

Mario Balbi

Secure AI & Backend Engineer | Data-Driven Ecosystems & Privacy-by-design

Italy (Open to Global Remote / Contractor / Task-Based Freelancing) | (+39) 346 343 6949 | mariobalbi95@gmail.com
linkedin.com/in/mariobalbi95 | github.com/Balbus95 | mariobalbi.is-a.dev

PROFESSIONAL SUMMARY

Secure AI & Backend Engineer specializing in scalable infrastructure design. Integrates modern AI models (Agentic Systems, XAI) with native security and compliance (Privacy-by-design), leveraging Python and Node.js. Drives automation (Docker, CI/CD) for rapid, resilient releases in distributed environments.

WORK EXPERIENCE

AI & NLP Consultant

BiX Incubator SpA

Sep. 2025 – present

Remote/Italy

- Designed an LLM-based pipeline to extract structured data from unstructured Italian cadastral documents, applying Generative AI and NLP techniques via openapi.it external APIs.

Backend Software Engineer

TechEalthVolution SRL

Jan. 2025 – June 2025

Remote/Italy

- **Backend Architecture & Security:** Engineered and secured 50+ RESTful endpoints across 5 clinical modules (Appointments, Patients, Devices, Requests, Auth), implementing JWT/Spring Security standards.
- **Complex Data Modeling:** Architected a 50+ table relational schema (PostgreSQL) and NoSQL (MongoDB) data models for healthcare workflows, enforcing referential integrity and optimizing JPA queries for high-concurrency data access.
- **Automation & DevOps:** Automated deployment to a single-command operation via a custom script handling Docker permissions and container startup; deployed containerized services to AWS EC2 with Traefik reverse proxy and Let's Encrypt SSL, ensuring consistent dev and pre-production environments.

PROJECTS

ZeekXAI | Critical Infrastructure Attack Analysis System (github.com/Balbus95/ZeekXAI)

Machine Learning & Security

- **ML Detection & XAI:** Developed a detection system classifying attacks on large-scale Zeek logs (Parquet/PySpark), achieving Precision/Recall above 95% across MITRE ATT&CK tactics; integrated SHAP and PDP for auditable, corporate-ready explainability.

EvoFolio | Portfolio Optimization with NSGA-II (github.com/Balbus95/EvoFolio)

Algorithm & FinTech

- **Algorithmic Engineering:** Custom NSGA-II implementation in Python to balance risk and return; published in *Neural Computing and Applications* (Springer Nature, 2024) — Sharpe Ratio 1.64 vs. 0.20 benchmark in quarterly optimization — rdcu.be/dl8ZF.

NLP Filter Code | Autonomous AI Agent Automation

GenAI Engineering

- **Agentic Pipeline:** Designed a system that translates natural language intent into executable JS code with 90% accuracy, automating boilerplate logic generation using Llama 3 and Qwen; dataset built via Selenium web crawling across ~1,750 records.

SKILLS

Core Languages & Paradigms: Python, Java, JavaScript (Node.js), SQL, Bash.

GenAI & Agentic Systems: LLM Integration (Llama 3, Qwen), Prompt Engineering, AI Agents, Model Context Protocol (MCP).

Data Engineering & ML: PySpark, Pandas, scikit-learn, TensorFlow. Explainable AI (SHAP, PDP), Deep Learning (CNN).

Backend & APIs: Spring Boot, Node.js, REST API Design, Microservices Architecture, Postman, Swagger.

Infrastructure & Remote Ops: Docker, AWS EC2, GCP Compute Engine, Proxmox VE, NAS configuration, Self-Hosted Homelab, Linux Hardening.

Cybersecurity: Network Traffic Analysis (Zeek), Intrusion Detection, Vulnerability Assessment, OWASP ZAP, Privacy-by-design.

Async & Workflow Tools: Git, GitHub, CI/CD basics, Selenium, Markdown, LaTeX.

Languages: Italian (Native), English (B2/Professional Working Proficiency).

EDUCATION

University of Salerno

Master Degree in Computer Science (Cybersecurity)

Fisciano, Italy

Feb. 2023 – Dec. 2025

- Final grade: 104/110

University of Salerno

Bachelor Degree in Computer Science

Fisciano, Italy

Sep. 2014 – Feb. 2023

I authorize the processing of my personal data present in my CV pursuant to art. 13 d. lgs. 30 June 2003 n. 196 and art. 13 GDPR 679/16.