Grafana API, Jinja2, JavaScript

Network Device Monitoring with Grafana (2025)

The Network Device Monitoring with Grafana project is a comprehensive, real-world implementation of a real-time monitoring system that leverages open-source tools like Nmap, MariaDB, Prometheus, Grafana, and Python scripting. This platform focuses on monitoring device availability, port activity, and service health across enterprise networks. It transforms traditional manual network auditing into an automated, visual, and scalable solution.

Technologies: Grafana, Prometheus, Nmap, Python, Bash, MariaDB, AlertManager, Cron