



## KỸ SƯ AN TOÀN THÔNG TIN

TRẦN MINH ANH

### MỤC TIÊU NGHỀ NGHIỆP

Tôi mong muốn trở thành cầu nối giữa đội ngũ DevOps và bảo mật (DevSecOps), giúp tích hợp quy trình bảo mật vào vòng đời phát triển phần mềm ngay từ giai đoạn đầu.

### THÔNG TIN CÁ NHÂN

26/09/1995

Hà Nội

thaolinh252512@gmail.com

0764798066

www.website.com

### 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

### HỌC VẤN

- An ninh mạng tại Đại học FPT

### KỸ NĂNG

- Identity and Access Management (IAM)

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

### SỞ THÍCH

- Tập gym

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

## NGƯỜI GIỚI THIỆU

- Ông Đỗ Minh Tiến (Head of Cloud Security - CloudBase VN) -  
tien.do@cloudbase.vn - 0911555666

+ 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

- **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

- **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

- **2020** - Nhân viên triển khai SIEM hiệu quả nhất tại bộ phận bảo mật
- **2022** - Top 3 kỹ sư có đóng góp lớn nhất vào chương trình bảo vệ dữ liệu khách hàng
- **2021** - Được đề cử danh hiệu 'Gương mặt trẻ lĩnh vực An ninh mạng'
- **2022** - Giải thưởng 'Kỹ sư có sáng kiến bảo mật nội bộ' của năm
- **2020** - Top 5 kỹ sư có phản ứng sự cố nhanh nhất trong hệ thống nội bộ

## CHỨNG CHỈ

- **2023** - AWS Certified Security – Specialty
- **2020** - GIAC Security Essentials (GSEC) – SANS Institute
- **2021** - Cisco Certified CyberOps Associate – Cisco
- **2022** - Certified Information Systems Security Professional (CISSP) – ISC<sup>2</sup>

## 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.

**- 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.

**- Thành viên câu lạc bộ An toàn thông tin tại CLB Sinh viên An ninh mạng - Học viện Kỹ thuật Mật mã (2020 - 2022)**

- + Tổ chức các buổi workshop về bảo mật Wi-Fi, DNS spoofing.
- + Tham gia thi đấu CTF nội bộ và luyện tập giải bài reversing.
- + Chia sẻ tài liệu và tổng hợp hướng dẫn học về pentest.

## 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

### - 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

### - 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

### - 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