LAILA HAMMOUCH

Élève ingénieure Réseaux Intelligents et Cybersécurité

+212 624337391 | lailahammouch38@gmail.com | Mobilité nationale

linkedin.com/in/laïla-hammouch | Portfolio | github.com/LailaHammouch

Profil

Élève ingénieure en 3e année à l'ENSA Khouribga, passionnée par la cybersécurité (SOC, IAM, GRC, IT/OT) et souhaitant mettre ses compétences en pratique dans un environnement professionnel. Actuellement à la recherche d'un stage de fin d'études (PFE) dès février 2026.

Formation

Cycle Ingénieur – Réseaux Intelligents & Cybersécurité – *ENSA Khouribga* 2023 – Présent
Classes Préparatoires Intégrées – *ENSA Khouribga* 2021 – 2023
Baccalauréat Sciences Physiques – *Lycée Ibn Khaldoun* 2021

Expérience

3D Smart Factory Août – Sept 2025
Stage PFA : Détection intelligente des menaces

- Conception d'un **agent intelligent de détection et de réponse aux incidents**.
- Mise en place d'une **infrastructure SOC** (SIEM, IDS/IPS, corrélation).
- Développement d'une **interface web** de visualisation des alertes.

LafargeHolcim Maroc Juil – Août 2025
Stage PFA : Analyse de risques et gouvernance cybersécurité

- Analyse de risques **EBIOS RM** sur environnements IT/OT.
- Identification des actifs critiques et évaluation de la conformité.
- Proposition de recommandations de sécurité.

CodeAlpha Oct – Nov 2024
Stage d'initiation : Détection d'intrusions

- Déploiement et configuration d'un **IDS Snort**.
- Développement d'un **outil Python** d'analyse du trafic.

Projets Académiques

- **Plateforme Passwordless d'entreprise (FIDO2 + Device Trust)** : déploiement d'une solution **Passwordless** basée sur **Keycloak WebAuthn**, intégrant **Passkeys** et clés matérielles (**YubiKey**, **SoloKey**), avec contrôle de posture des endpoints (**Osquery**) et corrélation des événements d'authentification via **Wazuh SIEM** et **ELK**.
- **NIDS basé sur le Deep Learning** : détection des comportements réseau anormaux.
- **Orchestration des vulnérabilités avec DefectDojo et analyseurs open-source** : automatisation complète du scan, de la corrélation et du suivi des vulnérabilités via **DefectDojo**, intégrant **OWASP ZAP**, **Trivy**, **OpenVAS** et **Nmap**.
- **SOC Use Cases basés sur MITRE ATT&CK** : conception de cas de détection avancés, déploiement d'un **SIEM Wazuh**, création de règles personnalisées et validation par simulation d'attaques contrôlées.
- **Attaques et durcissement d'applications Cloud** : simulation d'attaques web et cloud, exploitation de vulnérabilités applicatives et mise en œuvre de contre-mesures de sécurité (configuration **WAF**).
- **Mise en place d'un cluster de calcul quantique dans le Cloud** : déploiement, configuration et tests d'exécution de workloads quantiques distribués dans un environnement cloud.

Compétences

Réseaux & Outils : TCP/IP, OSPF, VLAN, QoS, NAT, MPLS — GNS3, Cisco Packet Tracer
Virtualisation : VMware, VirtualBox, Hyper-V, ESXi
Cloud : AWS, OpenStack
Conteneurs : Docker, Kubernetes
Développement : Python, C++, HTML, CSS, PHP, SQL
Scripting : Bash, PowerShell
Compétences personnelles : Esprit d'équipe, Autonomie, Rigueur, Adaptabilité, Gestion du temps, Résolution de problèmes

SOC : SIEM (Wazuh, ELK, Splunk), IDS/IPS, Zeek, DefectDojo, OpenVAS, ZAP, Trivy
Analyse Malware & Forensics : Autopsy, Volatility, PEStudio, Cuckoo Sandbox, REMnux
Sécurité : VPN, Firewalls (WAF, pfSense)
Conformité : ISO 27001, EBIOS RM
Frameworks : MITRE ATT&CK, OWASP Top 10
IAM : Keycloak, SSO, MFA, RBAC, OAuth, LDAP/AD
Pentest : Nmap, Metasploit, Burp Suite, Feroxbuster, Hydra, LinPEAS

Certifications

- CCNAv7, CyberOps (Cisco)
- Python3 (Hack The Box)
- AWS Cloud Foundations
- Fundamentals in Cybersecurity (Fortinet)

Langues

Arabe : Natif
Français : Courant
Anglais : Courant

Activités

- Membre **B-Secure**
- Membre **JLM**
- Membre **Enactus**
- Membre **Comité Masjid**
- Membre **NetcomDay.6**