CURRICULUM VITAE

EMMANUEL THABO SAKONTA | South Africa | thabosakonta@gmail.com | 0824607960 | https://www.linkedin.com/in/thabo-sakonta-377a3748 | GitHub: https://github.com/thabosakonta-wq

PROFILE SUMMARY

Microsoft Certified Security Operations Analyst (SC-200) with hands-on SOC, Detection Engineering, Threat Hunting, DFIR, Microsoft Sentinel and Python/Bash automation portfolio.

Featured Projects: Python SOC Automation, Microsoft Sentinel, Detection Engineering, Threat Hunting, Velociraptor DFIR, Network Traffic Analysis, Windows Event Analysis, MITRE ATT&CK; Mapping.

Core Skills: Security Monitoring, Incident Response, Threat Hunting, Sigma Rules, Microsoft Sentinel, Python, Bash, Windows, Linux, Git/GitHub

Seeking to contribute analytical, investigative, and security operations capabilities within a SOC Analyst, Cybersecurity Analyst, or Security Operations role.

CERTIFICATIONS

Cybersecurity and Digital Transformation

- **Microsoft Certified: Security Operations Analyst Associate (SC-200) -** NEMISA (2026)
- **Google Cybersecurity Professional Certificate –** Coursera (2025)
- **Career Essentials in Cybersecurity -** NEMISA (2025)
- **Cybersecurity Foundations -** LinkedIn Learning (2025)
- **Career Essentials in Generative AI –** NEMISA (2025)
- **Microsoft 101 & Digital Literacy -** NEMISA (2025)
- **Introduction to Artificial Intelligence -** LinkedIn Learning (2025)

CYBERSECURITY PORTFOLIO PROJECTS

SOC Mini SIEM Lab | GitHub Portfolio Project

- Designed and implemented a Bash-based Security Operations Center (SOC) Mini SIEM Lab using Linux and Termux.
- Developed automated log monitoring, File Integrity Monitoring (FIM), event correlation, burst detection, and incident logging.
- Created a real-time SOC dashboard for security event monitoring and alert visualization.
- Produced incident reports and simulated SOC workflows including detection, triage, investigation, escalation, and reporting.
- Technologies: Bash, Linux, Termux, Git, GitHub, Log Analysis, File Integrity Monitoring (FIM), SOC Operations.

Windows Event Analysis Lab

- Investigated Windows Security Event Logs to identify authentication failures, account creation events, privilege escalation, and PowerShell execution.
- Correlated Windows Event IDs with MITRE ATT&CK techniques.
- Produced executive summaries and incident investigation reports demonstrating SOC analyst workflows.
- Technologies: Windows Event Logs, Event Viewer, MITRE ATT&CK, Bash, GitHub.

Detection Engineering Lab

- Developed Sigma detection rules for Windows security events including failed logins, privilege escalation, account creation, and PowerShell execution.
- Mapped detections to MITRE ATT&CK techniques and documented detection coverage.
- Produced detection engineering documentation, executive summaries, and investigation reports.
- Technologies: Sigma, MITRE ATT&CK, Detection Engineering, GitHub.

Threat Hunting Lab

- Built a Bash-based threat hunting platform for proactive security investigations.
- Implemented failed login detection, brute-force detection, suspicious IP identification, privilege escalation monitoring, and persistence detection.
- Produced threat hunting dashboards and structured investigation reports.
- Technologies: Bash, Linux, Threat Hunting, Log Analysis, MITRE ATT&CK.

Velociraptor Investigation Lab

- Simulated Digital Forensics and Incident Response (DFIR) investigations using endpoint artifacts.
- Conducted process, network, file, and endpoint investigations based on Velociraptor concepts.
- Documented findings through executive summaries, investigation reports, and MITRE ATT&CK mapping.
- Technologies: DFIR, Endpoint Investigation, Velociraptor Concepts, Threat Hunting.

Microsoft Sentinel Lab

- Simulated Microsoft Sentinel alert triage and incident investigation workflows.
- Investigated alerts, correlated security events, and mapped findings to MITRE ATT&CK.
- Produced SOC investigation reports, executive summaries, and analyst documentation.
- Technologies: Microsoft Sentinel, SIEM, MITRE ATT&CK, Incident Response.

Network Traffic Analysis Lab

- Investigated simulated network communications to identify suspicious IPs, DNS activity, and HTTP traffic.
- Performed threat hunting and mapped findings to MITRE ATT&CK techniques.
- Produced network investigation reports and executive summaries.
- Technologies: Network Analysis, DNS, HTTP, Threat Hunting, MITRE ATT&CK.

