|  |  |  |
| --- | --- | --- |
| Decorative |  | Kỹ sư An toàn Thông tin |
|  | Đỗ Hà LinhMỤC TIÊU NGHỀ NGHIỆP **Tôi mong muốn tham gia các hội thảo, chương trình đào tạo chuyên sâu về bảo mật từ các tổ chức uy tín như Offensive Security, EC-Council, SANS để nâng cao trình độ chuyên môn.** |
| THÔNG TIN CÁ NHÂN  10/07/1985  Hà Nội  thaolinh252512@gmail.com  0370244817  www.website.com  HỌC VẤN - Công nghệ thông tin tại Đại học Công nghệ – ĐHQG Hà Nội KỸ NĂNG  - DevSecOps (GitLab CI + SAST/DAST)  - Burp Suite  - Cloud Security (AWS, Azure)  - Network Security SỞ THÍCH - Trồng cây  - Nấu ăn NGƯỜI GIỚI THIỆU - Bà Lương Thị Thanh (Incident Response Manager – SafeNet) - thanh.luong@safenet.vn - 0977333555  - Ông Vũ Văn Duy (Quản lý hệ thống bảo mật – DataSafe Solutions) - duy.vu@datasafe.vn - 0909111222  - Ông Nguyễn Thành Trung (Trưởng phòng An toàn Thông tin – Công ty AnToanTech) - trung.nguyen@antoantech.vn - 0908666777  - Ông Đỗ Minh Tiến (Head of Cloud Security – CloudBase VN) - tien.do@cloudbase.vn - 0911555666 |  | 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 emailDANH HIỆU VÀ GIẢI THƯỞNG - **2022** - Bằng khen vì phát hiện sớm lỗ hổng bảo mật nghiêm trọng trong hệ thống email CHỨNG CHỈ - **2021** - CompTIA Security+ – CompTIA  - **2020** - GIAC Security Essentials (GSEC) – SANS Institute  - **2021** - Microsoft Certified: Security, Compliance, and Identity Fundamentals  - **2022** - Offensive Security Certified Professional (OSCP)  - **2022** - Certified Information Systems Security Professional (CISSP) – ISC² HOẠT ĐỘNG **- 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.  **- 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. 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  **- 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  **- 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 |
|  |  |  |