LAI QUAN THIEN

Security Operations Center Analyst Intern

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: 8.51/10

Huynh Man Dat High School For The Gifted, Rach Gia City, Kien 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 Platforms & SIEM:** Security Onion, ELK Stack, Suricata, Snort
- **Cryptography Libraries:** CryptoPP, OpenSSL, Charm-Crypto
- **Cloud:** AWS (EC2, S3, RDS)**,** Firebase (Realtime Database, Firestore, Authentication)
- **Operating Systems & Virtualization:** Kali Linux, Ubuntu, Windows, macOS; VMWare, KVM
- **Core Expertise & Specializations:** SIEM/SOC Operations**,** Cryptography**,** Threat Detection, Incident Response, Secure Data Processing
- **Compliance & Frameworks:** ISO 27001, ISO 27002, MITRE ATT&CK, Metasploit Framework
- **Productivity**: Microsoft 365 Suite, Apple iWork, Google Workspace
- **Languages**: Vietnamese (Native), English (Basic)

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:**
  - **Languages & Build Tools:** C/C++, Visual Studio, g++ on Ubuntu 22.04
  - **Cryptography Libraries:** CryptoPP, Rabe-ffi
  - **Packaging:** Static & shared libraries, VSCode tasks.json
  - **OS Environments:** Windows, Linux
- **Responsibilities**
  - Designed, optimized and implemented CP-ABE AC17 key generation, encryption, and decryption routines.
  - Built and configured cross-platform build using cl.exe and g++
  - Tested library functionality with demo CLI validated correct policy enforcement and interoperability.
  - Documented build and usage instructions in README for seamless developer onboarding.

TEAM PROJECTS:

1. SIEM Project, 01/2025 – Present (Leader)

- **Project***:* Research and Implementation of a Centralized Management and Processing System for Cyber Attack Events *(In Progress)*
- **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 and pfSense in a simulated environment.

- **Technologies:** Elastic Stack (ELK), Network/Security Devices (pfSense), Inline IDPS (Suricata), Nginx Web Server, VMware Workstation Pro.
- **Responsibilities:**
  - Designed and deployed a full-stack SIEM using ELK Stack. Integrated logs from Windows, Linux, pfSense, and Suricata for real-time monitoring.
  - Developed Logstash pipelines to parse and normalize diverse log formats.
  - Configured Suricata in Inline IDS/IPS mode with custom rules.
  - Built Kibana dashboards and detection rules aligned with MITRE ATT&CK.
  - Simulated attacks (e.g., ICMP Flood, SSH Brute Force) to test detection accuracy.

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

- **Project:** Confidentiality and Access Control in Amazon RDS MySQL
- **Github**: github.com/WanThinnn/Cryptography-Project.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**:
  - **Frontend:** PyQt6
  - **Backend:** Python 3.10.11, MySQL Connector, PyMongo
  - **Encryption & Access Control:** AES-GCM-256, CP-ABE-AC17, Bcrypt, Py-ABAC
  - **Cryptography Libraries:** OpenSSL, PBC, GMP, Charm-Crypto
  - **Databases:** Amazon RDS MySQL, MongoDB
  - **Operating Systems:** macOS, Linux
- **Responsibilities**:
  - Led project planning, task assignment, and team coordination
  - Designed modular system architecture with security and performance optimizations
  - Implemented AES/CP-ABE hybrid encryption aligned with access policies
  - Deployed AWS RDS MySQL with secure configuration and encryption strategies

3. Networks and Systems Administration Project, 09/2024 – 02/2025 (Leader)

- **Project**: Virtualization with KVM
- **Github:** github.com/WanThinnn/NT132_Networks-And-Systems-Administration-Project.git
- **Description**: Researched and deployed KVM (Kernel-based Virtual Machine) as a Type-1 hypervisor on Linux, leveraging Virt-Manager, libvirt, and QEMU
- **Technologies**: KVM, QEMU, libvirt, Virt-Manager, Cloud-Init, SSH, virtual networks, TLS/SSL.
- **Responsibilities:** Led team in planning and coordinating deployment scenarios; compared KVM and VMware performance; built a virtual network with web and data servers.

4. Some other typical projects (Leader):

- Network Security Project: github.com/WanThinnn/NT140_Network-Security-Project.git
- Web and Application Security Project: github.com/WanThinnn/Goatlin.git
- ML for Information Security Project: github.com/WanThinnn/PagPassGPT.git
- Malware Modus Operandi Project: github.com/WanThinnn/MAGIC.git

SOFT SKILLS & ACTIVITIES

- Presentation Skills/Public Speaking
- Team Leadership: Organization, Coordination, Event Planning, Collaboration
- Leadership Experience:
  - Secretary of the Ho Chi Minh Communist Youth Union since 2019
  - Led various project teams during academic coursework, demonstrating strong leadership and problem-solving skills.
  - Worked as team leader for more than 10 course projects
- Achievements:
  - Received a Certificate of Commendation as an Information Security student for Very Good academic performance and extracurricular involvement during the 2022–2023, 2023–2024, and 2024–2025 academic years.
  - Received a Certificate of Commendation for outstanding contributions to Youth Union and Youth

Movement activities at University of Information Technology – Term 2022–2024

  - Received a Certificate of Commendation for being an Outstanding Youth Exemplifying Ho Chi Minh’s Teachings in 2023 and 2024 (Thanh Niên Tiên Tiến Làm Theo Lời Bác)

INTERESTS

- Passionate about technology trends, including smartphones, PC hardware, and computer architecture
- Highly interested in computer vision techniques applied in camera phones (image processing algorithms, Apple image processing technologies, etc.)
- Curious about biometric authentication technologies (e.g., Face ID, Touch ID, under-display fingerprint sensors, iris recognition) and their underlying security models