



## KỸ SƯ AN TOÀN THÔNG TIN

TRẦN LINH NAM

### MỤC TIÊU NGHỀ NGHIỆP

Tôi hướng đến việc phát triển năng lực triển khai và quản trị các công cụ SIEM như Splunk, ELK, nhằm giám sát thời gian thực các hoạt động bất thường và đưa ra cảnh báo kịp thời để ngăn chặn rủi ro.

### THÔNG TIN CÁ NHÂN

06/05/1997

Hà Nội

thaolinh252512@gmail.com

0807438854

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

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

### HỌC VẤN

- An ninh mạng tại Đại học FPT

### KỸ NĂNG

- SIEM (Splunk, ELK)

- Metasploit Framework

- Penetration Testing

### SỞ THÍCH

- Nghe nhạc

- Học ngoại ngữ

- Thể thao

+ 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

## NGƯỜI GIỚI THIỆU

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

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

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

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

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

+ 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

- **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

## DANH HIỆU VÀ GIẢI THƯỞNG

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

## CHỨNG CHỈ

- **2022** - Offensive Security Certified Professional (OSCP)

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

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

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

## HOẠT ĐỘNG

- **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.

- **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.

**- 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.

**- 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.

## 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

**- 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

