

Le Duong Phi

CYBER SECURITY ENGINEER

Hanoi, Vietnam | phildhe160155@gmail.com | feeiuna.io.vn | github.com/fee-191 | linkedin.com/in/leduongphi191 | Born 19 Jan 2002

SKILLS

OPERATING SYSTEMS

Linux · Windows

NETWORKING

TCP/IP · OSI model

SIEM & OBSERVABILITY

Wazuh · ELK ·

Prometheus · Grafana ·

Zabbix

SECURITY TOOLS

Snort · ModSecurity ·

pfSense · Burp Suite ·

Acunetix

INFRASTRUCTURE & CLOUD

Proxmox · Docker ·

Kubernetes · AWS · OCI ·

GCP

SCRIPTING

Bash · Python

CI/CD

GitLab CI · GitHub

Actions · Jenkins

CERTIFICATIONS

CCNAv7 — Introduction to Networks

Cisco Networking Academy

Security Operations & Application Security

Coursera · (ISC)² curriculum

EDUCATION

BSc Information Security

FPT University Hanoi · 2021

– 2025

GPA 3.0 / 4.0

PROFILE

Cyber Security Engineer with a degree in Information Security (FPT University Hanoi) and over a year of experience running defensive operations for multi-cloud infrastructure and building security into a financial product from its early stages. Work spans security monitoring and incident investigation (SIEM, detection engineering, SOAR automation), infrastructure and cloud hardening, and Application Security / DevSecOps. Aiming to grow into a Security Engineer specialising in the operation of defensive systems and in application security.

EXPERIENCE

DevSecOps Engineer

07/2026 – present

Just Engineer

Full-stack security across product and infrastructure · DevSecOps focus

SECURITY OPERATIONS, INFRASTRUCTURE & CLOUD

- Operating security and performance monitoring (SIEM combined with infrastructure metrics); writing detection rules, reducing alert noise and standardising the investigation and traceback workflow
- Automating alert triage and IOC enrichment (SOAR) to shorten response time; writing operational runbooks and periodic security reports for stakeholders
- Hardening servers and internet-facing services; reviewing cloud permissions across AWS, OCI and GCP against least privilege, centralising secrets management and separating environments

DEVSECOPS & SECURE SDLC

- Embedding security controls shift-left: SAST, dependency scanning, secret scanning and infrastructure configuration checks running automatically in CI/CD, with gates tiered by severity
- Building secure coding standards and review checklists for sensitive flows (authentication, authorisation, transactions, personal data); delivering internal secure coding training — OWASP Top 10, threat modeling (STRIDE), abuse cases

Security Engineer (Blue Team)

09/2025 – 06/2026

Digital asset exchange project (for a bank)

Internal security team

MONITORING & INCIDENT INVESTIGATION (SOC)

- Built an on-premise SOC lab (network configuration, Wazuh installation and tuning, centralised log collection); contributed to research on the production SOC design on AWS
- Researched and built an Incident Response AI Agent (POC) — takes an alert, queries the SIEM, enriches IOCs and opens a ticket with a summary; every containment step requires human approval (validated across 3 scenarios: brute-force, cloud anomaly, data exfiltration)

APPLICATION SECURITY & DEVSECOPS

- Built the security pipeline (pre-commit → CI/CD → AI review) and a secure coding template (as a submodule) for the team's projects — two-tier CI blocking CRITICAL at merge request and warning on HIGH (SAST, secret and dependency scanning), with an AI bot reviewing each MR diff
- Designed and presented an internal Secure Coding workshop (~10 people including the CTO); authored Secure Coding, Trust Boundary (Zero Trust, NIST SP 800-207) and IAM guidance, mapped to ISO 27001

SOC Tier 1 Intern · NetNam

06/2025 – 07/2025

- Hands-on SOC Tier 1 practice — log analysis, alert triage, investigation workflow.

IT Operations & System Admin Intern · FSI Technology JSC

08/2023 – 12/2023

- Server/VPS operations (Ubuntu), Docker and Kubernetes; basic infrastructure incidents; DevOps pipeline support.

SELECTED PROJECTS

Security Handbook — bilingual technical documentation

Personal · 2025 – present · feeiuna.io.vn

17 chapters in Vietnamese and English, from fundamentals (networking, Linux, Windows & Active Directory, cryptography) to real operations (SIEM & logging, SOC/IR, network defence, cloud, containers, threat intel, GRC) — with runnable commands and configuration.

LynxGuard — Mini-SOC for web applications

Capstone, FPT University · 2024 · team of 4 · github.com/fee-191/lynxguard

SOC platform on a virtualised network segmented by pfSense — Wazuh, Snort, ModSecurity and Zabbix integrated for real-time intrusion detection and blocking, with Telegram bot alerting (Python); validated with Acunetix and Burp Suite.

CEX Incident Research — incident analysis

Personal · 2025 – 2026 · github.com/fee-191/cex-incident-research

Analysis of 31 exchange breaches (2014 – 2025, ~\$6.8B) — attack patterns, kill chain and MITRE ATT&CK mapping.