Nguyen Truong Bao

0937 420 973 bigzero3939@gmail.com https://www.linkedin.com/in/nguyen-truong-bao-347437250/ Da Nang

PROFESSIONAL SUMMARY

Information Security student with hands-on experience in SIEM deployment, security monitoring, network infrastructure, and web application security assessment. Experienced with Wazuh, Suricata, pfSense, and Python automation through academic and internship projects. Currently pursuing CCNA and practical blue-team training through Hack The Box. Seeking an entry-level SOC Analyst, Cybersecurity Analyst, or Network Security Engineer position.

EDUCATION

DUY TAN UNIVERSITY | Da Nang, Vietnam Expected Graduation: - **2027**

- Cyber Security

Relevant Coursework: Computer Networks, Network Configuration, Network Security, Digital Forensics & Incident Response.

TECHNICAL SKILLS

Security:	• Wazuh SIEM • Suricata IDS/IPS • Burp Suite • Wireshark • Nmap • Kali Linux
Networking:	• Routing & Switching • VLAN • Inter-VLAN Routing • STP • OSPF • ACL • NAT/PAT • Subnetting & VLSM
Programming :	Python, Bash Scripting.
Code Review (Understanding):	PHP, HTML, JavaScript, Java.

PROFESSIONAL EXPERIENCE

FORE-Z 09/2024 - 09/2025

Cybersecurity Research Intern

- Conducted deep-dive source code review of WordPress PHP plugins to explicitly identify logic flaws, SQL Injection (SQLi), and Cross-Site Scripting (XSS) vulnerabilities.
- Executed targeted vulnerability assessments using manual techniques and automated scanning tools within simulated testing environments.
- Documented findings by authoring comprehensive internal vulnerability analysis reports outlining remediation steps for discovered weaknesses.

PROJECTS

AI-APW: AI-Powered Alert Prioritization for Wazuh | Capstone 1 08/2025 - 12/2025

Backend & DevOps Engineer

• Designed and deployed a simulated enterprise security environment consisting of WAN, LAN, and DMZ segments using pfSense Firewall, Wazuh SIEM, Suricata IDS/IPS, Ubuntu Server, and Kali Linux.
• Developed Python FastAPI services to automatically collect, normalize, and process security events from Wazuh Indexer for centralized analysis.
• Built an AI-assisted alert prioritization module that classifies security events such as SQL Injection, XSS, Brute Force, LFI, and DoS attacks, reducing manual triage workload.
• Implemented event correlation logic to identify multi-stage attack patterns by analyzing source IPs, destination assets, and attack timelines across multiple log sources.
• Integrated automated Telegram notifications for high-severity incidents, enabling real-time alert delivery to analysts and reducing response time.
• Participated in infrastructure deployment, SIEM tuning, detection rule validation, and attack simulation within a controlled lab environment.

Personal SOC & Network Security Lab -

• Built and maintained a cybersecurity home lab using VMware Workstation.
• Deployed Wazuh SIEM, Suricata IDS/IPS, pfSense Firewall, Ubuntu Server, Kali Linux, and Windows endpoints.
• Configured VLANs, Inter-VLAN Routing, OSPF, ACLs, NAT/PAT, and DMZ segmentation.
• Simulated brute force, SQL injection, XSS, and network scanning attacks for security monitoring and incident investigation.
• Practiced log analysis, alert triage, rule tuning, and threat detection using Wazuh dashboards and custom detection rules.

CERTIFICATIONS & TRAINING

Google Cybersecurity Professional Certificate	Dec 31, 2024
Cisco Certified Network Associate (CCNA)	(In Progress – 70%)
Hack The Box Certified Junior Cybersecurity Analyst Path	(In Progress – 60% Completed)
PortSwigger Web Security Academy	(80% Labs Completed)

LANGUAGES

Vietnamese – Native Proficiency

English – Intermediate Working Proficiency
• Strong reading and listening comprehension
• TOEIC Mock Test: 665