



# PHAM HUYNH KHANH LINH

SOC Analyst Intern (Tier 1)

**Dob:** 01/03/2005

**Gender:** Female

**Phone:** 0392980607

**Email:** phamkhanhlinh103@gmail.com

**Address:** Thu Duc District, Ho Chi Minh City

## CAREER OBJECTIVE

Seeking to start my career as a SOC Tier 1 Analyst, focusing on security monitoring, log analysis, and initial incident handling on SIEM platforms. My goal is to continuously enhance my analytical skills, deepen my understanding of systems and SOC processes, and gradually progress to the role of SOC Tier 2/ Security Analyst.

## EDUCATION

2023 - Present

**Ho Chi Minh City University of Technology and Engineering (HCMUTE)**

Major: Information Security

Academic Activities:

- Participated in scientific research projects.
- Participated in Capture The Flag (CTF) competitions.

## PROJECTS AND PRACTICAL EXPERIENCE

Jan 2026 - Present

**Scientific Research Project**

**Project Title: Design and implementation of a smart boarding house system integrating Two-Factor Authentication (2FA), AI Camera- based behavior monitoring, and SIEM security management.**

Responsibilities:

- Researched 2FA, AI Camera, SIEM technologies, and existing IoT models.
- Deployed and configured Snort IDS integrated with SIEM (ELK Stack/ Wazuh) in a virtualized environment.
- Collected, searched, and analyzed logs from systems and devices for security monitoring.
- Participated in writing a scientific paper published in an international conference with ISBN/ ISSN.

## SKILLS

Systems and Networking

Fundamental knowledge of computer systems and networking.

Experience with Windows and Linux for monitoring and incident analysis.

Security Monitoring and Incident Handling

Hands-on experience in monitoring systems and security events.

Capable of identifying and handling security incidents at an initial level.

SIEM & Log Analysis

Practical experience using SIEM (Splunk) and ELK Stack to collect, search, and analyze logs.

SOC Tier 1 Process

Understanding and practicing SOC Tier 1 workflows, including monitoring, alert triage, and incident escalation.

Supporting Skills

Ability to read and understand technical documentation in English.

Teamwork collaboration skills.

Careful, proactive, and able to work under pressure.