Sofiene Hamzaoui

SYSTEMS ARCHITECT · SECURITY LEADER · TELECOM SECURITY · FULL-STACK ENGINEER

admin@vaultguard.eu.org | +216 22 090 800 | Tunisia · Remote-First | spaypeur.github.io | github.com/spaypeur

EXECUTIVE SUMMARY

Multidisciplinary Systems Architect and Senior Security Engineer with **20+ years of hands-on expertise** spanning offensive security, telecom protocol defense (SS7/GTP/Diameter), C2 framework development, backend and full-stack engineering, systems architecture, infrastructure automation, cryptography, and operational consulting. Independent consultant since 2017 with a **100% engagement success rate on Upwork (Top Rated Plus)**. Founder of **VaultGuard** — an institutional crypto security and P2P OTC platform live on Cloudflare's global edge. Proven across international environments with multilingual operations (Arabic, French, English, Russian, German). Available for senior architect, security leadership, telecom security, CTO-level, and high-value consulting roles.

PROFESSIONAL EXPERIENCE

Cybersecurity Architect / Threat Detection Consultant

Oct 2024 — May 2025

Adarma (Remote) — Banking & Enterprise Security

- Designed and deployed **Threat Intelligence solutions** for global Tier-1 banks and enterprises, covering SIEM integration, threat feeds, and behavioral analytics
- Built event correlation and behavioral analysis modules in **Python/Go** integrated with SIEM/SOC platforms, reducing false positives by **40%**
- Conducted penetration tests and resilience assessments across cloud (AWS/GCP) and on-premise infrastructures with zero client-side incidents post-engagement
- Architected Zero-Trust network segmentation and access control frameworks for regulated financial environments

Cybersecurity Architect / Network Security Consultant

Dec 2020 — Sep 2024

IronNet (Remote) — Network Architecture & Threat Detection

- Architected secure network infrastructures for Cybera, NetFortis, and ShieldWave — **30–35% reduction in active security incidents**
- Secured multi-tenant cloud environments with advanced encryption (AES-256), MFA, and automated incident response pipelines
- Built real-time Prometheus/Grafana monitoring dashboards with automated alerting for SOC teams
- Led secure data migration during enterprise restructuring with zero data-loss and zero downtime

Cybersecurity Architect / Security Consultant

Feb 2018 — Dec 2020

Rubica — SMB & Enterprise Security

- Deployed network segmentation, endpoint protection, and AWS/GCP cloud hardening for 20+ SMB and enterprise clients
- Built custom IDS using **Python, ELK Stack, and Suricata** — reduced mean-time-to-detect (MTTD) by 60%
- Secured REST APIs with AES-256, JWT, MFA, and Zero-Trust policies — eliminated API-layer breaches across all managed clients
- Implemented **Prometheus/Grafana monitoring** — achieved 40% incident reduction across managed portfolio

CORE COMPETENCIES

- Offensive Security / Red Team — 97%
- Penetration Testing — 96%
- C2 Framework Development — 95%
- Python / FastAPI / Node.js — 95%
- Network Architecture — 92%
- OSINT & Intelligence — 93%
- Telecom Security (SS7/GTP) — 90%
- Cloud Security (AWS/GCP) — 85%
- Blockchain / ZKP / Crypto — 82%

TELECOM SECURITY

SS7 Exploitation · GTP Attacks · Diameter · SIM Hijacking · GSM Interception · IMSI Catchers · VoIP Security · 5G/LTE Hardening

TECH STACK

Python · FastAPI · Node.js · TypeScript · React · Go · Bash · C/C# · Docker · PostgreSQL · Redis · WebSocket · AES-256 · ZKP · JWT · ELK Stack

SECURITY TOOLS

Metasploit · Burp Suite · Nmap · Wireshark · Nessus · SQLmap · Ghidra · Frida · Volatility · mimikatz · Shodan · Maltego

CERTIFICATIONS

- IBM — Incident Response & Systems Forensics (SkillsBuild)
- IBM — Security Operations & Management
- IBM — System & Network Security
- IBM — Cloud Security
- IBM — Vulnerability Management
- IBM — GRC & Data Privacy
- IBM — Cybersecurity Fluency (6 Microcredentials)
- HuggingFace — AI Agents Course
- Fundamentals of LLMs — DeepLearning.AI

Independent Cybersecurity & Full-Stack Consultant

Apr 2017 — Present

Upwork — Top Rated Plus ⭐ | Global Clients

- Delivered **100% mission success rate** across security audits, penetration tests, and backend engineering engagements
- Built production security tools, hardened API backends, and internal dashboards for clients in banking, fintech, healthcare, and e-commerce
- Clients span North America, Europe, and Middle East — all engagements remote

