KỸ SƯ AN TOÀN THÔNG TIN

PHẠM HIẾU YẾN

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

04/09/1988
Hà Nội
thaolinh252512@gmail.com
0897688699
www.website.com

HỌC VẤN

- Khoa học máy tính tại Đại học Quốc tế – ĐHQG TP.HCM

KỸ NĂNG

- Penetration Testing

- Network Security

- DevSecOps (GitLab CI + SAST/DAST)

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

- **PENETRATION TESTER** TẠI SECURECODE LABS (2019-2021)

SỞ THÍCH

- Chơi cờ vua

- Sưu tầm sách lập trình

NGƯỜI GIỚI THIỆU

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

+ 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

DANH HIỆU VÀ GIẢI THƯỞNG

- **2022** - Giải thưởng 'Kỹ sư có sáng kiến bảo mật nội bộ' của năm

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

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

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

CHỨNG CHỈ

- **2023** - CompTIA PenTest+ – CompTIA

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

- **2022** - Certified Cloud Security Professional (CCSP) – ISC²

HOẠT ĐỘNG

- Tình nguyện viên hỗ trợ sự kiện CTF tại Vietnam Cybersecurity Week (2022)

+ Hỗ trợ kỹ thuật cho các đội chơi trong cuộc thi Capture The Flag.

+ Cài đặt và cấu hình máy chủ hosting bài thi.

+ Giám sát an toàn hệ thống trong suốt thời gian diễn ra sự kiện.

- 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

- 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

- 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