THIEN BAO MINH DANG

Phone: 0415855950 (Australia) | 0357858208 (Vietnam)
Email: dangthienbaominh@outlook.com
LinkedIn: https://www.linkedin.com/in/thien-bao-minh-dang-47a640299/
GitHub: https://github.com/lilmilo2704

SUMMARY

A third year university student pursuing Bachelor of Computing Science at UTS. My area of Interest is cybersecurity and all other information technology aspects in general. I am seeking for a job in technology field to enhance all my professional skills and to gain more knowledge as well as hands-on skills that are valuable in the industry.

TECHNICAL SKILLS

- Wireshark
- Snort
- Linux (Ubuntu, Kali)
- Virtual Computing (VMware, VirtualBox)
- Netwag
- Bash Scripting
- Python (Numpy, Pandas, scikit-learn, tkinter, pygame)
- Java (Spring Boot, JavaFX)
- SQL (MySQL)
- Javascript
- Cloud Computing (AWS, Azure)

EDUCATION

University of Technology Sydney (present)

- Course: Bachelor of Computing Science (Honor)
- Major: Cybersecurity and Privacy
- Current GPA: 6.75 / 7 (High Distinction)

UTS College

- Course: Diploma of IT
- GPA 5.9 / 7 (Distinction)
- Database Fundamental, Programming 1, Programming 2: HD

Le Hong Phong high school for gifted

- GPA 9.0/10

PROJECT

SOC Automation System Intergrating Cloud Service Lab

- Description: Developed a cloud-based Security Operations Center (SOC) automation lab on Microsoft Azure, integrating Wazuh (SIEM), TheHive (incident response platform), and Shuffle (SOAR) to automate security event detection, enrichment, case management, and response. The lab simulates real-world attack scenarios using Mimikatz on a Windows 11 endpoint to validate detection engineering and end-to-end SOC workflows. The environment was designed using a two-VM Azure architecture with secure networking and controlled access, demonstrating hands-on experience in SOC operations, cloud security, and security automation.
- Key technical implementations:
  - Deployed and configured Wazuh SIEM for log collection, alerting, and detection engineering
  - Implemented custom detection rules and validated alerts using attack simulation techniques
  - Integrated Shuffle SOAR to automate alert ingestion, enrichment, and response workflows
  - Enriched indicators of compromise (IOCs) using VirusTotal threat intelligence
  - Configured TheHive for incident tracking and case management

    - Designed secure Azure networking and firewall rules (NSGs) to restrict access
    - Enabled analyst-approved response actions to balance automation with human oversight
- GitHub link: https://github.com/lilmilo2704/SOC-automation-lab-on-Microsoft-Azure

Hands-on Cybersecurity Lab: Intrusion Detection & Prevention with Snort

- Description: This is a lab project for the subject Cybersecurity - 48730 at UTS. In this lab, I completed a practical cybersecurity lab focused on configuring and operating Snort, an open-source Intrusion Detection and Prevention System (IDS/IPS), in a simulated attack–defense environment using separate Server and Attacker virtual machines.
- Key tasks:
    - Configured Snort core settings (HOME_NET, rule paths) and validated configurations using test mode
    - Wrote and deployed custom Snort rules to detect and log malicious traffic, including ICMP packets, web access requests, ICMP Source Quench attacks, SSH, and Telnet connection attempts
    - Operated Snort in both IDS mode (console alerts) and IPS mode (actively rejecting connections)
    - Triggered real attacks (ICMP ping, web requests, SSH/Telnet attempts) from an attacker VM and verified detection through Snort alerts and log analysis
    - Analyzed alert timestamps using Unix epoch conversion and inspected packet captures for forensic understanding
- Technologies:
    - VMware
    - Ubuntu Linux
    - Snort

EXPERIENCE

AI Model Evaluator, DataAnnotation **Dec 2025 - present**

- Evaluated and improved AI-generated outputs across text, code, reasoning, and creative tasks to support the training and refinement of large language models (LLMs).
- Reviewed, generated, and validated Python, JavaScript, and SQL code produced by AI systems, ensuring logical correctness, efficiency, and adherence to requirements.
- Conducted fact-checking and hallucination detection
- Provided structured human feedback to improve LLM quality and reliability.

Cybersecurity Analyst Intern, KhaiFrost **Jan 2026 - Feb 2026**

- Completed a mentored internship gaining hands-on experience in enterprise IT infrastructure and information security operations
- Supported virtualisation technologies and virtual machine deployment in a professional environment
- Assisted with enterprise network design, implementation, and configuration
- Worked with cloud-based storage solutions and data management
- Applied information security principles and best practices to ensure secure access, system reliability, and data protection

Teaching Assistant, Le Hong Phong high school for gifted **2022 - 2023**

- Assist teachers to delivery the content of Computer Science subject for high school students as a peer helper, improve their final grade by 30%.
- Applying Excel and Python to make reports about students' grades and analyse them to help teacher to monitor the students' performance.

ADDITIONAL INFORMATION

- **Languages:** Vietnamese, English
- **Certifications:** Canvas WIL (issued by UTS), Cybersecurity Essentials (issued by IBM), Generative AI with Large Language Models (issued by DeepLearning.AI), Introduction to Machine Learning (issued by AWS)