LAI QUAN THIEN

SOC ANALYST

Thu Duc, Ho Chi Minh City • Thienlai159@gmail.com • 0941 841 870
Portfolio: wanthinnn.github.io • GitHub: github.com/WanThinnn • LinkedIn: linkedin.com/in/WanThinnn

SUMMARY

Information Security student specializing in SOC operations, SIEM/SOAR engineering, and cryptography. Experienced in threat detection, incident response, and secure data processing. Skilled in building centralized cyber-attack event management systems to enhance organizational security posture.

EDUCATION

University of Information Technology, Vietnam National University, Ho Chi Minh City
Bachelor of Information Security | GPA: 8.53/10 | Academic Years: 10/2022 – 03/2026 (Expected)

Huynh Man Dat High School For The Gifted, Rach Gia Ward, An Giang Province
Specialization: Information Technology | Specialized Subject GPA: 9.6/10 | Academic Years: 09/2019 – 07/2022

TECHNICAL SKILLS

- **Programming Languages:** Python, C/C++, Bash
- **Featured Security Tools:** Security Onion, Elastic Stack, DFIR-IRIS, Suricata, Zeek, pfSense, IntelOwl
- **Cryptography Libraries:** CryptoPP, OpenSSL, Charm-Crypto
- **Cloud:** AWS (EC2, S3, RDS)**,** Firebase (Realtime Database, Firestore)
- **Operating Systems & Virtualization:** Kali Linux, Ubuntu, Windows, macOS; VMWare, KVM
- **Core Expertise:** SOC Operations, SIEM/SOAR Engineering, Cryptography, AI-powered Analysis and Secure Data Processing
- **Security Frameworks**: ISO 27001, ISO 27002, MITRE ATT&CK
- **Offensive & Testing Tools**: Metasploit Framework, Kali Linux Tools
- **Languages**: Vietnamese (Native), English (Basic)

CERTIFICATIONS

Google Cybersecurity Google IT Support Office of the CISO Institute: Cybersecurity Essentials

PROFESSIONAL EXPERIENCE

WORK EXPERIENCE

SOC Engineering Intern, VNU-HCM - Certified Network Security Center, 09/2025 – Present

- **Responsibilities:**
  - Participated in designing and building the SOC environment, including log pipelines, alerting flows, and monitoring dashboards.
  - Assisted in deploying and configuring SIEM/SOAR components and network security tools. Supported incident analysis, alert triage, and improvement of detection rules.
  - Contributed to documentation, system optimization, and internal SOC procedures.
- **Tools & Platforms:** Elastic Stack (ELK), Wazuh, Suricata, Zeek, DFIR-IRIS, IntelOwl, MISP, n8n.

PERSONAL PROJECT

Hybrid CP ABE Library, 09/2024 – Present

- **Project**: Hybrid Ciphertext Policy Attribute Based Encryption Library for C/C++
- **Github:** github.com/WanThinnn/Hybrid-CP-ABE-Library
- **Description:** Developed a cross-platform C/C++ library implementing the CP-ABE AC17 scheme combined with AES-GCM-256 for hybrid encryption.
- **Technologies:** C/C++, CryptoPP, rabe-ffi; static & shared libraries.

- **Responsibilities:** Designed, optimized, and implemented hybrid CP-ABE AC17 + AES-GCM-256 library in C++, built and tested cross-platform; documented for developers.

FEATURED TEAM PROJECTS

1. Bachelor's Thesis, 09/2025 – Present (Leader)

- **Project*:*** An Intelligent SOC Ecosystem for Monitoring, Detection, and Response to Cyber Attacks
- **Website:** cyberfortress-labs.github.io
- **Github:** github.com/Cyberfortress-Labs
- **Description:** Research and Implementation of an intelligent SOC ecosystem combining SIEM, SOAR, and SmartXDR—an AI-enhanced OpenXDR model—to reduce false positives, improve detection accuracy, and automate incident response.
- **Technologies:** Elastic Stack, SOAR Stack (DFIR-IRIS/IntelOwl/MISP/n8n), SmartXDR (AI-assisted OpenXDR), Network/Security Tools (Wazuh, Suricata, Zeek, pfSense, ModSecurity), Nginx Web Server, VMware Workstation Pro.
- **Responsibilities:** Led the design and deployment of an intelligent SOC ecosystem integrating SIEM, SOAR, and SmartXDR. Built the data pipeline, configured key log sources (pfSense, Suricata, Zeek, Wazuh), and integrated AI-assisted SmartXDR for semantic alert analysis. Developed automated SOAR playbooks. Managed team coordination and project documentation.

2. SIEM Project, 01/2025 – 07/2025 (Leader)

- **Project*:*** Research and Implementation of a Centralized Management and Processing System for Cyber Attack Events
- **Github:** github.com/WanThinnn/SIEM-Central
- **Description:** Research and Implementation of a SIEM solution using the ELK Stack to collect, analyze, and visualize security events from Windows/Linux systems and tools like Suricata, Zeek, pfSense in a simulated environment.
- **Technologies:** Elastic Stack, Network/Security Devices (Zeek, pfSense), Inline IDPS (Suricata), Nginx Web Server, VMware Workstation Pro.
- **Responsibilities**: Designed and deployed ELK-based SIEM ingesting logs from 6+ sources, built Kibana dashboards with MITRE ATT&CK detection rules, configured Suricata inline IDS/IPS with Zeek, pfSense, and reverse proxy, and tested detection with simulated attacks.

3. Security Onion IDS Project, 02/2025 – 06/2025 (Leader)

- **Project**: Research and Implementation of Commercial IDS Solution - Security Onion
- **Github:** github.com/WanThinnn/Security-Onion-IDS-Project
- **Description**: Implemented Security Onion for intrusion detection and network security monitoring, configuring core components like Suricata, Zeek, ELK Stack.
- **Technologies**: Security Onion, Suricata, Zeek, ELK Stack, Wazuh, pfSense.
- **Responsibilities:** Deployed and configured Security Onion in various network scenarios. Researched and analyzed NSM methodologies, focusing on full packet capture, intrusion detection, and alert data analysis.

SOFT SKILLS & ACTIVITIES

- Leadership & Teamwork: Led 10+ academic project teams; Secretary of Ho Chi Minh Communist Youth Union since 2019.
- Communication: Strong public speaking and technical presentation skills.
- Achievements: Received multiple commendations for academic very good and outstanding youth leadership (2022–2025).

INTERESTS

- Cryptography & Architecture: Applied & Post-Quantum Cryptography, Computer Architecture.
- AI in Security: Computer Vision, Biometrics, and Advanced Authentication Models.