Emmanuel Sogomo

Nairobi, Kenya | 0708 200 003 | sogomokip@gmail.com
LinkedIn | GitHub

Profile

I'm a cybersecurity analyst with a strong foundation built through the Moringa Cybersecurity Bootcamp with Flatiron School, and I've continued developing those skills since. I have hands-on experience working in Splunk to monitor and analyze security data, using Metasploit for penetration testing, and writing Python scripts to support automation and detection work. I bring a detail-oriented, methodical approach to assessing risk and ensuring alignment with compliance requirements, and I communicate well across teams, since most security issues require coordination beyond the security function. I'm looking for a Security Analyst role where I can apply these skills to real-world challenges and continue to grow professionally.

Key Qualifications

- Security Monitoring & SIEM: Skilled in collecting, filtering, and analyzing security data in Splunk across firewalls, IDS/IPS, and network devices to detect and triage threats.
- Network Security: Solid grasp of network protocols, common attack vectors, and corresponding mitigation strategies.
- Systems Security: Working knowledge of system architecture, operating systems, and exploitation techniques, with hands-on experience using Metasploit and Linux command-line tools.
- Cyber Threat Intelligence: Apply structured intelligence analysis methods to assess adversary tactics and evolving threat landscapes.
- Governance, Risk & Compliance (GRC): Understanding of how to align security controls across an organization with enterprise security best practices.
- Logging & Detection Engineering: Designed and tuned log-based detection rules to surface and respond to security incidents.
- Python Scripting & Automation: Use Python for automation, debugging, code analysis, and secure coding practices.
- Application Security & Penetration Testing: Identify vulnerabilities in applications and network infrastructure using standard penetration testing methodologies.
- Applied Cryptography: Practical understanding of cryptographic principles, including secure web server configuration and email encryption.

Projects

- Capstone Project, Flatiron School: Delivered a scenario-based cybersecurity assessment and professional report applying threat analysis, detection, and risk assessment methodologies to a real-world scenario.
- Hands-On Security Labs (TryHackMe / CTFs): Completed practical labs and capture-the-flag challenges covering exploitation, detection, and defensive techniques, sharpening analytical problem-solving under pressure.
- Home Lab / Cloud Security Projects: Built and hardened a personal lab environment to practice system hardening, network monitoring, and security tool deployment.
- Splunk Fundamentals / Security Training: Built hands-on log analysis and detection-engineering skills to support incident response and threat identification.

Experience

- Investigated operational issues and system anomalies to identify root causes and implement effective fixes, applying the same investigative mindset used in incident analysis and troubleshooting.

- Collected, reviewed, and interpreted data across technical systems, building skills directly transferable to log analysis, monitoring, and pattern recognition.
- Maintained rigorous attention to detail and documentation standards, ensuring accuracy, compliance, and clear reporting of findings.
- Partnered with cross-functional teams to communicate technical information clearly, reflecting the coordination required during security incidents and risk assessments.
- Adhered to established procedures, policies, and compliance requirements while handling sensitive information, reinforcing risk awareness and policy discipline.
- Managed multiple priorities in a fast-paced environment, developing time-management skills critical to SOC and security operations roles.
- Adopted technology-driven workflows to improve efficiency, reflecting an automation- and process-optimization mindset valuable in cybersecurity operations.

Technologies & Tools

- Operating Systems: Linux, Windows
- Scripting & Automation: Python (foundational)
- Security & Analysis Tools: Splunk (log analysis), Metasploit (lab environments)
- Networking Concepts: TCP/IP, ports, protocols, traffic analysis
- Documentation & Reporting: Technical writing, structured reporting

Education

Cybersecurity Bootcamp, Moringa School — Completed, awaiting graduation (29/06/2026)

Coursework, Moi University School of Law — 57 Units Completed 2019-2022