CURRICULUM VITAE (CV), QUALIFICATIONS AND EXPERIENCE OF VICTOR NTHULI

Name: VICTOR NTHULI
Profession: Security Operations Engineer | SOC & DevSecOps Specialist
Position: Managing Director at SOCDEV LIMITED
(Security Operation Center & Development Company)
Nationality: Kenyan
Telephone: +254 724 082859
E-MAIL: victornthuli269@gmail.com
LinkedIn: linkedin.com/in/victor-nthuli
Portfolio: nthuli.com
P.O. Box: 55207 - 00200, Nairobi, Kenya

PROFESSIONAL SUMMARY

Cybersecurity leader with 5+ years of technical and strategic experience building SOC infrastructure, automating security workflows, and implementing DevSecOps practices. Passionate about enabling secure digital transformation across Africa through scalable, open-source-first security engineering. Proven expertise in threat intelligence integration, vulnerability management, and regulatory compliance with a strong focus on continuous improvement of organizational security posture.

KEY QUALIFICATIONS

Security Operations Engineer with specialized experience in SOC environments, incident response, and threat intelligence integration. Proven expertise in implementing custom security solutions and comprehensive suites of security tools. Demonstrated success in vulnerability management, system hardening, and regulatory compliance. Skilled in building real-time monitoring solutions and automating security processes through DevSecOps pipelines. Committed to continuously enhancing organizational security posture across cloud and on-premises environments.

EMPLOYMENT RECORD:

1. **Year/Date:** April 2025 – Present
   Employing Organization: SOCDEV LIMITED

Title of Position Held: Managing Director
Location of Assignment: Nairobi, Kenya

- 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.

2. **Year/Date:** May 2023 – April 2025
Employing Organization: Webmasters K Ltd
Title of Position Held: Security Operations Engineer
Location of Assignment: Nairobi, Kenya

- **Security Infrastructure Development:**
    - Architected and deployed a custom SIEM solution integrating multiple threat intelligence feeds and platforms, boosting threat detection by 40%.
    - Implemented enterprise-grade load balancing and SSL termination, achieving 99.9% service availability.
- **Vulnerability Management & Security Testing:**
    - Established systematic vulnerability scanning with enterprise security tools, reducing average remediation time by 35%.
    - Conducted penetration tests that uncovered critical vulnerabilities (SQLi, XSS, authentication flaws) in web applications.
- **Cloud & DevSecOps Security:**
    - Managed a multi-tenant private cloud environment with advanced security controls and network isolation.
    - Integrated security scanning tools into CI/CD pipelines to prevent credential exposure.
- **Incident Response & Threat Hunting:**
    - Led investigations using advanced correlation techniques and custom detection rules based on the MITRE ATT&CK framework, improving threat coverage by 25%.

3. **Year/Date:** July – September 2022
   Employing Organization: Umar Auto Garage
   Title of Position Held: Intern
   Location of Assignment: Nairobi, Kenya

    - **Vehicle System Diagnostics:**
        - Gained hands-on experience with engine diagnostics and electrical systems.
        - Developed systematic troubleshooting methodologies that enhanced analytical skills applied later to security incident triaging.

CORE COMPETENCIES

Security Monitoring & Incident Response

- Optimized enterprise SIEM solutions with custom threat intelligence platform integration for comprehensive threat detection.
- Developed custom correlation rules and fine-tuned alert thresholds, reducing false positives by 40%.

Threat Intelligence & Analysis

- Integrated automated IOC enrichment through various threat intelligence platforms and feeds.
- Employed threat emulation tools for realistic adversary simulation and defense validation.

Infrastructure & Cloud Security

- Deployed secure private cloud environments with robust tenant isolation and IAM controls.
- Implemented secure container deployments with comprehensive vulnerability scanning and runtime protection.

Network Security & Monitoring

- Designed comprehensive network traffic monitoring systems coupled with custom visualization dashboards.
- Configured high-availability load balancing solutions with SSL termination, achieving 99.9% uptime.

Regulatory Compliance & System Hardening

- Achieved 80%+ compliance scores using system auditing tools against industry frameworks.

- Mapped security controls to GDPR, PCI-DSS, and ISO 27001 requirements.

DevSecOps & Security Automation

- Integrated security scanning tools into CI/CD pipelines to prevent credential exposure.
- Automated security testing with custom scripts, reducing manual review time by 35%.

