|  |  |  |
| --- | --- | --- |
| Decorative |  | Kỹ sư An toàn Thông tin |
|  | Phạm Anh ChâuMỤC 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  27/09/1986  Hà Nội  thaolinh252512@gmail.com  0955059793  www.website.com  HỌC VẤN - Kỹ thuật máy tính tại Đại học Sư phạm Kỹ thuật TP.HCM KỸ NĂNG  - SIEM (Splunk, ELK)  - Zero Trust Architecture  - IDS/IPS (Snort, Suricata)  - Penetration Testing SỞ THÍCH - Thử nghiệm công nghệ mới  - Viết blog kỹ thuật  - Xem phim khoa học viễn tưởng  - Tập gym NGƯỜI GIỚI THIỆU - Bà Phạm Thị Mai (Cybersecurity Lead – TechShield) - mai.pham@techshield.vn - 0988999666  - Ông Trần Quang Minh (Security Operations Manager – FinSec Việt Nam) - minh.tran@finsec.vn - 0933666888 |  | KINH NGHIỆM LÀM VIỆC- **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 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 - **2023** - Bằng khen vì hoàn thành kiểm thử xâm nhập sớm hơn kế hoạch 2 tuần  - **2020** - Top 5 kỹ sư có phản ứng sự cố nhanh nhất trong hệ thống nội bộ  - **2023** - Giải nhất cuộc thi 'Capture The Flag' toàn quốc do VietCyber tổ chức  - **2022** - Bằng khen vì phát hiện sớm lỗ hổng bảo mật nghiêm trọng trong hệ thống email  - **2021** - Được đề cử danh hiệu 'Gương mặt trẻ lĩnh vực An ninh mạng' CHỨNG CHỈ - **2023** - CompTIA PenTest+ – CompTIA 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. 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 |
|  |  |  |