Laurent SEKONGO
Cybersecurity Engineer

+33 6.05.60.40.36
laurent.sekongo.pro@gmail.com
https://cyber-owl.xyz

I'm passionate about systems protection and threat response. I'm looking for a position in offensive security, operational security, or governance and risk management, where I can use my skills to anticipate, detect and neutralize cyberthreats.

WORK EXPERIENCES

Cybersecurity engineer (Freelance), Nantes | Since January 2025

- Web application and WEB server penetration testing
  - Enhance by 30% the likelihood for the company to be hacked internet bots and using automated tools
  - Propose security measures concerning vulnerabilities and server hardening
- Bug Bounty Insurance web application
  - Discovered an SSRF vulnerability

Network and Cybersecurity Consultant | **SETEC IS**, Paris | October 2023 to October 2024

SOC deployment

Analyzed customer needs, designed architecture, supervised the installation of security tools, set incident and access policies, tested system.

Strategic study of Active Directory scalability

Analysis of AD infrastructure, proposal of a more scalable and secure target architecture, security recommendations

Design of a sensitive or restricted information system (PACS, ANSSI)

- Design: Establishment of scenarios, physical and logical architecture, flow matrix, equipment benchmark and expression of DELL and STORMSHIELD requirements.
- Policies and procedures: data security management policy, account management, trace log management and analysis; logical access management procedures

Comparative study of risk analysis methods

- Risk analysis: State of the art of risk analysis methods (EBIOS RM, ISO27005, MEHARI, OCTAVE), analyzed the advantages and disadvantages, classified the methods according to use-cases.

L2 SOC Analyst | **IPgarde**, Lyon | April to September 2023

Context: Integration of a honeypot into the SIEM and continuous improvement of SOC processes and tools.

- Implementation of honeypots: Kerberoasting, ASREP-roasting
- Forensic investigation: log timeline monitoring, PC, server and firewall log analysis, anomaly and malicious behavior detection, in-depth file and malware analysis
- Incident response: Handling and investigation of N1 and N2 security alerts, incident report writing, implementation of detection rules, real-time attack simulation, vulnerability scans

EDUCATION

MSc in cyber security — IMT Atlantique, France (2023)
MSc in Networks and Telecommunications — INP-HB, Côte d'Ivoire (2021)

Certifications:
TryHackMe (Top 2%), Jr Penetration Tester 1, Google Cybersecurity Certificate, English (IELTS B2)

SKILLS AND TOOLS

Risk Management and Compliance: ISO27001 & ISO27005, EBIOS RM, MITRE ATT&CK, NIS, RGPD, NIST, PACS
Supervision: Graylog, Splunk, ELK, Wazuh, Malwarebytes, Graphana
Firewalls: PFsense, OPNsense
Threat Intelligence: OpenCTI, MISP, VirusTotal, scripting et automatisation (Python, PowerShell, Bash)
Pentest: NESSUS, Nmap, Metasploit, Burp Suite, NIKTO, Hydra.

PERSONAL PROJECTS

CyberHomeLAB: Design of a cybersecurity LAB — 2025

- LAB design (sub-networking, addressing plan and flow matrix)
- Configuration of hypervisor (Proxmox) and firewall (OPNSense)
    - Creation of 5 coexistent virtual interfaces on one physical interface
    - Creation of flow rules to allow traffic according to the flow matrix
    - VLAN creation (SIEM ELK and WAZUH, ATTACK, AD, SANDBOX)
- Create and configure virtual machines (Windows 10 and Windows Server, Kali, Debian), and install agents
- AD configuration
    - Add windows vms
    - Creating AD users
    - GPO testing

Wazuh: Cloud deployment (Akamai) — 2024

- Deploying Wazuh on a Linode VM
- Installation of agents on local VMs (Windows, Debian)
- Analysis of security logs (Brute Force, and attempted access to LSASS)

Study and solution for setting up an IPsec link behind a NAT - 2023

- Analysis of IPsec and NAT protocols
- Highlighting incompatibilities between IPsec and NAT
- NAT traversal
- Experimentation on GNS3