



## KỸ SƯ AN TOÀN THÔNG TIN

VŨ KHANH PHƯƠNG

### MỤC TIÊU NGHỀ NGHIỆP

Tôi định hướng trở thành một Kỹ sư An toàn Thông tin có năng lực toàn diện trong việc giám sát, phát hiện và xử lý các mối đe dọa mạng, đặc biệt tập trung vào phòng chống tấn công từ bên ngoài và bên trong hệ thống doanh nghiệp.

### THÔNG TIN CÁ NHÂN

05/11/1998

Hà Nội

thaolinh252512@gmail.com

0853939171

www.website.com

### KINH NGHIỆM LÀM VIỆC

- **SECURITY ENGINEER** TẠI CÔNG TY ANTOANTECH  
(2021-2023)

+ TRIỂN KHAI VÀ GIÁM SÁT HỆ THỐNG SIEM (ELK STACK) ĐỂ PHÁT HIỆN HÀNH VI BẤT THƯỜNG

+ CẤU HÌNH TƯỜNG LỬA NỘI BỘ VÀ VPN BẢO VỆ TRUY CẬP TỪ XA

+ PHÂN TÍCH LOG HỆ THỐNG, ĐIỀU TRA SỰ CỐ BẢO MẬT VÀ ĐƯA RA BIỆN PHÁP XỬ LÝ

- **SECURITY ANALYST** TẠI CYBERDEFENSE VIỆT NAM  
(2020-2021)

### HỌC VẤN

- An ninh mạng tại Đại học FPT

### KỸ NĂNG

- Incident Response

- Linux Security

- Burp Suite

- Metasploit Framework

## SỞ THÍCH

- Du lịch
- Học ngoại ngữ
- Chơi đàn guitar
- Nghe nhạc
- Viết blog kỹ thuật

+ GIÁM SÁT HỆ THỐNG IDS/IPS SNORT VÀ XỬ LÝ CẢNH BÁO

+ XÂY DỰNG QUY TRÌNH PHẢN HỒI SỰ CỐ THEO CHUẨN NIST

+ PHỐI HỢP BỘ PHẬN PHÁT TRIỂN ỨNG DỤNG TÍCH HỢP SAST/DAST VÀO CI/CD

## NGƯỜI GIỚI THIỆU

- Ông Trịnh Văn Kiên (Pentest Team Lead – SecureTest Lab) -  
kien.trinh@securetest.vn - 0944222333

- Bà Nguyễn Ngọc Ánh (Senior Security Engineer – BizSecure) -  
anh.nguyen@bizsecure.vn - 0966888777

- Ông Nguyễn Thành Trung (Trưởng phòng An toàn Thông tin – Công ty AnToanTech) -  
trung.nguyen@antoantech.vn - 0908666777

- Bà Lương Thị Thanh (Incident Response Manager – SafeNet) -  
thanh.luong@safenet.vn - 0977333555

- Ông Vũ Văn Duy (Quản lý hệ thống bảo mật – DataSafe Solutions) -  
duy.vu@datasafe.vn - 0909111222

- **PENETRATION TESTER** TẠI SECURECODE LABS (2019-2021)

+ THỰC HIỆN KIỂM THỬ XÂM NHẬP MẠNG NỘI BỘ VÀ ỨNG DỤNG WEB

+ VIẾT SCRIPT TỰ ĐỘNG HÓA KHAI THÁC LỖ HỔNG CƠ BẢN VỚI PYTHON

+ TƯ VẤN CẢI TIẾN CẤU HÌNH BẢO MẬT HỆ THỐNG CHO KHÁCH HÀNG DOANH NGHIỆP

- **CYBERSECURITY SPECIALIST** TẠI FINSEC VIỆT NAM (2020-2022)

+ ĐÁNH GIÁ LỖ HỔNG ĐỊNH KỲ BẰNG NESSUS VÀ VIẾT BÁO CÁO KHUYẾN NGHỊ

+ KIỂM THỬ BẢO MẬT ỨNG DỤNG WEB NỘI BỘ THEO TIÊU CHUẨN OWASP TOP 10

+ TRIỂN KHAI XÁC THỰC HAI YẾU TỐ (2FA) CHO HỆ THỐNG ERP VÀ EMAIL

- **CLOUD SECURITY ENGINEER** TẠI CLOUDGUARD ASIA (2021-2023)

