

WILFREDO PAULO A. PEREZ III

Naga City, Camarines Sur, Philippines 4400

☎ +63 956-943-6779 | ✉ pauloperez9754@gmail.com | 🔗 linkedin.com/in/wppereziii | 🐙 github.com/C0deRhino | 📁 portfolio.wpperez.com

EDUCATION

Ateneo de Naga University

2022 – 2026

B.S. Computer Science — *Magna Cum Laude*, Silver Achievement Awardee

Naga City, Philippines

- **Thesis:** Vendor-Agnostic, Explainable Software-Defined IPS for SOHO Networks using PPO, Policy Distillation & TreeSHAP-IQ
- QPI: 3.64 — Consistent President's Lister — DOST Scholar

WORK EXPERIENCE

Nueca Technologies Inc.

May 2025 – Present

Cybersecurity Engineer, Vice Chair – AI Transformation Team & Compliance Officer for Privacy

Onsite

- Spearheaded a 3-phase company-wide AI transformation roadmap (individual experimentation → team-level AI workflows → cross-department harmonization) across **all 5 departments**; achieved **~78% AI-assisted workflow adoption** among 55 employees within 3 months of rollout.
- Maintain and scale **6+ production AI systems** (RAG chatbot, hybrid OCR, offline transcriber, AI orchestration platform, on-premise HR assistant, email security responder) — all architected with **zero cloud data exposure** for privacy-sensitive enterprise operations.
- Administer and secure the company's internal LAN serving **55 employees across 5 departments**, enforcing segmentation, access control, and 99%+ uptime of critical network services; intercepted **100+ phishing emails** to reduce phishing exposure by **~70%**.
- Serve as the **Global Administrator** for the enterprise Microsoft suite, managing Entra ID, Microsoft 365, and Azure environments for **55 users**; enforced Zero-Trust frameworks and restricted tenant roles to achieve a **80% reduction** in privileged access vulnerabilities.
- Deployed Wazuh SIEM across **8 Kubernetes nodes**; appointed **Compliance Officer for Privacy (COP)** leading NPC compliance; conducted full network audit identifying **12 segmentation gaps** — redesign **approved and funded**.
- Led the development of an internal ERP system with integrated IAM and HR modules, consolidating workflows for all 55 users and reducing administrative overhead by **~60%**; resolved **3 critical DNS misconfigurations** (SPF, DKIM, DMARC) and scanned **3 network segments** for vulnerabilities.
- Promoted through successive roles from Network Security Analyst [Intern] to Cybersecurity Associate (Part-Time), and finally to full-time Cybersecurity Engineer & Vice Chair of the AI Transformation Team within 12 months.

Mindrift

November 2025 – April 2026

AI Engineer (Task-Based) — LLM Training & Data

Remote

- Contributed to LLM training pipelines by delivering **3,200+ annotated data samples** across multiple task batches while maintaining a **94% task acceptance rate** for fine-tuning datasets.
- Engineered a fully automated web scraping pipeline (Python, BeautifulSoup, Selenium) that reduced manual processing time by **~85%**, enabling consistent high-volume output with zero scheduling conflicts.

PROJECTS

Agent-to-Agent Coordination Lobby Platform | TypeScript, A2A, MCP, PostgreSQL

August 2026 – Present

- Built and deployed a **live 1:1 employee agent coordination platform** using A2A + MCP, replacing manual human-mediated handoffs with governed messaging, durable state, and bilateral approvals; validated through a **29-test automated suite**.

PII-Redacting Privacy Gateway LLM Proxy | Python, FastAPI, Presidio, DLP

August 2026 – Present

- Built and deployed a **live LLM privacy gateway** integrated with the Privacy-First Agent Harness, enforcing a **3-stage redaction/pseudonymization pipeline** and **3 protection modes** to centrally prevent sensitive data exposure to external AI providers.

Privacy-First Isolated AI Agent Harness | VPS, Sandboxed Runtime, LLM Orchestration, Context-Layer Compression

April 2026 – August 2026

- Designed a **fully isolated AI agent runtime** on a dedicated VPS with its own Google account, phone number, and credentials — **zero access to local machines or personal data**; achieved **97% task-completion parity** with local agent setups while eliminating **100% of local credential exposure** and reducing PII leakage surface by **~94%**.

CheatScale: Enterprise AI Development Orchestration | OpenCode, Python, Multi-Agent

March 2026 – June 2026

- Built a **24-agent 3-tier orchestration system** with wave-based task routing and Obsidian graph-linked documentation across **120+ project nodes**; reduced project scaffolding overhead by **~88%** with enforced **80%+ unit test coverage**.

Corp-Mind-AI: On-Premise HR Knowledge Assistant | FastAPI, Qdrant, Ollama, React

March 2026 – May 2026

- Architected a **fully on-premise RAG HR assistant** with hybrid semantic + BM25 search (RRF fusion) and source-cited answers with page-level traceability — zero employee data leaves the network; **2-hr TTL cache** reduced redundant LLM inference by **~65%**.

AI-Centric Email Security Responder | Power Automate, n8n, LLM API

March 2026 – April 2026

- Automated end-to-end email security response drafting using LLM-powered orchestration (Power Automate, n8n); reduced analyst drafting time by **~76%** across **3 monitored mailboxes**, eliminating an estimated **~5 manual hours/week** of triage and reply work.

Home-Laboratory Software-Defined Firewall | pfSense, Suricata, OSI Layer 1–4, VLAN Segmentation

April 2025 – June 2025

- Deployed a software-defined firewall across a **4-VLAN segmented home-lab** enforcing **60+ custom rules** with real-time IDS visibility via Suricata; achieved **zero lateral movement** during internal threat simulations.

ACTIVITIES

Competitions: Regional CTF Hack4Gov 2 & 3 — School (AdNU) Representative; National CTF Hack4Gov 3 — School (AdNU) Representative

SKILLS & CERTIFICATIONS

AI/ML: RAG, Multi-Agent Orchestration, LLM Fine-Tuning Data, Prompt Engineering, Vector DBs (Qdrant), Embeddings, Compression, Wiki, Retrieval, Whisper, Ollama, n8n, Vision AI, OCR

Security: Wazuh SIEM, Suricata IDS, Nmap, OpenVAS, MITRE ATT&CK, pfSense, Data Privacy Compliance (NPC), Threat Modeling

DevOps/Cloud: Docker, Kubernetes, AWS, DigitalOcean, GitHub Actions, CI/CD, IaC

Languages: Python, TypeScript/JavaScript, C/C++, Java, React, FastAPI, Node.js, Bash

Certifications: ISC² CC, Google Cybersecurity, CCSP-AWS, CNSP, TOPCIT Level III, BTLO, FIT-SM