PHỤ LỤC

I. NHÂN VIÊN KIỂM TRA, ĐÁNH GIÁ AN TOÀN THÔNG TIN

1. Mô tả công việc

Kiểm tra, đánh giá an toàn thông tin cho Website/Application, các thiết bị IOT, các hệ thống hạ tầng, network theo yêu cầu của Trung tâm VNCERT/CC.

2. Yêu cầu kiến thức

- Hiểu biết về python, golang và ít nhất 1 ngôn ngữ lập trình web, app.

- Hiểu biết về các lỗ hổng, điểm yếu về bảo mật như cơ bản owasp, và các biện pháp phòng chống, khắc phục lỗ hổng.

- Hiểu biết về các giải pháp bảo mật như Firewall, IDS/IPS, SIEM, …

- Hiểu biết về 1 số tool đánh giá an toàn thông tin như burpsuite, nmap, kalilinux, metasploit, wireshark, nessus, …

- Hiểu biết về 1 số tiêu chuẩn an toàn thông tin như NIST, CIS, MITRE ATT&CK.

3. Yêu cầu kỹ năng

- Kỹ năng sử dụng các công cụ tự động để kiểm tra, đánh giá an toàn thông tin.

- Kỹ năng tự viết các đoạn mã để khai thác, đánh giá an toàn thông tin.

- Kỹ năng cập nhật, nghiên cứu, tìm hiểu các lỗ hổng mới.

- Kỹ năng đánh giá, tư vấn về an toàn thông tin đối với kiến trúc, hạ tầng trong các dự án, đề xuất các mô hình an toàn thông tin, biện pháp bảo mật.

4. Yêu cầu kinh nghiệm

- Có kinh nghiệm kiểm tra, đánh giá an toàn thông tin đối với website hoặc application hoặc thiết bị IOT.

- Có CVE, GitHub, blog chia sẻ về trải nghiệm là lợi thế.

II. NHÂN VIÊN NGHIÊN CỨU XÂY DỰNG TIÊU CHUẨN, QUY CHUẨN AN TOÀN THÔNG TIN

1. Mô tả công việc

- Nghiên cứu các tiêu chuẩn quốc tế về an toàn thông tin mạng (Tiêu chuẩn của các tổ chức quốc tế như ISO, IEC, NIST, CODEX, ITU, ASTM …)

- Đề xuất, xây dựng, triển khai, áp dụng các tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin phù hợp với tình hình thực tiễn Việt Nam.

2. Yêu cầu kiến thức

- Kiến thức cơ bản về quản trị hệ thống, quản trị mạng hoặc quản lý chất lượng sản phẩm dịch vụ số, Công nghệ thông tin.

- Kiến thức cơ bản về kiến trúc, lỗ hổng ATTT, bảo mật ứng dụng …

- Kiến thức cơ bản về quy trình phát triển, cung cấp sản phẩm dịch vụ CNTT, ATTT.

- Kiến thức về các tiêu chuẩn về an toàn thông tin (ISO 27000/ISO 27017; ISO 27035/NIST ...), hệ thống quản lý chất lượng (ISO 9001).

3. Yêu cầu kỹ năng

- Có khả năng giao tiếp tốt, làm việc nhóm, làm việc độc lập.

- Có khả năng đọc hiểu tài liệu chuyên ngành Tiếng Anh.

4. Yêu cầu kinh nghiệm

- Kinh nghiệm làm việc về lĩnh vực an toàn thông tin.

- Kinh nghiệm triển khai các tiêu chuẩn ISO 27001, ISO 27017,… là một lợi thế.

III. NHÂN VIÊN PHÁT TRIỂN ỨNG DỤNG

1. Mô tả công việc

Lập trình, phát triển các hệ thống, ứng dụng web theo yêu cầu của Trung tâm VNCERT/CC.

2. Yêu cầu kiến thức

- Hiểu biết về các ngôn ngữ sau: JavaScript, Golang, PHP.

- Hiểu biết về CRUD với các DB: MySQL, MongoDB, PostgreSQL.

- Hiểu biết về docker, docker-compose.

- Hiểu biết về backend, api, realtime và các tác vụ hệ thống.

3. Yêu cầu kỹ năng

- Kỹ năng lập trình, phát triển backend với NodeJS (Fastify), Golang (fasthttp), PHP (thuần).

- Kỹ năng query và update dữ liệu lớn, đảm bảo performance trên MySQL, MongoDB và PostgreSQL.

