Grace Funmilayo Smith

SOC Analyst | Cybersecurity Engineer | Threat Intelligence | OSINT | Incident Response

smithgrace361@gmail.com | 07018045705 | Ekiti State, Nigeria | linkedin.com/in/grace-smith59b77133b | gracesec.lovable.app

PROFESSIONAL SUMMARY

Detail-oriented Cybersecurity Engineer and aspiring SOC Analyst with hands-on experience in security operations, threat intelligence, OSINT investigations, network forensics, and malware analysis. Proficient in monitoring and analysing security events, triaging alerts, and conducting incident response and root cause analysis. Skilled at mapping adversary behaviour to the MITRE ATT&CK; framework, identifying indicators of compromise (IOCs), and producing structured threat reports. Experienced with SIEM concepts, log analysis, and network traffic analysis using Wireshark. Actively pursuing CompTIA Security+ to further strengthen security operations expertise.

CORE COMPETENCIES

Security Operations (SOC) | Threat Intelligence & Analysis | OSINT & Open-Source Research | Incident Response & Triage | Malware Analysis | Digital Forensics | Log Analysis & SIEM | Vulnerability Assessment | Network Traffic Analysis | MITRE ATT&CK; Framework | Indicator of Compromise (IOC) Analysis | Threat Hunting | Phishing Investigation | Identity & Access Management (IAM) | Firewall & Network Security | Python Scripting & Automation

TECHNICAL SKILLS

SIEM & Log Analysis: Log correlation, alert triage, event monitoring, security log review (Windows Event Logs, network logs)

Threat Intelligence & OSINT: MITRE ATT&CK;, VirusTotal, Malware Bazaar, ThreatFox, IOC extraction & enrichment, threat actor profiling, OSINT automation (Python)

Network & Traffic Analysis: Wireshark, PCAP analysis, TCP/IP, DNS, DHCP, OSPF, VLANs, C2 traffic detection, beaconing analysis

Incident Response & Digital Forensics: Alert triage, root cause analysis, postmortem reporting, CyberChef, ExifTool, Steghide, Fcrackzip, Audacity

Scripting & Automation: Python (threat detection scripts, OSINT automation, forensic tooling), Bash

Security Platforms & Tools: Active Directory, Fortigate Firewall, Packet Tracer, CyberChef

Email & Phishing Analysis: Header inspection, URL defanging & analysis, phishing triage, awareness campaign design

PROFESSIONAL EXPERIENCE

Cybersecurity Intern
March – September 2025

New Horizons Training Centre

- Monitored and analysed simulated network events, practising alert triage and security event correlation aligned with SOC workflows.
- Configured and managed enterprise network environments using TCP/IP, VLANs, and OSPF routing protocols.
- Developed Python automation scripts for network scanning, threat detection, log parsing, and security reporting.
- Deployed and administered Active Directory, managing users, group policies, DNS, and shared resources.
- Completed CompTIA Network+ exam-prep training; certification earned upon programme completion.

Information Security Analyst Intern
August 2025

Telstra Security (Forage)

- Investigated and contained a live malware incident, performing full alert triage, root cause analysis, and impact assessment.
- Produced a structured postmortem report with detailed timeline reconstruction — demonstrating core SOC incident documentation skills.
- Developed Python-based mitigation scripts to harden existing firewall rules and reduce attack surface.

Cybersecurity Awareness Specialist Intern

Mastercard (Forage)

- Functioned as a security analyst on Mastercard's Security Awareness Team, identifying, analysing, and reporting phishing threats.
- Conducted security gap assessments across business units and designed targeted training programmes to reduce human risk.

Cybersecurity Analyst Intern
Deloitte (Forage)
- Analysed web activity logs to detect anomalous user behaviour and identify indicators of compromise during a simulated breach.
- Supported client-facing incident response activities, producing documentation of findings and remediation steps.

Cybersecurity Analyst Intern
Tata Consultancy Services (Forage)
- Completed an Identity & Access Management (IAM) simulation, aligning access controls with business security requirements.
- Delivered technical documentation and stakeholder presentations communicating complex security findings clearly.

PROJECTS

Network Forensics Investigation: Analysed malicious PCAP files to detect beaconing patterns, C2 communication, and credential theft. Mapped all findings to MITRE ATT&CK; TTPs and produced a structured threat intelligence report.

Python OSINT & Forensics Toolkit: Built a suite of Python scripts for steganography detection, ZIP password cracking, log parsing, and automated OSINT data collection — simulating SOC analyst tooling.

Phishing Awareness Campaign: Designed and executed a simulated phishing campaign including awareness posters and training quizzes, successfully reducing test click rates and demonstrating measurable security improvement.

Active Directory Lab: Designed and managed a Windows Server Active Directory environment — configuring domain users, group policy objects (GPOs), shared folders, and DNS infrastructure.

More projects available at: Grace Smith — Security Engineer & SOC Analyst

EDUCATION

B.Sc. Computer Science – Landmark University, Nigeria Expected 2026

CERTIFICATIONS & TRAINING

- Google Cybersecurity Certificate – Google / Coursera
- Introduction to Digital Forensics, OSINT & Dark Web – Security Blue Team
- MITRE ATT&CK; Beginner & Intermediate – AttackIQ Academy
- Foundations of Purple Teaming – AttackIQ Academy
- Python Programming for App Development and Cybersecurity – New Horizons
- Virtual Security Internships: Mastercard, Deloitte, Tata Consultancy Services, Telstra – Forage

In Progress:
- CompTIA Network+ – Full exam-prep training completed at New Horizons
- CompTIA Security+ – Structured training completed via Cybrary and New Horizons

More certifications and credentials available at: Grace Smith — Security Engineer & SOC Analyst

ADDITIONAL INFORMATION

Soft Skills: Analytical thinking · Critical reasoning · Threat report writing · Team collaboration · Data analysis & presentation · Security compliance & risk assessment · Attention to detail · Excellent written and verbal communication

Languages: English (fluent) · Yoruba (fluent)

REFERENCES

Dr. Emmanuel Igbekele – Lecturer, Landmark University | 08066950350 | igbekele.emmanuel@lmu.edu.ng

Austin Emmanuel – Cybersecurity Instructor, New Horizons | 08166908790 | austineemmy69@gmail.com