



OMAR LYAHYAI

INGÉNIEUR SYSTÈMES,
RÉSEAUX & SÉCURITÉ
MASTER 2 CYBERDÉFENSE

CONTACT

LOCALISATION
Tanger-Assilah, Maroc

TÉLÉPHONE
+212 6 56 59 95 81

E-MAIL
omar_lyahyai@hotmail.fr

LINKEDIN
linkedin.com/in/lyahyai-omar

GITHUB
github.com/OLYAHYAI

PORTFOLIO
olyahyai.dev

PROFIL

Plus de 7 ans d'exploitation d'infrastructures de production (systèmes, réseaux, virtualisation, ordonnancement, sauvegardes) en environnement à forte disponibilité. Je conçois des systèmes complets de bout en bout : une plateforme SOC/SOAR auto-hébergée, un SaaS e-commerce et un homelab Proxmox à 3 nœuds. À l'aise entre exploitation, sécurité, automatisation et DevOps, je documente ce que je construis.

SAVOIR-ÊTRE

- Analyse de cause racine
- Autonomie
- Documentation
- Esprit d'équipe
- Communication
- Gestion du stress
- Adaptabilité
- Proactivité

LANGUES

Français — Bilingue
Anglais — Professionnel
Espagnol — Intermédiaire

PROFIL & OBJECTIF

Administrateur systèmes et réseaux avec plus de 7 ans d'expérience en environnements de production hétérogènes (Windows, Linux, AS400, VMware/Hyper-V), en traitement d'incidents N2/N3, en ordonnancement et en automatisation. En parallèle, j'ai conçu et j'exploite un mini-SOC/SOAR auto-hébergé, qui constitue mon projet de fin d'études de Master. Il repose sur le SIEM Wazuh, l'IDS Suricata, l'automatisation n8n, un triage assisté par IA et le DFIR Velociraptor, sur un cluster Proxmox à 3 nœuds.

En Master 2 Cyberdéfense (double diplôme franco-marocain), je suis ouvert aux postes IT en infrastructure, cloud/DevOps et cybersécurité (SOC, ingénierie de détection, architecture sécurisée), où je peux apporter à la fois une culture de l'exploitation et une pratique concrète de l'ingénierie sécurité.

COMPÉTENCES TECHNIQUES

Opérations de sécurité & détection

- Wazuh SIEM / XDR
- OpenSearch
- Suricata IDS
- CrowdSec
- Velociraptor (DFIR)
- Sysmon
- MITRE ATT&CK
- Atomic Red Team
- Kali Linux
- Décodeurs & règles custom

Systèmes & virtualisation

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

Supervision & observabilité

- Zabbix
- SCOM
- Datadog
- Sentry

Réseau & périmètre

- pfSense
- VPN IPsec FortiGate
- Switching/routage Cisco
- VLAN & segmentation
- TLS / PKI
- Tailscale
- Cloudflare WAF & Tunnels
- pfBlockerNG
- LAN/WAN

Automatisation, DevOps & IA

- Python
- Bash
- PowerShell
- n8n
- SMA OpCon
- Git / GitHub Actions
- Docker
- Kubernetes (bases)
- Serveurs MCP
- Agents LLM

Développement & données

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

EXPÉRIENCES PROFESSIONNELLES

Administrateur système et réseau — Groupe VILAVI

Tanger | Avr. 2019 – Aujourd'hui

- Exploitation de l'infrastructure de production et pilotage de projets transverses avec les équipes internes et les prestataires, sous fortes contraintes de disponibilité et de sécurité.
- Administration de l'ordonnanceur **SMA OpCon** pour automatiser et centraliser les traitements récurrents sur Windows, Linux, AS400, Informatica, EDI et ODI, et industrialiser les rapports de production.
- Mise en production de workflows, jobs et batchs (Informatica, ODI), avec support aux équipes de développement, data et métiers lors des POC et déploiements.
- Traitement des **incidents de production N2/N3**, suivi du plan de production et participation à la planification des opérations critiques.
- Administration de Windows, Windows Server et Unix, de la virtualisation VMware/Hyper-V, et des sauvegardes et restaurations (Veeam, MIMIX).
- Suivi des incidents réseau et télécom, escalade opérateurs, administration des **tunnels VPN IPsec site-à-site sur FortiGate** et du réseau Cisco.
- Rédaction et mise à jour de la documentation d'exploitation (DAT, DEX, DIN, PMEOP, MODOP) et amélioration des procédures.

Technicien réseau et système — KONTACTEL

Tanger | Sept. 2018 – Déc. 2018

- Gestion de plus de 200 postes en centre de contact, installation de serveurs physiques et virtuels pour la téléphonie et le CRM.
- Administration d'Asterisk (plus de 500 appels par jour) et intégration de CRM call center (VOX CRM, Goautodial, PhingooCRM).

Technicien réseau et infrastructure — STM

Tanger | Août 2017 – Sept. 2017

- Conception et déploiement de câblage fibre et cuivre, interventions sur liens WAN et diagnostic de pannes réseau.

