MOHAMED EL GHAZI RECHERCHE STAGE PFE

Berrechid / Casablanca | (+212) 6 72 27 08 64 | mohamedelghazi704@gmail.com

https://linkedin.com/in/mohamedelghazi/ | https://me.packprotv.com

RÉSUMÉ

Futur ingénieur (ENSET Mohammedia) passionné par la défense active et l'investigation numérique. Fort d'une expérience freelance en sécurisation de systèmes critiques et de projets avancés mêlant IA et Cybersécurité (Deep Learning appliqué aux IDS). Je cherche à rejoindre **une équipe SOC/CSIRT** pour mettre à profit mes compétences en **Threat Intelligence, analyse forensique et détection d'intrusions pour traquer les menaces avancées (APTs)**.

EXPÉRIENCE

Ingénieur Cybersécurité (Mission Freelance) | ISE-TECHNOLOGIE - France(Remote) **Oct. 2025 – Janv. 2026**

- Intégration d'un SOC intelligent pour un **écosystème véhicule–cloud–IoT**.
- Déploiement d'IDS intelligents pour la détection d'anomalies sur cartes embarquées et flux IoT.
- Mise en place d'un SIEM ELK (collecte, corrélation, alertes temps réel).
- Intégration de MISP Threat Intelligence pour l'enrichissement et la priorisation des incidents.
- Automatisation des réponses aux incidents via scripts Python (SOAR léger).

Stagiaire Cybersécurité | DATA SOFTWARE (Hybride) (2 mois) **Juillet 2025 - Sept. 2025**

Développement d'un HIDS IA pour la détection d'anomalies et sécurisation Cloud VPS OVH via la Défense en Profondeur(Network Hardening,Firewall OVH,VPN).

Stagiaire Cyber Sécurité | ZINTEL, Technopark Casablanca (1 mois) **Août. 2024**

Réalisation de tests d'intrusion (Pentest) web et analyse de vulnérabilités.

Animateur Atelier Sensibilisation Menaces Cyber Address: MJW3+RVQ, Rue El Jahid, Mohammédia 20800 **Mars 2024**

Organisation et animation d'ateliers de sensibilisation aux menaces et bonnes pratiques cyber.

PROJETS CLÉS

SOC Intelligent & Défense en Profondeur **Oct. 2025**

- Construction d'un labo complet **segmenté en 3 zones** (Attaquant, DMZ/Honeypot, Ressources) - Machines Virtualbox.
- Développement d'un **IDS basé sur l'IA** (GRU/Deep Learning) pour analyser les logs pare-feu en temps réel.
- Mise en place d'un **Honeypot** et Integration **ELK**.

LLM Sentinel Guard – Pare-feu Intelligent LLM – académique (4 membres) **Dec. 2025**

- Conception d'un firewall applicatif (Layer 7) pour la protection des LLM contre prompt injection, jailbreak et abus.
- Développement d'un proxy FastAPI intégrant détection IA (BERT), règles Regex et orchestration LLM locale (Ollama).
- Conteneurisation Docker, supervision via stack ELK (logs, alertes, traçabilité des requêtes).

SOC Interne avec Wazuh, Suricata & ELK Stack - binôme **Avr. 2025**

- Projet de Fin de Module en Etude des vulnérabilités et la détection des intrusions.
- Suricata détecte les anomalies réseau et génère des alertes captées par le Wazuh Agent, qui les transmet au Wazuh Manager. Le pare-feu nftables régule les connexions selon des règles de sécurité.

COMPÉTENCES TECHNIQUES

- **SOC & DFIR** : Wazuh (EDR/XDR), Suricata (NIDS), ELK Stack, Splunk, Wireshark (Traffic Analysis), Volatility (Memory Forensics), MITRE ATT&CK.
- **Threat Intelligence (CTI)** : MISP (Malware Information Sharing Platform), IOC Extraction, OpenCTI, Analyse de campagnes (APT tracking).
- **DevSecOps & IA** : Python (Scripting & Automation), TensorFlow/Keras (Détection d'anomalies), Docker, Git, Bash.
- **Infrastructure & Cloud** : Linux Hardening (Debian/Kali), Azure (NSG), AWS, OVH, Firewalling (nftables/pfSense).
- **Gouvernance** : ISO 27001, Analyse de risques (EBIOS RM), Défense en Profondeur.

FORMATION

Programme Ingénierie | Cybersécurité, Confiance Numérique
École Normal Supérieur d'Enseignement Technique, Mohammedia **2023 - Prévu 2026**

Technologie et Sciences Industrielles
Classes préparatoires aux grandes écoles | Settat **2021 - 2023**

CERTIFICATIONS, LANGUES & INTÉRÊTS

Certifications : Cisco CyberOps (05/2025) | CCNA Networking (04/2024) | Google Cybersecurity (09/2023).

Langues : Arabe, Français, Anglais(Assez bien).

Intérêts : Blue Team, CTF, Veille Cyber Blogging.