LẠI QUAN THIÊN

CYBERSECURITY ENGINEER

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

SUMMARY

Entry-level Cybersecurity Engineer experienced in SIEM/SOAR/XDR deployment, applied cryptography, and threat detection. Skilled in building security monitoring environments, automating response workflows with AI, and developing secure data applications.

EDUCATION

University of Information Technology, Vietnam National University, Ho Chi Minh City
Bachelor of Information Security | GPA: 8.59/10 | Academic Years: 2022 – 2026

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: 2019 – 2022

TECHNICAL SKILLS

- **Core Expertise:** SOC, SIEM/SOAR/XDR, Cryptography, AI in CyberSecurity and Secure Data Processing
- **Security Frameworks:** ISO 27001, ISO 27002, MITRE ATT&CK
- **Featured Security Tools:** Security Onion, Elastic, DFIR-IRIS, Suricata, Zeek, pfSense, MISP, IntelOwl
- **Automation**: n8n, Docker
- **Programming Languages:** Python, C/C++, Bash
- **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
- **Offensive & Testing Tools**: Metasploit Framework, Kali Linux Tools
- **Languages**: Vietnamese (Native), English (B2 VSTEP)

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 – 12/2025

- **Responsibilities:**
  - Designed and built the SOC environment, including establishing log pipelines, alerting flows, and Kibana monitoring dashboards.
  - Deployed and configured SIEM/SOAR components and network security tools. Conducted incident analysis, alert triage, and optimized detection rules.
  - Engineered automated incident response workflows via n8n, integrating DFIR-IRIS, IntelOwl, and AI for automated IOC enrichment and report generation.
  - Analyzed 9M+ system logs (Q4/2025) to identify and extract 7,100+ valid security events; successfully tuned detection rules to reduce false-positive rates by 94%.
- **Tools & Platforms:** Elastic Stack (ELK), Wazuh, Suricata, ModSecurity, DFIR-IRIS, IntelOwl, MISP, n8n.

FEATURED TEAM PROJECTS

1. Bachelor's Thesis, 01/2025 – 02/2026 (Leader)

- **Project*:*** An Intelligent SOC Ecosystem for Monitoring, Detection, and Response to Cyber Attacks
- **Project Page:** cyberfortress-labs.github.io | **Github:** github.com/Cyberfortress-Labs

- **Description:** An advanced evolution of the SIEM Central project. Architected a comprehensive SOC ecosystem integrating SIEM, SOAR, and SmartXDR to drastically reduce false positives, improve threat detection accuracy, and automate incident response via LLMs.
- **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 team in designing and deploying the core SOC architecture and centralized data pipelines. Configured and ingested logs from key network/security sources.
  - Integrated LLM Models into the SmartXDR module for semantic alert analysis and automated log classification.
  - Developed and optimized automated SOAR playbooks to streamline incident triage and threat response.

2. SIEM Central 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.

PERSONAL PROJECT

Cloud Policy Crypto Access, 2025 – Present

- **Project**: Cloud Policy Crypto Access
- **Github**: https://github.com/WanThinnn/Cloud-Policy-Crypto-Access
- **Description**: An enterprise-grade secure file storage system featuring Hybrid CP-ABE and zero-trust multi-layer access control.
- **Technologies**: Django, C++, Hybrid CP-ABE, ABAC, Supabase, Redis, Docker, Shared library, HashiCorp Vault.
- **Responsibilities:** Engineered a zero-trust file management system featuring a Django backend API integrated with a custom C++ encryption library and an interactive SPA with a visual CP-ABE policy builder. The robust security architecture combines Hybrid CP-ABE, Casbin ABAC, and AES-256-GCM database encryption, utilizing HashiCorp Vault for centralized key management. Additionally, the entire system's performance and deployment were optimized using Supabase, Redis, and Docker.

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 strong academic performance 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.