Yulan Galagoda

Cyber Security Engineer & AI Researcher

Defending everything from enterprise networks to intelligent machines.

Plymouth, United Kingdom | +44 7833 034848 | hi@yulan.me | Portfolio **yulan.me** | linkedin.com/in/yulangalagoda | github.com/yulangalagoda | ORCID 0009-0009-3470-0359

PROFILE

Cyber security engineer and AI researcher working where security operations meets machine learning. Defended enterprise estates across the Microsoft security stack, owned an ISO 27001 implementation through external certification audit, and worked a 24/7 rota protecting a national ISP backbone. Current research hardens deep-learning intrusion detection against adversarial attacks on automotive CAN bus traffic.

RESEARCH

Adversarial Training to Improve Deep Learning Intrusion Detection in the Internet of Vehicles

MSc dissertation, University of Plymouth | Supervisor: Dr. Shaymaa Al-Juboori | In progress, 2026

- Investigating whether adversarial training can act as targeted data augmentation, restoring deep-learning IDS performance on strictly de-duplicated CAN bus data where a 1D-CNN otherwise collapses below a Random Forest baseline.
- Training a 1D-CNN on CICIoV2024 against a Random Forest baseline, attacking both with FGSM and PGD through the Adversarial Robustness Toolbox, and measuring clean accuracy, adversarial accuracy, false-positive rate and compute cost across attack budgets.

EXPERIENCE

Cyber Security Engineer

Union Assurance PLC (John Keells Group) | Sri Lanka | Nov 2024 to May 2025

- Monitored and investigated security events across cloud, endpoint, identity and network environments using Microsoft Sentinel and Microsoft Defender XDR, triaging 20 to 25 production alerts a month with initial response under 10 minutes.
- Owned the ISO/IEC 27001:2022 programme end to end, writing policies and procedures and taking the organisation through its Bureau Veritas audit, closing 11 of 12 findings including both critical findings.
- Led vulnerability assessment and penetration testing, uncovering a significant Microsoft Sentinel configuration weakness around prolonged remote-access sessions and driving the remediation and tooling review that followed.
- Advised the in-house software development team on secure development practice, auditing their remediation commits in GitHub and verifying fixes through application vulnerability assessment.

Associate Engineer

Lanka Communication Services (LankaCom) | Sri Lanka | Aug 2024 to Nov 2024

- Operated a 24/7 shift-based NOC covering nights, weekends and public holidays, defending the national ISP backbone and secure enterprise VPN services for banking, government and industrial customers.
- Conducted internal ISO/IEC 27001:2022 audits and resolved over half of the findings raised, and expanded DCIM asset coverage from approximately 20% to 100% by mapping data centre infrastructure.

Trainee Associate Engineer

Lanka Communication Services (LankaCom) | Sri Lanka | Feb 2024 to Jul 2024

- Diagnosed ISP backbone and VPN faults in a 24/7 NOC, maintaining SLA compliance, and supported ISO/IEC 27001:2022 ISMS implementation for the data centre colocation services.

Technology Intern

AXYYA Digital | Sri Lanka | Jul 2022 to Oct 2022

- Technical research and documentation across assigned projects; appointed intern group leader from September 2022, coordinating tasks across the team.

EDUCATION

MSc Artificial Intelligence

University of Plymouth, United Kingdom | Sep 2025 to Sep 2026 (expected)

BSc (Hons) Computer Security, First Class Honours

University of Plymouth, United Kingdom | Sep 2021 to Aug 2024

SELECTED PROJECTS

Full case studies, method and source at yulan.me

Glean, local-LLM OSINT pipeline. Runs curated FOSS reconnaissance tooling, normalises output into one provenance-tracked entity model, correlates deterministically in code, and produces a prioritised analyst brief. Python, Ollama. In development, reserved on PyPI as glean-osint.

AdverSec, adversarial robustness of neural intrusion detection on the CAN bus, and the basis of the MSc dissertation. Python, PyTorch, scikit-learn, Adversarial Robustness Toolbox.

NetEAGLE, Raspberry Pi network security gateway unifying Nmap discovery, a UFW firewall and Suricata IDS/IPS behind a Flutter control plane and Flask REST API. Scope set by a survey of non-technical home users.

Domain Hygiene Audit, passive Certificate Transparency audit of my own domain. Separated a pre-ownership spam issuance pattern from routine renewals across 600 plus records, verified by passive DNS.

The Meridian and **Rampe**, Notion-backed static archives for antiques and for Sri Lankan and global cooking. Schema-first design on Cloudflare Pages, publishing automatically from a single source of truth.

LAB

Interactive security instruments that run live in the browser and show their own working.

Adversarial Examples Playground, a live FGSM and PGD attack that flips a neural classifier on an imperceptible perturbation. **Live Global Attack Traffic**, a real-time read of internet background attack noise from the SANS Internet Storm Center honeypot network. **Password Strength Lab**, transparent entropy maths with pattern and breach detection, nothing leaving the page.

PUBLICATION

Nothing Is Magic: Machine Learning Mathematics. Zenodo, 2026. DOI: 10.5281/zenodo.21541212

Open book on the mathematics underlying machine learning, built on intuition rather than memorisation, with ideas implemented from scratch in NumPy. Part one, twelve chapters, complete and published.

SKILLS

Security Operations: Microsoft Sentinel (SIEM), Microsoft Defender XDR, SentinelOne, alert triage and investigation, incident response and escalation, threat monitoring, 24/7 shift operations

Offensive and Defensive: Vulnerability assessment and penetration testing, vulnerability management, threat modelling, OSINT and reconnaissance, IDS/IPS (Suricata), firewalls (UFW, iptables), Nmap, Wireshark

Cloud and Infrastructure: Microsoft Azure security, Microsoft 365 security, Zscaler ZTNA, enterprise networking and VPN, Windows Server, Linux administration, Raspberry Pi and embedded Linux, Cloudflare

Governance: ISO/IEC 27001:2022 implementation and internal audit, policy and procedure development, risk management, security awareness, supplier and stakeholder management

Machine Learning: Deep learning (CNN, RNN, LSTM), adversarial machine learning, Adversarial Robustness Toolbox, PyTorch, TensorFlow and Keras, scikit-learn, NumPy, local LLMs (Ollama), machine learning mathematics

Engineering: Python, Bash and shell scripting, Flask, Git, CI/CD pipelines, Notion API and database design, Quarto, technical writing and documentation

CERTIFICATIONS

Certified in Cybersecurity (CC) ISC2, 2024

ISO/IEC 27001:2022 Information Security Associate SkillFront, 2024

AI Security Fundamentals Microsoft, 2026

AI Security & Governance Securiti, 2026

Introduction to Cybersecurity Cisco Networking Academy, 2021