



## KỸ SƯ AN TOÀN THÔNG TIN

NGUYỄN LINH THẢO

### MỤC TIÊU NGHỀ NGHIỆP

Tôi kỳ vọng phát triển kỹ năng xây dựng kiến trúc bảo mật tổng thể cho doanh nghiệp, từ phân tầng bảo mật vật lý đến an toàn dữ liệu và an ninh mạng nội bộ.

### THÔNG TIN CÁ NHÂN

11/06/1990

Hà Nội

thaolinh252512@gmail.com

0748088293

www.website.com

### HỌC VẤN

- Quản trị và bảo mật hệ thống mạng tại Đại học CNTT - ĐHQG TP.HCM - An ninh mạng tại Đại học FPT

### KỸ NĂNG

- Identity and Access Management (IAM)
- Linux Security
- DevSecOps (GitLab CI + SAST/DAST)
- SIEM (Splunk, ELK)
- Security Compliance (ISO 27001, NIST, PCI-DSS)

### 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

- **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

## SỞ THÍCH

- Nấu ăn
- Xem phim khoa học viễn tưởng
- Thể thao
- Chụp ảnh
- Thiết kế sản phẩm cá nhân

+ 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

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

## NGƯỜI GIỚI THIỆU

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

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

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

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

- Bà Lê Thị Huyền (Giám đốc An ninh Thông tin (CISO) – CloudSecure Corp) - huyen.le@cloudsecure.vn - 0912888999

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

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

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

- Bà Trần Kim Ngân (Security Compliance Officer – DevSecure) - ngan.tran@devsecure.vn - 0933444555

+ 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

- **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

## DANH HIỆU VÀ GIẢI THƯỞNG

- **2023** - Giải nhất cuộc thi 'Capture The Flag' toàn quốc do VietCyber tổ chức

## CHỨNG CHỈ

- **2020** - GIAC Security Essentials (GSEC) – SANS Institute

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

- **2020** - Certified Ethical Hacker (CEH) – EC-Council
- **2022** - Certified Information Systems Security Professional (CISSP) – ISC<sup>2</sup>
- **2023** - CompTIA PenTest+ – CompTIA

## HOẠT ĐỘNG

### - 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.

### - 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 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.

## - 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

### - 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

#### **- 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

#### **- 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