MITRE ATT&CK Mapping Lab

- Classified security detections using the MITRE ATT&CK Framework.
- Mapped brute-force attacks, valid accounts, password guessing, and privilege escalation techniques.
- Produced ATT&CK-based investigation reports and detection documentation.
- Technologies: MITRE ATT&CK, Threat Classification, Detection Engineering.

TECHNICAL CYBERSECURITY EXPERIENCE

- Performed **network traffic analysis** using Wireshark to identify anomalies, suspicious traffic patterns, and protocol behavior.
- Practiced **firewall and IDS concepts**, reviewing alerts and understanding intrusion detection workflows.
- Conducted **SIEM log analysis** exercises, including alert triage, event correlation, and identification of potential security incidents.
- Utilized **Linux command-line tools** for security administration tasks such as file permissions, user management, and process monitoring.
- Developed **basic Bash scripts** to automate routine security checks and administrative tasks.
- Applied **Python scripting fundamentals** for log parsing and introductory security automation tasks.
- Conducted **vulnerability assessment and risk identification exercises**, applying foundational GRC principles and threat modeling concepts.
- Participated in **incident response simulations**, following structured response steps including detection, analysis, containment, and reporting.

Technologies Used: Bash, Linux, Termux, Git, GitHub, Log Analysis, Security Monitoring

CYBERSECURITY COMPETENCIES

- **Security Operations (SOC):**• Alert Monitoring• Incident Triage• Threat Detection• Event Correlation• Security Monitoring• Incident Documentation
- **Threat Hunting & Investigation:** • Log Analysis• File Integrity Monitoring (FIM) • Phishing Investigation• Security Event Analysis• Root Cause Analysis• Evidence Collection
- **Security Technologies:** • Microsoft Sentinel• Microsoft Defender XDR• Wireshark• Linux• Bash Scripting• Git• GitHub
- **Networking:** • TCP/IP• DNS• HTTP/HTTPS• Network Traffic Analysis
- **Governance, Risk & Compliance:** • Risk Identification• Compliance Monitoring• Policy Adherence• POPIA Awareness• NIST Awareness• ISO 27001 Awareness

KEY CYBERSECURITY ACHIEVEMENTS

• Microsoft Certified: Security Operations Analyst Associate (SC-200).
• Completed the Google Cybersecurity Professional Certificate.
• Designed and published cybersecurity portfolio projects demonstrating SOC monitoring, threat hunting, incident investigation, and detection engineering.
• Developed Bash-based security monitoring and threat detection solutions.
• Completed cybersecurity, AI, and digital skills training through Microsoft, and LinkedIn Learning.

PROFESSIONAL EXPERIENCE

Cybersecurity Portfolio Developer (Threat Hunting & SOC Projects) - Independent Developer | Nov 2024 - Present ·City of Johannesburg, Gauteng, South Africa · Designed and implemented a hands-on Threat Hunting Lab to simulate Security Operations Centre (SOC) workflows. - Developed Bash-based detection logic to identify suspicious activity and security events. - Performed log analysis and alert investigations using structured incident response procedures. - Created investigation reports, evidence documentation, and incident timelines. - Maintained project documentation and version control using Git and GitHub. - Practiced threat hunting methodologies, event correlation, and security monitoring concepts. - Produced supporting screenshots and technical documentation to demonstrate investigative findings and remediation recommendations.

Independent Electoral Commission (IEC)

Registration Officer – Electoral Services | Aug 2023 – October 2024 - Conducted and verified voter registration drives, ensuring compliance with IEC procedures. - Maintained secure and accurate voter registration records and documentation. - Supported public voter education initiatives and community engagement. - Ensured data integrity and confidentiality during registration processes. - Provided operational support for logistics, materials, and election readiness. - Liaised with community stakeholders to ensure smooth voter registration activities.

Department of Labour (DoL)

Senior Personnel Officer – Human Resource Management (HRM) | Oct 2009 – Jun 2021 - Managed employee service conditions, benefits, and leave processes on SAP/ESS. - Coordinated recruitment and selection logistics, including candidate communication and interview documentation. - Ensured policy and legislative compliance (Public Service Act, BCEA, EE Act, and PFMA). - Compiled HR statistical reports and maintained accurate personnel data records. - Served as Secretary for interview panels, Employment Equity, and Risk Committees.

EDUCATION

- **Result-Based Project Management: Monitoring & Evaluation (NQF 5)** – Wits University (2016)
- **Gender Mainstreaming Projects & Programs (NQF 5)** – PALAMA (2009)
- **N6 Business Management (NQF 5)** – Krugersdorp Technical College (2020)

Driver's Licence

- Valid South African Code 10 (C1) Driver's Licence

ADDITIONAL PROFESSIONAL DEVELOPMENT

SAP HCM & SuccessFactors | Project Management Foundations | Risk Management & Fraud Prevention | Communication & Leadership Development

---

REFERENCES

Available upon request.