- Kỹ năng lập trình an toàn, hiểu biết về các lỗ hổng gây mất an toàn thông tin cho ứng dụng web: SQL Injection, XSS, LFI, SSRF,...

- Kỹ năng CI/CD và deploy hệ thống, ứng dụng trên máy chủ.

4. Yêu cầu kinh nghiệm

- Có ít nhất 01 dự án/sản phẩm về ứng dụng, hệ thống web có thể demo/trải nghiệm.

- Có account github và các hoạt động trên github là một lợi thế.

- Biết HTML, CSS là một lợi thế.

IV. NHÂN VIÊN CHỐNG THƯ RÁC

1. Mô tả công việc

- Quản lý, phòng chống, xử lý thư điện tử rác, tin nhắn rác.

- Vận hành hệ thống kỹ thuật hỗ trợ phòng chống, ngăn chặn thư điện tử, tin nhắn rác.

- Quản lý tên định danh.

2. Yêu cầu kiến thức

- Kiến thức nền tảng về hệ thống, mạng, CNTT/ATTT.

- Kinh nghiệm về việc xây dựng, áp dụng các văn bản quy phạm pháp luật Việt Nam.

- Có khả năng đọc hiểu tài liệu chuyên ngành Tiếng Anh.

3. Yêu cầu kỹ năng

- Kỹ năng quản lý đội, nhóm.

- Kỹ năng tổ chức, điều phối xử lý tin nhắn rác, thư điện tử rác.

- Kỹ năng tổng hợp, phân tích, báo cáo, tham mưu, xử lý công việc.

- Kỹ năng áp dụng, cập nhật, nghiên cứu tài liệu, các quy định về chuyên môn, nghiệp vụ.

4. Yêu cầu kinh nghiệm

- Có tối thiểu 01 năm quản lý đội nhóm.

- Có tối thiểu 03 năm hoạt động, làm việc trong lĩnh vực CNTT/ATTT.

- Đã từng triển khai các dự án về liên quan tới tin nhắn, thư điện tử.

V. NHÂN VIÊN GIÁM SÁT AN TOÀN THÔNG TIN

1. Mô tả công việc

- Phát triển và duy trì chính sách an ninh mạng, quy trình và hướng dẫn liên quan.

- Thực hiện đánh giá rủi ro an ninh thông tin và đề xuất các biện pháp giảm nhẹ.

- Giám sát và phân tích các cảnh báo an ninh mạng, đảm bảo các sự cố được xử lý nhanh chóng và hiệu quả.

- Phối hợp các đội khác để thực hiện kiểm tra an ninh hệ thống và ứng dụng, bao gồm cả kiểm tra xâm nhập và quét lỗ hổng.

2. Yêu cầu kiến thức

- Hiểu biết về các chuẩn an ninh thông tin như ISO 27001, NIST, CIS, và PCI DSS.

- Kiến thức về kiến trúc mạng, hệ điều hành, ứng dụng và cơ sở dữ liệu.

- Hiểu biết về các công cụ và phương pháp an ninh mạng, bao gồm Firewall, IDS/IPS, WAF, và SIEM, ...

- Hiểu biết về hệ thống máy chủ, hệ thống mạng.

3. Yêu cầu kỹ năng

- Có kỹ năng lập trình, triển khai hệ thống, giải pháp bảo mật, giám sát đảm bảo tính ổn định, hiệu quả.

- Khả năng tổ chức và quản lý thời gian hiệu quả, đảm bảo đáp ứng các mục tiêu và thời hạn.

- Kỹ năng tìm hiểu và xử lý vấn đề, giải quyết các lỗi hệ thống, sự cố trong quá trình triển khai, vận hành hay các sự cố an ninh.

- Kỹ năng tìm hiểu, nghiên cứu và phát triển các tính năng, giải pháp mới phục vụ công việc.

4. Yêu cầu kinh nghiệm

- Kinh nghiệm trong lĩnh vực an ninh mạng, bao gồm kinh nghiệm trong vai trò phân tích hoặc giám sát.

- Kinh nghiệm trong việc thực hiện đánh giá rủi ro, kiểm tra xâm nhập, và quản lý sự cố an ninh.

- Kinh nghiệm triển khai các hệ thống giám sát, giải pháp bảo mật.

VI. NHÂN VIÊN ỨNG CỨU SỰ CỐ

1. Mô tả công việc

Ứng cứu, điều phối, xử lý sự cố an toàn thông tin.

2. Yêu cầu kiến thức

- Hiểu biết về các mối đe dọa an ninh mạng, lỗ hổng bảo mật, và phương pháp phòng chống tấn công.

