



OMAR LYAHYAI

SYSTEMS, NETWORK
& SECURITY ENGINEER
MASTER 2 CYBER-DEFENSE

CONTACT

LOCATION
Tangier-Assilah, Morocco

PHONE
+212 6 56 59 95 81

E-MAIL
omar_lyahyai@hotmail.fr

LINKEDIN
[linkedin.com/in/lyahyai-omar](https://www.linkedin.com/in/lyahyai-omar)

GITHUB
github.com/OLYAHYAI

PORTFOLIO
olyahyai.dev

PROFILE

7+ years running production infrastructure (systems, networks, virtualization, scheduling, backups) in high-availability environments. I build complete systems end to end: a self-hosted SOC/SOAR platform, a SaaS e-commerce product and a 3-node Proxmox homelab. I am comfortable across operations, security, automation and DevOps, and I document what I build.

SOFT SKILLS

- Root-cause analysis
- Autonomy
- Documentation
- Teamwork
- Communication
- Stress management
- Adaptability
- Proactivity

LANGUAGES

French — Bilingual
English — Professional
Spanish — Intermediate

PROFILE & OBJECTIVE

Systems and network administrator with 7+ years in heterogeneous production environments (Windows, Linux, AS400, VMware/Hyper-V), N2/N3 incident handling, job scheduling and automation. Alongside this role, I designed and run a self-hosted mini-SOC/SOAR, which is my Master's final-year project. It uses Wazuh SIEM, Suricata IDS, n8n automation, AI-assisted triage and Velociraptor DFIR on a 3-node Proxmox cluster.

Currently completing a Master 2 in Cyber-Defense (French-Moroccan double degree), I am open to IT roles across infrastructure, cloud/DevOps and cybersecurity (SOC, detection engineering, secure architecture), where I can bring both an operations mindset and hands-on security engineering.

TECHNICAL SKILLS

Security Operations & Detection

- Wazuh SIEM / XDR
- OpenSearch
- Suricata IDS
- CrowdSec
- Velociraptor (DFIR)
- Sysmon
- MITRE ATT&CK
- Atomic Red Team
- Kali Linux
- Custom decoders & rules

Systems & Virtualization

- Linux (Debian)
- Windows Server / AD
- IBM OS/400
- Proxmox VE (3-node cluster)
- VMware
- Hyper-V
- LXC
- Veeam
- MIMIX

Monitoring & Observability

- Zabbix
- SCOM
- Datadog
- Sentry

Network & Perimeter

- pfSense
- FortiGate IPsec VPN
- Cisco switching/routing
- VLANs & segmentation
- TLS / PKI
- Tailscale
- Cloudflare WAF & Tunnels
- pfBlockerNG
- LAN/WAN

Automation, DevOps & AI

- Python
- Bash
- PowerShell
- n8n
- SMA OpCon
- Git / GitHub Actions
- Docker
- Kubernetes (basics)
- MCP servers
- LLM agents

Development & Data

- Next.js / Vercel
- Strapi CMS
- PostgreSQL
- Kotlin (Android)

PROFESSIONAL EXPERIENCE

System and Network Administrator — VILAVI Group

Tangier | Apr. 2019 - Present

- Run production infrastructure and cross-functional projects with internal teams and external providers, under strict availability and security constraints.
- Administer the **SMA OpCon** scheduler to automate and centralize recurring jobs across Windows, Linux, AS400, Informatica, EDI and ODI, and industrialize production reports.
- Deploy workflows, jobs and batches (Informatica, ODI) to production, and support development, data and business teams during POCs and rollouts.
- Handle **N2/N3 production incidents**, follow the production plan and help plan critical operations.
- Administer Windows, Windows Server and Unix systems and VMware/Hyper-V virtualization, and run backup and restore operations (Veeam, MIMIX).
- Track network and telecom incidents, escalate to carriers, and administer site-to-site **IPsec VPN tunnels on FortiGate** and the Cisco network.
- Write and maintain operational documentation (DAT, DEX, DIN, PMEP, MODOP) and improve procedures.

Network and System Technician — KONTACTEL

Tangier | Sept. 2018 - Dec. 2018

- Managed 200+ workstations in a contact center, and installed physical and virtual servers for telephony and CRM.
- Administered Asterisk (500+ calls per day) and integrated call-center CRMs (VOX CRM, Goautodial, PhingooCRM).

Network and Infrastructure Technician — STM

Tangier | Aug. 2017 - Sept. 2017

- Designed and deployed fiber and copper cabling, worked on WAN links, and diagnosed network faults.

