KIM KHƯƠNG DUY

0833 033 013 kimkhuongduy@gmail.com

KINH NGHIỆM LÀM VIỆC

TỪ 2023 ĐẾN NAY: CÔNG TY CỔ PHẦN CÔNG NGHỆ VÀ DỊCH AN TOÀN BMC

QUẢN TRỊ HỆ THỐNG

- Cấu hình/ cài đặt và vận hành hệ thống phát hiện và ngăn chặn xâm nhập (IPS/IDS, Firewall)
- Cấu hình/ cài đặt và vận hành các giải pháp giám sát an ninh SIEM (MaxPatrol, Wazuh, ELK)
- Quản trị vận hành hệ thống mạng nội bộ (VPN, Firewall, Mail Server,...)

TƯ VẤN BẢO ĐẢM AN TOÀN THÔNG TIN THEO CẤP ĐỘ

- Tham gia khảo sát, đánh giá và tư vấn bảo đảm an toàn hệ thống thông tin theo 05 cấp độ cho các doanh nghiệp và cơ quan nhà nước, bao gồm các biện pháp bảo vệ, phát hiện, ứng phó và khắc phục.
- Tham gia phân tích và đánh giá lỗ hổng bảo mật, tư vấn biện pháp phòng chống tấn công cho các tổ chức nhà nước và doanh nghiệp tư nhân

ĐẢM BẢO AN TOÀN THÔNG TIN

Red Team

- Tham gia các thử thách CTF trên các nền tảng Tryhackme, Hackthebox, Vulhub
- Hiểu biết về các lỗ hổng bảo mật trong Top 10 web application security OWASP
- Kiểm tra, phân tích và đánh giá các lỗ hổng bảo mật website và hệ thống hạ tầng CNTT
- Khai thác lỗ hổng, đưa ra các minh chứng về lỗ hổng trong hệ thống và viết báo cáo sau khi khai thác
- Nắm vững các kỹ thuật leo thang đặc quyền trên Windows và Linux
- Tham gia nghiên cứu các framework mã nguồn mở, viết mã khai thác dựa trên các CVE đã công bố

Blue Team

- Phân tích log files được gửi tới SIEM, từ đó viết rules để tối ưu/ cập nhật tệp rules cho thiết bị IPS/IDS và trên các agent, sensor
- Có kiến thức cơ bản trong việc rà soát, phát hiện các thành phần mã độc, và các loại tấn công
- Nghiên cứu các giải pháp xác thực, uỷ quyền và mã hoá
- Phụ trách điều tra số, xử lý sự cố cho một vài trang web sau khi bị tấn công Deface

DỰ ÁN: TRIỂN KHAI HỆ THỐNG GIÁM SÁT AN NINH MẠNG CHO HỆ THỐNG MẠNG NỘI BỘ CÔNG TY

- Triển khai hệ thống giám sát an ninh mạng cho mạng nội bộ công ty, sử dụng IPS/IDS, Tường lửa,máy chủ SIEM,...
- Phát triển ứng dụng quản lý cho các thiết bị IPS/IDS và Tường lửa, cho phép giám sát và điều khiển hệ thống.
- Thiết kế các kịch bản tấn công, xây dựng phòng thí nghiệm kiểm tra để chứng minh khả năng của hệ thống.
- Thực thi các demo tấn công, viết báo cáo và thuyết trình cho khách hàng về các tính năng của thiết bị/hệ thống và cách chúng phản ứng với các mối đe dọa này

TRÌNH ĐỘ HỌC VẤN

- **Học viện Kỹ thuật Mật mã** 2016 - 2017
  An toàn thông tin
- **Học viện Bảo vệ Liên Bang FSO - Liên Bang Nga** 2017 - 2023
  Công nghệ điện tử viễn thông và Hệ thống liên lạc đặc biệt

CHỨNG CHỈ

- Certified AppSec Practitioner (CAP)
- Cyber kill chain and Unified kill chain
- Cyber Threat Intelligence
- Network Security and Traffic Analysis
- Security Information and Event Management (SIEM)

KỸ NĂNG

Programing

C++ Python JavaScript Bash Script

Systems

Kali Linux Ubuntu Windows Centos

Tools

Security related: Metasploit Burp Suite Nmap John the Ripper Nikto Hydra Sqlmap Autopsy Bloodhound LinPEAS WinPEAS WireShark Mimikazt Gobuster Volatility

Framework & Softwares

Security related: Suricata Snort Elastic Stack ImpulseXDR Keycloak MaxPatrol SIEM

Network related: Software-Defined Networking mininet OpenDaylight Floodlight

Designer related: Figma Inkscape Photoshop Visio

Language

English Russian