



KỸ SƯ AN TOÀN THÔNG TIN

NGÔ LAN QUANG

MỤC TIÊU NGHỀ NGHIỆP

Tôi mong muốn triển khai các chính sách bảo mật nội bộ như phân quyền truy cập theo nguyên tắc 'least privilege', mã hóa dữ liệu đầu cuối và xác thực đa yếu tố trong doanh nghiệp.

THÔNG TIN CÁ NHÂN

06/11/1997

Hà Nội

thaolinh252512@gmail.com

0937655567

www.website.com

HỌC VẤN

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

KỸ NĂNG

- Web Application Security
- Network Security
- Identity and Access Management (IAM)

KINH NGHIỆM LÀM VIỆC

- **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

DANH HIỆU VÀ GIẢI THƯỞNG

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

SỞ THÍCH

- Tham gia cộng đồng lập trình
- Thiết kế sản phẩm cá nhân
- Thử nghiệm công nghệ mới
- Thể thao
- Trồng cây

NGƯỜI GIỚI THIỆU

- Bà Lê Thị Huyền (Giám đốc An ninh Thông tin (CISO) - CloudSecure Corp) - huyen.le@cloudsecure.vn - 0912888999
- Bà Phạm Thị Mai (Cybersecurity Lead - TechShield) - mai.pham@techshield.vn - 0988999666
- Ông Trần Quang Minh (Security Operations Manager - FinSec Việt Nam) - minh.tran@finsec.vn - 0933666888
- Bà Lương Thị Thanh (Incident Response Manager - SafeNet) - thanh.luong@safenet.vn - 0977333555
- Bà Nguyễn Ngọc Ánh (Senior Security Engineer - BizSecure) - anh.nguyen@bizsecure.vn - 0966888777

thống nội bộ

- **2020** - Nhân viên triển khai SIEM hiệu quả nhất tại bộ phận bảo mật
- **2022** - Giải thưởng 'Kỹ sư có sáng kiến bảo mật nội bộ' của năm

CHỨNG CHỈ

- **2022** - Certified Cloud Security Professional (CCSP) - ISC²
- **2022** - Offensive Security Certified Professional (OSCP)
- **2020** - Certified Ethical Hacker (CEH) - EC-Council
- **2020** - GIAC Security Essentials (GSEC) - SANS Institute
- **2023** - AWS Certified Security - Specialty

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.

- **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.

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

- 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

