THÔNG TIN YÊU CẦU TUYỂN DỤNG NHÂN SỰ PHÒNG BẢO MẬT

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: 03 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.

3.1. Vị trí An toàn thông tin chính sách, tuân thủ (GRC & Compliance)

Tốt nghiệp Đại học chính quy trở lên các chuyên ngành: CNTT/ATTT và các ngành liên quan CNTT khác

+ Hiểu biết về ISO/IEC 27001:2022, ISO 27005, ISO 27701, NIST CSF, ITIL.
+ Nắm rõ các quy định pháp lý Việt Nam: Nghị định 13/2023/NĐ-CP, Nghị định 85/2016/NĐ-CP, Luật ATTT mạng.
+ Có các chứng chỉ về bảo mật liên quan

3.2. Vị trí An toàn thông tin hệ thống, giám sát (SOC/Infra/Network/Endpoint Security)

+ Tốt nghiệp Đại học chính quy trở lên các chuyên ngành: CNTT/ATTT và các ngành liên quan CNTT khác.
+ 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).

3.3. Vị trí An toàn thông tin ứng dụng (AppSec/DevSecOps/Secure SDLC)

+ Tốt nghiệp Đại học chính quy trở lên các chuyên ngành: CNTT/ATTT và các ngành liên quan CNTT khác.
+ Có các chứng chỉ về bảo mật liên quan
+ Có nền tảng tốt về lập trình, kiến trúc ứng dụng, hệ thống thông tin.
+ Có kiến thức vững về:
    - Bảo mật ứng dụng web/API/mobile
    - OWASP Top 10, OWASP ASVS, OWASP API Security
    - Các lỗ hổng phổ biến: SQL Injection, XSS, IDOR, CSRF, …
+ Có hiểu biết: Vòng đời phát triển phần mềm an toàn (Secure SDLC / DevSecOps), Kiến trúc ứng dụng nhiều lớp, các cơ chế xác thực, phân quyền

+ Có khả năng: Đọc, hiểu và phân tích mã nguồn (Java, .NET, PHP, …), Đánh giá rủi ro ATTT ứng dụng và đề xuất biện pháp khắc phục phù hợp.
+ Có hiểu biết cơ bản về: Hệ điều hành Windows/Linux.

4. Kinh nghiệm làm việc: Tối thiểu 01 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:

5.1. Vị trí An toàn thông tin chính sách, tuân thủ (GRC & Compliance)

+ Tham gia xây dựng, rà soát, cập nhật Bộ chính sách, quy trình và tiêu chuẩn ATTT.
+ Quản lý tài liệu, hỗ trợ vận hành hệ thống quản lý an toàn thông tin ISO 27001:2022.
+ Thực hiện đánh giá rủi ro, cập nhật, theo dõi tình trạng khắc phục rủi ro (Risk Treatment Plan)
+ Theo dõi và đảm bảo tuân thủ các yêu cầu pháp lý & tiêu chuẩn quốc tế: ISO 27001:2022, Nghị định 13/2023/NĐ-CP, Luật ATTT mạng, Nghị định 85/2023
+ Xác định nhu cầu, đánh giá rủi ro, lập đề xuất & trình phê duyệt các giải pháp ATTT mới.
+ Đánh giá, quản lý tuân thủ ATTT.
+ Hỗ trợ triển khai chương trình truyền thông, đào tạo nhận thức ATTT (E-learning, workshop, phishing simulation).

5.2. Vị trí An toàn thông tin hệ thống, giám sát (SOC/Infra/Network/Endpoint Security)

+ 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.

5.3. Vị trí An toàn thông tin ứng dụng (AppSec/DevSecOps/Secure SDLC)

+ Đảm bảo công tác kiểm thử bảo mật định kỳ (pentest, fuzzing, API testing) đối với ứng dụng nội bộ và ứng dụng của đối tác. Phối hợp với bên thứ ba khi thực hiện kiểm thử độc lập.
+ Xây dựng, triển khai và duy trì chu trình phát triển phần mềm an toàn (SDLC), Checklist bảo mật cho từng giai đoạn: yêu cầu – thiết kế – phát triển – kiểm thử – triển khai
+ Tích hợp các công cụ SAST (Static Application Security Testing), DAST (Dynamic), SCA (Software Composition Analysis) vào pipeline CI/CD (GitHub Actions…).

+ Xây dựng rule và quy trình tự động quét mã nguồn, phát hiện lỗ hổng, gửi cảnh báo cho Dev team, thiết lập tiêu chí Security Gate trong quy trình release ứng dụng.
+ Theo dõi và xác minh việc khắc phục các lỗi bảo mật (remediation verification).
+ Kiểm tra, giám sát API Gateway đảm bảo xác thực & phân quyền đúng quy định. Rà soát cấu hình bảo mật ứng dụng web & container.
+ Hướng dẫn Dev team thực hành Secure Coding theo OWASP Top 10, Hỗ trợ phân tích nguyên nhân gốc khi có lỗ hổng tái diễn.
+ Báo cáo kết quả kiểm thử, phát hiện lỗ hổng, chỉ số bảo mật ứng dụng định kỳ cho Ban LĐ.

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:

2.1. Vị trí An toàn thông tin chính sách, tuân thủ (GRC & Compliance)

Kỹ năng/kinh nghiệm một trong các công việc sau: tối thiểu 01 năm kinh nghiệm trong lĩnh vực xây dựng chính sách, quản lý rủi ro IT, kiểm toán CNTT, ISO 27001, hoặc tuân thủ bảo mật. Kỹ năng viết quy trình, quản lý tài liệu, lập báo cáo, phân tích rủi ro. Kỹ năng giao tiếp, phối hợp liên phòng ban, làm việc nhóm và độc lập. Ưu tiên có kinh nghiệm làm việc trong tổ chức đã chứng nhận ISO 27001/27701 hoặc trong ngành BFSI.

2.2. Vị trí An toàn thông tin hệ thống, giám sát (SOC/Infra/Network/Endpoint Security)

+ Có kiến thức và kinh nghiệm thực tế trong một hoặc nhiều mảng:
o Network security, System Hardening.
o Vulnerability Assessment.
o SOC monitoring/Incident Response.

+ Kỹ năng/kinh nghiệm một trong các công việc sau: tối thiểu 01 năm kinh nghiệm trong lĩnh vực ATTT hệ thống, mạng, SOC. Ưu tiên ứng viên có kinh nghiệm trong môi trường BFSI hoặc có chứng chỉ Security+, CEH, Microsoft Security Certifications.

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

2.3. Vị trí An toàn thông tin ứng dụng (AppSec/DevSecOps/Secure SDLC)

Kỹ năng/kinh nghiệm một trong các công việc sau: tối thiểu 01 năm kinh nghiệm trong lĩnh vực ATTT ứng dụng, Audit/Pentest, DevSecOps, Secure Code Review. Ưu tiên ứng viên có kinh nghiệm trong môi trường BFSI, đã tham gia các đợt pentest độc lập/thuê ngoài hoặc có các chứng chỉ quốc tế AppSec uy tín: OSCP, OSWE, GWAPT, …

3. Kỹ năng khác:
   - Kỹ năng giao tiếp và thuyết trình.
   - Nhanh nhạy trong việc học hỏi kiến thức.
   - Kỹ năng làm 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
   - Quản lý thời gian và ứng biến, xử lý vấn đề

III. 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.