KỸ SƯ AN TOÀN THÔNG TIN

VŨ QUANG NGA

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

19/10/1998
Hà Nội
thaolinh252512@gmail.com
0989138359
www.website.com

HỌC VẤN

- Mạng máy tính và truyền thông dữ liệu tại Đại học Giao thông Vận tải - Kỹ thuật an toàn thông tin tại Đại học Duy Tân

KỸ NĂNG

- Security Compliance (ISO 27001, NIST, PCI-DSS)

- DevSecOps (GitLab CI + SAST/DAST)

- OWASP Top 10

- Python

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

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

SỞ THÍCH

- Chơi cờ vua

- Nấu ăn

- Thử nghiệm công nghệ mới

- Tham gia hackathon

- Thể thao

NGƯỜI GIỚI THIỆU

- Bà Phạm Thị Mai (Cybersecurity Lead – TechShield) - mai.pham@techshield.vn - 0988999666

+ 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

- **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

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

+ 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

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

DANH HIỆU VÀ GIẢI THƯỞNG

- **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'

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

- **2020** - Nhân viên triển khai SIEM hiệu quả nhất tại bộ phận bảo mật

CHỨNG CHỈ

- **2022** - Certified Cloud Security Professional (CCSP) – ISC²

- **2021** - Microsoft Certified: Security, Compliance, and Identity Fundamentals

- **2022** - Certified Information Systems Security Professional (CISSP) – ISC²

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

- **2022** - Offensive Security Certified Professional (OSCP)

HOẠT ĐỘNG

- 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.

- Người viết blog bảo mật thông tin tại infosecjournal.vn (2021 - nay)

+ Chia sẻ kiến thức về bảo mật hệ thống và ứng dụng web.

+ Hướng dẫn kiểm tra bảo mật với Kali Linux và Metasploit.

+ Viết phân tích kỹ thuật về các cuộc tấn công thực tế.

- 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.

- 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.

- 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.

DỰ ÁN

- 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

- 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