

OBJECTIVE

Security Engineer & Technical Lead with 8+ years of experience specializing in the **Microsoft Security Stack**, Cloud Architecture (AWS/Azure), and Identity Management. Proven track record in architecting Zero Trust environments, deploying enterprise SIEM/EDR solutions, and managing full-scale vulnerability remediation. Expert in aligning technical infrastructure with global frameworks (NIST, ISO 27001). Recognized community leader in cybersecurity awareness and technical instruction.

TECHNICAL SKILLS

- **Microsoft Security Stack:** Microsoft Sentinel (SIEM), Microsoft Defender for Endpoint (MDE), Entra ID (Identity), Microsoft Purview (DLP), Azure Security Center.
- **Cloud & Identity:** AWS Security, SSO/SAML, PIM/PAM, Okta, Zscaler, Netskope.
- **Network & Perimeter:** Cisco Umbrella, Palo Alto Firewalls, F5 ASM (WAF), Cisco Meraki.
- **Detection & Response:** Splunk (Power User), CrowdStrike, SentinelOne, FireEye ETP, Proofpoint.
- **Vulnerability & Engineering:** Qualys, Tenable Nessus, Tanium, Jira, Confluence, PowerShell, Python.

PROFESSIONAL EXPERIENCE

Security Engineering & Technical Lead ZEBKA LLC

June 2022- now

- **Cloud Security & Identity (IAM):** Architected and deployed **AWS** cloud environments using **Single Sign-On (SSO)** and managed **Microsoft Entra ID** (formerly Azure AD) to enforce Zero Trust principles and Least Privilege access.
- **SIEM & Threat Detection:** Engineered and optimized **Microsoft Sentinel** and **Splunk** environments for centralized log aggregation; developed custom detection rules to identify and mitigate sophisticated security breaches.
- **Incident Response:** Executed incident response actions within **AWS** and **Azure**, reducing threat response time by 40% through automation using **PowerShell** and **Python** scripts.
- **Endpoint & Perimeter Defense:** Managed the full deployment of **Microsoft Defender** and **Cisco Umbrella**, providing robust endpoint protection (EDR) and secure internet gateway (SIG) filtering across the enterprise.
- **Vulnerability & Lifecycle Management:** Orchestrated comprehensive vulnerability scans using **Nessus**, prioritizing remediation efforts within **Jira** and documenting security playbooks in **Atlassian Confluence** for streamlined incident response.
- **GRC & Regulatory Compliance:** Audited project architectures against **NIST, ISO 27001, HIPAA, and PCI-DSS** frameworks to ensure data privacy and regulatory alignment in both on-prem and cloud-native environments.
- **Technical Instruction:** Translated complex engineering tasks into hands-on curricula, training students on the deployment and management of the **Microsoft Security Stack** and **Cisco** security solutions.

Cyber Security Consultant Nehemie Institute & Consulting

February 2020- April 2024

- **Hybrid Infrastructure Consulting:** Acted as a lead technical consultant for diverse clients, architecting and deploying **Cloud Security** measures in **AWS and Azure** to bridge the gap between legacy on-premise systems and modern cloud environments.

- **Perimeter & Network Security:** Managed and configured enterprise **Firewalls (Palo Alto, Cisco Meraki)** and **Web Application Firewalls (WAF)** to secure client network boundaries and prevent unauthorized external access.
- **Endpoint Defense & AV Migration:** Directed the transition from legacy Antivirus solutions to modern **EDR (SentinelOne, CrowdStrike)** and **Microsoft Defender**, hardening local endpoints and reducing malware infection rates by 60%.
- **Incident Response (IR) Leadership:** Led the end-to-end incident response lifecycle for client breaches; performed root cause analysis, containment, and post-incident remediation using **Splunk** and **Digital Forensics** workflows.
- **Data Loss Prevention (DLP):** Designed and executed tailored DLP strategies for clients using **Symantec DLP** and **Spirion**, successfully mitigating unauthorized data exfiltration for high-sensitivity projects.
- **Threat Mitigation:** Deployed enterprise-grade email security solutions (**Proofpoint, FireEye ETP**) for consulting clients, effectively reducing phishing-related incursions by 50%.
- **On-Premise Security & Patching:** Hardened the firm's internal on-premise infrastructure using **Tanium**, achieving a 95% compliance rate for patch management and vulnerability remediation.
- **Vulnerability Assessments:** Conducted recurring on-site audits using **Qualys**, identifying critical gaps in physical and digital infrastructure and providing prioritized remediation roadmaps.

Lead IT Engineer

Dec 2017- Feb. 2020

NcobNkun Cameroon

- **Infrastructure Founding & Design:** Spearheaded the end-to-end design and implementation of IT and network infrastructures for a diverse client base, moving the startup from initial concept to a fully functional service provider.
- **Security & System Deployment:** Directed the "One Student, One Laptop" initiative, configuring and securing hardware for hundreds of users while establishing secure baseline configurations and local network defenses.
- **Service Desk Engineering:** Built and managed the company's internal and client-facing service desk, implementing **Splunk** for log monitoring and system health analytics, which improved breach detection capabilities by 25%.
- **Enterprise Security Solutions:** Deployed and managed **CASB** and **WAF** solutions for clients to secure cloud-bound traffic and web applications, reducing data loss incidents by 40%.
- **Technical Leadership:** Trained and mentored junior staff and students on IT security best practices, hardware maintenance, and secure networking protocols, fostering a culture of security awareness from the project's inception.

COMMUNITY LEADERSHIP & VOLUNTEERING

Workshop Facilitator & Speaker | han-tak.com/events | 2023 – Present

- **Cyber Awareness Initiatives:** Organize and facilitate community workshops designed to educate families and individuals on digital safety, data privacy, and threat prevention.
- **Public Speaking:** Delivered keynote sessions for **Intelligentsia Corporation** on data privacy, reaching diverse audiences to foster a culture of security awareness.
- **Content Creation:** Develop accessible security resources and guides to simplify complex cybersecurity concepts for non-technical users.

EDUCATION

- **Business Communications for Microsoft Specialists** | Sheridan College, Canada (2024)
- **Bachelor's in Computer Science** | University of Yaoundé 1 (2018)
- **Certifications:** CompTIA Security+, Cisco CyberOps Associate, NDG Linux Essentials.
- **Certifications (2026):** CISSP. In Progress: Microsoft AZ-500 (Azure Security Engineer Associate).