Oussama **ABDELFATTAH**

INGÉNIEUR EN CYBERSÉCURITÉ · AUDIT, OFFENSIF & DÉTECTION

Rabat, Maroc · Permis B · Mobilité Maroc / Europe · Disponible immédiatement

abdelfattah.oussama.pro@gmail.com | (+212) 696-280916 | OussamaABDELFATTAH | OussamaAbdelfattah |
www.oussama-abdelfattah.tech

Profil

Ingénieur en cybersécurité généraliste, formé et pratiqué sur les trois piliers du métier : **audit & conformité** (ISO 27001, NIST CSF, IEC 62443), **sécurité offensive** (Red Team, pentest, Kali/Metasploit/Burp) et **détection & SIEM** (Splunk, Zeek, threat hunting). Double expérience d'audit de sécurité sur des systèmes critiques réels — **DataProtect** (BU Critical Infrastructure Cybersecurity) et **Groupe ONCF** — incluant la conception d'un cyber range complet (**CyberRail-OT**) et une campagne Red Team alignée MITRE ATT&CK. Je recherche un poste d'ingénieur en cybersécurité (GRC/audit, SOC, pentest ou sécurité offensive) au Maroc ou en Europe.

Expériences Professionnelles

Projet de Fin d'Études (PFE) — Ingénieur Cybersécurité
Février – Juin 2026 · 4 mois

DATAPROTECT — BU CRITICAL INFRASTRUCTURE CYBERSECURITY — *Casablanca / Rabat, Maroc*

- Conception d'un **cyber range** complet (**CyberRail-OT**) : environnement de test isolé, architecture segmentée à 4 zones, 22 conteneurs Docker — méthodologie transposable à tout environnement critique.
- Campagne **Red Team** (17 scénarios) alignée MITRE ATT&CK ; kill chain neutralisée en moins de 65 secondes après durcissement.
- Audit de sécurité selon **IEC 62443** portant le niveau de sécurité de **62 à 88/100** ; référentiel de 46 contrôles réutilisable, applicable à d'autres cadres de conformité.
- Développement d'un **proxy applicatif (L7)** de filtrage et blocage de commandes dangereuses ; supervision et détection via Splunk / Zeek / Nozomi.

Stage de Perfectionnement — Audit de Sécurité des Systèmes Critiques
Juin – Juillet 2025 · 2 mois

GROUPE ONCF — OFFICE NATIONAL DES CHEMINS DE FER — *Rabat, Maroc*

- Audit de sécurité complet d'un système d'infrastructure critique (plus de 20 équipements).
- Évaluation multicritère (ISO 27001, IEC 62443-3-3, NIST CSF, MITRE ATT&CK, STRIDE) et analyse de risques selon le modèle Purdue / ISA-95.
- Priorisation de 15+ vulnérabilités critiques (matrice DREAD) ; rapport d'audit et roadmap de conformité validés par la direction technique.

Stage d'Initiation — Administration Systèmes & Réseaux
Juillet 2024 · 1 mois

TRANSDEV — *Salé, Maroc*

- Durcissement d'une infrastructure IT de production (OWASP, CIS Benchmarks) ; supervision centralisée avec alertes automatisées.
- Disponibilité des services critiques portée de 95 % à 99,2 %.

Stage de Découverte — Développeur Back-End
Juillet 2023 · 1 mois

HIGHNESS — *Kénitra, Maroc*

- Modules back-end RESTful sécurisés (PHP / Laravel) : authentification JWT, validation stricte des entrées, protection CSRF / XSS / SQLi.

Projets Techniques

Secure File Transfer — *Chiffrement AES-256-GCM · Zero Trust*
Plateforme de transfert de fichiers sécurisée : chiffrement AES-256-GCM, authentification WebAuthn/FIDO2 + MFA, architecture Zero Trust et conformité RGPD (expiration automatique, RBAC, rate limiting).

PentestMaster CLI — *Framework Python · IA/ML*
Framework de tests d'intrusion automatisés : 80+ modules offensifs/défensifs, priorisation des cibles par ML, reporting professionnel multiformat.

AgentStrike — *CLI red-teaming agents IA · OWASP LLM/ASI · MITRE ATLAS*
CLI de red-teaming pour agents IA et applications LLM : 10 modules d'attaque (prompt injection, jailbreak, excessive agency) mappés simultanément OWASP LLM Top 10, OWASP ASI Top 10 et NIST AI RMF ; attaquant LLM adaptatif, audit MCP, export SARIF pour CI/CD. 187 tests, 97 % de couverture.

SENTINEL-OT — Crisis Room — *Simulateur de crise cyber OT/ICS · IEC 62443 / NIS2 / ATT&CK ICS*
Plateforme de simulation de crise pour infrastructures critiques : 9 scénarios sectoriels réels (ferroviaire, énergie, eau, santé...), décisions chronométrées mappées MITRE ATT&CK for ICS, scoring anti-triche recalculé côté serveur, mode équipe temps réel.

Formation

Diplôme d'Ingénieur d'État — Ingénierie Informatique — Majorant de promotion
2021 – 2026 · Diplômé

GROUPE ISGA — OPTION RÉSEAUX, SYSTÈMES & SÉCURITÉ (IRSS) — *Rabat, Maroc*

Baccalauréat — Sciences Mathématiques A (BIOF)
2020

LYCÉE AL MANSOUR EDDEHBI

Compétences Techniques

Audit & GRC : ISO 27001 • NIST CSF • IEC 62443 • MITRE ATT&CK / D3FEND • STRIDE / DREAD
Offensif / Red Team : Kali • Metasploit • Burp Suite • Nmap • exploitation
Détection & SIEM : Splunk • Zeek • Nozomi • Wireshark • threat hunting
Sécurité OT/ICS : Purdue / ISA-95 • Modbus / OPC-UA • SCADA • threat modeling
DevOps & Infrastructure : Docker • Git • CI/CD • pfSense • Linux • Windows Server
Développement : Python • JS/TS • C/C++ • SQL • React • FastAPI

Langues

Langues : Arabe — Maternelle • Français — Courant (C1) • Anglais — Professionnel (B2+)

Certifications & CTF

En préparation : CISSP, CompTIA Security+, CEH • **Techniques :** Fortinet NSE 1/2/3, LinkedIn Learning, Cisco, IBM, Google, Microsoft
CTF & veille : HackTheBox • TryHackMe • CVE / CERT / Threat Intelligence