SALEM KAWEINA NGAMDERE

About Me

Passionné par la cybersécurité,, j'ai transformé cette curiosité en expertise technique. Mon parcours est marqué par une soif constante d'apprendre les mécanismes de défense et d'attaque dans des environnements digitaux. Mon objectif : contribuer à bâtir des environnements plus résilients face aux cybermenaces modernes.

+237-688-79-94-46

salemkawein65@gmail.com

Douala, Cameroun

Compétences

- Analyse et corrélation d'événements de sécurité
- Détection d'attaques via SIEM
- Réponse à incidents
- Protocoles réseau (TCP/IP, DNS, VPN, SMB, LDAP etc)

Outils

SOC/ Blue Team :
Wazuh, Suricata, Opensense, shuffle, Grafana

Pentest:
Burp Suit, ZAP, OpenVas, Nikto, Nmap, Metasploit, Impacket,

Scripting and automation :
Bash, Powershell, Python

Langue

- Français
- Anglais (basic)

Expériences

ANALYSTE CYBERSÉCURITÉ | STAGE

RhopenLabs, Douala, Cameroun | Août 2025 - 02 Fev 2026

- Evaluation des attaques et analyse de la securite sur des environnements Active Directory
- Mise en œuvre de mécanismes de réponse à incident (désactivation de comptes compromis, blocage d'adresses IP, alertes SOC)
- Réponse automatisée et orchestrée avec Shuffle, pour une flexibilité accrue (notification vérification etc)

ADMINISTRATEUR SYSTÈME ET RÉSEAU | STAGE

Heaven SARL- Douala, Cameroun | Juin - Semptembre 2022

- Gestion des infrastructures réseaux et des serveurs avec .
- Mise en place d'un parfeu OPNsense pour filtrer le trafic renforcant ainsi la resilience du systeme .
- Surveillance des performances système avec Grafana et résolution des incidents techniques.
- Participation à la planification et à la mise en œuvre de projets d'infrastructure.

Éducation

🎓 MASTER CYBERSECURITE ET CYBERDEFENSE

Ecole Normale Superieure Polytechnique de Douala |
2024 - En cours

🎓 LICENCE RESEAU ET SECURITE INFORMATIQUE

Douala Institute of Technology | 2022

Projets et Réalisations

🧪 Lab Blue Team – Défense multi-couche
Conception et test d'un environnement de défense multi-couche pour évaluer la résilience, le MTTD et le MTTR face aux attaques.
• Pare-feu et segmentation réseau avec OPNsense
• Détection réseau avec Suricata (IDS)
• Centralisation et corrélation des logs via Wazuh
• Tests d'attaques (scan, exploitation, élévation de privilèges)
• Orchestration de la réponse à incident avec Shuffle (blocage IP, notifications, vérifications)