- Hiểu biết về quản lý log và giám sát hệ thống.

- Hiểu biết về các ngôn ngữ lập trình: Python, Powershell, Bash.

- Hiểu biết về các hệ thống máy chủ: Windows, Linux.

- Hiểu biết về các sản phẩm bảo mật như: Firewall, IDS/IPS, SIEM, EDR, WAF.

3. Yêu cầu kỹ năng

- Kỹ năng phát hiện và phân tích sự cố an toàn thông tin.

- Kỹ năng phân tích sự kiện, log: access logs, windows event logs (sysmon logs), auth/secure logs.

- Kỹ năng viết tài liệu và báo cáo sự cố an toàn thông tin chi tiết và đầy đủ.

- Kỹ năng giao tiếp và làm việc nhóm.

- Sẵn sàng làm việc ngoài giờ và trong các tình huống khẩn cấp.

4. Yêu cầu kinh nghiệm

- Có kinh nghiệm làm việc với các công nghệ bảo mật và các hệ thống, máy chủ, thiết bị mạng.

- Có kinh nghiệm phân tích, điều tra sự cố.

- Có kinh nghiệm chơi CTF mảng Forensics, Reverse hoặc làm việc với các công cụ giám sát hệ thống, phát hiện xâm nhập, quản lý log, và báo cáo sự cố an toàn thông tin là một lợi thế.

- Tiếng Anh giao tiếp tốt là một lợi thế.

VII. NHÂN VIÊN SĂN LÙNG CÁC MỐI ĐE DỌA (THREAT HUNTING)

1. Mô tả công việc

Triển khai các hoạt động săn lùng mối nguy hại (Threat Hunting).

2. Yêu cầu kiến thức

- Hiểu biết về các mối đe dọa an ninh mạng, lỗ hổng bảo mật phổ biến

- Nắm bắt được Cyber kill chain và ATT&CK.

- Nắm bắt, sử dụng thành thạo các công cụ rà soát, phân tích như: Loki, Autoruns, PCHunter, splunk, GRR.

- Hiểu biết về các ngôn ngữ lập trình: Python, Powershell, Bash.

- Hiểu biết về các hệ thống máy chủ: Windows, Linux.

3. Yêu cầu kỹ năng

- Kỹ năng phân tích sự kiện, log ứng dụng, máy chủ, thiết bị.

- Kỹ năng dịch ngược, phân tích mã độc cơ bản trên Windows .

- Sẵn sàng làm việc ngoài giờ và trong các tình huống khẩn cấp.

4. Yêu cầu kinh nghiệm

- Có kinh nghiệm xử lý các sự cố liên quan đến Ransomware, tấn công APT.

- Có kinh nghiệm phân tích điều tra các hệ thống bị xâm nhập.

- Có kinh nghiệm threat hunting diện rộng trên nhiều hệ thống là 1 lợi thế.

VIII. TỔ CHỨC, ĐIỀU PHỐI TRIỂN KHAI HOẠT ĐỘNG BẢO VỆ TRẺ EM TRÊN MÔI TRƯỜNG MẠNG

1. Mô tả công việc

- Rà soát, hoàn thiện hành lang pháp lý, cơ chế chính sách về bảo vệ và hỗ trợ trẻ em tương tác lành mạnh trên môi trường mạng.

- Tổ chức các chương trình giáo dục, truyền thông nâng cao nhận thức và trang bị kỹ năng bảo vệ trẻ em trên môi trường mạng.

- Triển khai các biện pháp, giải pháp kỹ thuật, ứng dụng công nghệ hỗ trợ bảo vệ trẻ em trên môi trường mạng.

2. Yêu cầu kiến thức

- Kiến thức cơ bản về an toàn thông tin.

- Kiến thức về bối cảnh chung của các hoạt động phát triển ở Việt Nam cũng như các quy định, luật, chiến lược quốc gia mới nhất liên quan đến quyền trẻ em và việc thực hiện Luật Trẻ em.

3. Yêu cầu kỹ năng

- Kỹ năng quản lý & điều phối, giao tiếp và phát triển mối quan hệ tốt.

- Kỹ năng Tiếng Anh tốt.

4. Yêu cầu kinh nghiệm

- Kinh nghiệm triển khai các hoạt động truyền thông.

- Kinh nghiệm làm việc về lĩnh vực an toàn thông tin/ Kinh nghiệm về công tác xã hội, dịch vụ trợ giúp trẻ em và quyền trẻ em.