

MARCO BELLINGERI

CLOUD PLATFORM & AI SECURITY ENGINEER

mkdevpy@proton.me · github.com/MK023 · linkedin.com/in/marco-bellingeri · credly.com/users/marco-bellingeri

PROFESSIONAL SUMMARY

Cloud Platform & AI Security Engineer with experience designing and delivering cloud systems, secure backend applications, and AI-native solutions. I build RAG and agentic AI systems with a security-by-design approach, integrating AI Security, OWASP LLM Top 10 practices, DevSecOps, software supply chain security, and AI governance. Hands-on experience with enterprise production platforms, Python backend engineering, and CI/CD automation with integrated security gates.

TECHNICAL SKILLS

Backend & API: Python, FastAPI, Flask, Falcon, REST API Design, Clean Architecture, DDD.

Cloud & Platform: AWS (Lambda, SQS, SNS, SES, S3, EC2, IAM, VPC, CloudWatch), OCI, Cloudflare, Railway, Docker, Kubernetes, Terraform, Linux.

Data: PostgreSQL/PostGIS, MySQL, Redis, MongoDB, SQLite FTS5, Alembic.

AI Engineering & Security: RAG, AI Agents, MCP, pgvector, Voyage AI, Claude API, OpenRouter, Langfuse, Groq LLaMA, HuggingFace, LLM evaluation, prompt injection defense, OWASP LLM Top 10, MITRE ATLAS, human-in-the-loop workflows.

DevSecOps & Supply Chain: GitHub Actions, CodeQL, Bandit, pip-audit, Gitleaks, Dependabot, CycloneDX SBOM, Sigstore keyless/OIDC, zizmor, SonarCloud, OpenTelemetry, Prometheus, Grafana, Sentry.

PROFESSIONAL EXPERIENCE

VETRERIA MONFERRINA | AI Engineer | Cloud Platform & Security

03/2026 - Present | Casale Monferrato (AL), Remote

- Independently develop production web and AI solutions for a real business environment, focusing on application security, software quality, automation, and AI governance.
- Built a production website with Astro 6 SSG/SSR and Sanity CMS: 31 pages, Lighthouse 100/100/100, WCAG 2.1 AA, 138 Vitest tests, Playwright E2E, and a SonarCloud Quality Gate.
- Implemented security hardening with hash-based CSP without unsafe-inline, HSTS, X-Frame-Options, rate limiting, honeypot protection, CSRF controls, Cloudflare WAF, CodeQL, and Dependabot.
- Built MonferrinoAI, a GitHub Actions-scheduled agent for SEO/AEO and competitor monitoring, using RAG with Supabase pgvector, Voyage AI embeddings, Firecrawl ingestion, and reviewable micro-PRs.
- Implemented AI governance with human-oversight logging and ongoing DPIA/FRIA documentation; end-to-end monitoring with Checkly.

FAIRFIELD S.p.A. | Backend Engineer | Cloud Platform

12/2025 - 02/2026 | Figline e Incisa Valdarno (FI), Remote

- Developed an enterprise debt-recovery platform comprising backend APIs, a commission-processing system, and a multi-role SPA.
- Built a Python 3.10/Falcon backend using Clean Architecture and DDD: 100+ RESTful endpoints, 50+ MySQL tables, AWS Lambda, SQS, SNS, SES, S3 and Pinpoint integrations, 35+ background processors, and 23+ Lambda functions.
- Developed a Python commission-processing system with Pandas/NumPy and Excel, PDF, CSV, and HTML reporting; contributed to a React/TypeScript SPA using Redux/Redux-Saga, Google Maps, push notifications, i18n, and PWA capabilities.

GECO S.r.l. | Cloud Platform & Security Engineer

04/2025 - 12/2025 | Galliate (NO), Italy

- RTSP Streaming Supervisor, Rome Metro Line C: developed a 24/7 supervision system for 400+ displays using MediaMTX, ffmpeg, and ConVis, with automated restart/backoff, graceful shutdown, credential masking, and protected distribution via Nuitka.
- SmartAirway Diagnostics, Etihad Airways: developed an enterprise network diagnostics tool using Scapy, ICMP/traceroute deep-path analysis, DNS/speed tests, psutil, and CSV logging for post-mortem analysis.
- Implemented CI/CD checks with pre-commit, Bandit, and pip-audit; worked with OCI, Prometheus/Grafana, Docker, and Linux for infrastructure and monitoring.

