# DANG DUC TAI

**DevOps & SOC Engineer**

Binh Tan, HCM City  dangductai6410@gmail.com  (+84) 828 644 926

linkedin.com/in/ddducktai  github.com/ddducktai  ddducktai.dev

## EXPERIENCES

**SOC Intern - Cybersecurity and Network Security Center, at UIT** *Jun 2025 – Sep 2025*

- Deployed and monitored a K6 distributed testing system on Kubernetes integrating Kafka, Telegraf, InfluxDB, and Grafana
- Configured Loki, Prometheus, and Grafana dashboards for centralized log and performance monitoring
- Automated deployments with Helm and managed persistent storage using Longhorn and MinIO
- Implemented High Availability and autoscaling for WordPress–MariaDB workloads
- **Tools Used:** Kubernetes, K6, Kafka, InfluxDB, Grafana, Prometheus, Loki, Helm, Longhorn, MinIO

## SKILLS

- **Programming Languages & Scripting:** Python, C/C++, C#, Bash, JavaScript
- **DevOps & Cloud:** Docker, Kubernetes, Microsoft Azure, Helm, AWS EC2, MinIO, Longhorn
- **Databases:** MySQL, PostgreSQL, MongoDB, Microsoft SQL Server
- **Operating Systems:** Linux, Windows Server
- **Security Tools:** Wireshark, Snort, Suricata
- **Soft Skills:** Teamwork, Problem-Solving, Adaptability, Time Management, Communication

## PERSONAL PROJECTS

**Deploy KVM Virtualization Tools (4 Main Scenarios)** . *Sep 2024 – Dec 2024*

- Built a simple internal network on VMWare consisting of 3 virtual machines using KVM virtualization
- Deployed one web server and one data server
- **Tools Used:** KVM, Linux, Django, Gunicorn, Nginx, MySQL

**Confidentiality and Access Control in Amazon RDS MySQL** . *Jan 2024 – May 2024*

- Implemented data encryption for SQL databases using AES-GCM-256
- Encrypted AES key with Ciphertext-Policy Attribute-Based Encryption (CP-ABE)
- Applied Attribute-Based Access Control (ABAC) to enforce fine-grained cloud access
- **Tools Used:** Amazon RDS, MySQL, AES-GCM-256, CP-ABE, ABAC

**Hybrid Intrusion Detection using Suricata and Machine Learning** . *Jan 2025 – May 2025*

- Built a test network to simulate cyberattacks
- Trained a machine learning model using the CICIDS2017 dataset
- Integrated the trained model into Suricata as a plugin for vulnerability detection
- **Tools Used:** Suricata, Python

**Detecting APT Attacks Based on Provenance Graph Analysis and Meta-Path Aggregated Graph Neural Networks** . *Jan 2025 – May 2025*

- Built and labeled heterogeneous provenance graphs from DARPA E3 logs
- Designed meta-paths to capture high-level semantics between entities (processes, files, network flows)
- Reconstructed attack paths to trace malicious behaviors
- Applied GNN-based classification to detect APT stages such as privilege escalation, code injection, C2 communication, and stealthy file operations
- **Tools Used:** Python, PyTorch Geometric, NetworkX, dgl, MAGNN, TinyBERT

## EDUCATION

**University of Information Technology - VNU-HCM** *2022 - 2026*

*Major in Cyber Security*

- GPA: 8.47/10 .

## CERTIFICATES

TOEIC RL: 730 *2022 - 2026*

## AWARDS

**Academic encouragement scholarship by UIT** . *Oct 2024*

*(*Top 10% of students in Cyber Security major)