Nguyen Van Tien Phat

0976 459 403 nguyenphat0976459403@gmail.com
tienphat.tech Ho Chi Minh City, Vietnam

PROFESSIONAL SUMMARY

Cybersecurity student pursuing a career in security operations, with hands-on experience configuring network and monitoring infrastructure, analyzing security logs, and automating incident response workflows. Experienced with Kaspersky KUMA, Wazuh, Suricata, pfSense, and n8n. Seeking a SOC Intern or Security Analyst role to strengthen detection engineering skills and contribute to enterprise security operations.

EDUCATION

HCMC University of Foreign Languages - Information Technology (HUFLIT) **09/2023 - Expected 03/2027**
Cybersecurity, Faculty of Information Technology *Ho Chi Minh City, Vietnam*

WORK EXPERIENCE

Confidential Technology Company **01/2026 - 05/2026**
SOC Intern *Ho Chi Minh City, Vietnam*

- Deployed and configured Kaspersky KUMA SIEM to monitor Apache and Nginx web server logs; developed correlation rules to detect DDoS activity, web scanning, and website defacement.
- Built attack-scenario proofs of concept and corresponding monitoring use cases to validate SOC infrastructure and detection coverage.
- Authored incident response playbooks and swimlane workflows aligned with NIST SP 800-61 Rev. 2.

SELECTED PROJECTS

SDN Centralized Log Collection System **03/2026 - 05/2026**

- Built a software-defined networking lab with **Mininet** and the **Ryu Controller**.
- Developed a centralized log ingestion pipeline for virtual switches and routers, providing consistent visibility across the SDN environment.
- **Outcome:** Improved traffic monitoring and enabled earlier detection of anomalous behavior across the SDN infrastructure.

Enterprise SOC Monitoring & SOAR System **10/2025 - 11/2025**

- Segmented the network with VLANs on **pfSense** and implemented **WPA2-Enterprise** authentication with FreeRADIUS.
- Deployed **Suricata** in inline mode to detect and automatically block DDoS activity and Nmap scans.
- Created **Wazuh SIEM** rules for centralized monitoring and detection of rogue DHCP and SSH brute-force activity.
- Automated incident response with **n8n**, including risk scoring, Telegram alerts, and malicious IP blocking on the firewall.
- Developed a real-time security monitoring dashboard with **ReactJS** and **Supabase**.
- **Outcome:** Delivered a closed-loop SOC prototype that detected and blocked simulated attacks within seconds.

TECHNICAL SKILLS

Security Monitoring & SOC Operations: SIEM (Wazuh, KUMA), log analysis (Sysmon, Windows Event Logs, Syslog), IOC identification, and security alert configuration.

Security Tools & Automation: Firewalls and routing (pfSense, iptables), IDS/IPS (Suricata), network authentication (FreeRADIUS), SOAR and integration (n8n), Docker, and Docker Compose.

Systems & Networking: Windows Server (Active Directory, DNS, DHCP, GPO), basic Linux administration, OSI model, and TCP/IP fundamentals.

Programming & Databases: C#, Java, JavaScript, Python, and Supabase.

LANGUAGES

English: Intermediate proficiency; comfortable reading technical documentation.