Cyprus | +357 97678511 | Greek & English
thanasisgeo0001@gmail.com
github.com/EvilMortys-lab

Thanasis Georgiou

Security Engineer | Security Operations & AI Security Tooling

Portfolio: tgcv.qd.je

Profile

Security and IT operations engineer who secured the network of a law firm handling privileged client data, after six years in Trust & Safety operations at a global online platform. I build Python tooling that applies automation and AI to detection engineering, including an automated YARA rule pipeline and a MITRE ATT&CK-based synthetic log generator. A self-taught polymath across security, AI and cognitive science. Seeking SOC, security or detection engineering roles. Live projects: **tgcv.qd.je**

Experience

IT & Security Operations | Marinos Mavrogenis Law Firm, Cyprus — 2025 – 2026

- Ran day-to-day IT and security for network, servers, endpoints and user access.
- Hardened Linux servers with firewall rules, fail2ban and an automated Nginx reverse-proxy setup, to limit exposed services.
- Deployed encrypted remote access with WireGuard and OpenVPN so staff could work securely off-site.
- Managed onboarding, offboarding and least-privilege access; configured NAS storage and asset inventory.

Content Analyst, Trust & Safety | Aylo — 2019 – 2025

- Reviewed and actioned high volumes of user-generated content against platform policy and legal requirements under strict time and quality targets.
- Escalated platform risks to cross-functional teams and streamlined review workflows with Jira, Zendesk and Make.com automations.

Projects

Safer World | Cybersecurity services for startups and small businesses — saferworld.digital

- Cybersecurity company I work on: code audits, authorised penetration testing (apps, APIs, networks, cloud), secure development with threat modelling and hardened websites. Scanning platform and EDR in development.

Cryptic | Invite-only encrypted messenger — crypticnet.cc

- E2E encrypted messaging, voice and video with a built-in VPN, QR-only invites and a GrapheneOS phone option.

YARA Sentinel Automaton | Python, yara-forge — github.com/EvilMortys-lab/YARA-Sentinel-Automaton

- Pipeline that collects fresh malware samples, then generates and deploys YARA rules automatically.

Ornith: MITRE ATT&CK Data Synthesizer — github.com/EvilMortys-lab/Ornith-MITRE-Data-Synthesizer

- Generates realistic attack logs mapped to MITRE ATT&CK for testing detections and training ML models.

The Polymath's Workspace | in progress

- Public write-up of my AI-assisted development workflow: Ponytail and custom agent skills for leaner, cheaper and more accurate code, custom MCP servers, and uncensored local models for authorized penetration testing.

Skills

Security operations	SIEM (Splunk, Wazuh), network monitoring (Suricata, Zeek, Wireshark), honeypots, threat intelligence, MITRE ATT&CK, YARA
Offensive & testing	Burp Suite, SQLmap, ffuf, Hashcat, BloodHound, phishing simulation, vulnerability scanning (Trivy)
Infrastructure	Linux server hardening, Docker, Nginx, WireGuard, OpenVPN, firewalls, fail2ban, IAM, NAS, XMPP
Development	Python, FastAPI, Streamlit, JavaScript, React, PHP, Laravel, Swift and Xcode (iOS), Stripe API & SDK; AI-assisted development workflows
AI engineering	Model Context Protocol (MCP) servers, multi-agent systems, local LLMs (Ollama, vLLM), LoRA fine-tuning, Ponytail and agent skills, uncensored models for authorized pentesting
Automation	Make.com workflows, Python scripting, AI agent pipelines, Jira and Zendesk workflow automation
Social media & ads	Social media management, ad creation, campaign setup on social media ad platforms

Certifications & Learning

Google Cybersecurity Professional Certificate *completed*

Google Cloud Professional ML Engineer *in preparation*

HarvardX: Fundamentals of Neuroscience *in progress*

Publication & Education

Find The Butterfly In Your Chaotic Life *book, Amazon*
Stoicism, chaos theory and first-principles thinking applied to personal psychology.

Secondary education, Olympion Greek Private School