TECHNICAL EXPERTISE

Security Operations & Monitoring

- Enterprise SIEM platforms with custom detection engineering
- Advanced network traffic analysis and packet inspection
- Real-time security telemetry visualization and alerting

Vulnerability & Risk Management

- Enterprise vulnerability assessment and management platforms
- Dynamic and static application security testing methodologies
- Supply chain security and software composition analysis

Cloud & Infrastructure Security

- Multi-cloud security architecture and implementation
- Container orchestration security and runtime protection
- Infrastructure-as-Code security scanning and compliance

Identity & Access Management

- Zero-trust architecture design and implementation
- Privileged access management and directory services
- Multi-factor authentication and SSO integration

Offensive Security & Red Team Operations

- Advanced adversary emulation and purple team exercises
- Security assessment frameworks and penetration testing
- Reverse engineering and malware analysis techniques

DevSecOps & Automation

- Security orchestration and automated response (SOAR)
- Continuous security validation and feedback loops
- Security-focused CI/CD pipeline integration
- Custom security automation with Python and infrastructure tools

EDUCATION

1. **Year:** 2019 – 2023
   School/College: United States International University – Africa
   Degree Obtained: BSc. Applied Computer Technology
   Concentration: Cybercrime & Forensic IT
   Relevant Coursework: Computer Forensics & Investigations, Information Systems Auditing
2. **Year:** 2015 – 2018
   School/College: Light Academy High School
   Degree Obtained: KCSE
3. **Year:** 2007 – 2014
   School/College: Rockfields Junior School
   Degree Obtained: KCPE

CERTIFICATIONS

- Certified Cyber Security Technician (CCT) – In Progress
- Getting Started in Security with BHIS and MITRE ATT&CK (16 Hours) – November 2024
- Burp Suite Basics – October 2024
- Zero to Linux with Hal Pomeranz (4 Hours) – September 2024
- How Logging Strategies Can Affect Cyber Investigations – September 2024
- Conquering Your CISSP with Jason Gillam – September 2024
- The Illustrated Pentester - Short Stories of Security VOL3 – August 2024
- Fearless Forensic Shell Fu – August 2024
- New Methods to Attack & Defend Active Directory – August 2024
- Offense for Defense w/ Jason Downey – August 2024
- Beginner's Guide to Webapp Vuln Scanning Using Nuclei – August 2024
- Securing Speed: Safeguarding CI/CD Pipelines – July 2024
- OPSEC Awareness for Military Members, DOD Employees, and Contractors – July 2024
- Introduction to OSINT – July 2024
- Active Defense & Cyber Deception w/ John Strand (16 Hours) – July 2024

NOTABLE ACHIEVEMENTS & RECOGNITION

- **Security Implementation Excellence:** Reduced average vulnerability remediation time by 35% through implementation of automated security workflows.

- **Threat Detection Optimization:** Decreased false positive rates by 40% through custom correlation rule development and fine-tuned detection engineering.
- **Infrastructure Reliability:** Achieved 99.9% uptime for critical security infrastructure through high-availability design and implementation.
- **Open Source Contributor:** Active contributor to several security-focused open-source projects.
- **Operational Efficiency:** Reduced manual security review time by 35% through custom automation and workflow improvements.
- **Community Recognition:** Featured speaker at local cybersecurity community events and knowledge-sharing forums.

VOLUNTEER EXPERIENCE

Technology Instructor | Mary Immaculate Rehabilitation Centre

- Provided over 100 hours of computer skills training to disadvantaged children.
- Developed and delivered a digital literacy curriculum to improve community technology access.

LANGUAGES

- **Natural Languages:** English (Fluent), Swahili (Fluent)
- **Programming & Scripting:** Python, Bash, C (Intermediate), SQL (Advanced), YAML/JSON, PHP (Basic)

LEADERSHIP RESPONSIBILITIES

- Strategic oversight of cybersecurity operations and infrastructure for diverse client portfolio
- Architecture and implementation of comprehensive security solutions across multiple environments
- Executive leadership of security initiatives with direct C-level reporting
- Team building and professional development of security practitioners
- Security governance, risk management, and compliance oversight

CERTIFICATION

I, the undersigned, certify that to the best of my knowledge and belief, these data correctly describe me, my qualifications, and my experience.

VICTOR NTHULI
Signature: **Victor Nthuli**
Date: May 2, 2025

REFERENCES

1. **LEONARD RONO**
   P.O. Box 55207-00200, Nairobi
   Phone: +254 725 491320
2. **Prof. JOSEPH NGUGI**
   USIU-Africa, P.O. Box 14634, Nairobi
   Phone: +254 721 643690