|  |  |  |
| --- | --- | --- |
| Decorative |  | Kỹ sư An toàn Thông tin |
|  | Đỗ Hiếu TùngMỤC TIÊU NGHỀ NGHIỆP **Tôi muốn góp phần xây dựng hệ thống Security Awareness Training trong doanh nghiệp, giúp nhân viên hiểu về các nguy cơ như phishing, malware và tăng cường ý thức bảo vệ tài sản số.** |
| THÔNG TIN CÁ NHÂN  18/10/1997  Hà Nội  thaolinh252512@gmail.com  0398175979  www.website.com  HỌC VẤN - Quản trị và bảo mật hệ thống mạng tại Đại học CNTT – ĐHQG TP.HCM - Công nghệ thông tin tại Đại học Công nghệ – ĐHQG Hà Nội KỸ NĂNG  - Network Security  - Linux Security  - Vulnerability Assessment (Nessus, OpenVAS) SỞ THÍCH - Chơi đàn guitar  - Xem phim khoa học viễn tưởng  - Du lịch  - Thử nghiệm công nghệ mới NGƯỜI GIỚI THIỆU - Ông Trịnh Văn Kiên (Pentest Team Lead – SecureTest Lab) - kien.trinh@securetest.vn - 0944222333  - Bà Phạm Thị Mai (Cybersecurity Lead – TechShield) - mai.pham@techshield.vn - 0988999666  - Bà Lê Thị Huyền (Giám đốc An ninh Thông tin (CISO) – CloudSecure Corp) - huyen.le@cloudsecure.vn - 0912888999  - Ông Nguyễn Thành Trung (Trưởng phòng An toàn Thông tin – Công ty AnToanTech) - trung.nguyen@antoantech.vn - 0908666777 |  | KINH NGHIỆM LÀM VIỆC- **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- **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- **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- **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- **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 lýDANH HIỆU VÀ GIẢI THƯỞNG - **2022** - Top 3 kỹ sư có đóng góp lớn nhất vào chương trình bảo vệ dữ liệu khách hàng  - **2023** - Giải nhất cuộc thi 'Capture The Flag' toàn quốc do VietCyber tổ chức CHỨNG CHỈ - **2023** - AWS Certified Security – Specialty HOẠT ĐỘNG **- Thành viên nhóm nghiên cứu bảo mật tại Phòng Lab An toàn Thông tin - Đại học Bách khoa (2021 - 2023)**  + Nghiên cứu về các lỗ hổng bảo mật phổ biến như XSS, SQLi, CSRF.  + Tham gia diễn tập phát hiện và ứng phó sự cố tấn công mạng.  + Viết báo cáo kỹ thuật và trình bày tại hội nghị sinh viên NCKH.  **- 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.  **- 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 **- 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 |
|  |  |  |