MAKHOSI ANDILE SURGE

JUNIOR SOC ANALYST

Location: South Africa | andilemakhosisurge@outlook.com | https://github.com/The-man-of-books | https://www.linkedin.com/in/makhosi-andile-surge-8141b1316

PROFESSIONAL SUMMARY

Aspiring SOC Analyst with hands-on training in threat detection, log analysis, and security incident response. Completed ISC2 Certified in Cybersecurity (CC) training (exam pending), currently pursuing Microsoft SC-200 certification. Skilled in SIEM tools, packet analysis, and building defensive labs. Passionate about protecting digital systems and contributing to security operations teams.

TECHNICAL SKILLS

- SIEM Tools: Splunk, ELK Stack (ElasticSearch, Kibana), Graylog
- Network Analysis: Wireshark, Zeek, Security Onion, tcpdump
- Tools & Frameworks: Kali Linux, Nmap, Suricata, Snort, MITRE ATT&CK
- Operating Systems: Windows (Event Logs), Linux (Ubuntu, Kali)
- Scripting: Bash, PowerShell (basic)
- Soft Skills: Incident reporting, team communication, security awareness

CERTIFICATIONS & TRAINING

- ISC2 Certified in Cybersecurity (CC) – Training completed, exam pending
- Microsoft SC-200: Security Operations Analyst – In progress
- TryHackMe Blue Team Path – Ongoing
- Cybersecurity Foundations – Google/LinkedIn Learning
- Security Onion & Wireshark Lab Environments – Home Setup

PROJECTS & LAB EXPERIENCE

Windows Event Log Analysis – [Self-Guided]
- Investigated brute force login attempts via Event ID correlation
- Extracted Indicators of Compromise (IoCs) and created a basic report

Security Onion Mini-SOC Lab – [Home Setup]
- Deployed Security Onion on VirtualBox, configured Suricata and Zeek
- Analyzed captured traffic and generated alerts for suspicious activity

PCAP Traffic Dissection – [Wireshark]
- Analyzed malicious pcap file, identified beaconing, DNS tunneling
- Documented timeline and attack indicators

Alert Rule Writing (Zeek/Suricata)
- Created basic detection rules for port scans and suspicious HTTP traffic
- Mapped to MITRE ATT&CK Tactics/Techniques

EDUCATION

- Grade 10 Completion (SA Curriculum)
- Self-taught in cybersecurity through bootcamps, online labs, and certifications

CONTACT

- Email: andilemakhosisurge@outlook.com
- GitHub: https://github.com/The-man-of-books