KEY FIGURES

SOC DATA SOURCES
pfSense, Suricata, CrowdSec, DHCP, DNS, endpoints

DETECTION REGRESSION SUITE
20 / 20 test cases passing

DFIR COVERAGE
Velociraptor on 9 endpoints

ATOMIC RED TEAM
345 techniques staged on the AD lab

INFRASTRUCTURE
3-node Proxmox cluster, VMs and LXC

CERTIFICATIONS

Google Cybersecurity Certificate (2025)
Cisco Certified Network Associate (CCNA)
Fortinet NSE 1 & NSE 2

INTERESTS

CybersecurityHomelab

AutomationAI for security

Jiu-JitsuDIY

PROJECTS & ACHIEVEMENTS

Autonomous Mini-SOC / SOAR — Master's final-year project

Self-hosted on Proxmox · no public exposure (Tailscale-only access)

2026 – Present

- SIEM:** deployed Wazuh (manager and indexer) to centralize pfSense firewall logs, Suricata IDS (EVE JSON), CrowdSec, DHCP and Unbound DNS, plus about a dozen Linux, Windows and Android agents. Encrypted the syslog transport with **TLS** (stunnel, internal PKI).
- Detection engineering:** wrote custom decoders and rules mapped to **MITRE ATT&CK**, added GeolIP enrichment and built a threat-geolocation dashboard. Fixed silent ingestion failures at the root cause (decoder anchoring, chrooted daemons, a syslog boot race after a pfSense upgrade).
- Detection-as-code:** put the ruleset under Git with a written change procedure and a **non-regression suite that replays real logs** (20/20 passing). Added a pipeline health watchdog that alerts on drops in volume, parsing or freshness.
- SOAR (n8n):** Wazuh webhooks feed AbuseIPDB enrichment, multi-rule correlation, deduplication, enriched Telegram alerts and a daily digest. Designed and validated **automatic IP blocking** on pfSense through Wazuh Active Response (least-privilege SSH account, pf table).
- AI-assisted triage:** each critical alert opens a ticket that an LLM agent triages through **home-built read-only MCP servers** (Wazuh, Proxmox). The agents are controlled from a Matrix/Element X SOC room. Agent privileges were hardened after an observed tool-bypass attempt.
- DFIR:** deployed Velociraptor on 9 endpoints and forwarded its audit log to Wazuh, with rules for remote execution and agent tampering.
- Purple-team lab** on an isolated network: Windows AD domain controller (Kerberos and DCSync auditing, Sysmon-modular, Atomic Red Team), DVWA and Metasploitable 3.

Wazuh · OpenSearch · Suricata · CrowdSec · pfSense · n8n · Python · MCP · Velociraptor · Sysmon · Git

PurpleOps — Android SOC & assessment app

2026

- Native Kotlin app on a rooted Pixel (LineageOS, KernelSU) that runs a Kali chroot and shows a **live Wazuh dashboard** (agents, alerts, posture score) over Tailscale.
- GitHub Actions CI** builds and publishes signed releases, and the app updates itself silently. Tool installs on the phone are traced in Wazuh. Public repository: github.com/OLYAHYA/PurpleOps.

JBR.ma — E-commerce SaaS platform

2025 – 2026

- Designed and built a Moroccan SaaS that lets artisans and merchants open an online store without technical skills. An Android app was published on Google Play.
- The containerized backend ran in LXC on Proxmox. The frontend is on Vercel with a **CI/CD pipeline** (GitHub, auto-deploy, one-click rollback). Traffic went through Cloudflare Tunnels, with strict multi-tenant isolation and a dedicated firewall. Datadog and Sentry monitored the platform.

Next.js · Strapi v5 · PostgreSQL · n8n · Docker · Cloudflare · Datadog · Sentry

Homelab infrastructure — 3-node Proxmox cluster

Ongoing

- The pfSense perimeter runs Suricata, CrowdSec and pfBlockerNG, with VLAN segmentation and an isolated lab bridge. Remote access goes only through Tailscale.
- Hosted services include Active Directory, PostgreSQL, Docker and n8n, plus a Matrix server and the AI agent platform on a dedicated VM. Workloads are isolated in resource pools.

EDUCATION

Master in Networks & Telecommunications — Cyber-Defense, IS Security

Sept. 2025 – June 2027

French-Moroccan double degree: UPHF / INSA Hauts-de-France & ENSI

Professional Degree — Enterprise Network Security and Administration

2015 – 2018

SUPTeM – BMHS / University of Saint-Quentin-en-Yvelines

High School Diploma

2014 – 2015

Lycée Al Hadifa – Tangier