CHIFFRES CLÉS

SOURCES DU SOC
pfSense, Suricata, CrowdSec, DHCP, DNS, postes et serveurs

TESTS DE NON-RÉGRESSION
20 / 20 cas validés

COUVERTURE DFIR
Velociraptor sur 9 machines

ATOMIC RED TEAM
345 techniques prêtes sur le lab AD

INFRASTRUCTURE
Cluster Proxmox 3 nœuds, VM et LXC

CERTIFICATIONS

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

CENTRES D'INTÉRÊT

- Cybersécurité
- Homelab
- Automatisation
- IA & sécurité
- Jiu-Jitsu
- Bricolage

PROJETS & RÉALISATIONS

Mini-SOC / SOAR autonome — Projet de fin d'études (Master)

2026 – Aujourd'hui

Auto-hébergé sur Proxmox · aucune exposition publique (accès Tailscale uniquement)

- SIEM** : déploiement de Wazuh (manager et indexer) pour centraliser les logs du pare-feu pfSense, l'IDS Suricata (EVE JSON), CrowdSec, DHCP et le DNS Unbound, ainsi qu'une douzaine d'agents Linux, Windows et Android. Transport syslog chiffré en **TLS** (stunnel, PKI interne).
- Ingénierie de détection** : décodeurs et règles custom mappés sur **MITRE ATT&CK**, enrichissement GeoIP et tableau de bord de géolocalisation des menaces. Pannes d'ingestion silencieuses corrigées à la racine (ancrage des décodeurs, démons chrootés, race au démarrage de syslog après une mise à jour pfSense).
- Detection-as-code** : ruleset versionné sous Git avec une procédure de changement écrite et une **suite de non-régression qui rejoue des logs réels** (20/20 validés). Sonde de santé du pipeline qui alerte sur les chutes de volume, de parsing ou de fraîcheur.
- SOAR (n8n)** : les webhooks Wazuh alimentent l'enrichissement AbuseIPDB, la corrélation multi-règles, la déduplication, des alertes Telegram enrichies et un digest quotidien. Conception et validation du **blocage automatique d'IP** sur pfSense via l'Active Response Wazuh (compte SSH à moindre privilège, table pf).
- Triage assisté par IA** : chaque alerte critique ouvre un ticket qu'un agent LLM trie via des **serveurs MCP maison en lecture seule** (Wazuh, Proxmox). Les agents se pilotent depuis un salon SOC Matrix/Element X. Leurs droits ont été durcis après une tentative de contournement d'outil observée.
- DFIR** : Velociraptor déployé sur 9 machines, son journal d'audit remonté dans Wazuh avec des règles d'exécution à distance et d'altération de l'agent.
- Lab purple team** sur réseau isolé : contrôleur de domaine Windows AD (audit Kerberos et DCSync, Sysmon-modular, Atomic Red Team), DVWA et Metasploitable 3.

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

PurpleOps — Application Android SOC & audit

2026

- Application Kotlin native sur un Pixel rooté (LineageOS, KernelSU) qui exécute un chroot Kali et affiche un **tableau de bord Wazuh en direct** (agents, alertes, score de posture) via Tailscale.
- CI GitHub Actions** qui compile et publie des versions signées, avec mise à jour silencieuse de l'application. Les installations d'outils sur le téléphone sont tracées dans Wazuh. Dépôt public : github.com/OLYAHYA/PurpleOps.

JBR.ma — Plateforme SaaS e-commerce

2025 – 2026

- Conception et développement d'un SaaS marocain qui permet aux artisans et commerçants de créer leur boutique en ligne sans compétences techniques. Application Android publiée sur Google Play.
- Backend conteneurisé en LXC sur Proxmox, frontend sur Vercel avec **pipeline CI/CD** (GitHub, déploiement automatique, retour arrière en un clic). Trafic via Cloudflare Tunnels, isolation multi-tenant stricte et pare-feu dédié. Supervision Datadog et Sentry.

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

Infrastructure homelab — Cluster Proxmox 3 nœuds

En continu

- Périmètre pfSense avec Suricata, CrowdSec et pfBlockerNG, segmentation VLAN et pont isolé pour le lab. Accès distant uniquement via Tailscale.
- Services hébergés : Active Directory, PostgreSQL, Docker et n8n, ainsi qu'un serveur Matrix et la plateforme d'agents IA sur une VM dédiée. Charges isolées par pools de ressources.

FORMATION

Master Réseaux & Télécommunications — Cyberdéfense, Sécurité des SI

Sept. 2025 – Juin 2027

Double diplôme franco-marocain : UPHF / INSA Hauts-de-France & ENSI

Licence professionnelle — Sécurité et administration des réseaux d'entreprise

2015 – 2018

SUPTeM – BMHS / Université de Saint-Quentin-en-Yvelines

Baccalauréat

2014 – 2015

Lycée Al Hadifa – Tanger