



KỸ SƯ AN TOÀN THÔNG TIN

BÙI MINH HÒA

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

15/06/1983

Hà Nội

thaolinh252512@gmail.com

0731861365

www.website.com

KINH NGHIỆM LÀM VIỆC

- **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

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

HỌC VẤN

- Mạng máy tính và truyền thông dữ
liệu tại Đại học Giao thông Vận tải

KỸ NĂNG

- OWASP Top 10
- Web Application Security
- DevSecOps (GitLab CI + SAST/DAST)
- Zero Trust Architecture
- IDS/IPS (Snort, Suricata)

SỞ THÍCH

- Viết blog kỹ thuật

NGƯỜI GIỚI THIỆU

- Bà Lê Thị Huyền (Giám đốc An ninh Thông tin (CISO) – CloudSecure Corp) - huyen.le@cloudsecure.vn - 0912888999

- Ông Vũ Văn Duy (Quản lý hệ thống bảo mật – DataSafe Solutions) - duy.vu@datasafe.vn - 0909111222

+ 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

- **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

DANH HIỆU VÀ GIẢI THƯỞNG

- **2023** - Bằng khen vì hoàn thành kiểm thử xâm nhập sớm hơn kế hoạch 2 tuần

- **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
- **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

- **2021** - Cisco Certified CyberOps Associate – Cisco
- **2022** - Certified Information Systems Security Professional (CISSP) – ISC²
- **2022** - Certified Cloud Security Professional (CCSP) – ISC²

HOẠT ĐỘNG

- 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.

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

- 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

- 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

- 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