LE PHAN HUU NGHIA (STEVEN)

SECURITY ENGINEER

0367364506 - Tan Ky Tan Quy, Tan Phu District, HCM city

17/08/2002 - https://github.com/Nghia-nee

nghialph2002@gmail.com

SUMMARY

Passionate about Defensive and Cloud Security with hands-on experience in log analysis, threat detection, and backend API development. Currently expanding expertise in cloud security controls, IAM, and compliance frameworks while contributing to security baselines and monitoring solutions. Aspiring to become a Cloud Security Consultant, combining technical depth with practical security governance.

EDUCATION

University of Information Technology Vietnam National University

Major: Information Security | Graduation: 2025

SKILLS

Technical: Python (API Development & Automation), Linux, AWS, Machine Learning (Research & Model Development)

Security: Threat Detection, Log Analysis, SIEM (Splunk → OpenSearch), IAM, Cloud Security Compliance

WORK EXPERIENCES

National Australia Bank (NAB) – Backend & Cloud Security (Team member)

May 2024 – Present

- Developed backend APIs using Python to support internal services.
- Participated in the migration of monitoring and logging infrastructure from Splunk to OpenSearch, ensuring system continuity and data integrity.
- Worked on Cloud Security Compliance, managing security controls and helping define Minimum Security Baseline (MSB) standards for internal systems.
- Collaborating on the upcoming implementation of CI/CD pipelines using Jenkins (in progress).

Viettel Cyber Security - Incident Response

Dec 2023 – Mar 2025

- Performed malware scanning and removal on compromised client machines.
- Monitored and analyzed security events to detect and respond to potential threats.
- Automated repetitive operational tasks using custom scripts, helping reduce manual workload.
- Conducted research on common web vulnerabilities and operating system architecture to support threat analysis.
- Developed proof-of-concept malware samples (Windows & Linux) to simulate real-world attacks for internal defense testing.
- Performed behavioral and static analysis on captured malware across different complexity levels.
- Published security research & write-ups here

PUBLICATION

PowerGNN: A source code structural and textual awareness approach for dentifying malicious PowerShell scripts

Published my first scientific paper on IEEE Xplore, presenting PowerGNN — a machine learning model that leverages Graph Convolutional Networks (GCN) and fastText embeddings to detect malicious PowerShell scripts through structural and textual feature analysis.

Practical applications: By applying the model to tools like firewalls or input checks on web services, it helps detect and prevent the impact of malicious PowerShell scripts.

Find out here

PROJECTS

Living-Off-The-Land Command Detection Using Active Learning

Building a framework capable of detecting commands that could potentially be exploited in a Living-off-the-land attack. We use word embedding models and machine learning to learn aggregated features from labeled commands.

Practical applications: Integrating the trained model into security solutions such as EDR or SIEM can enhance threat detection capabilities, reduce the risk of missing threats.

Find out here

ArkiCata: A defense system combining Arkime and Suricata for real-time warning

This project integrates Arkime with Suricata to create an effective network monitoring system. Arkime collects and stores network traffic, while Suricata acts as an Intrusion Detection and Prevention System (IDS/IPS) to detect and block threats, providing real-time alerts for unusual behavior.

Find out here

Baby Naming Web App

A web application built with Django framework that helps parents choose names for their children based on feng shui, considering factors like birth date, desired career, and more.

Find out here