



## KỸ SƯ AN TOÀN THÔNG TIN

NGÔ MINH THỊ

### MỤC TIÊU NGHỀ NGHIỆP

Tôi muốn nghiên cứu và triển khai các cơ chế bảo mật nâng cao như Zero Trust, Network Segmentation, và bảo vệ dữ liệu trong môi trường hybrid cloud.

### THÔNG TIN CÁ NHÂN

28/07/1991

Hà Nội

thaolinh252512@gmail.com

0859242909

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

### HỌC VẤN

- Kỹ thuật phần mềm tại Đại học Bách khoa Hà Nội - Kỹ thuật an toàn thông tin tại Đại học Duy Tân

### KỸ NĂNG

- Security Compliance (ISO 27001, NIST, PCI-DSS)

- Vulnerability Assessment (Nessus, OpenVAS)

- Identity and Access Management (IAM)

- Bash Scripting

+ PHÂN TÍCH LOG HỆ THỐNG, ĐIỀU TRA SỰ CỐ BẢO MẬT VÀ ĐƯA RA BIỆN PHÁP XỬ LÝ

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

- Linux Security

+ GIÁM SÁT HỆ THỐNG IDS/IPS SNORT VÀ XỬ LÝ CẢNH BÁO

## SỞ THÍCH

- Tham gia hội thảo công nghệ

- Chụp ảnh

+ 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

## NGƯỜI GIỚI THIỆU

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

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

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

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

- Bà Nguyễn Ngọc Ánh (Senior Security Engineer – BizSecure) -  
anh.nguyen@bizsecure.vn - 0966888777

## DANH HIỆU VÀ GIẢI THƯỞNG

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

- **2020** - Nhân viên triển khai SIEM hiệu quả nhất tại bộ phận bảo mật

- **2020** - Top 5 kỹ sư có phản ứng sự cố nhanh nhất trong hệ thống nội bộ

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

- **2022** - Bằng khen vì phát hiện sớm lỗ hổng bảo mật nghiêm trọng trong hệ thống email

## CHỨNG CHỈ

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

## 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.

## **- 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.

## **DỰ ÁN**

### **- 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

### **- 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

#### **- 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

