IKWUKA OKOYE

Cybersecurity Analyst | Cloud Security Analyst

Global (Authorised to Work Remotely in EU/USA) | **Email** | **GitHub** | **X (formerly Twitter)**

Professional Summary

Results-driven Cyber Security Analyst with comprehensive training across industry-leading frameworks (NIST, CIS, MITRE ATT&CK, Cyber Kill Chain, ISO 27001). Expert in **threat detection, incident response, vulnerability management, SIEM, network security, endpoint security, cloud security, development, security,** and **operations (DevSecOps)**. Recently completed intensive training through ISC2, Google, Cisco, Fortinet, and IBM programs. Proven ability to identify, analyze, and mitigate cyber threats using tools such as Splunk, Wireshark, ELK Stack, Chronicle, Autofocus, and Security Onion. Seeking to protect organizational assets in a Security Operations Center (SOC) environment.

Entrepreneurial efficacy with exceptional strategic planning, critical thinking, delegation, collaboration, and problem solving skills. Effective in fostering positive and cohesive communication while maintaining strong interpersonal relations with stakeholders. Reputable confidentiality, branding, and excelling in coaching, mentoring, and negotiation. Proficient data, change, and time management. Motivational, inspirational, empathetic, enthusiastic, creative, adaptive, persuasive, and selfless in approach. Impeccable ethics and integrity.

Certifications

- **ISC2 Certified in Cybersecurity (CC)** – Completed
- **Google Cybersecurity Professional Certificate** – Completed
- **Google Cloud Cybersecurity Professional Certificate** – In Progress (Dec 2025)
- **Microsoft Azure Security Engineer Associate (AZ-500)** – In Progress (Jan 2026)
- **IBM Cybersecurity Analyst Professional Certificate** – In Progress (Feb 2026)
- **Fortinet NSE 1-4 – Network Security Professional (Core Topics)** – In Progress (Apr 2026)
- **Cisco Cybersecurity Associate (CyberOps)** – In Progress (May 2026)
- **AWS Certified Solutions Architect Professional Certificate** – In Progress (June 2026)

Core Technical Skills

Security Frameworks & Standards: NIST Cybersecurity Framework, CIS Controls, MITRE ATT&CK, Cyber Kill Chain, Diamond Model, ISO/IEC 27001, PCI-DSS, HIPAA Security Rule

Security Domains: Asset Security, Security Operations, Network Security, Identity and Access Management (IAM), Security Assessment & Testing, Security Architecture & Engineering, Communication & Network Security, Software Development Security

Threat Detection & Incident Response: SIEM (Splunk, Google Chronicle, ELK), IDS/IPS, EDR/XDR, SOC Tier 1–2–3 workflows, incident handling, triage, escalation, forensics basics

Network Security: TCP/IP, OSI model, packet analysis (Wireshark, tcpdump), firewalls (FortiGate, Cisco ASA), VPN, VLANs, NAT, proxy, DNS security, SD-WAN security

Vulnerability Management: Nessus, OpenVAS, CVSS scoring, patch management, vulnerability scanning, risk ranking

Endpoint Security: Antivirus, EDR (CrowdStrike, Microsoft Defender), host-based firewalls, application whitelisting

Cloud Security: AWS, Azure, GCP shared responsibility model, cloud logging, IAM roles, S3 bucket security

Tools & Platforms: Splunk, Wireshark, Security Onion, Autofocus, VirusTotal, Shodan, theHarvester, Nmap, Metasploit basics, Kali Linux, Windows/Linux security hardening, Active Directory security, PowerShell security

Cryptography: Symmetric/asymmetric encryption, hashing, digital signatures, PKI, TLS/SSL

Risk Management: Risk assessment, risk treatment, threat modeling, security controls selection

Programming/Scripting: Python (for security automation), Bash, PowerShell

Professional Experience

Cybersecurity Analyst – Capstone / Final Project (Google, Cisco & IBM Programs) Jan 2026 – Mar 2026

- Performed full i**ncident response lifecycle** using NIST 800-61 in simulated enterprise environment
- Analyzed real-world PCAPs with Wireshark and applied **MITRE ATT&CK** mapping and **Cyber Kill Chain**
- Configured and tuned **SIEM alerts** in Splunk and Google Chronicle; reduced false positives by 40%
- Conducted **vulnerability scans** with Nessus and prioritized remediation using CVSS v3.1
- Built and deployed **Security Onion** sensor for network traffic analysis and threat hunting
- Wrote **Python scripts** to automate log parsing and phishing URL detection
- Documented findings in professional **incident reports** and executive summaries

SOC Analyst – Simulated Blue Team Operations (Cisco CyberOps & Fortinet NSE 4 Labs) Dec 2025 – Feb 2026

- Monitored and analyzed security events in a 24/7 SOC environment using **ELK Stack** and **Splunk**
- Responded to alerts from **FortiGate firewalls**, Cisco Firepower, and endpoint protection platforms
- Performed p**acket capture analysis** and reconstructed attack timelines
- Executed **playbooks** for phishing, malware, ransomware, and privilege escalation incidents
- Hardened Windows and Linux systems following **CIS Benchmarks**

Junior Cybersecurity Analyst – Hands-on Labs (ISC2 CC & Google Certificate) Oct 2025 – Dec 2025

- Conducted **risk assessments** using NIST 800-30 methodology
- Implemented **access control models** (RBAC, ABAC) and least privilege principles
- Performed **phishing analysis** and reverse engineering of malicious attachments
- Configured secure network architecture with VLAN segmentation and firewall rules
- Applied **cryptographic controls** (AES, RSA, SHA-256, TLS 1.3) in real scenarios

Education

Bachelor of Science in Computer Science – University of the People – California, USA (Expected to Graduate in 2027)