


PHỤ LỤC: BẢNG PHÂN BẠC KỸ SƯ, LỘ TRÌNH NGHỀ NGHIỆP VÀ CHI TIẾT VỀ PHÂN BẠC NGHỀ

Tên chức danh	Xử lý sự cố ATTT - Cyber Incident Responder			
Nghề	An toàn thông tin (002)			
Các level và bậc HRL	Junior Responder Experienced Responder Senior Responder Expert Responder			
Tóm tắt về vị trí công việc	Mục tiêu chính: Điều tra, phân tích và ứng phó với các sự cố ATTT xảy ra trên hạ tầng CNTT của Tổ chức			
Lộ trình				
Nội dung	Các level			
	Junior Responder	Experienced Responder	Senior Responder	Expert Responder
A. Tiêu chí phân bậc				
Kiến thức & Kỹ năng chuyên môn	<ul style="list-style-type: none"><li>Kiến thức về các khái niệm &amp; giao thức mạng máy tính, cũng như các phương pháp luận về An ninh mạng</li><li>Kiến thức về mô hình OSI và các giao thức mạng cơ bản (ví dụ: TCP/IP, DNS, DHCP)</li><li>Kiến thức về các dịch vụ &amp; giao thức truyền thông mạng (ví dụ: HTTP, FTP, SMTP, POP)</li><li>Kiến thức về quản trị hệ thống, mạng và OS hardening</li><li>Kiến thức về những kẻ tấn công mạng (ví dụ: script kiddies, blackhat, whitehat, nation sponsored, ...)</li><li>Kiến thức về các phương pháp phân tích lưu lượng mạng (Network traffic)</li><li>Kiến thức về các mối đe dọa (threat) &amp; lỗ hổng (vulnerability) ATTT</li><li>Kiến thức về sao lưu và phục hồi dữ liệu</li><li>Kỹ năng xác định, thu thập, xử lý, báo cáo về phần mềm độc hại</li><li>Kỹ năng báo mật thông tin trao đổi trên môi trường mạng</li></ul>	<p><b>Các yêu cầu như level 1 và:</b></p> <ul style="list-style-type: none"><li>Kiến thức về phương pháp ứng phó và xử lý sự cố</li><li>Kiến thức về các phương pháp và kỹ thuật phát hiện xâm nhập để phát hiện các cuộc tấn công xâm nhập dựa trên lớp máy chủ và lớp mạng</li><li>Kiến thức về các khái niệm và phương pháp phân tích phần mềm độc hại (malware analysis)</li><li>Kiến thức về các giai đoạn tấn công mạng (ví dụ: trinh sát (reconnaissance), dò quét (scanning), liệt kê (enumeration), giành quyền truy cập (gaining access), nâng đặc quyền (escalation of privileges), duy trì quyền truy cập (maintaining access), xóa vết (covering tracks))</li><li>Kiến thức về các mối đe dọa, lỗ hổng bảo mật hệ thống &amp; ứng dụng (Ví dụ: Tràn bộ đệm, mã độc, XSS, SQLi, injection, hijacking, ...)</li><li>Kiến thức về rủi ro bảo mật ứng dụng (ví dụ: top 10 OWASP)</li><li>Kỹ năng nhận biết, phân loại các loại lỗ hổng &amp; các cuộc tấn công liên quan</li><li>Kỹ năng sử dụng các công cụ tương quan sự kiện bảo mật</li></ul>	<p><b>Các yêu cầu như level 2 và:</b></p> <ul style="list-style-type: none"><li>Kiến thức về các loại sự cố, ứng phó sự cố và tiến trình phản ứng</li><li>Kiến thức về các quy trình quản lý rủi ro (ví dụ: các phương pháp đánh giá và giảm thiểu rủi ro)</li><li>Kiến thức về những gì cấu thành một cuộc tấn công mạng và mối quan hệ giữa cuộc tấn công mạng với các mối đe dọa và lỗ hổng bảo mật</li><li>Kiến thức về các chính sách, phương pháp, quy định về phòng thủ mạng và an toàn thông tin</li><li>Kiến thức về các hình thức tấn công khác nhau (ví dụ: passive, active, nội gián (insider), close-in (physical), phân tán (distribution), ...)</li><li>Kiến thức về các nguyên tắc kiến trúc ATTT (ví dụ: phòng thủ chiều sâu (defense-in-depth), bảo vệ đa lớp (multi-layered approach))</li><li>Kiến thức về các tác động cụ thể của việc mất ATTT</li><li>Kỹ năng bảo vệ hệ thống chống phần mềm độc hại (ví dụ: NIPS, anti-malware, restrict/prevent external devices, spam filters)</li><li>Kỹ năng thực hiện đánh giá thiệt hại</li></ul>	<p><b>Các yêu cầu như level 3 và:</b></p> <ul style="list-style-type: none"><li>Kiến thức về các mô hình dịch vụ điện toán đám mây (Cloud) và khả năng các mô hình đó có thể gây hạn chế công tác ứng phó sự cố</li><li>Kiến thức về phân loại thông tin &amp; phương cách ứng phó với xâm phạm thông tin của một tổ chức</li><li>Kiến thức về luật, quy định, chính sách, văn đề đạo đức liên quan đến an ninh mạng và quyền riêng tư</li><li>Kỹ năng thiết kế chương trình xử lý sự cố cho các mô hình dịch vụ Cloud</li><li>Kỹ năng bảo quản tính toàn vẹn của chứng cứ theo tiêu chuẩn quốc gia, quốc tế</li></ul>
Kỹ năng mềm	<ul style="list-style-type: none"><li>Khả năng tìm kiếm thông tin</li><li>Tuân thủ kỷ luật, giờ giấc và mức độ commitment</li></ul>	<p><b>Có các kỹ năng của level 1 và:</b></p> <ul style="list-style-type: none"><li>Tập trung vào khách hàng</li><li>Nhiệt tình và tích cực</li></ul>	<p><b>Có các kỹ năng của level 2 và:</b></p> <ul style="list-style-type: none"><li>Liên tục học hỏi</li><li>Khả năng chủ động</li></ul>	<p><b>Có các kỹ năng của level 3 và:</b></p> <ul style="list-style-type: none"><li>Kỹ năng giao tiếp</li><li>Kỹ năng Mentor</li></ul>
Chứng chỉ/ Khóa học	<p><b>Khoá học:</b> <u>Must:</u> - CEH nội bộ - OSCP nội bộ <u>Should:</u> #N/A <u>Nice:</u> - SEC401 - SEC504</p> <p><b>Chứng chỉ:</b> <u>Must:</u> Chứng chỉ nội bộ CEH và OSCP <u>Should:</u> - CEH, OSCP, GREM, GSEC <u>Nice:</u> - CySA+, ICSP, SSCP, Security+</p>	<p><b>Khoá học:</b> <u>Must:</u> Một trong 2 khóa: Malware Reverse/Web Security <u>Should:</u> SEC487, FOR578 <u>Nice:</u> #N/A</p> <p><b>Chứng chỉ:</b> <u>Must:</u> - 1 trong 2 chứng chỉ: Malware Reverse hoặc Web Security <u>Should:</u> - CEH, OSCP, GREM, GCTI <u>Nice:</u> #N/A</p>	<p><b>Khoá học:</b> <u>Must:</u> Một trong 2 khóa: Malware Reverse/Web Security <u>Should:</u> SEC487, FOR578 <u>Nice:</u> #N/A</p> <p><b>Chứng chỉ:</b> <u>Must:</u> - 1 trong 2 chứng chỉ: Malware Reverse hoặc Web Security <u>Should:</u> - CEH, OSCP, GREM <u>Nice:</u> #N/A</p>	<p><b>Khoá học:</b> <u>Must:</u> Một trong 2 khóa: Malware Reverse/Web Security <u>Should:</u> SEC487, FOR578 <u>Nice:</u> #N/A</p> <p><b>Chứng chỉ:</b> <u>Must:</u> - 1 trong 2 chứng chỉ: Malware Reverse hoặc Web Security <u>Should:</u> - CEH, OSCP, GREM, GSE <u>Nice:</u> #N/A</p>
Kinh nghiệm	Thông thường kinh nghiệm dưới 1 năm	Thông thường có kinh nghiệm từ 1-3 năm	Thông thường có kinh nghiệm từ 4-7 năm	Thông thường có kinh nghiệm trên 8 năm

