



AGENTIC AI · SECURITY

CONTACT

- +33 6 51 56 82 89
- luongnv89@gmail.com
- Paris, France
- luongnv.com
- linkedin.com/in/luongnv89
- github.com/luongnv89

CORE EXPERTISE

AGENTIC AI & LLMs

- AI Agents MCP LLM Fine-tuning
- LangGraph RAG Ollama / vLLM

SECURITY

- Network Security
- Deep Packet Inspection
- Threat Intelligence Phishing Defense

DIGITAL TWINS & IOT

- Digital Twins IoT Simulation

ENGINEERING

- Python C/C++ TypeScript
- Swift React Node.js Docker
- Kubernetes

LANGUAGES

- English PROFESSIONAL
- French WORKING
- Vietnamese NATIVE

EDUCATION

- MSc, Software Engineering for Ambient Intelligence
Télécom SudParis · 2012 – 2014
- Engineer's Degree, Computer Science
Hanoi University of Science and Technology · 2007 – 2012

Luong NGUYEN

AGENTIC AI & SECURITY ENGINEER

Senior software engineer with 15+ years in security and AI, from packet inspection in C to fine-tuned language models and AI agents. Lead developer on EU R&D projects; author of *claude-howto* (40k+ GitHub stars).

PROFESSIONAL EXPERIENCE

Montimage

2014 – Present

Senior Software Engineer · Paris, France

- LLM adaptation:** Built a fine-tuning pipeline for security-focused small models (synthetic data, LLM-as-judge, Unsloth/LoRA), run locally via Ollama for phishing detection
- MCP servers:** Created mitre-mcp and sec-mcp (PyPI, official MCP Registry), giving AI assistants MITRE ATT&CK knowledge and threat-intelligence checks
- Network security:** Lead developer of MMT-DPI, Montimage's C deep packet inspection engine (~80% of commits since 2015), incl. its 2026 hardening overhaul
- Phishing defense:** Built a gamified awareness-training platform (5 languages), an LLM-based email analysis service and the GEIGER cyber range (900+ users)
- Digital twins:** Lead developer of COGNIMAN industrial pilot software and the secSIM cybersecurity twin platform; sole developer of the TaS IoT test platform
- Community:** Organizing Committee, IEEE CloudCom 2026 and IFIP ICTSS 2026 (Paris); built both conferences' registration and payment platforms

EU R&D PROJECTS (H2020 · HORIZON EUROPE · DIGITAL EUROPE)

- COGNIMAN SECASSURED AIAgent4Cyber NERO CyberSuite INTACT GEIGER PUZZLE ENACT

Percevio · Full-Stack Developer · Paris

Mar 2014 – Feb 2016

- WebRTC-based P2P content delivery network, video conferencing and live broadcasting

FPT Software / VTC Online · Software Developer · Hanoi

May 2011 – Apr 2012

- Developed Java and Android applications; led small development teams

OPEN SOURCE & PRODUCTS

43k+ GitHub stars · ~1k followers · github.com/luongnv89

- claude-howto:** Visual guide to Claude Code; 40k+ stars, 5k+ forks, #1 on GitHub Trending
- asm:** Skill manager for AI coding agents across 21 platforms (npm); 900+ stars
- Agent tooling:** pi-extensions, skills, context-stats and sleek-ui; each 100+ stars
- Apps:** Ask Milo, TextWiz, CUStats (App Store); VS Code extensions, 2,000+ installs

SELECTED PUBLICATIONS

- ICTSS 2026** SecSIM: A Digital Twin Management System for Simulation-Driven Cybersecurity Assessment
- ARES 2025** LLMs in Security Testing and Monitoring: An Initial Study
- IFIP IoT 2024** SINDIT: A Framework for Knowledge Graph-Based Digital Twins in Smart Manufacturing
- QUATIC 2022** Digital Twin for IoT Environments: A Testing and Simulation Tool
- Book, 2021** Validation, Verification and Root-Cause Analysis, in *DevOps for Trustworthy Smart IoT Systems*
- IEEE TIFS 2019** Reliable Detection of Interest Flooding Attack in Real Deployment of Named Data Networking
- WF-IoT 2014** DPWSim: A Simulation Toolkit for IoT Applications Using Devices Profile for Web Services