THÔNG TIN YÊU CẦU TUYỂN DỤNG
NHÂN SỰ PHÒNG BẢO MẬT AN TOÀN THÔNG TIN HỆ THỐNG, GIÁM SÁT

I. YÊU CẦU CHUNG:

1. Vị trí tuyển dụng: Kỹ sư/Chuyên viên lĩnh vực An toàn thông tin – Bảo mật An toàn thông tin.
2. Số lượng nhân sự: 01 người
3. Trình độ học vấn, chuyên môn: Tốt nghiệp Đại học chính quy trở lên các chuyên ngành: CNTT/ATTT và các ngành liên quan CNTT khác.
4. Kinh nghiệm làm việc: Tối thiểu 03 năm kinh nghiệm trong lĩnh vực Công nghệ thông tin/An toàn thông tin và chuyên môn phù hợp với lĩnh vực.
5. Mô tả tóm tắt công việc các vị trí cần tuyển dụng:

An toàn thông tin hệ thống, giám sát:

+ Triển khai & quản lý cấu hình bảo mật Network/Server: FW, IPS/IDS, VPN, NAC, WAF, …
+ Quản lý hardening baseline cho hệ thống máy chủ vật lý/ảo, thiết bị mạng, dịch vụ nền tảng (AD, OS, SQL, IIS…)
+ Thực hiện quét lỗ hổng định kỳ, phân loại theo mức độ rủi ro, phối hợp bộ phận vận hành để triển khai bản vá bảo mật (Patch Tuesday, Zero-day), theo dõi và báo cáo tỷ lệ khắc phục lỗ hổng.
+ Tham gia thiết kế, thử nghiệm và triển khai các giải pháp bảo mật mới cho hạ tầng mạng, hệ thống. Đánh giá hiệu năng, khả năng tích hợp và chuyển giao vận hành (SOC hoặc bộ phận vận hành).
+ Theo dõi các cảnh báo liên quan đến hạ tầng/mạng trên hệ thống SIEM/SOAR.
+ Phối hợp SOC & IR xử lý sự cố (malware infection, DDoS, brute-force, data leak…). Thu thập bằng chứng số (forensics), lập Incident Ticket và Post-Incident Report.
+ Thu thập, phân tích thông tin Threat Intelligence (từ nguồn nội bộ & bên ngoài).
+ Báo cáo tình trạng bảo mật hạ tầng, mạng định kỳ Ban LĐ, đề xuất cải tiến kỹ thuật, tối ưu cấu hình bảo mật, cải thiện hiệu quả hệ thống giám sát và khả năng phản ứng.

II. YÊU CẦU VỀ KỸ NĂNG

1. Ngoại ngữ: Ưu tiên các ứng viên sử dụng thành tạo Tiếng Anh giao tiếp và tiếng Anh chuyên ngành CNTT.
2. Kỹ năng chuyên môn:

+ Có nền tảng tốt về kiến trúc ứng dụng, hệ thống thông tin.
+ Có các chứng chỉ về bảo mật liên quan
+ Có kiến thức & kỹ năng chuyên môn
    - ✓ Kiến thức về Network Security: TCP/IP, Firewall, VPN, IDS/IPS, Network segmentation.
    - ✓ Kiến thức System Security & Hardening cho Windows Server/Linux/Active Directory.
    - ✓ Kinh nghiệm sử dụng các công cụ Vulnerability Assessment (Rapid7, Nessus, Qualys hoặc tương đương).
    - ✓ Có khả năng phân tích log và cảnh báo bảo mật từ SIEM, EDR/XDR, NDR.
    - ✓ Hiểu biết cơ bản về Threat Intelligence, Malware, Phishing và MITRE ATT&CK.

- ✓ Có kinh nghiệm tham gia giám sát SOC, phối hợp điều tra và xử lý sự cố ATTT (Incident Response).Có kiến thức và kinh nghiệm thực tế trong một hoặc nhiều mảng:
- ✓ Network security, System Hardening.
- ✓ Vulnerability Assessment.
- ✓ SOC monitoring/Incident Response.

+ Có kinh nghiệm triển khai hoặc vận hành các giải pháp Microsoft Security là một lợi thế (Microsoft Defender/EDR, Intune, Purview).

3. Kỹ năng khác

- Giao tiếp & là việc nhóm
- Phân tích và tổng hợp số liệu; soát xét và viết báo cáo.
- Khả năng lập kế hoạch và quản lý công việc
- Phản biện & giải quyết vấn đề
- Quản lý thời gian và ứng biến, xử lý vấn đề khác

II. YÊU CẦU PHẨM CHẤT

- Có phẩm chất trung thực, khách quan, ý thức tuân thủ kỷ luật, chấp hành pháp luật
- Chuyên nghiệp, lịch sự, quyết đoán và có tinh thần học hỏi, tinh thần trách nhiệm cao.
- Tinh thần hợp tác trong công việc, tâm huyết với công việc và cam kết làm việc lâu dài tại PVI.