Ho Yin Li (Cliff)

London, Ontario, Canada | irugnim@gmail.com
linkedin.com/in/ho-yin-li-7a247728b | github.com/irugniM | cliff-li-portfolio.pages.dev

SUMMARY

Computer Science student with hands-on systems administration, networking, and security monitoring experience from coursework, a Computer Systems Technician diploma, and self-run home lab infrastructure. Builds and ships working software, including a published Chrome extension, an ML-based DNS threat detection agent, and deployed web applications.

EDUCATION

The University of Western Ontario September 2024 - Present

Bachelor of Science, Computer Science, London, Ontario

- Software Tools and Systems Programming (CS 2211): C, Unix/Linux command line, and shell scripting for system automation.
- Computer Science Fundamentals I (CS 1026): Python programming and problem-solving fundamentals.
- Introduction to Computer Architecture (CS 2208): memory management and ARM Assembly at the hardware level.

Seneca College, Toronto September 2022 - December 2023

Diploma, Computer Systems Technician

- Active Directory (WIN 700): AD DS structure, Group Policy, and user authentication.
- Security Incident Response (SEC 320): SIEM with Splunk and the incident response lifecycle.
- Microsoft Cloud Administration (MST 400): Azure and cloud administration.

TECHNICAL SKILLS

Systems Administration: Windows Server, Active Directory, Azure, AWS EC2, Group Policy
Networking: Ethernet/IP, DNS, DHCP, OSPF, switch and router configuration, Wi-Fi management, wired and wireless networks
Security and Monitoring: Splunk, Wireshark, Suricata, Pi-hole, incident response, digital forensics
Programming: Python, C, Java, JavaScript, Bash scripting, ARM Assembly, HTML, PHP
Tools and Platforms: Linux/Debian, Git and GitHub, Cloudflare Pages, TensorFlow, pytest

PROFESSIONAL EXPERIENCE

DSV, Hong Kong - Warehouse Assistant November 2021 - February 2022

- Maintained accurate inventory records using Microsoft Excel and internal database systems.
- Collaborated with a team to streamline logistics processes and meet daily operational targets.
- Resolved customer inquiries regarding shipment details, maintaining high customer satisfaction.

Senior in IT Club, The University of Western Ontario - Volunteer September 2024 - Present

- Provide technical support to seniors, troubleshooting hardware and software issues on laptops and mobile devices.
- Simplify complex technical concepts to teach digital literacy and basic cyber hygiene practices.
- Resolve connectivity and application errors with patience and clear communication.

PROJECTS

RealCost - Chrome Extension (Published)

JavaScript, Chrome Extension APIs

- Published Chrome extension that estimates the true checkout cost of products in Canada by reading retailer sticker prices, applying provincial tax rules, and adding eco-fees when available.
- Displays the calculated total next to the product so shoppers see the real price before checkout.

DGA Detection Engine

Python, TensorFlow (CNN-LSTM), Pi-hole, Suricata

- Built a real-time agent that monitors Pi-hole DNS query logs and classifies domains with a trained CNN-LSTM model to detect algorithmically generated malicious domains.
- Automated defensive response: Pi-hole blocklist updates, non-blocking Suricata ruleset reloads over a Unix socket, and Telegram alerting.
- Delivered a synthetic DGA training pipeline, pytest suite, and cross-platform mock mode for testing.

Security Incident Response and Forensics Lab Seneca, SEC 320

- Applied the full incident response lifecycle (preparation, detection, analysis, containment, eradication, recovery) to simulated breaches.
- Deployed and configured Splunk to aggregate system logs and wrote SPL searches to identify suspicious activity.
- Performed live and dead-box forensics plus static and dynamic malware analysis to produce Indicators of Compromise.
- Developed incident response playbooks to formalize procedures for identifying and neutralizing threat types.

Network-Wide Intrusion Detection System Home lab

- Architected a monitoring solution using Suricata and a custom Python agent that parses eve.json logs and automates real-time alerting through a Telegram API bot.
- Documented system configurations and troubleshooting procedures for repeatable deployment.

Network Governance and Infrastructure Home lab

- Deployed Pi-hole as a DNS sinkhole to govern local network traffic, optimize bandwidth, and enforce privacy policies.
- Managed Active Directory environments to control user access and device permissions in a lab domain.

Spell Dungeon Web Edition

JavaScript, HTML5 Canvas, Cloudflare Pages

- Developed a browser dungeon crawler where spells are cast by typing sentences against tiered words-per-minute goals, with procedural mazes, combat, save slots, and a live typing HUD.
- Deployed to Cloudflare Pages and maintained the source on GitHub.

SpellBattle 2D Software Engineering group project

Java, libGDX

- Built a desktop dungeon crawler with a course team, covering requirements, design documentation, implementation, and testing.

LANGUAGES

English, Cantonese, Mandarin, Italian (beginner)