



KỸ SƯ AN TOÀN THÔNG TIN

VŨ THÀNH THỊ

MỤC TIÊU NGHỀ NGHIỆP

Tôi muốn trở thành chuyên gia trong việc phân tích và phản hồi sự cố bảo mật, từ việc thu thập log, phân tích forensics đến khôi phục hệ thống sau sự cố một cách nhanh chóng và hiệu quả.

THÔNG TIN CÁ NHÂN

03/04/1984

Hà Nội

thaolinh252512@gmail.com

0346830312

www.website.com

KINH NGHIỆM LÀM VIỆC

- **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

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

HỌC VẤN

- Kỹ thuật an toàn thông tin tại Đại học Duy Tân - An ninh mạng tại Đại học FPT

KỸ NĂNG

- Burp Suite

- SIEM (Splunk, ELK)

- Wireshark

- Bash Scripting

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

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

SỞ THÍCH

- Viết blog kỹ thuật
- Chơi đàn guitar
- Chụp ảnh
- Thiết kế sản phẩm cá nhân

+ 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

NGƯỜI GIỚI THIỆU

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

- **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

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

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

CHỨNG CHỈ

- **2022** - Certified Information Systems Security Professional (CISSP) – ISC²
- **2021** - CompTIA Security+ – CompTIA
- **2020** - GIAC Security Essentials (GSEC) – SANS Institute
- **2022** - Certified Cloud Security Professional (CCSP) – ISC²

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.

- 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

- 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

- 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

