**VICTOR NTHULI**
Security Operations Engineer | SOC & DevSecOps Specialist
Email: victornthuli269@gmail.com | Phone: +254 724 082859
LinkedIn: [linkedin.com/in/victor-nthuli](https://www.linkedin.com/in/victor-nthuli)
P.O. Box 55207 - 00200, Nairobi, Kenya

### PROFESSIONAL SUMMARY

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

### CORE COMPETENCIES

**Security Monitoring & Incident Response**
• Optimized SIEM solutions (Microsoft Sentinel, custom MISP/OpenCTI 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 MISP and OpenCTI.
• Employed threat emulation tools (OpenBAS, Caldera) for realistic adversary simulation and defense validation.

**Infrastructure & Cloud Security**
• Deployed secure OpenStack private cloud environments with robust tenant isolation and IAM controls.
• Implemented secure container deployments with vulnerability scanning (Trivy) and runtime protection (Falco basics).

**Network Security & Monitoring**
• Designed comprehensive monitoring using Zeek and Wireshark, coupled with custom Grafana dashboards.
• Configured HAProxy for secure load balancing and SSL termination, achieving high availability.

**Regulatory Compliance & System Hardening**
• Achieved 80%+ compliance scores using Lynis for system audits against industry frameworks.
• Mapped security controls to GDPR, PCI-DSS, and ISO 27001 requirements.

**DevSecOps & Security Automation**
• Integrated TruffleHog and GitLeaks into CI/CD pipelines to prevent credential exposure.
• Automated security testing with custom Python and Bash scripts, reducing manual review time by 35%.

### TECHNICAL EXPERTISE

**Security Operations & Monitoring**

* **SIEM & Threat Intelligence:** MISP, OpenCTI, Microsoft Sentinel, Wazuh, Suricata
* **Network Analysis:** Zeek, Wireshark, TCPdump, Tshark, WatchYourLAN
* **Logging & Monitoring:** Grafana, Prometheus, Loki, Graylog, Uptime Kuma, BlueWave Uptime

**Vulnerability Management & Testing**

* **Scanning Tools:** OpenVAS, Nuclei, Nikto, Trivy (container security)
* **Web Application Testing:** Burp Suite, OWASP ZAP, Dirb, Gobuster, SQLmap
* **Code Security:** TruffleHog, GitLeaks, Repo-supervisor

**System Security & Infrastructure**

* **Linux Expertise:** Ubuntu, CentOS, Arch Linux, FreeBSD
* **System Hardening:** Lynis, Auditd, AppArmor, SELinux, CIS Benchmarks
* **Cloud Security:** OpenStack, ScoutSuite, basic Kubernetes security

**Identity & Access Management**

* **Authentication Systems:** OpenLDAP, Active Directory, SSSD, basic Keycloak
* **Access Control:** RBAC implementation, zero-trust architecture design

**Security Assessment Tools**

* **Red Team Tools:** Metasploit, Caldera, Sliver C2, Atomic Red Team, Hydra
* **Forensics & Analysis:** Ghidra, radare2, binwalk, ltrace, strace

**Expanded Security Tools & Frameworks**

* **Threat Intelligence & SIEM:** MISP, OpenCTI, Microsoft Sentinel, Wazuh, Suricata, OSSEC
* **Attack Simulation & Purple Teaming:** OpenBAS, Caldera, Sliver C2, Atomic Red Team, Mitre ATT&CK Navigator
* **Vulnerability Scanning:** OpenVAS, Nuclei, Nessus (familiar), Nikto, Trivy, Nmap
* **Network & Traffic Analysis:** Zeek, Wireshark, TCPdump, Tshark, Netcat, WatchYourLAN
* **Web & Application Security:** Burp Suite, OWASP ZAP, Dirb, Gobuster, SQLmap, XSStrike
* **Reverse Engineering & Malware Analysis:** Ghidra, radare2, Cutter, x64dbg, binwalk, strings
* **System Auditing & Hardening:** Lynis, Auditd, AppArmor, SELinux, CIS Benchmarks
* **Exploitation & Red Team:** Metasploit, Bettercap, Responder, Hydra, CrackMapExec, John the Ripper, Hashcat
* **Secrets & Credential Scanning:** TruffleHog, GitLeaks, Repo-supervisor, detect-secrets
* **Cloud & Container Security:** ScoutSuite, kube-hunter, Dockle, Falco
* **Authentication & Access Tools:** OpenLDAP, SSSD, Keycloak (basic), Authentik (basic), Fail2Ban
* **Logging & Monitoring Tools:** Grafana, Prometheus, Loki, Graylog, Filebeat, Logstash, Uptime Kuma, BlueWave Uptime
* **DevSecOps & Automation:** GitLab CI/CD, Jenkins, Ansible, Cron, Systemd timers, YAML automation
* **DNS & Infrastructure Monitoring:** Custom DNS propagation checker, DNSRecon, Dig, nslookup
* **Miscellaneous:** SSLyze, WhatWeb, Amass, Shodan CLI, Sublist3r, TheHarvester

### PROFESSIONAL EXPERIENCE

**Security Operations Engineer | Webmasters K Ltd**
May 2023 – Present

* **Security Infrastructure Development:**
• Architected and deployed a custom SIEM solution integrating MISP and OpenCTI, boosting threat detection by 40%.
• Implemented HAProxy for load balancing and SSL termination, achieving 99.9% service availability.
* **Vulnerability Management & Security Testing:**
• Established systematic vulnerability scanning with OpenVAS, 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 OpenStack environment with advanced security controls and network isolation.
• Integrated security scanning tools (TruffleHog, GitLeaks) into CI/CD pipelines to prevent credential exposure.
* **Incident Response & Threat Hunting:**
• Led investigations using advanced correlation in Microsoft Sentinel and custom detection rules based on the MITRE ATT&CK framework, improving threat coverage by 25%.

**Intern | Umar Auto Garage**
July – September 2022

* **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.

### EDUCATION

**BSc. Applied Computer Technology**
United States International University – Africa (2019 – 2023)
• Concentration: Cybercrime & Forensic IT
• Relevant Coursework: Computer Forensics & Investigations, Information Systems Auditing

**High School (KCSE)**
Light Academy High School (2015 – 2018)

**Primary School (KCPE)**
Rockfields Junior School (2007 – 2014)

### 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

### LANGUAGES

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

### 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.

### REFEREES

**Leonard Rono**
P.O. Box 55207-00200, Nairobi
Phone: +254 725 491320

**Prof. Joseph Ngugi**
USIU-Africa, P.O. Box 14634, Nairobi
Phone: +254 721 643690