Nkem Nkwi Morfaw

P: (302) 898-7470 **LinkedIn** **E:** morfawnkem@gmail.com

Risk Assessment | Network Vulnerability Scan | Encryption | Traffic Analysis | Web Application | Penetration Testing | Ethical Hacking | Phishing Analysis and Response | Malware Analysis | Intrusion Detection | IBM SPSS | Troubleshooting

Compliance Analyst/ Vendor Risk Analyst/ SOC Analyst

Education:

- **Saint University of MN, Minneapolis, MN:** Masters of Science in Cyber security **| GPA: 4.00** **Anticipated May 2024**
- **University of Buea, Cameroon:** Bachelor of Science in Geology and Environmental Sciences **Dec 2013**
- **Hennepin Technical College, Minnesota:** Associate Degree in Network Administration/Analyst **May 2022**

Certification:

- **CCNA | CompTIA Security+ | CompTIA Security+ | Splunk Fundamentals 1**

Technical Skills:

- **Programming Languages:** Python, Java, SQL, Shell Scripting **| Operating Systems:** Windows, Linux, MAC
- **Networking Firewalls:** OSI Model, TCP/IP, Firewalls / IPS/IDS, Networking Protocols, ICS / IDS, Wireshark
- **Cyber Security Tools:** Wireshark, Metasploit, VMware, Nessus, Splunk, Burp Suite, Nmap, cryptography (OpenSSL), Brute force (John), Kali Linux, CAINE, Qualys, Cisco Packet Tracer, Autopsy
- **Tools**: Nessus, Nexis Diligence, eMASS, D&B, GRC Archer, Wireshark, CrowdStrike, HP Fortify, Microsoft SCCM, Microsoft Azure, Web Inspect, Snort, ServiceNow, Veracode, Burp Suite, Aqua, Knowbe4, Splunk, Kiteworks, BitSight, Box.com, Active Directory, SonicWall, Microsoft Office 365 products.
- **Core Competencies:** Patch Management, Key & Host Compromise, Container Security, Terraform, Authentication and Access Control, Privacy Control Analysis, FISMA compliance, NIST, FIPS, OMB, FedRAMP, Risk Management Framework (RMF), POA&M Creation and Monitoring, A&A package, Vulnerability Management, Threat Detection & Analysis, Risk Management & Assessment, Developing Security Policies, Developing System Security Plan (SSP), Incident Response and Contingency Planning, CIA TRIAD, Data Security, Disaster Recovery Planning, Firewall Configuration, Malware Identification, Network Security, Microsoft Excel, Common vulnerability scoring system (CVSS) & CVE, OWASPs, SOX – SOC REPORTS, Due Diligence**s**

Work Experience

Software Development Engineer Intern | OCTO, Reston, VA **Aug 2021 – Present**

- Ensured all vendors were classified & assessments completed in accordance with vendor risk assessment & security assessment policies.
- Managed an updated Vendor Management repository with essential vendor data, including due diligence documents, and policies.
- Managed the creation, implementation, and upkeep of compliant policies and standards rooted in NIST 800-53 and NIST CSF
- Conducted risk assessments to document system vulnerabilities & establish mitigation protocols before engaging third-party services.
- Drives remediation activities from identification, plan preparation, and closure. Ensures accountability with respect to the Service Level Agreement (SLA).
- Performed vulnerability management for monthly scans, ensuring that deadlines are met, operational requirements are sufficiently documented, and the risk register is promptly updated with all entries and milestone updates.
- Researched best practices and stayed abreast of key internal controls, security, and IT regulations such as HIPAA, PCI-DSS, ISO 27001, GDPR, COBIT, SOX and other regulatory guidelines.

Cloud Security/Compliance Analyst | Home Depot, Minneapolis, MN **April 2020 – June 2021**

- Collaborated with the project team to execute established policies within the AWS (IAM) solutions cloud infrastructure.
- Communicated and enforced security policies, procedures, and safeguards for all systems and staff, based upon NIST.
- Participated in the consultative process and advised personnel in IT departments to coordinate Cybersecurity activities.
- Organized meetings with IT administrators to talk about remediation plans for the vulnerabilities picked up by scanning the network.
- Follow up with IT administrators and vendors to make sure the security alerts from these tools are resolved.
- Found vulnerabilities in client systems using Nessus, Claire, and NMAP; revealing exploitable vulnerabilities; worked with the red team to remediate vulnerabilities, and fortified firewall and access control rules.

IT Support Special II | The Vomela Companies, St Paul, MN **March 2018 – March 2020**

- Provided comprehensive support for LAN switches & wireless network equipment, including installation, configuration, troubleshooting.
- Conducted re-imaging, hardware/software installation, and remote assistance for employees, ensuring optimal functionality.
- Played a key role in educating and training employees on identifying and mitigating phishing emails, enhancing cybersecurity awareness.
- Contributed to network documentation, maintained hardware and software systems, and participated in VPN setup for users.
- Assisted in diagnosing and resolving technical issues, managed network printers, and supported server configurations.
- Actively engaged in continuous improvement initiatives to enhance service desk performance and worked with vendors to support third-party equipment.