PHẠM TIẾN ĐỒNG

SOC ANALYST

THÔNG TIN CÁ NHÂN

0915976795

phamtiendong6795@gmail.com

www.phamtiendong.com

HỌC VẤN

Đại học Công nghệ TP. Hồ Chí Minh (HUTECH)
Công nghệ thông tin – Chuyên ngành An ninh mạng (09/2022 – nay)
GDP: 3.17
Nền tảng: Mạng máy tính, Hệ điều hành, Mật mã học, Lập trình, CSDL, Hệ thống

KỸ NĂNG

- SIEM: Splunk, Splunk Forwarder, ...
- Scripting: Python, PowerShell, ...
- Hệ điều hành: Windows Server, Linux cơ bản
- Network: TCP/IP, TLS/SSL, IDS/IPS
- AI: Ứng dụng và thành thạo một số công cụ AI hỗ trợ học tập & công việc

NGOẠI NGỮ

- English
- Giao tiếp, đọc hiểu tài liệu tiếng Anh ở mức cơ bản

MỤC TIÊU NGHỀ NGHIỆP

Mong muốn trở thành SOC Analyst. Đam mê, chủ động học hỏi công nghệ và quy trình Blue Team. Sẵn sàng trực 24/7 và tham gia khắc phục sự cố để bảo vệ hệ thống doanh nghiệp.

THÀNH TỰU

- Đạt danh hiệu sinh viên tiêu biểu (2025)
- Thành viên đội tuyển sinh viên An ninh mạng HUTECH (2025)
- Tham gia các cuộc thi: HDBANK (2024), CTF The Maze of Shadows (2025)
- Tích cực tham gia hoạt động:Trường, khoa, đoàn – hội, sự kiện, tình nguyện, hiến máu

PROJECT NỔI BẬT

SOC Lab – Blue Team

- Triển khai hệ thống SOC với Splunk trên Windows & Ubuntu
- Mô phỏng và phát hiện các tấn công: Brute-force RDP/SMB, Reverse Shell, DoS, Malware
- Thực hiện: phát hiện – phân tích – phản ứng – khắc phục
- Viết báo cáo phân tích log chi tiết

PHÂN TÍCH LOG WINDOWS/LINUX ĐỂ PHÁT HIỆN TẤN CÔNG

- Công nghệ sử dụng: Splunk, Wazuh, n8n, Python/Node.js, Google Gemini API, Docker.
- Phân tích Log chuyên sâu: Thực hiện quy trình: Phát hiện – Phân tích – Phản ứng – Khắc phục dựa trên khung 5W1H và chuẩn hóa dữ liệu log từ Sysmon và Auditd.
- Tự động hóa vận hành (SOAR): Thiết kế và tối ưu hóa các workflow trên n8n, kết nối Splunk với AI (Google Gemini) và Code JS để tự động hóa 100% các tác vụ phân tích Tier 1.

CHỨNG CHỈ