



KỸ SƯ AN TOÀN THÔNG TIN

BÙI NAM CHÂU

MỤC TIÊU NGHỀ NGHIỆP

Tôi hướng đến việc phát triển năng lực triển khai và quản trị các công cụ SIEM như Splunk, ELK, nhằm giám sát thời gian thực các hoạt động bất thường và đưa ra cảnh báo kịp thời để ngăn chặn rủi ro.

THÔNG TIN CÁ NHÂN

26/01/2000

Hà Nội

thaolinh252512@gmail.com

0807550871

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

HỌC VẤN

- Công nghệ thông tin tại Đại học Công nghệ - ĐHQG Hà Nội - Kỹ thuật máy tính tại Đại học Sư phạm Kỹ thuật TP.HCM

KỸ NĂNG

- Bash Scripting

- Python

- Cloud Security (AWS, Azure)

- Incident Response

- Zero Trust Architecture

+ PHỐI HỢP BỘ PHẬN PHÁT TRIỂN ỨNG DỤNG TÍCH HỢP SAST/DAST VÀO CI/CD

- **CYBERSECURITY SPECIALIST** TẠI FINSEC VIỆT NAM
(2020-2022)

+ ĐÁNH GIÁ LỖ HỔNG ĐỊNH KỲ BẰNG NESSUS VÀ VIẾT BÁO CÁO KHUYẾN NGHỊ

SỞ THÍCH

- Nấu ăn

+ KIỂM THỬ BẢO MẬT ỨNG DỤNG WEB NỘI BỘ THEO TIÊU CHUẨN OWASP TOP 10

NGƯỜI GIỚI THIỆU

- Ông Trịnh Văn Kiên (Pentest Team Lead – SecureTest Lab) -
kien.trinh@securetest.vn - 0944222333

+ TRIỂN KHAI XÁC THỰC HAI YẾU TỐ (2FA) CHO HỆ THỐNG ERP VÀ EMAIL

- **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

DANH HIỆU VÀ GIẢI THƯỞNG

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

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

- **2021** - Nhân viên An toàn Thông tin xuất sắc quý III tại Công ty AnToanTech
- **2021** - Được đề cử danh hiệu 'Gương mặt trẻ lĩnh vực An ninh mạng'

CHỨNG CHỈ

- **2022** - Certified Information Systems Security Professional (CISSP) – ISC²
- **2023** - CompTIA PenTest+ – CompTIA

HOẠT ĐỘNG

- **Diễn giả khách mời tại Hội thảo 'CyberSec Career Day' (2023)**

- + Trình bày lộ trình nghề nghiệp dành cho kỹ sư An toàn Thông tin.
- + Chia sẻ kinh nghiệm thực tế về triển khai hệ thống SIEM.
- + Tư vấn sinh viên về định hướng chuyên sâu Red Team và Blue Team.

- **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.

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

- 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

