EMMANUEL THABO SAKONTA

City of Johannesburg, Gauteng, South Africa | 082 460 7960 | thabosakonta@gmail.com
LinkedIn: thabo-sakonta-377a3748 | GitHub: thabosakonta-wq | Portfolio: thabosakonta-wq.github.io

PROFESSIONAL SUMMARY

Microsoft Certified: Security Operations Analyst Associate (SC-200) with hands-on experience developing a practical cybersecurity portfolio focused on Security Operations, Microsoft Sentinel, Detection Engineering, Threat Hunting, DFIR, Windows security analysis and SOC automation.

Experienced in analysing security events, investigating alerts, developing detection logic, conducting threat hunts, mapping activity to the MITRE ATT&CK Framework, documenting findings and developing security automation using Python and Bash.

Brings more than a decade of professional experience in investigation, compliance, records management, evidence-based documentation and stakeholder coordination within the South African public sector. This combination provides a strong foundation for structured SOC monitoring, incident triage, investigation, reporting and security operations.

Target roles: SOC Analyst | Junior SOC Analyst | Cybersecurity Analyst | Security Operations Analyst | Security Analyst

CORE TECHNICAL SKILLS

Security Operations: Alert Monitoring, Alert Triage, Incident Investigation, Event Correlation, Incident Documentation, Escalation

Detection & Threat Hunting: Detection Engineering, Sigma, KQL, Threat Hunting, IOC Investigation, Windows Event Analysis, MITRE ATT&CK

Microsoft Security: Microsoft Sentinel, Microsoft Defender concepts, Security Operations, SIEM Investigation

DFIR & Endpoint Security: Digital Forensics & Incident Response, Endpoint Investigation, Evidence Collection, Velociraptor Concepts, Windows Security Analysis

Automation & Systems: Python, Bash, Linux, Windows, PowerShell, Git, GitHub

Network Security: Wireshark, Network Traffic Analysis, DNS, HTTP, TCP/IP, Suspicious Network Activity

Governance & Compliance: Risk Identification, Compliance Monitoring, POPIA Awareness, NIST Awareness, ISO 27001 Awareness

CERTIFICATIONS & TRAINING

- Microsoft Certified: Security Operations Analyst Associate (SC-200) — 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

Microsoft Sentinel Detection Engineering Lab
Microsoft Sentinel | KQL | Detection Engineering | Threat Hunting | MITRE ATT&CK | SOAR

- Built a practical Microsoft Sentinel detection engineering environment covering security detection, threat hunting and incident investigation workflows
- Developed detection logic for suspicious PowerShell, failed authentication and process-creation activity
- Applied KQL-based investigation and hunting techniques to analyse security events and identify suspicious behaviour
- Mapped detections and investigative findings to the MITRE ATT&CK Framework
- Designed a SOAR host-isolation playbook demonstrating automated response concepts and operational guardrails
- Produced structured investigation reports and analyst-focused documentation

Repository: Microsoft-Sentinel-Detection-Engineering-Lab

Velociraptor Investigation Lab

DFIR | Endpoint Investigation | Threat Hunting | Evidence Analysis | MITRE ATT&CK

- Developed a practical endpoint investigation lab based on Velociraptor DFIR concepts
- Investigated process, network, file and endpoint artefacts within simulated incident scenarios
- Applied structured evidence analysis and investigation methodology to identify suspicious activity
- Documented findings through investigation reports, executive summaries and ATT&CK mapping

Repository: velociraptor-investigation-lab

Threat Hunting Lab

Threat Hunting | Bash | Linux | Log Analysis | MITRE ATT&CK

- Built a practical threat-hunting environment for investigating failed authentication, brute-force behaviour, suspicious IP activity, privilege escalation and persistence
- Developed hunting workflows using log analysis and evidence-based investigation
- Produced structured hunt findings, investigation reports and ATT&CK mappings

Repository: threat-hunting-lab

Detection Engineering Lab

Sigma | Windows Security Events | Detection Logic | MITRE ATT&CK

- Developed Sigma detection rules for Windows security events and suspicious activity
- Covered authentication failures, privilege escalation, account creation and PowerShell execution
- Mapped detection logic to relevant MITRE ATT&CK techniques
- Documented detection rationale, investigation methodology and expected analyst response

Repository: detection-engineering-lab

Python SOC Automation Lab

Python | Security Automation | Windows Event Logs | Alert Correlation

- Developed Python-based security automation workflows for Windows Event Log analysis
- Implemented log parsing, event correlation and security alert analysis
- Demonstrated how scripting can support repetitive SOC investigation and triage activities

Repository: Python-SOC-Automation-Lab

Additional Security Projects

- Network Traffic Analysis Lab — Wireshark, DNS, HTTP, network threat hunting and suspicious traffic analysis
- SOC Mini SIEM Lab — Bash/Linux log monitoring, file integrity monitoring, event correlation and burst detection
- Windows Security Analysis — Windows Event Logs, authentication activity, account creation, privilege escalation and PowerShell analysis

PROFESSIONAL EXPERIENCE

Independent Cybersecurity Developer — Cybersecurity Portfolio Nov 2024 – Present

Self-directed | City of Johannesburg, Gauteng

- Designed, developed and maintained a practical cybersecurity portfolio focused on SOC operations, detection engineering, threat hunting, DFIR, Microsoft Sentinel and security automation
- Developed and documented multiple security investigations, detection rules, hunting queries and incident-response workflows
- Applied MITRE ATT&CK to classify adversary behaviour and communicate detection coverage
- Maintained version-controlled cybersecurity projects and documentation using Git and GitHub
- Produced analyst-style investigation reports, executive summaries, evidence documentation and remediation recommendations
- Developed Python and Bash automation to support log analysis, event correlation and security monitoring
- Published projects through an integrated GitHub repository, cybersecurity portfolio website and LinkedIn professional profile

Registration Officer — Electoral Services Aug 2023 – Oct 2024; Jun 2026; Aug 2026

Independent Electoral Commission (IEC)

- Conducted and verified voter-registration activities in accordance with IEC procedures and operational requirements
- Maintained accurate and confidential registration records while ensuring data integrity throughout registration processes
- Verified information carefully and resolved discrepancies according to established procedures
- Liaised with community stakeholders and supported operational readiness during registration activities
- Re-appointed for the 2026 Local Government Elections registration weekends in June and August 2026

Senior Personnel Officer — Human Resource Management Oct 2009 – Jun 2021

Department of Labour

- Conducted and supported workplace investigations, employee-service processes and administrative reviews requiring confidentiality, accuracy and evidence-based documentation
- Managed employee records, service conditions, benefits and leave processes using SAP/ESS
- Coordinated recruitment and selection processes, including interview documentation and panel administration
- Ensured compliance with applicable legislation and public-service policies, including the Public Service Act, BCEA, Employment Equity Act and PFMA
- Compiled HR statistical reports and analysed personnel information to support management decision-making
- Served as Secretary for Interview Panels, Employment Equity and Risk Committees
- Coordinated with internal stakeholders while maintaining strict confidentiality and accurate records

EDUCATION

- N Diploma: Business Management (in progress, RPL) — N4/N5/N6 complete — Western TVET College / South West Gauteng TVET College, 2017–2020
- Result-Based Project Management: Monitoring & Evaluation (NQF Level 5) — University of the Witwatersrand, 2016
- Gender Mainstreaming Projects & Programmes (NQF Level 5) — PALAMA, 2009

ADDITIONAL PROFESSIONAL DEVELOPMENT

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

ADDITIONAL INFORMATION

- Driver's Licence: Valid South African Code C1 Driver's Licence
- References: Available on request