

Yi Hsuan Wu

Security Engineer | Product Security | AI Security Automation
London, United Kingdom | UK Youth Mobility Scheme visa, no sponsorship required
wiiwu959@gmail.com | github.com/wiiwu959 | wiiwu959.github.io

Profile

AI and product security engineer with 3+ years of experience across application security, red teaming, threat modelling and security automation. Builds internal multi-agent security-review workflows that provision repeatable audit environments, validate outputs, filter noise and produce structured reports. Works with engineers and technical PMs to turn findings into practical remediation and safer workflows.

Experience

AI Security Engineer

Crypto.com

Jul. 2026 – Present

Taiwan (Remote)

- Build and operate an internal AI security platform that accepts repository URLs, orchestrates n8n and proprietary services, and provisions OpenCode-based audit environments.
- Design multi-agent, multi-model workflows using curated vulnerability knowledge; compare and validate outputs, filter low-value findings and produce structured reports for security engineers.
- Maintain an internal LLM wiki and conduct adversarial testing of internal AI use cases, including prompt-injection and guardrail-bypass scenarios.
- Helped replace repeated guardrail patches with a two-agent design that separates task interpretation from execution and limits permissions by role.

Application Security Engineer

Crypto.com

Sep. 2025 – Jun. 2026

Taiwan (Remote)

- Performed pre-release Web, mobile and API security reviews using STRIDE threat modelling, manual testing, secure code review, SAST/DAST, Semgrep and Burp Suite across 5+ products.
- Managed external disclosures and third-party penetration-test findings from reproduction and severity assessment through remediation guidance, fix validation and closure.
- Partnered with engineers and technical PMs to explain root causes, prioritise risk, track remediation and retest fixes through closure.

Threat Researcher, Red Team

Trend Micro

Sep. 2023 – Sep. 2025

Taiwan

- Delivered 3 end-to-end red team engagements across enterprise infrastructure and Active Directory, compromising Domain Controllers and translating attack paths into actionable remediation guidance.
- Built Python and Bash tooling and phishing automation, discovered critical RCE and SSRF issues, and performed PCI-DSS assessments across AWS and Azure.

Research Intern, Red Team

DEVCORE

Sep. 2022 – Feb. 2023

Taiwan

- Researched Active Directory attack methodologies and created an internal hacking lab for repeatable experiments and training.
- Built an Angular-based platform to support repeatable offensive-security experiments and training.

Software Engineering Intern

MediaTek

Jul. 2021 – Aug. 2021

Taiwan

- Developed camera-firmware performance measurement scripts and a visualisation website used by engineers for debugging and analysis.
- Turned measurement output into visualisations that helped engineers compare performance and investigate regressions.

Technical Skills

AI Security: Multi-agent and multi-model workflows, prompt/context design, agent skills, output validation, prompt injection and guardrail testing

Product Security: Threat modelling, secure design and code review, Web/API/mobile security, vulnerability triage, remediation, SAST/DAST

Engineering: Python, Bash, JavaScript/Angular, REST APIs, n8n, OpenCode, Git, workflow automation, debugging

Offensive and Cloud: Red teaming, penetration testing, Active Directory, phishing simulations, AWS/Azure PCI-DSS security assessments

Certifications: OSCP (OS-101-57442), OSWE (OS-AWAE-9873), CRTP (ADLID8419)

Education

M.Sc. Network Engineering

National Chiao Tung University, GPA 4.3/4.3

2021 – 2023

Hsinchu, Taiwan

- Thesis: Minimising Attack Surface for Python Web Frameworks

B.Sc. Computer Science

National Taiwan University of Science and Technology, GPA 4.12/4.3

2017 – 2021

Taipei, Taiwan

- Undergraduate project: Attack Based on Containerized Rogue Base Station.
- Best Paper award, Cryptology and Information Security Conference 2020.