# KỸ SƯ AN TOÀN THÔNG TIN

## TRẦN TRUNG NGÂN

## MỤC TIÊU NGHỀ NGHIỆP

**Tôi định hướng trở thành một chuyên gia kiểm toán hệ thống thông tin, có thể đánh giá rủi ro bảo mật, thực hiện đánh giá tuân thủ (compliance) theo tiêu chuẩn ISO 27001, PCI-DSS, NIST.**

## THÔNG TIN CÁ NHÂN

09/05/1999
Hà Nội
thaolinh252512@gmail.com
0904750118
www.website.com

## HỌC VẤN

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

## KỸ NĂNG

- Linux Security

- Network Security

## SỞ THÍCH

## KINH NGHIỆM LÀM VIỆC

- **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

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

- Tham gia hội thảo công nghệ

- Xem phim khoa học viễn tưởng

- Chơi cờ vua

- Thử nghiệm công nghệ mới

## NGƯỜI GIỚI THIỆU

- Ông Trần Quang Minh (Security Operations Manager – FinSec Việt Nam) - minh.tran@finsec.vn - 0933666888

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

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

+ 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

- **2021** - Được đề cử danh hiệu 'Gương mặt trẻ lĩnh vực An ninh mạng'

- **2021** - Vinh danh cá nhân đóng góp nhiều nhất cho hệ thống cảnh báo an ninh mạng

- **2021** - Nhân viên An toàn Thông tin xuất sắc quý III tại Công ty AnToanTech

- **2023** - Bằng khen vì hoàn thành kiểm thử xâm nhập sớm hơn kế hoạch 2 tuần

## CHỨNG CHỈ

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

- **2022** - Certified Information Systems Security Professional (CISSP) – ISC²

## HOẠT ĐỘNG

**- 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.

**- Người viết blog bảo mật thông tin tại 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.

**- Diễn giả khách mời tại Hội thảo 'CyberSec Career Day' (2023)**

+ Trình bày lộ trình nghề nghiệp dành cho kỹ sư An toàn Thông tin.

+ Chia sẻ kinh nghiệm thực tế về triển khai hệ thống SIEM.

+ Tư vấn sinh viên về định hướng chuyên sâu Red Team và Blue Team.

**- 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.

## 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

**- 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