Kenneth Nnadi
Cybersecurity Engineer
Eugene, Oregon I kennethinnadi@gmail.com
LinkedIn: www.linkedin.com/in/kenneth-nnadi/ I Portfolio: https://kenneth-nnadi.github.io

PROFESSIONAL SUMMARY

CISSP-certified cybersecurity engineer with 5+ years of experience securing networks, cloud environments, and enterprise systems. Expert in Palo Alto XDR, xSOAR and NGFW, FortiSIEM, SentinelOne, Splunk etc with a proven record in incident response, vulnerability management, and compliance (NIST, PCI-DSS, ISO 27001). Drives innovative security solutions to protect digital assets.

TECHNICAL SKILLS

- Security Platforms: Palo Alto XSOAR, Splunk, CrowdStrike Falcon, SentinelOne, Niksun, Fortinet (FortiSIEM, FortiGate), Microsoft Sentinel, Rapid7, Tenable, Suricata, Snort, AWS, Azure security.
- Cloud Security: AWS (IAM, CloudTrail, CloudWatch), Azure (Entra ID, Sentinel, NSGs)
- Network Security: Cisco ASA, IDS/IPS, F5,VPNs, BGP, MPLS, Wireshark, Tcpdump
- Endpoint & IAM: CrowdStrike Falcon, XDR, Symantec, Okta, SailPoint, ADDS, LDAP
- Programming & CI/CD: Python, PowerShell, Bash, C/C++, Java, Git, Jenkins
- Compliance: NIST 800-53/37, ISO 27001/2, PCI-DSS, HIPAA, GDPR

PROFESSIONAL EXPERIENCE

University of Oregon, Eugene, OR
Cybersecurity Program Manager
11/2024 – Present

- Lead a NICE cybersecurity program for next-Gen students, deploying HTB, and Fortinet SIEM in labs.
- Develop and collaborate to build cyber security clinic for small governments and SMEs.
- Configure Palo Alto policies for APT simulations, enhancing student skills.
- Coordinate workshops and labs with hands-on tools like Nessus and Wireshark and HTB.
- Recruit and train mentors in cybersecurity tools and techniques.
- Align curriculum with NICE framework to promote career awareness to next-gen professionals.

SOC Operations & Security Engineering

- Supported SOC operations, including log analysis, alert triage, and incident response workflows.
- Built automated playbooks with Cortex XDR and XSOAR, reducing SOC response times.
- Built a TDX (TeamDynamix) ticketing system and iPaaS workflows to automate SOC processes.
- Built and integrated log aggregation and detection rules in the SentinelOne platform.
- Implemented a Vulnerability Management using Greenbone OpenVAS for proactive risk reduction.
- Developed Threat Intelligence with MISP, enriching SOC alerts with contextual threat data.
- Developed SentinelOne & Splunk dashboards to track threats and metrics, cutting analysis time by 25%.
- Built and managed Attack Surface Management using open-source ASM tools.
- Designed and managed dedicated HTB labs for penetration testing, privilege escalation, and adversary simulation.
- Collaborated with engineers to build a Training Security Operations Center (TSOC) from scratch.

Center for Cyber Security and Privacy Lab (UO), Eugene, OR
Cybersecurity Researcher
08/2024 – 10/2024

- Investigated APT/ransomware patterns via Splunk, Palo Alto telemetry.
- Designing an AI based cybersecurity awareness platform for pros/seniors, and students with data-driven phishing countermeasures.
- Devised labs probing zero-day exploits, ML-based detection.
- Synthesized OSI, TCP/IP, SDN courses from original threat studies.

- Dissected breach forensics, refining research-backed training modules.
- Integrated real-world examples to enhance technical understanding.

