DIVINE JUNIOR EZEWELE

Junior SOC Analyst | Cybersecurity Professional

📧 contact.divineezes@gmail.com | 📞 +234 708 167 9975 | Lagos, NG

Linkedin🔗 https://www.linkedin.com/in/divine-ezewele
Portfolio🔗 https://tinyurl.com/divine-ezewele-portfolio

Professional Summary

CompTIA Security+ certified and ISC2 Certified in Cybersecurity (CC), aspiring SOC Analyst (Tier 1) with hands-on experience in SIEM monitoring, threat detection, log analysis, and incident response. Skilled in deploying and monitoring Wazuh, Splunk, and Snort IDS to detect and investigate malicious activity. Experienced with Sysmon, Wireshark, and tcpdump for endpoint and network visibility. Adept at documenting incidents, escalating alerts, and collaborating with team members to support SOC operations and continuous improvement.

Experience & Projects

Cyblack — Cybersecurity Intern | Jan 2026 – Mar 2026

- Monitored Windows endpoints using Wazuh SIEM and performed log analysis.
- Conducted alert triage and escalated incidents to senior analysts.
- Collaborated on drafting incident reports and improving monitoring rules.

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

- Deployed Wazuh SIEM and configured Sysmon for enhanced threat visibility.
- Investigated alerts, documented findings, and practiced MITRE ATT&CK scenarios.
- Supported team handovers and incident reporting processes.

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

- Configured Snort IDS for intrusion detection and packet inspection.
- Built Splunk dashboards to detect brute-force and login anomalies.
- Traced malicious traffic with Wireshark and tcpdump.
- Conducted malware analysis using VirusTotal and Hybrid Analysis.

Certifications

- CompTIA Security+ — 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: Security Event Monitoring, Log Analysis, Threat Detection, Incident Response, Alert Triage, Threat Hunting, MITRE ATT&CK Framework, SOC Operations, Documentation, Team Collaboration

Security Tools: Wazuh SIEM, Splunk, Snort IDS, Sysmon, Wireshark, tcpdump, VirusTotal, Cisco Packet Tracer

Operating Systems: Windows, Linux (Ubuntu)

Networking: TCP/IP, DNS, Firewall Rules, Network Traffic Analysis