NGUYEN TAI TRUNG

SOC ANALYST INTERN | BLUE TEAM INTERN

CONTACT

☎ (+84) 354 981 667

nguyentaitrung26704@gmail.com

Thành phố Hồ Chí Minh

github.com/TrungNguyenZzZ

TECHNICAL SKILLS

- Network Security: Firewalls, VPN, IDS/IPS.
- SIEM: Wazuh, Elastic Stack (Elasticsearch, Logstash, Kibana).
- Threat Detection: SQLi, XSS, brute-force.
- Encryption: IPSec, SSL/TLS.
- Incident Response: Detection and mitigation.
- Security Programming: Python, Shell scripting.

SOFT SKILLS

- Communication
- Analytical Thinking
- Teamwork
- Problem-Solving
- Time Management
- Willingness to Learn

LANGUAGES

- English

SUMMARY

Motivated Cybersecurity student eager to apply theoretical knowledge and hands-on skills in a real-world Security Operations Center (SOC) environment. Seeking an internship opportunity to gain experience in attack detection, log analysis, and incident response, while contributing to a professional security team. Passionate about learning and developing expertise in cybersecurity practices.

PROJECT

SOC Mini Lab - Wazuh & Elastic SIEM 2025 - PRESENT

Description:

- Deployed SIEM system using Wazuh and Elastic Stack to collect and analyze logs from Linux servers.
- Simulated real-world attacks: SSH brute-force, SQL Injection (SQLi), Cross-Site Scripting (XSS), and File Integrity Monitoring (FIM).
- Analyzed alerts on Kibana Dashboard, tuned detection rules, and set up automated email alerts.
- Evaluated detection effectiveness using metrics like Precision, Recall, Latency.

Zero Trust Security Architecture 2024-2025

Description:

- Implemented a Zero Trust model using Keycloak (IAM) and OPA for access control and continuous user behavior monitoring.
- Integrated Zero Trust security model with existing security systems for enhanced protection.
- Managed user access policies and monitored user behavior to ensure continuous authentication and access control.
- Improved overall system security by applying Zero Trust principles to protect sensitive resources.

IPSec / VPN Implementation (Lab) 2024

Description:

- Implemented Site-to-Site VPN using IPSec/L2TP to secure remote office connections.
- Configured IPSec to encrypt and protect data during transmission over untrusted networks.
- Verified VPN security using Wireshark to ensure encryption and packet security.

EDUCATION

HUTECH University of Technology, Ho Chi Minh,city 2025