Oussama **ABDELFATTAH**

CYBERSECURITY ENGINEER · OT/ICS SECURITY SPECIALIST

Rabat, Morocco · Driving license · Open to relocation (Morocco / Europe) · Available immediately

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

Profile

Cybersecurity engineer specialized in the audit and protection of industrial control systems (OT/ICS) and critical infrastructure. Dual OT audit experience on real railway systems — **DataProtect** (Critical Infrastructure Cybersecurity BU) and the **ONCF Group** — with a strong command of **IEC 62443**, **MITRE ATT&CK ICS**, ISO 27001 and NIST CSF. For my final-year project, I designed **CyberRail-OT**, an end-to-end railway cyber range. I am seeking an OT/ICS security engineer role (audit, industrial pentest, OT SOC) in Morocco or Europe.

Professional Experience

Final-Year Project — Cybersecurity Engineer OT/ICS
February – June 2026 · 4 months

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

- Designed **CyberRail-OT**, a railway ICS/OT cyber range: digital twin of an ETCS corridor, 4-zone Purdue architecture, 22 Docker containers.
- **Red Team** campaign (17 scenarios) mapped to MITRE ATT&CK ICS; kill chain neutralized in under 65 seconds after hardening.
- **IEC 62443** audit raising the security level from **62 to 88/100 (SL-2)**; reusable 46-control audit framework.
- Developed an **application-layer (L7) Modbus proxy** blocking dangerous commands; monitoring with Splunk / Zeek / Nozomi.

Advanced Internship — Industrial Control Systems (OT) Security
June – July 2025 · 2 months

ONCF GROUP — NATIONAL RAILWAYS OFFICE — *Rabat, Morocco*

- Full security audit of a critical railway SCADA system (20+ OT devices).
- Multi-criteria assessment (ISO 27001, IEC 62443-3-3, NIST CSF, MITRE ATT&CK ICS, STRIDE) and cyber-physical risk analysis using the Purdue / ISA-95 model.
- Prioritized 15+ critical vulnerabilities (DREAD); audit report and compliance roadmap validated by technical management.

Introductory Internship — Systems & Network Administration
July 2024 · 1 month

TRANSDEV — *Salé, Morocco*

- Hardened a production IT infrastructure (OWASP, CIS Benchmarks); centralized monitoring with automated alerting.
- Raised critical-service availability from 95% to 99.2%.

Discovery Internship — Back-End Developer
July 2023 · 1 month

HIGHNESS — *Kénitra, Morocco*

- Secure RESTful back-end modules (PHP / Laravel): JWT authentication, strict input validation, CSRF / XSS / SQLi protection.

Technical Projects

Secure File Transfer — *AES-256-GCM encryption · Zero Trust*
Secure file-transfer platform: AES-256-GCM encryption, WebAuthn/FIDO2 + MFA authentication, Zero Trust architecture and GDPR compliance (auto-expiry, RBAC, rate limiting). — secure-transfer.vercel.app

PentestMaster CLI — *Python framework · AI/ML*
Automated penetration-testing framework: 80+ offensive/defensive modules, ML-based target prioritization, professional multi-format reporting.

AgentStrike — *AI-agent red-teaming CLI · OWASP LLM/ASI · MITRE ATLAS*
Red-teaming CLI for AI agents and LLM applications: 10 attack modules (prompt injection, jailbreak, excessive agency) mapped simultaneously to OWASP Top 10 for LLM, OWASP Top 10 for Agentic Applications and NIST AI RMF; adaptive LLM attacker, MCP audit, SARIF export for CI/CD. 187 tests, 97% coverage.

SENTINEL-OT — Crisis Room — *OT/ICS cyber crisis simulator · IEC 62443 / NIS2 / ATT&CK ICS*
Crisis-simulation platform for critical infrastructure: 9 real sector scenarios (rail, energy, water, healthcare...), timed decisions mapped to MITRE ATT&CK for ICS, server-side anti-cheat score replay, real-time team mode. — potential-pilot-suite.lovable.app

Education

State Engineering Degree — Computer Engineering
2021 – 2026 · Graduated

GROUPE ISGA — NETWORKS, SYSTEMS & SECURITY TRACK (IRSS) — *Rabat, Morocco*

Baccalaureate — Mathematical Sciences A
2020

LYCÉE AL MANSOUR EDDEHBI

Technical Skills

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

Languages

Languages: Arabic — Native • French — Bilingual (C1) • English — Professional (B2+)

Certifications & CTF

In progress: CISSP, CompTIA Security+, CEH • **Technical:** LinkedIn Learning, Cisco, IBM, Google, Microsoft
CTF & threat watch: HackTheBox • TryHackMe • CVE / CERT / Threat Intelligence