|  |  |  |
| --- | --- | --- |
| Decorative |  | Kỹ sư An toàn Thông tin |
|  | Trần Sơn HòaMỤC TIÊU NGHỀ NGHIỆP **Tôi muốn nghiên cứu và triển khai các cơ chế bảo mật nâng cao như Zero Trust, Network Segmentation, và bảo vệ dữ liệu trong môi trường hybrid cloud.** |
| THÔNG TIN CÁ NHÂN  10/12/1994  Hà Nội  thaolinh252512@gmail.com  0383301420  www.website.com  HỌC VẤN - An toàn thông tin tại Học viện Kỹ thuật Mật mã KỸ NĂNG  - SIEM (Splunk, ELK)  - DevSecOps (GitLab CI + SAST/DAST) SỞ THÍCH - Thiết kế sản phẩm cá nhân  - Chụp ảnh  - Nấu ăn  - Xem phim khoa học viễn tưởng  - Sưu tầm sách lập trình NGƯỜI GIỚI THIỆU - Bà Trần Kim Ngân (Security Compliance Officer – DevSecure) - ngan.tran@devsecure.vn - 0933444555  - Ông Vũ Văn Duy (Quản lý hệ thống bảo mật – DataSafe Solutions) - duy.vu@datasafe.vn - 0909111222 |  | 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/CDDANH HIỆU VÀ GIẢI THƯỞNG - **2021** - Được đề cử danh hiệu 'Gương mặt trẻ lĩnh vực An ninh mạng'  - **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 CHỨNG CHỈ - **2023** - AWS Certified Security – Specialty  - **2022** - Certified Cloud Security Professional (CCSP) – ISC² HOẠT ĐỘNG **- 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.  **- Mentor nhóm sinh viên nghiên cứu bảo mật web tại CLB IT trẻ (2022)**  + Hướng dẫn khai thác lỗi XSS, CSRF trên các bài thực hành.  + Giám sát và hỗ trợ quá trình viết báo cáo kỹ thuật.  + Chấm điểm phần trình bày đề tài bảo mật cuối kỳ. DỰ ÁN **- 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  **- 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  **- 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 |
|  |  |  |