SOC ANALYST · CYBERSECURITY · BLUE TEAM

NGUYEN CAO LAM

Security Monitoring · Threat Detection · Incident Response



OPEN TO SOC / SECURITY ROLES

CONTACT

EMAIL
1904caolam@gmail.com

PHONE
0937 025 017

LOCATION
Ho Chi Minh City, Vietnam

WEBSITE
nguyencaolam.info

GITHUB
github.com/1904caolam-tech

LINKEDIN
LinkedIn Profile

EDUCATION

HUFLIT

Bachelor of Information Technology

2023 – 2027 · Expected

Major: Cybersecurity

GPA: 3.2 / 4.0

LANGUAGE

English

Technical documentation and professional communication

CORE SKILLS

Security Operations

Security Monitoring, Alert Triage, Log Analysis, Threat Detection, Incident Response, MITRE ATT&CK

Security Tools

Wazuh, Suricata, Shuffle SOAR, Wireshark, pfSense

Network Security

Network Traffic Analysis, Firewall Rules, SDN Security, Ryu, Mininet, Mininet-WiFi

Systems & Cloud

Linux, Ubuntu, Windows Server 2022, Active Directory, AWS EC2, DNS

Automation

Python, Bash, C/C++, Log Processing, API Integration, Workflow Automation

Security Research

Ghidra, IDA Pro, x64dbg, PE Analysis, Malware Analysis

PROFESSIONAL SUMMARY

Final-year Information Technology student specializing in **Cybersecurity**, with a primary focus on **Blue Team and Security Operations**. Hands-on experience in security monitoring, alert triage, log analysis, threat detection, and incident response through SOC and SDN security labs. Experienced with **Wazuh, Suricata, Shuffle SOAR, Wireshark, and MITRE ATT&CK**. Seeking opportunities to develop deeper expertise in **security monitoring, detection engineering, incident response, and enterprise security infrastructure**.

CAREER DIRECTION

Blue Team → SOC → Security Operations

Primary interest in Security Monitoring, Threat Detection, SIEM/IDS integration, Alert Triage, Incident Response, Detection Engineering, and SOAR-based response automation.

SELECTED SECURITY PROJECTS

PROJECT 01 · 2025 – PRESENT

BLUE TEAM

SDN-based SOC with Automated Threat Detection & Response

Designed and implemented a lab-based Security Operations architecture integrating network monitoring, IDS, SIEM, SOAR, and automated network containment.

- Integrated **Suricata IDS** and **Wazuh SIEM** for centralized security monitoring and alert generation.
- Performed **alert triage, log analysis, network traffic investigation**, and mapped detected activity to **MITRE ATT&CK**.
- Integrated **Shuffle SOAR** with **Ryu SDN Controller** to automate response workflows and dynamically isolate malicious traffic.
- Built security scenarios using **Mininet / Mininet-WiFi** to simulate network threats and evaluate detection and response workflows.

Ryu | Mininet | Suricata | Wazuh | Shuffle SOAR | MITRE ATT&CK

PROJECT 02 · 2026

CLOUD / SECURITY

Cloud-based IoT Monitoring & Security Platform

Designed and deployed a cloud-based IoT monitoring platform connecting ESP32 edge nodes to a centralized backend and dashboard.

- Built telemetry collection and centralized event storage using **ESP32, FastAPI, AWS EC2, MongoDB Atlas** and a React dashboard.
- Configured **AWS Security Groups** with restricted inbound access and database authentication to reduce infrastructure exposure.
- Implemented HTTP polling for bidirectional device communication across NAT/firewall-restricted networks without port forwarding.

ESP32 | FastAPI | AWS EC2 | MongoDB Atlas | React

PROJECT 03 · 2025 – PRESENT

DIGITAL FORENSICS & INCIDENT RESPONSE

Digital Forensics Case Studies & Labs

Completed hands-on DFIR investigations across simulated enterprise and endpoint compromise scenarios.

- **The Stolen Szechuan Sauce:** examined disk, memory, pagefile, Autoruns, and PCAP artifacts across a Windows Server 2012 DC and Windows 10 host.
- **CyberDefenders — SpottedInTheWild:** investigated a suspected WinRAR-related endpoint compromise using Windows logs, Registry, NTFS, and SQLite artifacts.
- **CyberDefenders — Silent Breach:** analyzed a forensic image and Windows Mail (HxStore) artifacts to recover and decode case evidence.

FTK Imager | Eric Zimmerman Tools | Event & Registry Analysis | SQLite Viewer | CyberChef | Autopsy