Arturo Aguilera González

https://arturoaguilera.dev/en | Málaga, Spain

Personal Data

Email: arturoaguileraglez@gmail.com Github: https://github.com/arturoaguileraa
LinkedIn: https://linkedin.com/in/arturoaguileraglez

Work Experience

09/2026 - Present **Mid SWE (Backend & AI), FMIT Technologies S.L., Spain**
Designing an AI agent for Mercedes-Benz's internal Global Search platform, used to filter and search vehicle shipping and logistics processes. Uses Mastra and AG-UI.

05/2025 - 05/2026 **Founder Engineer at VirusTotal, GSEC Málaga (xWF)**
Developing 'Omnia', an AI-powered cybersecurity platform using Vite, FastAPI, and Pydantic. Built an ecosystem for security agents, RAG systems and MCP integrations.
https://omniasec.ai & https://app.omniasec.ai

01/2025 - 05/2025 **Fullstack SWE at San Juan De Dios, Málaga**
Developed Fullstack projects with a Next.js (React) frontend and a Django (Python) backend, using Whisper and Ollama to transcribe patient consultations and structure them into tables.

Education

11/2024 - 09/2025 **Master's Degree in Artificial Intelligence, International University of La Rioja (UNIR)**
Average grade: 8.65/10

10/2024 - 12/2024 **University Expert Diploma in Reverse Engineering and Malware Intelligence, GSEC Málaga**
Diploma developed by NICS Lab (UMA) and VirusTotal, in collaboration with Google, to train experts in a highly specialized cybersecurity field.

09/2019 - 09/2024 **Double Degree in Computer Science and Mathematics, University of Malaga (UMA)**
Double degree. Average grade: 7.02/10

Projects

Master thesis **Explainable AI (XAI) for Malware Detection in PE Files:** Comparative study of ML and Deep Learning models (CNN, MLP) using the EMBER dataset. Applied SHAP and LIME to interpret decision-making. Graded: 8.7/10. *[View Paper]*

Sift **Local PII Privacy Gateway for AI Coding Agents (Rust):** A reverse proxy between the agent and any OpenAI-compatible LLM API that reversibly pseudonymizes sensitive data (API keys, emails, names) before it leaves the machine and rehydrates the streamed response, so the model never sees real values. Hybrid regex + local GLiNER NER detection, shipped as a single binary. *[View Repository]*

skill-guard **Malware-Risk Triage for Agent Skills and MCP Servers:** Instead of asking an LLM for an opinion, scores each artifact with a "System One" model (TypeSafe Jev) that returns typed, calibrated probabilities, then classifies it as malicious, suspicious or benign. Includes a live playground where the risk dial updates as you edit the text, and a hub of real skills analyzed at scale by a mass-analysis worker. React 19, Vite, TanStack Router, Hono, oRPC, FastAPI, Neon Postgres, Vercel. *[Live App]* *[View Repository]*

See all my projects at **arturoaguilera.dev**

Skills

- **Programming:** TypeScript, Python, C++, Java.
- **Artificial Intelligence:** Mastra, AG-UI, MCP, RAG, AI agents, LangChain, Whisper, Ollama, Pydantic, AI Studio.
- **Web Development:** Next.js, React, Vite, TanStack Router, Astro, Angular, Node.js, Bun, Hono, oRPC, NestJS, Express, FastAPI, Django, Zod, Drizzle, Tailwind, PostgreSQL, MongoDB.
- **Networking & OS:** TCP/IP, Firewalls, VLANs, Linux & Windows administration.
- **Infrastructure & DevOps:** GCP (Compute Engine, Cloud Run), Terraform, Docker, CI/CD (GitHub Actions), Networking (VPC, DNS).
- **Languages:** Native Spanish, fluent English.