NETWORK SECURITY · SOC · SECURITY ENGINEERING

PHAM QUOC HUY

OPEN TO INTERN / FRESHER ROLES

CONTACT

EMAIL
huy2k57@gmail.com

PHONE
0778923371

LOCATION
Ho Chi Minh City, Vietnam

WEBSITE
phamquochuy.com

GITHUB
github.com/phamquochuydz

SKILLS

Networking

CCNA,TCP/IP, OSI Model, VLAN, VPN, ACL, Routing, Network Segmentation

Security Monitoring

Firewall, IDS/IPS, Threat Detection, Traffic Analysis, Incident Response Fundamentals

Tools

pfSense, Suricata, Wazuh, Splunk, Wireshark, tcpdump, Nmap, Burp Suite, Cisco Packet Tracer, GNS3

Automation & AI

n8n, Python, TCN, Transformer, Anomaly Detection

Cloud & DevOps

Vercel Deployment, Supabase, PostgreSQL, Prisma, GitHub

EDUCATION

HUFLIT

Bachelor of Cybersecurity

Sep 2023 – Present

`GPA: 3.26 / 4.0`

CERTIFICATIONS

ACMN
Microsoft System Administration
Athena

ACBN
Computer Networking Fundamentals
Athena

PROFESSIONAL SUMMARY

Cybersecurity student at HUFLIT with hands-on experience in network security, security monitoring, IDS/IPS deployment, and security automation. Experienced in building SOC lab environments using pfSense, Suricata, Wazuh, and n8n for threat detection and automated incident response.

Also interested in applying Deep Learning techniques such as TCN and Transformer for anomaly detection in network security logs. Seeking an Intern/Fresher Network Security or SOC Analyst position.

SELECTED PROJECTS

PROJECT 01

SOC Monitoring & Security Automation

Built / In Progress

Built a SOC laboratory environment capable of monitoring, detecting, and automating responses to security incidents.

- Designed VLAN segmentation and pfSense firewall rules for monitored network zones.
- Deployed Suricata IDS and centralized host/security telemetry in Wazuh.
- Connected Wazuh detections to n8n workflows for automated incident alerts.

pfSense Suricata Wazuh n8n

Demo: Watch Demo ↗

PROJECT 02

AI-Driven Network Log Anomaly Detection System

Research + Prototype

Designed and developed an AI-powered anomaly detection pipeline for network security monitoring, combining temporal behavioral analysis, risk scoring, and automated alert generation to support SOC operations.

- Built a preprocessing pipeline using the UNSW-NB15 dataset with Label Encoding, StandardScaler, and temporal sequence generation.
- Implemented a Temporal Convolutional Network (TCN) model to learn network behavior patterns and identify anomalous activities.
- Developed a Behavioral Accumulation Engine to track suspicious activities over time instead of evaluating individual events in isolation.
- Designed a risk scoring mechanism combining base anomaly score, behavioral risk, and trend analysis.
- Classified threats into LOW, MEDIUM, HIGH, and CRITICAL severity levels for SOC prioritization.
- Prepared the architecture for integration with Kafka, Wazuh, and n8n-based automated response workflows.

Python PyTorch TCN Kafka Anomaly Detection Risk Scoring Behavior Analytics

PROJECT 03

Cloud-Native Full-Stack Deployment Platform

Production Ready / Live Demo

Designed, secured, and deployed a production-ready full-stack web platform using Next.js, Prisma, Supabase, and Vercel, focusing on cloud deployment workflow, database migration, environment configuration, and application security hardening.

- Configured a GitHub-to-Vercel deployment workflow with production environment variables and deployment log debugging.
- Migrated the application from local PostgreSQL to Supabase PostgreSQL using Prisma migrations.
- Managed environment variables, database connection strings, authentication secrets, and production configuration.
- Applied CSRF protection, rate limiting, secure cookies, input validation, security headers, tenant isolation, and production-safe error handling.
- Implemented secure authentication, session validation, protected routes, session revocation, and access control.
- Deployed a publicly accessible production environment on Vercel.

Next.js TypeScript Prisma Supabase PostgreSQL Vercel GitHub Cloud Deployment App Security

Live Demo: https://plan-pocket.vercel.app/