

Nhat (Dinh) Phan

📍 Hanoi, Vietnam | @ contact@phannhat.com | ☎ +84 xx xxx xx xx | 🌐 phannhat.com

🌐 [linkedin.com/in/pdnhat](https://www.linkedin.com/in/pdnhat) | 🐙 github.com/phannhat17

Summary

Cybersecurity professional experienced across threat intelligence, SOC/IR operations, and enterprise security governance, backed by an offensive foundation from competitive CTF web exploitation and pentesting certifications (CPTS, CEH Master). Skilled at both hands-on technical analysis, reverse engineering malware and mapping C2 infrastructure, and the governance work of turning audit and incident findings into practical security improvements.

Experience

Cyber Threat Intelligence Analyst - Alice (Formerly ActiveFence) Hanoi, Jan 2026 – Now

- Track and dissect phishing campaigns targeting client platforms across four credential-theft delivery mechanisms: static kits exfiltrating harvested credentials to threat-actor Telegram bots, Browser-in-the-Browser (BitB) popups spoofing legitimate login windows, WebSocket-based kits that relay stolen credentials to attacker back-ends for real-time credential validation, and HTTP-polling (“HTTP live”) kits that receive commands and test captured credentials in near real time.
- Reverse engineer malicious browser extensions abusing client platforms, characterizing evasion techniques including CSP-header stripping with payload execution from invisible pixel images, runtime payload retrieval from C2 that defeats static analysis, and payload-less proxy extensions that open WebSocket channels to receive attacker commands.
- Analyze information-stealer malware end to end, from cookie theft on victim endpoints to abuse of client APIs for data collection and exfiltration to C2 infrastructure.
- Monitor underground marketplaces and threat-actor channels to surface emerging threats and deliver proactive intelligence notifications to affected clients.
- Extract IOCs, C2 infrastructure, and adversary TTPs into structured, client-facing intelligence reports mapped to MITRE ATT&CK.
- Built and operate CTI collection pipelines to accelerate detection, monitoring RSS and threat-actor sources for emerging campaigns and integrating urlscan.io and external CTI feeds via API for enrichment and pivoting.

Security Analyst Tier 3 - Viettel Cyber Security (rotation from Group HQ) Hanoi, Oct 2025 – Dec 2025

- Conducted Tier-3 threat hunting across Viettel’s group-wide infrastructure and client environments, targeting advanced threats, persistence mechanisms, and multi-stage attack chains.
- Led incident investigations through deep log analysis across endpoints, servers, and network layers, driving each case from detection to root-cause analysis and attacker TTP identification.
- Owned end-to-end incident response for advanced threats, from containment through post-incident findings.

Information Security Engineer - Viettel Group Headquarters Hanoi, Nov 2023 – Sept 2025

- Conducted enterprise-wide security audits across all Viettel business units in Vietnam (onsite) and remote audits of overseas subsidiaries, assessing compliance and security posture at scale.
- Authored and maintained the group-level information security regulation, the top-level policy governing all subordinate standards and procedures across the group, in alignment with international best practices.
- Investigated major cybersecurity incidents, globally and within the Viettel ecosystem, to extract lessons learned and risk implications.
- Conducted follow-up re-audits to verify remediation and drive units toward full compliance coverage.
- Translated audit and incident findings into actionable governance, control, and SOC/IR improvements.

Cybersecurity Intern - Viettel Digital Talent Hanoi, Jul 2023 – Oct 2023

- Selected as a **top 50 candidate**; researched NIST CSF and CIS Controls and contributed to internal security

policy development.

Skills

Threat Intelligence & Analysis: MITRE ATT&CK, malware analysis, C2 infrastructure analysis, phishing kit analysis, IOC extraction, TTP profiling, CTI data pipelines & ingestion (RSS monitoring, urlscan.io & CTI feed API integration, OpenCTI)

OSINT: urlscan.io, gitrecon, holehe, Epieos, Maigret, GitHub fork-network pivoting

Offensive Security: Web application pentest, CTF web exploitation, Burp Suite, Nmap, pwntools

Detection & Forensics: Threat hunting, log investigation, Sysmon, Wireshark, incident response

Systems & Scripting: Python, SQL, Docker, Linux

Languages: Vietnamese, English (TOEIC 865)

Achievements

Asean Cyber Shield 2025 - Busan, Korea

- Top 5 Overall (Student Division)
- Roles: Web Exploitation, Misc, Challenge Patch.

ASEAN Student Contest on Information Security (ASCIS)

- 2023: Attack-Defense Phase - Third Prize (9th place overall) - Roles: Web Exploitation, Misc; Attack and Patch challenge
- 2024: Attack-Defense Phase - Third Prize (4th place overall) - Roles: Web Exploitation, Misc; actively handled both Attack and Defense, including detection via logs, block rule adjustment.

PwC Hack A Day CTF 2024

- Second Prize
- Roles: Web Exploitation, Misc, AI jailbreak, OSINT.

Others international CTF tournaments - Main role: Web Exploiter

Projects

Phishkit Hunter (*in development*)

- OSINT tool crawling GitHub fork networks to identify phishing-kit source repositories, extract embedded Telegram bot tokens and chat IDs, and monitor victim-data exfiltration channels. Python / FastAPI backend with a vanilla JS front end.

Simple EDR System - [GitHub Repository](#)

- Designed and implemented a simple Endpoint Detection and Response (EDR) system, consisting of an EDR Agent and EDR Server.
- Built an EDR Server to aggregate logs from multiple endpoints, analyze suspicious activities, and enable remote threat response.

CTFd Docker Plugin - [GitHub Repository](#)

- A CTFd plugin that provides individual Docker containers per team for CTF competitions.
- Supports both local and remote Docker deployments with comprehensive container management.

Certificates

AWS Certified Solutions Architect – Associate - [Verify](#)

HTB Certified Penetration Testing Specialist (CPTS) - [Verify](#)

Certified Ethical Hacker (CEH) Master - [Verify](#)

Google Cybersecurity Specialization - [Verify](#)

NSE 1 Network Security Associate - [Verify](#)

NSE 2 Network Security Associate - [Verify](#)

Education

Hanoi University of Science and Technology, BS in Cyber Security

Sept 2021 – Jul 2025

- **Graduated:** July 2025 | GPA: 3.3/4.00
- **Degree classification:** Very Good
- **Coursework:** Computer Architecture, Network Defense, Malware Analysis, Digital Forensics

Referees

Mrs. Nguyen Thi Thu Huong - [Linkedin](#)

CISSP, IT Security Expert, Techcombank

More: Available upon request