Trần Hoàng Phúc

SOC Analyst Internship

Dob:	2003/10/02
Gender:	Male
Phone:	0901445362
Email:	phucphuctran23@gmail.com
Website:	https://thp23.hashnode.dev/
Address:	Linh Đông, TP.Thủ Đức

OBJECTIVE

I have always been interested in investigating security threats, which led me to study Network Security Monitoring. I hope to gain more experience in this field by working in a real-world environment. This will help me improve my skills and allow me to continue learning and growing in cybersecurity.

SKILLS

- SIEM Monitoring Fundamentals (Splunk, ELK)
- Threat Detection & Analysis (Cyber Kill Chain, MITRE ATT&CK, Pyramid Of Pain)
- Linux & Windows Fundamentals
- Web Application Security (OWASP Top 10)
- Windows Server Fundamentals
- Endpoint Security Fundamentals (Sysmon, Windows Event Logs)
- Network Security Fundamentals (IDS/IPS, Packet Analysis)
- Programming Languages (Python, Java)

PROJECTS

03/2025 - 03/2025

Cyber Threat Intelligence Platform Deployment (OpenCTI)

Deployed OpenCTI using Docker to build a centralized threat intelligence platform. Integrated OSINT feeds and STIX/TAXII sources to enrich threat data. Created structured objects (indicators, malware, attack patterns) and documented threat infomation releated to the BazazLoader malware campaign, including TTPs aligned with the MITRE ATT&CK framework.

02/2025 - 02/2025

Endpoint Threat Detection using Splunk & Sysmon

Configured Sysmon on Windows endpoints to collect detailed event logs, including process creation and network activity. Forwarded logs to Splunk for storage and basic search capabilities. Focused on data visibility and event categorization as preparation for building detection use cases.

03/2025 - 03/2025

Ransomware Detection Lab using Wazuh

Deployed a lab environment using Wazuh to explore endpoint visibility and threat detection capabilities. Simulated ransomware-like behavior and monitored alerts generated by default Wazuh rules. Focused on log analysis, rule tuning, and learning the detection flow for common ransomware techniques.

EDUCATION

2021 - 2025

Van Lang University

MAJOR: Information Technology

GPA: 7.22/10

HONORS & AWARDS

10/2024

Vietnam Information Security Student Contest 2024 – Participant

INTERESTS

- Reading Cybersecurity News & Staying Updated on Threats
- Learning English.
- Following Cybersecurity Blogs, Reports, and Threat Intelligence Feeds