



KỸ SƯ AN TOÀN THÔNG TIN

BÙI GIANG MINH

MỤC TIÊU NGHỀ NGHIỆP

Tôi mong muốn triển khai các chính sách bảo mật nội bộ như phân quyền truy cập theo nguyên tắc 'least privilege', mã hóa dữ liệu đầu cuối và xác thực đa yếu tố trong doanh nghiệp.

THÔNG TIN CÁ NHÂN

02/07/1983

Hà Nội

thaolinh252512@gmail.com

0852866125

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

- **PENETRATION TESTER** TẠI SECURECODE LABS (2019-2021)

HỌC VẤN

- Hệ thống thông tin tại Đại học Kinh tế Quốc dân

KỸ NĂNG

- Wireshark

- Firewall Configuration (iptables, UFW)

- DevSecOps (GitLab CI + SAST/DAST)

- Identity and Access Management (IAM)

SỞ THÍCH

- Thử nghiệm công nghệ mới
- Chụp ảnh
- Viết blog kỹ thuật

+ THỰC HIỆN KIỂM THỬ XÂM NHẬP MẠNG NỘI BỘ VÀ ỨNG DỤNG WEB

+ VIẾT SCRIPT TỰ ĐỘNG HÓA KHAI THÁC LỖ HỔNG CƠ BẢN VỚI PYTHON

NGƯỜI GIỚI THIỆU

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

- Ông Trần Quang Minh (Security Operations Manager – FinSec Việt Nam) -
minh.tran@finsec.vn - 0933666888

- Bà Lương Thị Thanh (Incident Response Manager – SafeNet) -
thanh.luong@safenet.vn - 0977333555

+ TƯ VẤN CẢI TIẾN CẤU HÌNH BẢO MẬT HỆ THỐNG CHO KHÁCH HÀNG DOANH NGHIỆP

- **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

- **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

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

+ 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

DANH HIỆU VÀ GIẢI THƯỞNG

- **2021** - Nhân viên An toàn Thông tin xuất sắc quý III tại Công ty AnToanTech

- **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

- **2022** - Giải thưởng 'Kỹ sư có sáng kiến bảo mật nội bộ' của năm

- **2021** - Được đề cử danh hiệu 'Gương mặt trẻ lĩnh vực An ninh

mạng'

CHỨNG CHỈ

- **2021** - Cisco Certified CyberOps Associate - Cisco
- **2021** - Microsoft Certified: Security, Compliance, and Identity Fundamentals
- **2020** - Certified Ethical Hacker (CEH) - EC-Council
- **2020** - GIAC Security Essentials (GSEC) - SANS Institute

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

- 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

- 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

- 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

