Yulan Galagoda

Cyber Security Engineer & AI Researcher

Defending everything from enterprise networks to intelligent machines.

Plymouth, UK · +44 7833 034848 · hi@yulan.me · Portfolio: **yulan.me** · linkedin.com/in/yulangalagoda · github.com/yulangalagoda

PROFILE

Cyber security engineer and AI researcher specialising in enterprise security operations and adversarial machine learning. Experienced in ISO/IEC 27001:2022, VAPT, SOC triage, and SIEM operations across insurance and telecoms. Current research hardens deep-learning intrusion detection against adversarial attacks on automotive CAN-bus traffic — bridging security operations and AI security for safety-critical systems.

RESEARCH

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

MSc Dissertation (PROJ518) · University of Plymouth · Supervisor: Dr. Shaymaa Al-Juboori · In progress, 2026

- Applying multi-strategy adversarial training as data augmentation to improve deep-learning IDS on realistic, de-duplicated CAN-bus data (CICIoV2024).
- Training a 1D-CNN against a Random Forest baseline, attacking both with FGSM and PGD via the Adversarial Robustness Toolbox (ART).
- Measuring clean vs. adversarial accuracy, false-positive rate, and compute cost to map robustness–performance trade-offs; building a reproducible evaluation pipeline for open-source release.

EXPERIENCE

Cyber Security Engineer (Executive)

Nov 2024 – May 2025

Union Assurance PLC · Sri Lanka

Microsoft Sentinel · Microsoft Defender (EDR/XDR) · SentinelOne · Zscaler ZTNA · Azure

- Led ISO/IEC 27001:2022 policy and procedure design at a leading insurer, closing 11 of 12 Bureau Veritas audit findings — including both critical findings — ahead of certification.
- Ran vulnerability assessments and penetration tests across production systems, and triaged SOC alerts end-to-end with initial incident response held under 10 minutes.
- Uncovered a Microsoft Sentinel misconfiguration through penetration testing, drove its remediation, and supplied the technical evidence behind negotiations that cut SIEM licensing costs.

Associate Engineer (promoted from Trainee Associate Engineer)

Feb 2024 – Nov 2024

Lanka Communication Services (LankaCom) · Sri Lanka

- Ran internal ISO/IEC 27001:2022 audits and closed more than half of all resulting findings ahead of the company's successful certification.
- Restored 5–10 enterprise VPNs daily in a 24/7 NOC, consistently meeting ISP SLA targets; expanded DCIM coverage from ~20% to 100%.

SELECTED PROJECTS

NetEAGLE — network security gateway

2024

Python · Flask · Suricata · Raspberry Pi

- Raspberry Pi security gateway with Suricata IDS/IPS and a mobile-friendly control plane for home and small-office networks.

yulan.me, The Meridian & Rampe — publishing platforms

2025–26

Next.js · TypeScript · Notion API · Cloudflare Pages

– Notion-backed portfolio and static-site archives with automated publishing via the Notion API, Cloudflare Pages, and CI/CD.

LAB

Interactive security instruments — small, working tools that run live in the browser.

– **Adversarial Examples Playground** — live FGSM/PGD attack that fools a neural classifier in-browser.
yulan.me/lab/adversarial

– **Password Strength Lab** — transparent entropy, pattern and breach detection, honest crack-time estimates.
yulan.me/lab/password

– **Live Global Attack Traffic** — real-time attack telemetry from the SANS ISC honeypot network.
yulan.me/lab/live

SKILLS

SECURITY

Network security · Zero Trust (Zscaler ZTNA) · EDR/XDR (Microsoft Defender, SentinelOne) · SIEM (Microsoft Sentinel) · IDS/IPS (Suricata) · Vulnerability management & VAPT · Incident response · ISO/IEC 27001 · Nmap · Wireshark · Linux firewalls (UFW)

MACHINE LEARNING

Deep learning (CNN, RNN, LSTM) · Adversarial ML · Adversarial Robustness Toolbox (ART) · PyTorch · TensorFlow/Keras · scikit-learn

ENGINEERING

Python · Bash/Shell · Linux administration · Microsoft Azure · Raspberry Pi & embedded Linux · Flask · Cloudflare (Pages, DNS) · Notion API · Technical writing

EDUCATION

MSc Artificial Intelligence

2025 – Present

University of Plymouth, UK

Dissertation in adversarial machine learning for vehicular intrusion detection — detailed under Research.

BSc (Hons) Computer Security — First Class Honours

2021 – 2024

University of Plymouth, UK

Focus on network security, intrusion detection, and secure systems engineering.

CERTIFICATIONS

Certified in Cybersecurity (CC)	ISC² · 2024
AI Security Fundamentals	Microsoft · 2026
AI Security & Governance	Securiti · 2026
ISO/IEC 27001:2022 Information Security Associate	SkillFront · 2024
Introduction to Cybersecurity	Cisco Networking Academy · 2021