LAI QUAN THIEN

Cybersecurity Engineer

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

I am a student majoring in Information Security, specializing in SIEM/SOC operations and Cryptography. I possess skills in threat detection, incident response, and secure data processing. I also understand how to implement centralized cyber-attack event management systems to strengthen an organization's defensive posture.

EDUCATION

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

Huynh Man Dat High School For The Gifted, Rach Gia Ward, An Giang Province
Specialization: Information Technology; Academic Years: 09/2019 – 07/2022
Specialized Subject GPA (3-year average): 9.6/10

TECHNICAL SKILLS

- **Programming Languages:** C/C++, C#, Python
- **Security Tools:** Security Onion, ELK Stack, Suricata, Snort, Zeek, pfSense
- **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:** SIEM/SOC Operations**,** Cryptography, Secure Data Processing
- **Compliance:** ISO 27001, ISO 27002, MITRE ATT&CK, Metasploit Framework
- **Languages**: Vietnamese (Native), English (Basic)

CERTIFICATIONS

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

PROFESSIONAL EXPERIENCE

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.git
- **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.

TEAM PROJECTS:

1. 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.git

- **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 (ELK), 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.

2. 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.git
- **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.

3. Cryptography Project, 02/2024 – 07/2024 (Leader)

- **Project:** Confidentiality and Access Control in Amazon RDS MySQL
- **Github**: github.com/WanThinnn/Cloud-RDS-Crypto-Access.git
- **Description:** Research and implementation of a multi-layered database encryption system using AES-GCM-256 and CP-ABE (AC17) on Amazon RDS MySQL. Sensitive columns were encrypted with AES, while key access was enforced via CP-ABE and ABAC.
- **Technologies**: Python 3, AES-GCM-256, CP-ABE, bcrypt, ABAC, OpenSSL, PBC, GMP, Charm-Crypto, Amazon RDS MySQL, MongoDB.
- **Responsibilities**: Led project planning and team coordination; designed and implemented AES-GCM + CP-ABE hybrid encryption for RDS MySQL with secure configuration and optimized performance.

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:
  - Academic Achievements: Received Certificates of Commendation for Very Good academic performance and extracurricular involvement (2022–2025).
  - Youth & Leadership Achievements: Recognized for outstanding contributions to Youth Union activities and exemplary youth leadership in 2022–2024.

INTERESTS

- Emerging technology trends, computer architecture, applied cryptography and post-quantum cryptography
- Computer vision and image processing for security applications
- Biometric authentication systems and advanced security models