EARLIER EXPERIENCE

PEROPTYX | Data Engineer | Geospatial Data

09/2024 - 03/2025 | Italy, Remote

- Analyzed, evaluated, and optimized geospatial data and digital maps for navigation services using Python, Google Maps, and data-quality workflows.

FONDAZIONE LUIGI CLERICI | Computer Science, Mathematics & Cybersecurity Teacher

09/2021 - 09/2024 | Mortara (PV), Italy

- Taught programming, networking, operating systems, cryptography, data security, and Linux in a vocational education environment.

FIWAY S.r.l. | IT Engineering Intern | Cloud Monitoring & IoT Platform

06/2021 - 09/2021 | Alessandria, Italy

- Developed and managed a cloud-monitoring platform for IoT and Industry 4.0, working with SQL, Linux, virtual machines, Prometheus/Grafana, VPNs, and network security.

TECHNICAL PROJECTS

MonferrinoAI | Production AI Agent Platform

- Production-oriented AI agent using RAG with PostgreSQL/pgvector, Voyage AI, and Firecrawl; scheduled through GitHub Actions with human-in-the-loop review and governance logging.
- AI & Software Supply Chain Security: CodeQL, Dependabot, secret scanning, CycloneDX SBOM, Sigstore keyless signing, and protected branches, making agent-generated changes reviewable and verifiable.

marcobellingeri.dev | Security-first Cloud Platform | 07/2026

- Self-auditing platform with runtime verification of HTTP security headers and a CSP without unsafe-inline, using hashes calculated at build time and verified in CI.
- Deployment gate with CycloneDX SBOM, keyless OIDC provenance, zizmor, Gitleaks, and SonarCloud; Supabase RLS rebuilt from scratch and verified in CI.
- AI-assisted monthly publication using a RAG pipeline for sourcing, verification, generation, LLM-as-judge evaluation, and human-in-the-loop publishing.

Agentic OS | Personal AI Ops Platform | 07/2026

- Claude Code observability using OpenTelemetry Collector, Prometheus, and Grafana; five Railway services protected through Cloudflare Tunnel.
- OTLP bearer authentication, metric-label allow-list to prevent identity leakage, single-email Grafana access, protected status API, SonarCloud Quality Gate, and post-deployment smoke tests.

LLM Council | Multi-model LLM Evaluation System | Claude Code Hackathon | 07/2026

- Anti-sycophancy architecture with three independent voters through OpenRouter, anonymous peer ranking, and an external chairman to reduce self-favor bias.
- Python standard-library-only runtime, API key with spending cap and expiry, Langfuse observability, and 122 tests with no network calls; evaluation thresholds defined before measurement.

TorinoParking | Real-time Parking API Platform | 02/2026 - 07/2026

- Async FastAPI on Python 3.12 with PostgreSQL/PostGIS, Redis, real-time ingestion, compressed caching, and ETag support.
- HMAC-SHA256 API-key hashing, multi-tier rate limiting, security headers, Pydantic validation, documented threat model in SECURITY.md, 51 tests, and CI/CD.

HappyKube | AI-powered Emotion Analysis Platform | 12/2025 - 05/2026

- Groq LLaMA 3.3 70B, Flask, PostgreSQL, and Redis; Fernet encryption for PII at rest, prompt-injection and cache-poisoning prevention, hashed API authentication, and webhook validation.

SELECTED CERTIFICATIONS

AI Security & Governance: AttackIQ, Foundations of AI Security (2026); Securiti Education, AI Security & Governance (2026).

OpenSSF / Linux Foundation: Secure AI/ML-Driven Software Development; Automating Supply Chain Security: SBOMs & Signatures; Securing Your Software Supply Chain with Sigstore; Understanding the EU Cyber Resilience Act (2026).

Anthropic Academy: Claude Code in Action; Building with the Claude API; Introduction to Model Context Protocol; Introduction to Agent Skills; Introduction to Subagents (2026).

Cloud & Development: GitHub Foundations (2025); IBM Docker Essentials (2024).

EDUCATION

University of Eastern Piedmont (Università degli Studi del Piemonte Orientale) | Degree Program in Computer Science | 09/2016 - Present | Vercelli, Italy

Polish-Japanese Academy of Information Technology (PJAiT) | Computer Science, Erasmus Program | 07/2018 - 03/2019 | Warsaw, Poland

Istituto Tecnico Commerciale Leardi | Diploma in Business Administration (I.G.E.A.) | 08/2005 - 07/2010 | Casale Monferrato, Italy

LANGUAGES

Italian: Native | English: B2 (Professional working proficiency)