M. Khalil Ghiati

Ingénieur Infrastructure & Sécurité

medkhalilghiati@gmail.com · 07 74 73 89 29 (WhatsApp) · Lyon, France · github.com/Khalil-secure · portfolio-khalil-secure.vercel.app

EXPÉRIENCES PROFESSIONNELLES

Bouygues Telecom
Sept. 2024 – Sept. 2025

Chef de Projet Télécom

Lyon, France

- Automatisation de la collecte et qualification des données sur **300+ sites** via APIs — gain d'efficacité **+90%**
- Gestion bout en bout de **4 projets majeurs** avec respect des jalons et reporting stakeholders
- Analyse de sécurité des infrastructures **5G** selon recommandations **ANSSI** et contribution aux audits de conformité
- Coordination de projets interservices et exploration de solutions IA pour l'optimisation opérationnelle

5G · LTE · 4G · Wi-Fi · FTTH · IMS · VoLTE · DWDM · ANSSI

CogniScan (Start-up)
Avr. 2024 – Août 2024

ML Engineer & Chef de Projet

Limoges, France

- Conception d'outils d'analyse et visualisation interactive de données (Python, Dash, Plotly)
- Optimisation de réseaux neuronaux convolutifs (**CNN**) pour détection d'anomalies sur imagerie médicale
- Développement d'algorithmes de traitement du signal pour extraction de signatures biologiques et réduction de bruit

Python · PyTorch · TensorFlow · Matlab · REST API · Embarqué

ETEX Group
Juin 2023 – Août 2023

Assistant Responsable Infrastructure IT Régional

Avignon, France

- Déploiement et administration d'une solution **Centreon** pour un parc de **1 200+ terminaux** en Europe de l'Ouest
- Migration réussie d'un parc serveur de **VMware vers Hyper-V** avec intégration complète au monitoring
- Durcissement sécurité des serveurs Linux selon benchmarks **CIS** et recommandations **ANSSI** (SSH, firewall, patching)

Linux · Docker · Centreon · Hyper-V · Bash · Python · MySQL · Firewall

PROJETS TECHNIQUES

Zero Trust Network Lab — Kubernetes & Infrastructure-as-Code
2025 – En cours

github.com/Khalil-secure/zero-trust-k8s-lab

- Architecture **Zero Trust** sur cluster **Kubernetes** (k3s) : segmentation par namespace, NetworkPolicies deny-by-default, mTLS via **Istio**
- Infrastructure provisionnée en **Terraform** (IaC) — reproductible, versionnée, déployable en **<5 min**
- VPN site-to-site **WireGuard** + WAF ; rotation automatique des certificats via cert-manager
- **SIEM** léger : logs centralisés **Loki + Grafana**, alertes temps réel sur comportements anormaux
- Pipeline **CI/CD** sécurisé (GitHub Actions) avec scan **Trivy** et enforcement **OPA/Gatekeeper**
- Simulations d'attaques **MITRE ATT&CK;** (T1021, T1046, T1190) avec rapports de posture de sécurité automatisés

Kubernetes · Terraform · Zero Trust · Istio · WireGuard · Loki/Grafana · OPA · Trivy · MITRE ATT&CK;

Homelab SOC — Détection & Réponse aux Incidents
2024 – 2025

github.com/Khalil-secure/homelab-soc

- Lab SOC complet sur Docker isolé (hardened-net) : SSH durci, **Fail2ban**, intégrité fichiers via **inotifywait**
- IDS/IPS **Suricata** avec règles mappées sur **MITRE ATT&CK;** ; corrélation alertes via **ELK Stack**
- Monitoring temps réel **Netdata** + logs centralisés (auth, fail2ban, intégrité fichiers)
- Pipeline **CI/CD** GitHub Actions avec validation automatique des contrôles de sécurité

Suricata · ELK Stack · Docker · Fail2ban · Netdata · MITRE ATT&CK; · IDS/IPS · GitHub Actions

COMPÉTENCES

Langages: Python, Bash, Ruby, Go, C/C++, Rust

Sécurité: Fail2ban, Suricata, IDS/IPS, MITRE ATT&CK;, ELK, SSH Hardening, OPA, Trivy

DevOps: Docker, Kubernetes, Terraform, GitHub Actions, CI/CD, Git

Infrastructure: Linux, Centreon, Netdata, VMware, Hyper-V, Kubernetes

Réseau: 5G, FTTH, VoIP, MPLS, Firewall

Bases de données: MySQL, PostgreSQL

Méthodes: Agile, Scrum, Jira

FORMATION / CERTIFICATIONS

ENSIL-ENSCI — Limoges

Ingénieur Électronique & Télécoms

2022 – 2025 · Limoges, France

Réseaux 5G/6G, systèmes embarqués, antennes.

Projet avec Ansys : détection des distances d'isolement des microprocesseurs.

TryHackMe — Jr Penetration Tester Path

TryHackMe — SOC Level 1 (certifié)

Microsoft Azure Fundamentals AZ-900

Root-Me — 100+ challenges résolus

TOEIC 940/990 — Anglais professionnel

LANGUES & CENTRES D'INTÉRÊT

Langues : Anglais — TOEIC 940/990 (professionnel) · Français — Courant · Arabe — Langue maternelle

Intérêts : Ceinture noire Karaté (Shodan) · BJJ débutant · Hackathons (Lablab.ai, équipes internationales) · CTF — Root-Me, TryHackMe