# AINSLEY WOO

PENTESTER
FORWARD DEPLOYMENT AI ORCHESTRATOR

45 Toh Tuck Road
+65 9824 8608
wooainsley@gmail.com
www.wooainsley.com

Hey, I'm Ainsley — a computer science undergrad at SUTD (Class of 2027) who's fallen hard for the space where AI and security meet. I like building things that hold up when the world is messy. I'm also starting AGIs, a Singapore-based venture built on the belief that everyone should have their own agentic AI. When I'm not coding, I'm usually organizing student sports or sitting in on committees — because the best systems need people as much as they need good code.

## FOLLOW ME

https://github.com/Kantosaurus
https://www.linkedin.com/in/ainsley-woo-
https://www.wooainsley.com

## CERTIFICATIONS

CERTIFIED CLOUD PRACTITIONER
Credential ID:
3b0d880300fc47cb8e30d194d3d555b1
Validates foundational understanding of AWS Cloud services, and terminology

## RELATED EXPERIENCES

IT RISK AND COMPLIANCE INTERN

SHOPEE/MONEE — FEB 2026 – APR 2026

As an IT Risk and Compliance intern on the SOX team at Shopee Digital Financial Services, I worked across fraud rule development, AML monitoring, investigation reporting, and UATs for anti-fraud systems. I also built a plugin and set up AI-orchestrated automations that replaced several manual processes that aggressively cut real hours out of the team's week.

SECURE AI ENGINEER INTERN

THE X TRIBE — NOV 2025 – JAN 2026

Architected and deployed AI frameworks from the ground up with integrated security safeguards, input validation, and adversarial resilience. Designed and rolled out a production openclaw orchestration Retrieval-Augmented Generation (RAG) system for intelligent document retrieval, implementing chunking strategies, embedding pipelines, and context-aware query processing to deliver accurate, grounded LLM outputs.

NATIONAL SERVICE (COMPLETED)

MILITARY POLICE — 2021 - 2023

## EDUCATION

BACHELOR OF ENGINEERING, COMPUTER SCIENCE AND DESIGN (CYBERSECURITY), MINOR IN ARTIFICIAL INTELLIGENCE

SINGAPORE UNIVERISITY OF TECHNOLOGY AND DESIGN
EXPECTED 2027

Building at the intersection of cybersecurity and AI. Active in independent research on agent security, post-quantum cryptography, and LLM defense — alongside student leadership in athletics and institutional governance.

## REFERENCES

RAYMOND
DIRECTOR, THE X TRIBE
T: +65 9871 5927
E: Raymond.xu@bindstack.ai

KAI XIN
MANAGER, MONEE
T: -
E: Kaixin.yee@seamoney.com

## RESEARCH

### HALLUCINATIONS AT THE FIREWALL

AAAI 2026 UNDERGRADUATE CONSORTIUM

https://underline.io/speakers/750841-ainsley-woo
Presented at the Association for the Advancement of Artificial Intelligence 2026 Undergraduate Consortium on Hallucinations at the firewall, research on why AI hallucinates and how does it negatively affect enterprises and consumers.

## PROJECTS

### AGENTGUARD

AGIS / SUTD

Built AgentGuard, a dual-stream (OS telemetry + LLM action log) Mamba/Transformer cross-attention anomaly detector for LLM agent servers, reaching F1 0.95 / AUROC 0.995 and beating 5 baselines (Isolation Forest, LSTM/CNN/Transformer-AE, Deep SVDD) by +0.22 AUROC across 3-seed × 5-fold agent-level CV, with an Optuna-tuned hybrid loss, 20-container data pipeline, and live Streamlit dashboard.

### SENTINELLM

AGIS / SUTD

Runtime safety layer for LLM applications. Multi-layer with dual-key neural+symbolic verdict architecture; deployed as an ASGI proxy with React/Docker GUI. Fine-tuned model results were ~500% better than normal base model

### QUANTUM ARMOURED SERVICE PROTOCOL

AGIS / SUTD

Designed and implemented QASP, a post-quantum secure network protocol for AI agent-to-agent communication, built on TCP/QUIC transports with a sans-I/O state-machine core, a custom handshake combining NIST-standardized ML-KEM-768 / ML-DSA-65 with hybrid X25519 key exchange, stream multiplexing, OCSP-style revocation, capability-based access tokens, Bayesian trust scoring, and MCP/A2A interoperability bridges for cross-protocol agent networking.

### PREDICTIVE VULNERABILITY ENGINE FOR POST QUANTUM CRYPTO

OPENSOURCE

https://github.com/Kantosaurus/Predictive-Vulnerability-Engine-for-Post-Quantum-Crypto
Built an enterprise-grade predictive vulnerability engine (Rust + Python) combining symbolic reasoning and ML to forecast quantum threats to cryptographic systems, scan codebases across 6 languages for at-risk primitives, and automate FIPS 140-2/FedRAMP-compliant migration planning to post-quantum algorithms (Kyber, Dilithium, SPHINCS+).

### AUTONOMOUS MALWARE BEHAVIOUR ATTRIBUTION SYSTEM

OPENSOURCE

https://github.com/Kantosaurus/Autonomous-Malware-Behaviour-Attribution-System
Built an autonomous malware attribution platform in Rust and Python that combines behavioural graph neural networks with rule-based detection across Windows/Linux/macOS endpoints, scaling to 10,000+ hosts with sub-second attribution latency and automatic MITRE ATT&CK technique mapping.

### CONTINUOUS SUPPLY CHAIN TRUST VERIFIER

OPENSOURCE

https://github.com/Kantosaurus/Continuous-Supply-Chain-Trust-Verifier
Built a Rust-based supply chain security platform (11-crate workspace with REST/GraphQL API, Leptos dashboard, and Postgres-backed worker queue) that continuously scans npm, PyPI, Maven, Cargo, and four other ecosystems for typosquatting, tampering, and provenance attacks, generating CycloneDX/SPDX SBOMs and SARIF reports to catch malicious dependencies before they reach production.