



## KỸ SƯ AN TOÀN THÔNG TIN

NGÔ THẢO QUỲNH

### MỤC TIÊU NGHỀ NGHIỆP

Tôi đặt mục tiêu dài hạn trở thành CISO (Chief Information Security Officer), người chịu trách nhiệm toàn diện về chiến lược và vận hành hệ thống bảo mật thông tin cho tổ chức.

### THÔNG TIN CÁ NHÂN

23/02/1987

Hà Nội

thaolinh252512@gmail.com

0870446185

www.website.com

### KINH NGHIỆM LÀM VIỆC

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

+ 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

### HỌC VẤN

- Kỹ thuật phần mềm tại Đại học Bách khoa Hà Nội

### KỸ NĂNG

- Vulnerability Assessment (Nessus, OpenVAS)

### SỞ THÍCH

- Tham gia hội thảo công nghệ

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

- Thử nghiệm công nghệ mới

- Chụp ảnh

+ ĐÁNH GIÁ LỖ HỔNG ĐỊNH KỲ BẰNG NESSUS VÀ VIẾT BÁO CÁO KHUYẾN NGHỊ

## NGƯỜI GIỚI THIỆU

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

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

- Bà Phạm Thị Mai (Cybersecurity Lead – TechShield) - mai.pham@techshield.vn - 0988999666

+ 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 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** - Top 3 kỹ sư có đóng góp lớn nhất vào chương trình bảo vệ dữ liệu khách hàng

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

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

## CHỨNG CHỈ

- **2020** - GIAC Security Essentials (GSEC) – SANS Institute
- **2021** - Cisco Certified CyberOps Associate – Cisco
- **2022** - Certified Cloud Security Professional (CCSP) – ISC<sup>2</sup>
- **2022** - Offensive Security Certified Professional (OSCP)

## 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.

### - 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.

### - 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.

## **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

#### **- 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

**- 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