



KỸ SƯ AN TOÀN THÔNG TIN

NGUYỄN HẠNH LINH

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

26/12/1988

Hà Nội

thaolinh252512@gmail.com

0786139077

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

- Kỹ thuật phần mềm tại Đại học Bách khoa Hà Nội - Quản trị và bảo mật hệ thống mạng tại Đại học CNTT - ĐHQG TP.HCM

KỸ NĂNG

- Network Security

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

SỞ THÍCH

DANH HIỆU VÀ GIẢI THƯỞNG

- **2021** - Vinh danh cá nhân đóng góp nhiều nhất cho hệ thống

- Viết blog kỹ thuật
- Thử nghiệm công nghệ mới
- Thể thao

NGƯỜI GIỚI THIỆU

- Ông Nguyễn Thành Trung (Trưởng phòng An toàn Thông tin – Công ty AnToanTech) -
trung.nguyen@antoantech.vn -
0908666777

cảnh báo an ninh mạng

- **2023** - Giải nhất cuộc thi 'Capture The Flag' toàn quốc do VietCyber tổ chức
- **2020** - Nhân viên triển khai SIEM hiệu quả nhất tại bộ phận bảo mật
- **2022** - Top 3 kỹ sư có đóng góp lớn nhất vào chương trình bảo vệ dữ liệu khách hàng

CHỨNG CHỈ

- **2020** - GIAC Security Essentials (GSEC) – SANS Institute
- **2022** - Certified Cloud Security Professional (CCSP) – ISC²
- **2023** - CompTIA PenTest+ – CompTIA
- **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.

- **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.

- 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.

- Thành viên câu lạc bộ An toàn thông tin tại CLB Sinh viên An ninh mạng - Học viện Kỹ thuật Mật mã (2020 - 2022)

- + Tổ chức các buổi workshop về bảo mật Wi-Fi, DNS spoofing.

- + Tham gia thi đấu CTF nội bộ và luyện tập giải bài reversing.

- + Chia sẻ tài liệu và tổng hợp hướng dẫn học về pentest.

- 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

**- 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

**- 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

**- 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