+ THIẾT LẬP CHÍNH SÁCH IAM VÀ MÃ HÓA DỮ LIỆU TRONG AWS

+ KIỂM SOÁT TRUY CẬP S3, CLOUDTRAIL VÀ QUẢN LÝ CLOUDWATCH ALERT

+ PHÁT HIỆN CẤU HÌNH SAI BẰNG AWS CONFIG VÀ VIẾT LAMBDA XỬ LÝ TỰ ĐỘNG

## DANH HIỆU VÀ GIẢI THƯỞNG

- **2020** - Top 5 kỹ sư có phản ứng sự cố nhanh nhất trong hệ thống nội bộ

## CHỨNG CHỈ

- **2023** - AWS Certified Security – Specialty

## HOẠT ĐỘNG

**- Thực tập sinh kiểm thử bảo mật tại Công ty SecureTech (2020)**

+ Thực hiện quét lỗ hổng hệ thống nội bộ bằng Burp Suite và OWASP ZAP.

+ Hỗ trợ viết báo cáo lỗ hổng và đề xuất giải pháp khắc phục.

+ Tham gia đánh giá bảo mật website khách hàng theo OWASP Top 10.

**- Tình nguyện viên hỗ trợ khóa học CEH tại CyberSecurity Training Center (2023)**

+ Chuẩn bị máy ảo tấn công và phòng thủ trong lab CEH.

+ Hỗ trợ học viên trong các bài thực hành hands-on.

+ Giải đáp thắc mắc về công cụ nmap, wireshark, metasploit.

**- Tình nguyện viên hỗ trợ sự kiện CTF tại Vietnam Cybersecurity Week (2022)**

+ Hỗ trợ kỹ thuật cho các đội chơi trong cuộc thi Capture The Flag.

+ Cài đặt và cấu hình máy chủ hosting bài thi.

+ Giám sát an toàn hệ thống trong suốt thời gian diễn ra sự kiện.

**- Thành viên nhóm nghiên cứu bảo mật tại Phòng Lab An toàn Thông tin - Đại học Bách khoa (2021 - 2023)**

+ Nghiên cứu về các lỗ hổng bảo mật phổ biến như XSS, SQLi, CSRF.

+ Tham gia diễn tập phát hiện và ứng phó sự cố tấn công mạng.

+ Viết báo cáo kỹ thuật và trình bày tại hội nghị sinh viên NCKH.

**- Mentor nhóm sinh viên nghiên cứu bảo mật web tại CLB IT trẻ (2022)**

- + Hướng dẫn khai thác lỗi XSS, CSRF trên các bài thực hành.
- + Giám sát và hỗ trợ quá trình viết báo cáo kỹ thuật.
- + Chấm điểm phần trình bày đề tài bảo mật cuối kỳ.

## DỰ ÁN

**- Tự động hóa kiểm tra cấu hình bảo mật hệ thống (DevSecOps Engineer, DevShield) 2021**

Xây dựng công cụ nội bộ dùng Python và Bash để kiểm tra định kỳ các cấu hình sai lệch và gửi báo cáo cho quản lý.

- + Phân tích các tiêu chuẩn cấu hình an toàn cho Linux server
- + Viết script kiểm tra các thiết lập quan trọng (sudo, ssh, firewall)
- + Gửi báo cáo HTML qua email mỗi tuần tự động

**- Triển khai hệ thống phát hiện xâm nhập mạng nội bộ (IDS) (Security Engineer, CyberDefense Việt Nam) 2022**

Xây dựng hệ thống Snort IDS để giám sát và cảnh báo các mối đe dọa trong mạng nội bộ của doanh nghiệp.

- + Cài đặt và cấu hình Snort trên server Ubuntu
- + Tích hợp Snort với hệ thống cảnh báo nội bộ qua email
- + Huấn luyện đội vận hành đọc log và phản hồi sự cố

**- Xây dựng hệ thống SIEM nội bộ (Security Analyst, FinSec Việt Nam) 2022**

Tập hợp log từ các hệ thống và phân tích cảnh báo an ninh bằng ELK Stack (Elasticsearch, Logstash, Kibana).

- + Cấu hình Logstash để thu thập log từ firewall, server, IDS

+ Tạo dashboard trong Kibana theo dõi bất thường

+ Viết quy tắc cảnh báo và quy trình xử lý sự cố