



KỸ SƯ AN TOÀN THÔNG TIN

ĐỖ HÙNG TÚ

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

01/07/1994

Hà Nội

thaolinh252512@gmail.com

0744276002

www.website.com

KINH NGHIỆM LÀM VIỆC

- **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

HỌC VẤN

- Quản trị và bảo mật hệ thống mạng
tại Đại học CNTT - ĐHQG TP.HCM -
Khoa học máy tính tại Đại học Quốc tế
- ĐHQG TP.HCM

KỸ NĂNG

- Linux Security

- DevSecOps (GitLab CI + SAST/DAST)

- IDS/IPS (Snort, Suricata)

- Identity and Access Management (IAM)

+ PHÂN TÍCH LOG HỆ THỐNG, ĐIỀU TRA SỰ CỐ BẢO MẬT VÀ ĐƯA RA BIỆN PHÁP XỬ LÝ

- **SECURITY ANALYST** TẠI CYBERDEFENSE VIỆT NAM
(2020-2021)

SỞ THÍCH

- Chơi cờ vua
- Thiết kế sản phẩm cá nhân
- Nghe nhạc
- Tham gia hội thảo công nghệ

+ 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

NGƯỜI GIỚI THIỆU

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

DANH HIỆU VÀ GIẢI THƯỞNG

- **2020** - Top 5 kỹ sư có phản ứng sự cố nhanh nhất trong hệ thống nội bộ
- **2022** - Top 3 kỹ sư có đóng góp lớn nhất vào chương trình bảo vệ dữ liệu khách hàng
- **2022** - Bằng khen vì phát hiện sớm lỗ hổng bảo mật nghiêm trọng trong hệ thống email

CHỨNG CHỈ

- **2020** - Certified Ethical Hacker (CEH) – EC-Council

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.

- Thành viên diễn tập Red Team nội bộ tại Ngân hàng Tài chính Việt (2022)

- + Thực hiện khai thác giả lập các lỗ hổng hệ thống nội bộ.

- + Viết script tự động hóa kiểm tra cấu hình sai trên firewall và IDS.

- + Lập kế hoạch và báo cáo lỗ hổng gửi nhóm Blue Team xử lý.

DỰ ÁN

- 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

