Oussama ABDELFATTAH

Ingénieur en Cybersécurité — Spécialiste Sécurité OT/ICS

(+212) 696-280916 • abdelfattah.oussama.pro@gmail.com • Rabat, Maroc • Permis B • Mobilité Maroc / Europe • Disponible immédiatement

linkedin.com/in/OussamaAbdelfattah • github.com/OussamaABDELFATTAH • oussama-abdelfattah.vercel.app

PROFIL

Ingénieur en cybersécurité spécialisé dans la protection des systèmes industriels (OT/ICS) et des infrastructures critiques. Double expérience d'audit OT sur des systèmes ferroviaires réels — **DataProtect** (BU Critical Infrastructure Cybersecurity) et **Groupe ONCF** — et maîtrise des référentiels **IEC 62443**, **MITRE ATT&CK ICS** et NIST CSF. Je recherche un poste d'ingénieur sécurité OT/ICS (audit, pentest industriel, SOC OT) au Maroc ou en Europe.

COMPÉTENCES TECHNIQUES

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

EXPÉRIENCE PROFESSIONNELLE

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

DATAPROTECT — BU Critical Infrastructure Cybersecurity — *Casablanca / Rabat, Maroc*

- Conception de **CyberRail-OT**, cyber range ferroviaire ICS/OT : jumeau numérique d'un corridor ETCS, architecture Purdue à 4 zones, 22 conteneurs Docker.
- Campagne **Red Team** (17 scénarios) alignée MITRE ATT&CK ICS ; kill chain neutralisée en moins de 65 secondes après durcissement.
- Audit **IEC 62443** portant le niveau de sécurité de **62 à 88/100 (SL-2)** ; référentiel de 46 contrôles réutilisable.
- Développement d'un **proxy Modbus applicatif (L7)** bloquant les commandes dangereuses ; supervision Splunk / Zeek / Nozomi.

Stage de Perfectionnement — Cybersécurité des Systèmes Industriels (OT)
Juin – Juillet 2025 · 2 mois

Groupe ONCF — Office National des Chemins de Fer — *Rabat, Maroc*

- Audit de sécurité complet d'un système SCADA ferroviaire critique (plus de 20 équipements OT).
- Évaluation multicritère (ISO 27001, IEC 62443-3-3, NIST CSF, MITRE ATT&CK ICS, STRIDE) et analyse des risques cyber-physiques via le modèle Purdue / ISA-95.
- Priorisation de 15+ vulnérabilités critiques (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. — potential-pilot-suite.lovable.app

FORMATION

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

Groupe ISGA — option Réseaux, Systèmes & Sécurité (IRSS) — *Rabat, Maroc*

Baccalauréat — Sciences Mathématiques A (BIOF)
2020

Lycée Al Mansour Eddehbi

LANGUES

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

CERTIFICATIONS & CTF

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