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

Cybersecurity Analyst with certifications including CompTIA CySA+, Security+, ISC2 CC, SOC 2, ISO 27001, and Microsoft Azure Fundamentals (AZ-900). Hands-on SOC experience in SIEM monitoring, threat detection, log analysis, and incident response. Skilled in Wazuh, Splunk, Snort IDS, Sysmon, Wireshark, and tcpdump. Experienced in Azure RBAC, Docker Compose, and AWS cloud hosting for threat intelligence platforms. Adept at applying MITRE ATT&CK for proactive defense and passionate about cybersecurity awareness campaigns that strengthen organizational resilience.

Experience & Projects

Hybrid Security Consult — SOC Analyst Intern | Apr 2026 – Present

- Analyzed Sysmon JSON logs to identify attacker entry points, persistence mechanisms, and objectives.
- Investigated suspicious network activity using Volatility memory analysis, isolating malicious processes.
- Deconstructed obfuscated AWS CloudTrail compromise, uncovering data exfiltration and credential theft.
- Conducted malware resurgence analysis with ANY.RUN, mapping threat landscape and developing detection mechanisms.

Cyblack — Cybersecurity Intern | Jan 2026 – Apr 2026

- Monitored endpoints with Wazuh SIEM, performed log analysis, and triaged alerts.
- Implemented Azure RBAC roles and hosted OpenCTI via Docker Compose on AWS.
- Developed IAM policies aligned with ISO 27002/NDPA and created security awareness campaigns.
- Conducted phishing and malware analysis (VS Code, ANY.RUN) and documented findings.
- Researched CVEs affecting mobile devices, performed vulnerability management, and recommended remediations.
- Implemented SOAR playbooks to automate and accelerate incident response workflows.
- Applied MITRE ATT&CK threat intelligence to strengthen organizational security posture.

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

- Deployed Wazuh agent and configured Sysmon for centralized alerting.
- Investigated alerts 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 to detect brute-force attempts.
- Traced malicious traffic with Wireshark and tcpdump.

Certifications & Professional Development

- CompTIA CySA+ (2026–2029) | CompTIA Security+ (2026–2029)
- ISC2 Certified in Cybersecurity (CC) (2025–2028) | CCEP (2025)
- Microsoft Press (Cert Prep): SC-900, AZ-900
- LinkedIn Learning: ISO 27001:2022, SOC 2 Compliance (Cloud & Essentials)
- Forage Virtual Job Simulations: ANZ Australia, Deloitte Australia, Mastercard — Cybersecurity

---

Education

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

Skills

Core Competencies: SIEM Monitoring, Threat Detection, Incident Response, Threat Hunting, MITRE ATT&CK, SOC Operations, SOAR Playbooks, Vulnerability Management
Security Tools: Wazuh, Splunk, Snort IDS, Sysmon, Wireshark, tcpdump, VirusTotal, Phishtool, ANY.RUN
Cloud & Infrastructure: Microsoft Azure (RBAC, IAM), AWS (EC2, CloudTrail), Docker Compose
Networking & OS: TCP/IP, DNS, Firewall Rules, Windows, Linux (Ubuntu & Kali)