

Samuel Chinaemerem Obiajunwa

SOC Analyst (Tier 1) • Alert Triage & Investigation • Threat Detection • Incident Response

Garland, TX | (678) 521-9361 | Obiajunwasamuel9@gmail.com | linkedin.com/in/obinwa012 | github.com/Obinwa012

SUMMARY

Cybersecurity professional pursuing a Tier-1 SOC Analyst role, with a B.S. in Cybersecurity & Information Assurance and 10+ industry certifications. Hands-on with alert triage, log analysis, threat detection, and incident response, built by deploying, defending, breaking, and rebuilding a cloud-based home-lab SOC against live attack traffic. Backed by five years of enterprise IT across networking, endpoint administration, access control, and HIPAA-regulated PHI handling.

CERTIFICATIONS

Completed: CompTIA Security+ • CompTIA CySA+ • ISC2 SSCP • CompTIA PenTest+ • ISC2 Certified in Cybersecurity (CC) • CompTIA Network+ • CompTIA A+ • LPI Linux Essentials • ITIL 4 Foundation • CompTIA Project+

In Progress: SC-300 (Identity & Access Administrator) • CCNA • AWS Certified Solutions Architect – Associate (SAA-C03) • Google AI Essentials

SELECTED PROJECTS

Cloud-Based Home-Lab SOC | Wazuh SIEM/XDR

Jun 2026 – Present

github.com/Obinwa012/cybersecurity-portfolio

- Built and operate a cloud-hosted blue-team SOC lab ("Nexus Freight") on Wazuh SIEM/XDR, with agent-based endpoint telemetry, log aggregation, correlation, and File Integrity Monitoring (FIM).
- Threat-hunted a brute-force campaign within two hours of exposure: 34 unique international source IPs and ~4,500 failed authentications against default accounts; confirmed no breach via log-signature analysis and hardened the host with key-only SSH, IP allowlisting, and Fail2Ban.
- Triaged a level-7 FIM alert (trojaned `/usr/bin/diff`) with a self-built four-step framework: package-log review, known-good integrity comparison, and VirusTotal (0/63); declared a false positive and preserved the clean SHA-256 hash instead of disabling the rule.
- Exposed a lab host to live attack traffic that a botnet weaponized for outbound DDoS (~91,000 pkt/s) before the provider isolated it; eradicated the malware and rebuilt into a segmented two-server architecture on Elastic Security (~2,000 rules) behind an NGINX/ModSecurity WAF and Suricata IDS, authoring a custom detection rule for a Node.js stack.

Enterprise Network Security Lab | FortiGate 500E + Cisco Catalyst C9200

github.com/Obinwa012/enterprise-network-security-lab

- Deployed and validated a segmented network on physical enterprise hardware: FortiGate 500E firewall (serial-console init, management/LAN interfaces, DHCP) integrated with a Cisco C9200 switch; verified Layer 2/3 connectivity and firewall implicit-deny through a documented configure, test, root-cause, remediate, retest loop. (WAN/NAT, VLANs, IPS/AV in progress.)

XHIBO.com | Full-Stack E-Commerce Platform

2023 – Present

- Built and operate a production e-commerce platform (React / Firebase); own user authentication, session management, access control, and secure handling of customer data.

EXPERIENCE

Network Diagnostics Technician | Sprout, Garland, TX

2026 – Present

- Execute DoD-compliant data sanitization and secure factory resets on decommissioned hardware; maintain serial-number traceability and chain-of-custody records in SmartERP, supporting data integrity and audit requirements.
- Diagnose and validate enterprise networking equipment (Cisco, Juniper, Arista) via POST, loopback, port/interface, and firmware testing; automated a high-volume manual workflow with a custom Python tool integrated into SmartERP.

IT Hardware Technician | Sprout, Garland, TX

2025 – 2026

- Installed, upgraded, and repaired enterprise systems and network equipment; diagnosed component-level faults, returned units to service, and harvested/cataloged reusable server components to reduce procurement costs.

Patient Relations Coordinator | Oak Street Health (Omni Interactions), Remote

2024 – 2025

- Handled Protected Health Information (PHI) daily under full HIPAA compliance, applying least-privilege access and accurate record documentation; managed scheduling and records in EMR systems alongside clinical teams in a regulated environment.

IT Specialist | FUFU Group, Norcross, GA

2020 – 2024

- Sole IT support for a multi-site restaurant and grocery operation; owned network infrastructure, POS systems, workstations, and end-user support, administering accounts and access control (provisioning, resets, permissions, offboarding) under least privilege.
- Secured payment-processing endpoints and store networking (routing and switching, Wi-Fi, ISP failover); trained non-technical staff on secure use of store systems.

EDUCATION

B.S., Cybersecurity & Information Assurance | Western Governors University

Mar 2026

TECHNICAL SKILLS

Security Operations: SIEM (Wazuh, Elastic Security; Splunk) • log analysis • alert triage • threat detection & hunting • incident response • endpoint telemetry & File Integrity Monitoring (FIM) • detection rule writing & tuning • IDS/IPS (Suricata) • WAF • vulnerability assessment • MITRE ATT&CK • NIST CSF • ISO 27001 • HIPAA • GRC

Networking: TCP/IP • DNS • DHCP • VPN • LAN / WAN • routing & switching • firewalls (FortiGate) • Wi-Fi • VLANs • subnetting • Cisco / Juniper / Arista

Systems & Cloud: Windows • Linux administration • Active Directory • Entra ID (Azure AD) • Microsoft 365 (Intune, Defender) • DigitalOcean

Tools & Programming: Wireshark • Nmap • Nessus • Fail2Ban • Jira • Python • Bash • PowerShell • SQL • JavaScript / React