DIVINE JUNIOR EZEWELE

Cybersecurity Analyst |
📧 contact.divineezes@gmail.com | 📞 +2349138432840 | Lagos, NG
LinkedIn 🔗 linkedin.com/in/divine-ezewele
Portfolio 🔗 tinyurl.com/divine-ezewele-portfolio

Professional Summary

CompTIA Cybersecurity Analyst (CySA+), Security+, and ISC2 Certified in Cybersecurity (CC) professional with hands-on SOC experience in SIEM monitoring, threat detection, log analysis, and incident response. Skilled in Wazuh, Splunk, Snort IDS, Sysmon, Wireshark, and tcpdump for endpoint and network visibility. Experienced in Azure RBAC, Docker Compose, and AWS cloud hosting for threat intelligence platforms, with IAM policy development aligned to ISO 27002 and NDPA compliance. Adept at applying MITRE ATT&CK threat intelligence for proactive defense against adversary tactics, and passionate about cybersecurity awareness campaigns that strengthen organizational resilience.

Experience & Projects

Cyblack — Cybersecurity Intern | Jan 2026 – Mar 2026

- Monitored endpoints with Wazuh SIEM and performed log analysis.
- Conducted alert triage, documented findings, and escalated true positives.
- Implemented RBAC in Microsoft Azure by creating Junior and Senior Admin groups.
- Hosted OpenCTI via Docker Compose on AWS Ubuntu, integrated with AlienVault.
- Developed IAM policies aligned with ISO 27002/NDPA for compliance readiness.
- Created a security misconfiguration awareness campaign using Vivida software.
- Conducted MITRE ATT&CK threat intelligence analysis on OpenCTI to identify adversary TTPs and improve organizational security posture.

Cyber Academy — SOC Level 1 Intern | Aug 2025 – Sep 2025

- Deployed Wazuh agent and configured Sysmon for centralized alerting (EDR).
- Investigated alerts, documented findings, and practiced MITRE ATT&CK scenarios.
- Supported incident reporting and team handovers.

Home Cyber Lab — Self-Paced Projects | Jun 2025 – Present

- Configured Snort IDS for intrusion detection and packet inspection.
- Built Splunk dashboards and detected brute-force attempts via log queries.
- Traced malicious traffic with Wireshark and tcpdump.
- Conducted phishing email analysis (metadata & content for IOCs).
- Performed malware analysis using VirusTotal and Phishtool.
- Set up Wazuh agent with Sysmon for centralized logging of login attempts (EDR).

Certifications

- CompTIA Cybersecurity Analyst (CySA+) — Apr 2026 – Apr 2029
- CompTIA Security+ (SY0-701) — Jan 2026 – Jan 2029
- ISC2 Certified in Cybersecurity (CC) — Jul 2025 – Jun 2028
- Certified Cybersecurity Educator Professional (CCEP) — Nov 2025

Education

B.Sc. Biochemistry, Ambrose Alli University, Ekpoma, Nigeria | 2014–2018

Skills

Core Competencies: SIEM Monitoring, Log Analysis, Threat Detection, Incident Response, Alert Triage, Threat Hunting, MITRE ATT&CK, SOC Operations, Documentation, Collaboration
Security Tools: Wazuh SIEM, Splunk, Snort IDS, Sysmon, Wireshark, tcpdump, VirusTotal, Phishtool, Cisco Packet Tracer
Cloud & Infrastructure: Microsoft Azure (RBAC, IAM), Docker Compose, AWS (EC2, Ubuntu hosting)
Operating Systems: Windows, Linux (Ubuntu)
Networking: TCP/IP, DNS, Firewall Rules, Traffic Analysis