Hotel Animator / Entertainment Coordinator

Summers 2008 — 2011

International Hotels — Tunisia & Turkey

- Caribbean World Monastir, Thalasso Monastir, Ksar Kervansaray (Tunisia) + 5-star hotel in Bodrum, Turkey
- ~3 years seasonal work: event coordination, guest relations, entertainment programming, multilingual daily operations
- Languages used daily: Arabic, French, English, Russian, German — strengthened cross-cultural communication and adaptability

Professional Heavy Vehicle Operator (Category C+E)

2005 — 2010

Commercial Transport — Tunisia

- 5 years operating heavy commercial vehicles with trailers (Cat. C+E license)
- Developed discipline, logistics awareness, and operational resilience under pressure
- Valid Class C+E heavy vehicle driving license — Vocational Training Diploma (2010)

Independent Archaeological Field Practitioner

Ongoing

Historical Sites — Tunisia & Mediterranean

- Independent field exploration of archaeological sites across Tunisia and North Africa
- Hands-on cultural heritage engagement, historical analysis, site documentation, and systematic field research
- Focus areas: Roman, Punic, and Islamic-era archaeological landscapes

KEY PROJECTS & FLAGSHIP INITIATIVES

🔐 VaultGuard — Institutional Crypto Security Platform

`Founder & Lead Architect · Live: vaultguard.eu.org · React + Cloudflare Workers + Supabase · 2025–Present`

Production-deployed institutional crypto security and P2P OTC trading platform. Addresses $14B/year in crypto crime losses. Five integrated defense layers: Threat Intelligence (8+ OSINT feeds), Zero-Trust Identity (AES-256-GCM, WebAuthn/FIDO2), P2P OTC Desk with progressive identity disclosure, Forensic Recovery, and Compliance Engine. **137 API endpoints, 14+ DB tables, 95% backend complete, deployed on Cloudflare's 300+ city edge network with sub-450ms global latency.** Seed round Q2 2026. TAM: $50B.

⚔ C2 Server — Advanced Command & Control Framework

`Lead Developer · Python / FastAPI / WebSocket / Redis / PostgreSQL / Docker`

Custom C2 server with **SS7/GSM real-world exploitation modules**, WebSocket real-time sessions, CVE exploit database (2,847 entries), OSINT services, satellite comms simulation, and full JWT/RBAC web dashboard. Purpose-built for red team operations and security research.

📊 UK Insolvency Monitor — Enterprise Risk Platform

`Full-Stack Developer · Python / FastAPI / React / Celery / PostgreSQL / Redis`

Tracks **1,000+ UK companies** for insolvency events, credit score drops (≥5%), and director changes. Automated daily/weekly/monthly Excel reports with configurable thresholds. Deployed with Docker Compose.

- ✦ Foundational C# — Microsoft / freeCodeCamp
- ✦ Scientific Computing with Python — freeCodeCamp
- ✦ Frontend Dev Libraries V8 — freeCodeCamp
- ✦ IELTS General Training — B2 (British Council)
- ✦ CMFC Flight Dispatcher Diploma (Civil Aviation)
- ✦ Upwork Top Rated Plus — 100% Job Success

LANGUAGES

Arabic	**NATIVE**
English	**FLUENT (IELTS B2)**
French	**FLUENT**
Russian	**GOOD**
German	**GOOD**

ATS KEYWORDS

Cybersecurity Architect · Systems Architect · Penetration Testing · Red Team · SS7 · GTP · Diameter · Telecom Security · C2 Framework · OSINT · Threat Intelligence · Zero Trust · SIEM · SOC · Malware Analysis · CVE Research · IDS/IPS · Cloud Security · AWS · GCP · Docker · Kubernetes · FastAPI · React · Node.js · Full-Stack Engineer · Backend Engineer · Infrastructure Automation · DevOps · Security Auditing · ZKP · Blockchain Security · Cryptography · AI/LLM Security · Consulting · Terraform · Ansible · Suricata · ELK Stack · PostgreSQL · Redis · WebSocket

GITHUB PRESENCE

⬡ github.com/spaypeur — 16 repos

⬡ github.com/sniper4u2 — 131 repos

147+ total repositories · 50+ security tools

🤖 Phalanx X — Local LLM API Server

`Developer · Python / llama.cpp / GGUF / CUDA`

Full OpenAI-compatible REST API server running any GGUF model locally with GPU acceleration, MoE architecture support, 1K–128K context window. Enables private, cost-free AI inference for security operations.

🍎 iOS Activation Bypass Toolkit

`Security Researcher · Bash / Python / libimobiledevice / Objective-C`

Complete iCloud activation lock bypass toolkit supporting checkra1n, SSH ramdisk injection, and patched mobileactivationd binary deployment. Supports **iPhone 6s → X, iOS 12–16**. Used in authorized device recovery engagements.

🌐 Cloudflare Real-IP Discovery Tool

`Developer · Python / asyncio / DNS / Scrapling`

Async subdomain enumeration tool scanning 40+ subdomains against all Cloudflare CIDR ranges to identify unprotected origin servers. StealthyFetcher bypass engine built-in.