



KỸ SƯ AN TOÀN THÔNG TIN

LÊ THỊ THANH

MỤC TIÊU NGHỀ NGHIỆP

Tôi hướng đến vai trò chuyên gia tư vấn bảo mật cho doanh nghiệp vừa và nhỏ, cung cấp giải pháp bảo mật tối ưu với chi phí hợp lý và hiệu quả bảo vệ cao.

THÔNG TIN CÁ NHÂN

03/09/1990

Hà Nội

thaolinh252512@gmail.com

0893216312

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

HỌC VẤN

- An ninh mạng tại Đại học FPT - Kỹ thuật máy tính tại Đại học Sư phạm Kỹ thuật TP.HCM

KỸ NĂNG

- IDS/IPS (Snort, Suricata)

- Network Security

- Linux Security

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

- DevSecOps (GitLab CI + SAST/DAST)

DANH HIỆU VÀ GIẢI THƯỞNG

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

bảo mật

SỞ THÍCH

- Tham gia hackathon
- Chụp ảnh
- Thể thao
- Chơi đàn guitar
- Tham gia hội thảo công nghệ

NGƯỜI GIỚI THIỆU

- Bà Nguyễn Ngọc Ánh (Senior Security Engineer – BizSecure) -
anh.nguyen@bizsecure.vn - 0966888777

CHỨNG CHỈ

- **2022** - Offensive Security Certified Professional (OSCP)
- **2020** - GIAC Security Essentials (GSEC) – SANS Institute

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.

- **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.

- **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.

- **Cộng tác viên chương trình đánh giá bảo mật hệ thống tại Công ty SafeNet (2021)**

- + Kiểm tra cấu hình tường lửa, phân quyền tài khoản trên hệ thống.
- + Thực hiện quét port, phát hiện dịch vụ không an toàn.
- + Tổng hợp báo cáo lỗ hổng gửi khách hàng.

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

- 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

