
Antonio Ruocco

Cybersecurity Analyst · Detection Engineering · Security Automation · AI-Powered Tooling

Naples, Italy · Open to international roles · antonioruocco.com · github.com/isilderr1 · linkedin.com/in/antonio-ruocco · antonio.ruocco2k@hotmail.com · +39 3349754922

PROFESSIONAL PROFILE

Cybersecurity enthusiast since 2010, with over 15 years of independent exploration of systems, networks, and vulnerabilities, complemented by a recent path of structured and intensive technical training. I am specializing in security automation, detection engineering, SOC operations, AI security, and LLM-assisted tooling, with a practical approach focused on building real-world tools.

I have developed an open-source portfolio that includes custom HIDS projects, hybrid SOC labs, adversary simulation tools for controlled environments, advanced cryptography projects, privacy-first log analysis pipelines, and NeuralForge, a full-stack platform for local LLM fine-tuning.

My goal is to bring intelligent automation, attacker-minded thinking, and defensive rigor into SOC, Detection Engineering, Threat Detection, and AI Security contexts.

CORE SKILLS

Offensive / Red Team

- Network Recon · Nmap/CVE
- LLM-driven Attack Planning
- CTF Design & Rev. Eng.
- Protocol Analysis

Defensive / Blue Team

- SIEM / Wazuh
- Detection Engineering
- HIDS / Endpoint Visibility
- Incident Response

Security Engineering

- Python Tooling
- Log Analysis (Regex+LLM)
- AES-256 / Shamir SSS
- API Security / OWASP

Infrastructure & AI

- Docker / VMware
- Linux Hardening
- Local LLM fine-tuning
- AI Workflow Automation

SELECTED OPEN-SOURCE PROJECTS

RedTeam-GPT — Autonomous Offensive Security Agent [AI × OFFENSIVE]

Autonomous AI offensive agent with ReAct framework · github.com/isilderr1/redteam-gpt

- Autonomous agent on Qwen2.5-14B-Instruct (native tool calling, GPU offload, Flash Attention): runs Nmap recon, CVE lookup with CVSS filtering, Nuclei on web endpoints, DirBuster with anti-false-positive logic and SQLMap with WAF detection — all in autonomous logical sequence.
- Modular architecture with 6 specialized tools, contextual memory, structured system prompt and Rich UI; full reporting covering attack surface, vulnerabilities, attack vectors and recommendations.

Stack: Python · Qwen2.5-14B · LM Studio · Nmap · Nuclei · SQLMap · CVE API · Rich UI

LogSentry AI — Hybrid Local Intelligence Log Analyzer [AI × DEFENSIVE]

Privacy-first log analyzer with hybrid Regex + local LLM engine · github.com/isilderr1

- Combines a high-speed deterministic Regex engine with a local LLM (DeepSeek-R1 via LM Studio) to detect anomalies, phishing attempts and malicious payloads in logs.
- Zero-Trust Privacy architecture: fully on-premise analysis, no data leaves the network; designed for enterprise environments with strict compliance requirements.

Stack: Python · Regex Engine · DeepSeek-R1 · LM Studio · Zero-Trust · Log Analysis

Argus-Eye — Linux Endpoint Monitoring & HIDS

Linux-first security monitor with TUI and native notifications · github.com/isilderr1/argus-eye

- Custom HIDS with process integrity monitoring, service monitoring and security-oriented automation; Textual TUI interface and native DBus notifications.
- Event persistence via SQLite, integrated as a systemd user service; used as the HIDS component in Hybrid-SOC-Lab.

Stack: Python · Linux · SQLite · Textual TUI · systemd · DBus

Hybrid-SOC Incident Response Lab

Physical SOC lab with managed switches, router and Wazuh SIEM · github.com/isilderr1/Hybrid-SOC-Incident-Response-Lab

- Hybrid security lab (physical + virtual) with managed switches, hardware router, Wazuh SIEM on Docker and Argus-Eye as custom HIDS for process integrity.
- Automated syslog log-bridge for centralised ingestion; full documentation of incident response scenarios.

Stack: Wazuh · Docker · Managed Switches · Syslog · OPNsense · Suricata

ShardLock — High-Security CLI Encryption Tool

Cross-platform CLI for distributed encryption: AES-256-GCM + Shamir's Secret Sharing

- Eliminates single points of failure in critical data custody: combines AES-256-GCM authenticated encryption with Shamir's Secret Sharing to fragment the key into distributable mathematical shards.
- Designed for high-security scenarios: private keys, offsite backups, disaster recovery with configurable threshold.

Stack: Python · AES-256-GCM · Shamir's Secret Sharing · Cryptography · CLI

NeuralForge — Local LLM Fine-Tuning Platform **[IN PROGRESS]**

Developer · Full-stack platform for local LLM fine-tuning · 2024–Present

- Milestone-driven modular system: system detector, model manager, dataset engine (193 tests passed), training engine with live monitor; GGUF export pipeline in roadmap.
- FastAPI backend + React/TypeScript frontend; Hugging Face integration, on-demand GPU benchmark and LLM-assisted smart converter for narrative datasets.

Stack: Python · FastAPI · React · TypeScript · Hugging Face · SQLite · GGUF

CERTIFICATIONS & TECHNICAL TRAINING

Cybersecurity Specialist & Ethical Hacking

Epicode · May 2026

Network security, ethical hacking, web security, SOC fundamentals, incident response, vulnerability assessment and reporting.

In progress / Goals 2026-2027

- CompTIA Security+ — in preparation
- Blue team Level 1 — under evaluation
- Cisco CyberOps — in preparation
- Ongoing: TryHackMe · HackTheBox · CTF competitions

Full Stack Developer Training Program — 450h

Adecco · June 2022

JavaScript, React, Node.js, REST API, databases, Git, frontend/backend fundamentals.

LPIC-1 Linux System Administrator

Linux Istitute · Jan 2026

GNU/Linux administration, command line, file system, Boot process, package management, networking, security, shell scripting.

WORK EXPERIENCE

Front Desk Agent **Royal Continental Hotel, Naples** · Aug 2022 – Present

- High-volume front desk operations: check-in/out, reservations, guest assistance and operational coordination in a 4-star property.
- Handling of sensitive guest data with focus on accuracy, confidentiality and GDPR compliance.
- Anomaly management, identity verification and security procedures during autonomous night shifts.
- Daily use of Protel PMS for operations, reporting and financial reconciliation.

Gaming Inspector **Casino St. Moritz, Switzerland** · Dec 2021 – May 2022

- Supervised gaming tables in a regulated casino environment, ensuring compliance with procedures and operational standards.
- Procedural integrity monitoring, fraud prevention and high-pressure situation management.

Senior Croupier **Dragonara Casino, Malta** · Jun 2021 – Nov 2021

- Live gaming table management in an international environment, high-volume financial transactions and table security control.

Logistics Manager / Warehouse Operations **Newlat S.p.A., Italy** · Jan 2019 – May 2021

- Warehouse operations coordination, supplier management and logistics documentation in a high-volume industrial process-driven environment.

ADDITIONAL PROFILE

Portfolio & Online Presence

antonioruocco.com — SOC dashboard featuring WINTERMUTE AI agent (Gemini 2.0), interactive SQLi/SSH cyber range, live threat intel feeds.

Hardware & Maker

Electronics, soldering, 3D printing, hardware prototyping, embedded systems troubleshooting.

Languages

Italian: Native

English: Professional (C1)

German: Working proficiency (B1)

French: Basic (A2)