



## KỸ SƯ AN TOÀN THÔNG TIN

BÙI YẾN BÌNH

### MỤC TIÊU NGHỀ NGHIỆP

Tôi muốn nghiên cứu và triển khai các cơ chế bảo mật nâng cao như Zero Trust, Network Segmentation, và bảo vệ dữ liệu trong môi trường hybrid cloud.

### THÔNG TIN CÁ NHÂN

23/12/1984

Hà Nội

thaolinh252512@gmail.com

0911749480

www.website.com

### HỌC VẤN

- Kỹ thuật máy tính tại Đại học Sư phạm Kỹ thuật TP.HCM

### KỸ NĂNG

- Python

- Zero Trust Architecture

- Security Compliance (ISO 27001, NIST, PCI-DSS)

### KINH NGHIỆM LÀM VIỆC

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

+ 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

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

## SỞ THÍCH

- Nấu ăn

- Tham gia hackathon

- Thử nghiệm công nghệ mới

- Chụp ảnh

- Chơi cờ vua

+ 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

## NGƯỜI GIỚI THIỆU

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

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

- **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

- **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

## DANH HIỆU VÀ GIẢI THƯỞNG

- **2022** - Giải thưởng 'Kỹ sư có sáng kiến bảo mật nội bộ' của năm

## CHỨNG CHỈ

- **2020** - Certified Ethical Hacker (CEH) – EC-Council

- **2021** - Microsoft Certified: Security, Compliance, and Identity Fundamentals

- **2022** - Certified Cloud Security Professional (CCSP) – ISC<sup>2</sup>

- **2022** - Certified Information Systems Security Professional (CISSP) – ISC<sup>2</sup>

- **2021** - Cisco Certified CyberOps Associate – Cisco

## HOẠT ĐỘNG

- **Người viết blog bảo mật thông tin tại [infosecjournal.vn](https://infosecjournal.vn) (2021 - nay)**

+ Chia sẻ kiến thức về bảo mật hệ thống và ứng dụng web.

+ Hướng dẫn kiểm tra bảo mật với Kali Linux và Metasploit.

+ Viết phân tích kỹ thuật về các cuộc tấn công thực tế.

**- Cộng tác viên chương trình đánh giá bảo mật hệ thống tại Công ty SafeNet (2021)**

- + Kiểm tra cấu hình tường lửa, phân quyền tài khoản trên hệ thống.
- + Thực hiện quét port, phát hiện dịch vụ không an toàn.
- + Tổng hợp báo cáo lỗ hổng gửi khách hàng.

**- 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.

**- Thành viên diễn tập Red Team nội bộ tại Ngân hàng Tài chính Việt (2022)**

- + Thực hiện khai thác giả lập các lỗ hổng hệ thống nội bộ.
- + Viết script tự động hóa kiểm tra cấu hình sai trên firewall và IDS.
- + Lập kế hoạch và báo cáo lỗ hổng gửi nhóm Blue Team xử lý.

## DỰ ÁN

**- 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

**- Bảo mật hệ thống cloud AWS (Cloud Security Engineer, CloudGuard Asia) 2023**

Đánh giá và cải thiện bảo mật cho hệ thống web triển khai trên hạ tầng AWS.

- + Thiết lập IAM theo nguyên tắc phân quyền tối thiểu

- + Kích hoạt CloudTrail và cảnh báo hoạt động bất thường

- + Kiểm tra cấu hình S3 bucket, RDS và các dịch vụ công khai

**- 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

**- Đánh giá bảo mật ứng dụng web nội bộ (Pentester, SecureCode Labs) 2021**

Thực hiện kiểm thử xâm nhập cho các ứng dụng web nội bộ nhằm xác định và khắc phục lỗ hổng OWASP Top 10.

- + Sử dụng Burp Suite, Nikto, OWASP ZAP để phân tích lỗ hổng

+ Viết báo cáo phân tích và hướng dẫn khắc phục chi tiết

+ Hỗ trợ đội phát triển sửa lỗi và tái kiểm tra