Emmanuel Thabo Sakonta
City of Johannesburg, Gauteng, South Africa | thabosakonta@gmail.com | 082 460 7960

Dear Hiring Manager,

Application for SOC Analyst / Cybersecurity Analyst Position

I am writing to express my interest in a SOC Analyst / Cybersecurity Analyst position within your organisation. I am a Microsoft Certified: Security Operations Analyst Associate (SC-200) with practical experience developed through hands-on cybersecurity projects covering Microsoft Sentinel, detection engineering, threat hunting, DFIR, Windows security analysis and SOC automation.

My cybersecurity portfolio is designed around realistic security operations workflows rather than purely theoretical exercises. I have developed and documented detection logic, investigated Windows security events, performed threat-hunting activities, analysed endpoint and network evidence, mapped findings to the MITRE ATT&CK Framework, and produced structured investigation reports and executive summaries.

My primary project, the Microsoft Sentinel Detection Engineering Lab, demonstrates my ability to work across the SOC lifecycle — from detection and alert investigation through threat hunting, incident analysis and response. I have also developed Sigma-based detection engineering work, a Velociraptor-focused DFIR investigation lab, threat-hunting workflows and Python/Bash security automation projects.

In addition to my technical development, I bring more than a decade of professional experience within the South African public sector. As a Senior Personnel Officer within the Department of Labour, I worked with sensitive information, supported workplace investigations, maintained detailed records, ensured legislative and policy compliance, coordinated stakeholders and produced accurate documentation for management and governance processes.

My qualifications include N4, N5 and N6 National Certificates in Business Management, with the N Diploma in Business Management currently in progress via Recognition of Prior Learning, taking into account my accumulated work experience — complementing my formal cybersecurity certifications and hands-on technical training.

I believe this background provides a valuable complement to my cybersecurity training. Effective security operations require more than technical knowledge; they also require analytical thinking, attention to detail, evidence handling, disciplined documentation, confidentiality, communication and the ability to follow structured investigative processes. These are capabilities I have developed throughout my professional career and have now applied to cybersecurity through practical hands-on work.

I would welcome the opportunity to contribute these skills to your security operations team while continuing to develop professionally in a real-world SOC environment.

Thank you for considering my application. I would appreciate the opportunity to discuss how my SC-200 certification, practical cybersecurity portfolio and investigative background could contribute to your organisation.

Yours sincerely,

Emmanuel Thabo Sakonta
Microsoft Certified: Security Operations Analyst Associate (SC-200)
GitHub: https://github.com/thabosakonta-wq | Portfolio: thabosakonta-wq.github.io |
LinkedIn: https://www.linkedin.com/in/thabo-sakonta-377a3748