Hoang Nguyen Dat

☎ 0362912783 ✉ dathn.254@gmail.com 🔗 https://radd254.github.io 📍 Hà Nội

CAREER OBJECTIVE

Seeking to develop a career in **Security Operations Center (SOC)**, starting in an **Intern / Junior SOC Analyst** role with responsibilities in monitoring, analyzing, and handling basic security events. Aiming to become a cybersecurity professional capable of operating and optimizing enterprise security systems and solutions, while contributing to the development and improvement of security monitoring and incident response processes.

EDUCATION

FPT University 10/2022 - Present

Major: **Information Assurance**

Cumulative GPA: **3.2 / 4.0**

WORK EXPERIENCE

CSP Technology and Solutions JSC 01/2025 - 04/2025

Security Intern (WAF)

- Assisted in configuring and managing **Web Application Firewall (CSP-WAF)** for internal web applications.
- Built and tested detection rules for common web attacks, including **SQL Injection, XSS, Directory Traversal**, and other **OWASP Top 10** vulnerabilities using simulated attack scenarios.
- Analyzed WAF logs, identified **false positives / false negatives**, and fine-tuned rules to improve detection accuracy while minimizing impact on legitimate users.

PERSONAL PROJECTS

Home Lab – SOC Mini for Web & Firewall Monitoring 08/2025 - 10/2025

Web and Firewall Log Monitoring with Splunk

- Designed a secure home lab network architecture (**DMZ**) including **FortiGate Firewall, Ubuntu Web Server, and Splunk Enterprise**.
- Configured the firewall to forward web and security logs to Splunk for centralized collection and analysis.
- Performed initial log analysis to identify **source IPs, attack timelines, attack vectors, and impact levels**.
- Report: https://hackmd.io/@raymond25/HyGp8fsb-e

Building a SOC Lab with OpenVAS Integration 09/2025 - 11/2025

Integrating SOC with OpenVAS for Vulnerability Monitoring

- Built a SOC lab model using **Splunk SIEM** integrated with **OpenVAS** for vulnerability scanning and management.
- Developed a data pipeline to ingest vulnerability scan results (**CVE, severity, affected hosts**) into SIEM and created dashboards to track risk-based vulnerability status.
- Simulated a SOC workflow: correlating scan results, prioritizing vulnerabilities by risk, and mapping vulnerabilities to security events.
- Proposed remediation approaches and risk mitigation strategies for lab systems.
- Currently optimizing OpenVAS scan configurations and workflows to enhance vulnerability assessment accuracy and efficiency.
- Report: https://hackmd.io/@raymond25/Hye4IRYZZe

SKILLS

Operating Systems	Windows, Windows Server, Linux (Ubuntu, Kali-Linux, CentOS)
Security & Monitoring Tools	SIEM & Monitoring: **Splunk, Wazuh** Firewalls: **FortiGate, pfSense** Analysis & Investigation: **Wireshark, Process Monitor, FTK Imager**
Programming & Scripting	Python, Java, C, Bash script.

CHỨNG CHỈ

CCNAv7: Introduction to Networks – (Cisco Networking Academy)	11/2023
ISC2 Systems Security Certified Practitioner (SSCP) Specialization – (ISC2, Coursera)	05/2025