



KỸ SƯ AN TOÀN THÔNG TIN

NGÔ HẠNH NGỌC

MỤC TIÊU NGHỀ NGHIỆP

Tôi định hướng phát triển thành một Security Engineer có tư duy phản biện cao, sẵn sàng phát hiện bất thường từ log hệ thống, mã nguồn, hoặc hành vi người dùng để ngăn chặn nguy cơ bị khai thác.

THÔNG TIN CÁ NHÂN

05/10/1997

Hà Nội

thaolinhh252512@gmail.com

0761371112

www.website.com

HỌC VẤN

- Kỹ thuật phần mềm tại Đại học Bách khoa Hà Nội
- An ninh mạng tại Đại học FPT

KỸ NĂNG

- OWASP Top 10
- Incident Response
- Security Compliance (ISO 27001, NIST, PCI-DSS)
- SIEM (Splunk, ELK)
- Burp Suite

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

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

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

SỞ THÍCH

- Đọc sách

- Trồng cây

- Đi bộ đường dài

+ 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

NGƯỜI GIỚI THIỆU

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

- **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

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

+ 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 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

- **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

CHỨNG CHỈ

- **2023** - CompTIA PenTest+ – CompTIA
- **2023** - AWS Certified Security – Specialty
- **2021** - Cisco Certified CyberOps Associate – Cisco
- **2022** - Certified Cloud Security Professional (CCSP) – ISC²

HOẠT ĐỘNG

- 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.

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

