LAIRGI SALAH EDDINE

JE CHERCHE UN **CDI** EN **CYBERSÉCURITÉ** (**AUDIT TECHNIQUE**, ANALYSE **SOC**)

IDF, France
+33 7 49 90 26 37
salahlairgi1@gmail.com
LinkedIn

A PROPOS DE MOI

Apprenant rapide, **rigoureux**, **autonome** et doté d'un bon **esprit d'équipe.**

COMPÉTENCES TECHNIQUES

SOC :
- Microsoft Defender for Endpoint
- Microsoft Intune
- Entra ID (Azure AD)
- Wireshark

Gestion des vulnérabilités et scans :
- Tenable Nessus / PingCastle
- Burp Suite
- Gobuster/Dirbuster/FUFF
- Nmap

Automatisation et scripting :
- Python C, Java / Bash / Powershell
- Docker

Outils de pentesting :
- Metasploit / John the Ripper / Hydra

Analyse de logs et surveillance :
- Graylog

LANGUES

Français: ●●●●●
Anglais: ●●●●●
Arabe: ●●●●●
Espagnol: ●●○○○

INTÉRÊTS

- **CTF** (Classé parmi les 10% tryhackme)
- **Musculation** (Discipliné: 6fois /semaine)
- **Voyages** (découverte de nouveaux challenges)

FORMATION

ENSEIRB 3ème Année (M2): 2022-2025
- Cours avancés en informatique, incluant la programmation, la cybersécurité (**pentesting**, **gouvernance & analyse de risques**, **audit de l'Active Directory**), les structures de données, les algorithmes, les bases de données, les systèmes d'exploitation et les réseaux.

CPGE Ibn Tahir, Maroc
- Classement parmi les 3 % meilleurs de la promotion.

EXPERIENCES PROFESSIONNELLES

Stage de fin d'étude Analyste Cybersécurité - BDO France

- Projet de sécurisation de l'**Active Directory** :
  → Analyse via **PingCastle** (comptes à privilèges, GPOs à risque, trusts, etc.)
  → **Implémentation de scripts PowerShell pour l'audit du trafic LDAP/NTLM sur le domaine.**
  → Rédaction et application de **plans de remédiation** (nettoyage, durcissement, suivi post-audit)
- Projet de réduction **de la surface d'attaque via Defender et Intune :**
  → **Durcissement** des postes, **limitation** des privilèges, vérifications régulières
- **Activités de sécurité opérationnelle (RUN) :**
  → Analyse des alertes **SOC** et EDR **Defender.**
  → **Réponse aux incidents** : isolement de machines, scan antivirus, suppression de payloads, blocage IP/URL
  → Rédaction des rapports de contrôles afin d'assurer le conformité ISO 27001

Outils : Microsoft Defender | Tenable Nessus | PingCastle | GLPI | PowerShell | Entra ID | Intune | Active Directory (AD)

Stage Analyste SOC - Chez iTrust

- **Analyse des alertes sécurité :** traitement des incidents via Reveelium, classification, rédaction de rapports d'investigation.
- **Surveillance des endpoints :** supervision des postes et serveurs via ESET EDR.
- **Analyse des logs :** exploitation de Graylog pour le filtrage et la détection d'anomalies de sécurité.
- **Automatisation SOC :** création d'un script Python pour automatiser des tâches récurrentes, optimisation du temps de réponse.

Outils : Graylog | ESET | SIEM (Reveelium) | Python

PROJETS

Analyse de risques ISO 27005 – Projet cybersécurité

- Réalisé une **analyse de risques complète** pour un site de paris en ligne.
- **Cartographie des actifs, menaces et scénarios.**

Benchmarking de schémas de chiffrement symétrique à seuil

- **Implémentation** et **benchmarking** des schémas sur un cluster pour comparer les performances des protocoles.