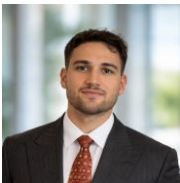


omar.altawil@hotmail.com
+962 776 671 283
Amman, Jordan
GitHub: omar7altawil
LinkedIn: oy-tawil
Website: omartawil.me

OMAR TAWIL

AI Agent Engineer



PROFILE

AI agent engineer and founder specializing in agentic systems, multi-agent orchestration, tool-using workflows, sandboxed execution, and LLM safety evaluation. Built and shipped an AI security-agent platform to 10+ paying customers, an open-source AI pentest CLI, and agent-safety research software. Ten years of end-to-end software delivery across product architecture, implementation, deployment, and customer delivery, with additional experience across security, industrial operations, and management.

EDUCATION

MSc, Cybersecurity	Princess Sumaya University	2024 - 2026
Thesis Configuration-Level Semantic Brittleness in Tool-Using LLM Agents.		
MSc, Computer Science	Technical University of Munich	2019 - 2020
Status Not completed.		
BSc, Computer Engineering	Abu Dhabi University	2014 - 2018

EMPLOYMENT

Founder	NullSquare	2026 - Present
Built AI-native security platform for autonomous penetration testing, vulnerability discovery, evidence-backed findings, reports, and compliance-readiness mapping.		
Shipped Null AI CLI, an open-source scoped pentest agent for safe reconnaissance, scanner orchestration, reproducible assessments, and evidence-backed reporting.		
Owns Full engineering lifecycle from architecture and implementation through deployment and production customer delivery.		
Lead Engineer	Orchestrator	2025 - 2026
Built Agent-native products and applied agent research across managed runtimes, automation flows, observability, policy controls, and sandboxed execution.		
Operations Lead	Advance Fertilizer	2023 - 2025
Led ERP implementation, corporate website, internal tooling, IT and security operations, access policies, and automated operational reporting.		
Managed A 40-person cross-functional operation while retaining ownership of technology systems and process improvements.		
Technology & Systems Manager	INFERT	2020 - 2023
Designed Production and process-control systems, plant workflows, internal tools, and reporting automation for industrial operations.		
Technical Specialist	Huawei	2019 - 2020
Supported 5G network switch deployment for a government infrastructure rollout, focusing mainly on device configuration and setup.		
Software Developer	Saal.ai	2018 - 2019
Delivered Early product-development work focused on hands-on software implementation after graduation.		

SELECTED PROJECTS

Null AI CLI

github.com/Null-Square/Null-CLI

Purpose Open-source scoped pentest agent with safe reconnaissance, scanner orchestration, reproducible assessments, and evidence-backed reporting.

License Apache-2.0.

Agent Behavior Lab

github.com/Null-Square/Agent-Behavior-Lab

Purpose Full-stack platform for agent-safety evaluation with semantic tool variants, personas, histories, deterministic judges, LLM-backed judges, and reproducible seeded experiments.

Tawil Studio

github.com/Tawil-Studio

Games Speed of Light (1M+ downloads), Retro Heist, SWAT, Attack on Zombies, Sinx, Oo, Nuke It, and Bong.

Apps Cardify (digital business card), Kittaby (ebook reading and publishing platform), and Zeus (social fitness app).

RESEARCH & PUBLICATIONS

Publications	Journal of Cybersecurity	2026
Title Configuration-Level Semantic Brittleness in Tool-Using LLM Agents: A Factor-Ranking Study of Persona, History, and Tool Definition.		
MSc thesis	Princess Sumaya University	2026
Topic Safety behavior of tool-using LLM agents across deployer-controlled configuration factors: system persona, conversation history, and tool definitions.		
Graduate research outputs	Princess Sumaya University	2024 - 2025
Selected Agentic Architecture for Post-Acquisition Digital-Forensic Triage; Runtime Enforcement Architecture for Secure and Compliant Agentic SecOps; LLM-Agent Framework for Malware Analysis.		

TECHNICAL SKILLS

Agentic AI	LLM agents; multi-agent orchestration; tool use / function calling; prompt and system design; agent evals and safety testing; LLM-as-judge and deterministic-judge pipelines.
Security Automation	Offensive-security automation; scanner orchestration; evidence validation; SARIF reporting; vulnerability management; OWASP Top 10, PCI DSS, ISO 27001, NIST CSF mapping.
Programming	TypeScript; JavaScript; Python; C#; SQL; C; Java.
Full Stack	Node.js; React; React Native; Next.js; Prisma; Drizzle; PostgreSQL; MongoDB; Supabase; Firebase; Unity.
Infrastructure	Linux; Docker; AWS EC2, S3, RDS, Amplify; GitHub Actions; Turborepo; n8n; deployment and DevOps.
Architecture	Monorepos; DDD / hexagonal architecture; Docker-sandboxed runtimes; multi-provider LLM integration.
Spoken Languages	Arabic (native); English (professional).