KỸ SƯ AN TOÀN THÔNG TIN

NGÔ NGÂN THU

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

13/10/1995
Hà Nội
thaolinh252512@gmail.com
0829386774
www.website.com

HỌC VẤN

- Khoa học máy tính tại Đại học Quốc tế – ĐHQG TP.HCM - An toàn thông tin tại Học viện Kỹ thuật Mật mã

KỸ NĂNG

- SIEM (Splunk, ELK)

- Penetration Testing

- Cloud Security (AWS, Azure)

- Zero Trust Architecture

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

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

SỞ THÍCH

- Thể thao

- Tham gia hội thảo công nghệ

- Chơi đàn guitar

NGƯỜI GIỚI THIỆU

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

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

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

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

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

+ 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

+ 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

DANH HIỆU VÀ GIẢI THƯỞNG

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

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

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

- **2022** - Top 3 kỹ sư có đóng góp lớn nhất vào chương trình bảo vệ dữ liệu khách hàng

CHỨNG CHỈ

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

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

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

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.

- 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.

- 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.

- 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

- 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