Khalil Abdul Karim

Étudiant M2 Cybersécurité · EPITA

Sécurité offensive & Défensive · IA appliqué à la cybersécurité

khalilabdelkarim@outlook.com | +33 7 78 12 11 63 | Paris, France

in linkedin.com/in/khalil-abdul-karim-2384ba217

⌥ github.com/KhalilAbdulKarim

Profil

Étudiant M2 Cybersécurité (EPITA), je recherche un stage pour intégrer une équipe sécurité opérationnelle (SOC, Pentest ou DevSecOps). Expérience terrain en SOC hospitalier · pentest web · sécurisation d'applications cloud. En production : Honeypot SSH autonome profilant des attaquants réels via pipeline LLM & MITRE ATT&CK

Expérience Professionnelle

Stagiaire Cybersécurité — New Mazloum Hospital — Liban *Août 2024 – Fév. 2025*

SOC N1 · SIEM Wazuh · Analyse de vulnérabilités · RBAC · Sécurité applicative

- Prise en charge et qualification de 3 à 5 incidents de sécurité par semaine : analyse de journaux systèmes, corrélation d'événements suspects et escalade structurée selon la criticité .
- Identification et remédiation de vulnérabilités critiques de contrôle d'accès : durcissement RBAC, implémentation du principe de moindre privilège et renforcement des mécanismes d'authentification sur les systèmes hospitaliers.

Projets

AI Honeypot & Attacker Profiling System *2026*

Python · Paramiko · LLM · React · Flask · Docker · SQLite · MITRE ATT&CK

- Conception et déploiement d'un faux serveur SSH (Paramiko) sur VPS exposé en production, émulant un environnement Linux réaliste pour attirer des attaquants réels et capture complète des sessions : credentials, commendes, timing comportemental et empreinte réseau. 100+ session collectées en 48h.
- Pipeline IA autonome classifiant chaque attaquant par niveau, outillage et intention (cryptomining / ransomware / reconnaissance) avec mapping MITRE ATT&CK et generation automatique de recommendations défensives.
- Dashboard React temps réel : carte mondiale des origines d'attaques, heatmap des credentials, timeline des commandes et profils d'attaquants générés par LLM, donnés live via Flask API, rafraîchissement automatique toutes les 15s.

Scanner de Sécurité Web — Security Misconfiguration & Sensitive Data Exposure *2026*

Node.js · OWASP Top 10 A02 · SSRF Protection · HTML · JSON Reporting

- Outil de crawling récursif détectant automatiquement 5 catégories de misconfigurations (headers HTTP manquants, cookies non sécurisés, CORS permissifs, fichiers sensibles exposés, info disclosure) sur 12 à 15 URLs par scan.
- Génération de rapports exploitables (HTML & JSON) avec dashboard de monitoring temps réel, historique des scans et recommandations de remédiation priorisées par finding directement utilisable en contexte de pentest ou d'audit.

SOC Lab — Détection d'Intrusions (Wazuh SIEM) — Infrastructure AWS *2026*

AWS · Wazuh SIEM · Kali Linux · Brute Force SSH · Privilege Escalation

- Déploiement d'un environnement SOC complet sur AWS (Wazuh Manager + Indexer + Dashboard) supervisant 2 agents (Windows & Ubuntu), avec simulation d'attaques réelles depuis Kali Linux (ex: brute force SSH et élévation de privileges).

CareCircle — Plateforme Télémédecine Sécurisée — Azure · NestJS · TypeScript *2024*

NestJS · TypeScript · Azure Cognitive Services · JWT · RBAC · WebSockets · RGPD

- Sécurisation d'une application web médicale gérant des données sensibles : RBAC granulaire sur 10 à 15 endpoints avec contrôle d'accès par rôle (patient, médecin, admin), authentification JWT et validation stricte des inputs.

Compétences Techniques

Offensif Tests d'intrusion web · OWASP Top 10 · Burp Suite · Nmap · Metasploit · ffuf · Paramiko · Scapy

Défensif SOC · SIEM Wazuh · Wireshark · Nessus · RBAC · Analyse de vulnérabilités · Honeypot · Deception Tech · Threat Intel · Attacker Profiling (LLM)

Dev & Cloud Python · Node.js · NestJS · TypeScript · AWS · Azure · Docker · Linux · Windows · HTTP/TCP-IP/DNS

Formation

Master Cybersécurité — EPITA — Le Kremlin-Bicêtre *Fév. 2025 – présent*

Ethical Hacking Program — Semicolon Security *Certification ISA*

Licence Informatique SE — University of Balamand, Liban *2021 – 2024*

Langues Arabe natif · Anglais C1 · Français B2 **Certifications** SEC+ (En Cours)