University of Oregon, Eugene, OR
Cybersecurity Lab Analyst
08/2022 – 06/2024

- Managed labs with Palo Alto NGFW, Splunk SIEM, and Fortinet SIEM, training 100+ students.
- Taught and curated Networking Fundamentals content, integrating OSI, TCP/IP, BGP, MPLS.
- Deployed Azure Sentinel with SOAR playbooks, integrating CI/CD via Azure DevOps.
- Taught Microsoft and security stack (Azure, Entra ID, M365, IoT Plug and Play, Sentinel) and AWS security to 80+ students, emphasizing cloud architecture and secure deployment.
- Automated AWS audits with CloudTrail and Python, demonstrating cutting vulnerabilities by 20% in lab.
- Taught network design and VLANs, using Wireshark and IDS/IPS (Suricata, Snort).
- Configured Azure AD with MFA and NSGs for secure lab access.
- Led OpenSSL PKI exercises for 100+ seniors reinforcing encryption and certificate management.
- Hardened Exchange Server with Microsoft Defender for anti-malware defense.
- Taught OWASP ZAP, IDS/IPS, Wireshark, Metasploit, Hashcat etc. to 100+ students, targeting vulnerability and packet analysis.

Springboard Cybersecurity Career Track, SF,CA

Cybersecurity bootcamp
06/2022 – 06/2023

- Engaged in over 380+ hours of immersive, hands-on course material, providing a comprehensive understanding of various aspects of cybersecurity.
- Benefited from personalized mentorship and guidance from industry experts, ensuring a valuable learning experience and professional oversight.
- Successfully completed an in-depth capstone project, showcasing the application of acquired knowledge and skills in a real-world scenario.
- Completed 35+ mini projects that provided practical, real-world context, enabling a deeper understanding of the cybersecurity landscape.
- Engaged in over 30+ labs that bridged theoretical concepts to practical implementation, enhancing proficiency in areas such as systems security, network security, vulnerability assessment, risk assessment, and more.

A7 Konzult Nig LTD, Port Harcourt
System and Security Administrator / Security Vulnerability Specialist
12/2019 – 04/2022

- Deployed Okta SSO/MFA with AD integration via SCIM, securing 200+ users.
- Conducted Nessus and Rapid7 scans, reducing identification time by 50% with Python.
- Configured Cisco ASA and Splunk for threat monitoring, improving detection by 60%.
- Prioritized risks with CVSS in Splunk, boosting remediation by 40%.
- Managed Ivanti patch deployment, ensuring PCI-DSS/HIPAA, ISO 27001 compliance with 60% faster rollouts.
- Optimized MikroTik routers with VPN, BGP, and QoS for 99.9% uptime.
- Reduced incident response time by 35% with Qualys monitoring.
- Designed backup and recovery plans, minimizing data loss risks.

Center for Information and Telecommunication Engineering, Port Harcourt.
Network Engineering Intern
06/2018 – 01/2019

- Managed DNS, VPN, and firewalls for 750+ users, ensuring 100% uptime.
- Deployed IDS/IPS and SNMP monitoring, reducing incidents by 15%.
- Tested 1300+ email accounts for phishing resilience in 48 hours.

- Configured VLANs and subnetting for network optimization.
- Supported Cisco routing and switching via CCNA training.
- Implemented VPN and MFA for enhanced security.

EDUCATION

University of Oregon, Eugene, OR
Master’s in computer science
06/2022 – 06/2024 I GPA: 3.79/4.0

University of Port Harcourt, Port Harcourt, Nigeria
Bachelor’s in computer science
09/2015 – 11/2019 I GPA: 3.64/5.0

CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- CompTIA Security+
- Springboard Cybersecurity Bootcamp (9-months)
- AWS Security - Specialty (In Progress)
- Microsoft AZ-500 (In Progress)

PROJECTS

- Automated Vulnerability Management: Python pipeline with OpenVAS API, cutting scan time by 20%.
- Zero Trust PKI: Implemented short-lived certificates for secure access.
- Sentinel Threat Hunting: Built playbooks for incident response.

Full portfolio: https://kenneth-nnadi.github.io/#projects