|  |  |  |
| --- | --- | --- |
| Decorative |  | Kỹ sư An toàn Thông tin |
|  | Hoàng Việt NamMỤC TIÊU NGHỀ NGHIỆP **Tôi muốn trở thành chuyên gia trong việc phân tích và phản hồi sự cố bảo mật, từ việc thu thập log, phân tích forensics đến khôi phục hệ thống sau sự cố một cách nhanh chóng và hiệu quả.** |
| THÔNG TIN CÁ NHÂN  23/09/1982  Hà Nội  thaolinh252512@gmail.com  0311055089  www.website.com  HỌC VẤN - Mạng máy tính và truyền thông dữ liệu tại Đại học Giao thông Vận tải - Khoa học máy tính tại Đại học Quốc tế – ĐHQG TP.HCM KỸ NĂNG  - Zero Trust Architecture  - Penetration Testing  - Cloud Security (AWS, Azure)  - IDS/IPS (Snort, Suricata)  - Wireshark SỞ THÍCH - Đọc sách  - Tham gia hackathon  - Thử nghiệm công nghệ mới  - Viết blog kỹ thuật  - Chụp ảnh NGƯỜI GIỚI THIỆU - Ông Trần Quang Minh (Security Operations Manager – FinSec Việt Nam) - minh.tran@finsec.vn - 0933666888 |  | 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/CD- **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 - **2020** - Top 5 kỹ sư có phản ứng sự cố nhanh nhất trong hệ thống nội bộ CHỨNG CHỈ - **2021** - CompTIA Security+ – CompTIA HOẠT ĐỘNG **- 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. DỰ ÁN **- 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 |
|  |  |  |