Số và ký hiệu: 1795/TB-VCS-TCHC  
Ngày ban hành: 09/10/2021

Nhiệm vụ	- Thu thập dữ liệu có khả năng phục vụ công tác điều tra và kiểm tra để xác định rõ các biện pháp Giảm thiểu/Khắc phục (Mitigation/Remediation) bước đầu - Thực hiện phân tích file log từ nhiều nguồn khác nhau (endpoint logs, network traffic logs, security product logs) để xác định các bằng chứng số (evidences) liên quan đến sự cố ATTT - Rà soát, thu thập các dấu hiệu xâm nhập (malware, webshell, user account, ...) - Phối hợp và cung cấp hỗ trợ kỹ thuật chuyên môn cho các kỹ thuật viên phụ trách ATTT trong toàn Tập đoàn & Khách hàng để giải quyết các sự cố ATTT	<b>Có khả năng làm được các công việc của level 1 và:</b> - Tương quan dữ liệu sự cố để xác định các lỗ hổng, điểm yếu cụ thể và đưa ra các khuyến nghị cho phép khắc phục nhanh chóng, triệt để - Săn tìm (Hunting) trên toàn bộ hệ thống, xác định các thành phần bị xâm nhập theo TTPs (Technique, Tactic & Procedure) của nhóm tấn công - Phân tích chuyên sâu các phương tiện Hacker sử dụng trong cuộc tấn công (malware, webshell, hacktool, ...) - Theo dõi và ghi lại hồ sơ sự cố từ lúc phát hiện đến khi hoàn thành xử lý	<b>Có khả năng làm được các công việc của level 2 và:</b> - Thực hiện phân tích sự cố, bao gồm xác định phạm vi, mức độ nghiêm trọng, khả năng ảnh hưởng, xác định điểm yếu, lỗ hổng cụ thể và đưa ra các khuyến nghị cho phép khắc phục nhanh chóng - Tương quan dữ liệu sự cố trong lịch sử, liên kết các nguồn dữ liệu bên ngoài (security vendor, tổ chức ứng cứu khẩn cấp máy tính, ...) định danh nhóm tấn công - Phối hợp với chuyên viên phân tích nguy cơ (Threat Analyst) để xác định tương quan dữ liệu đánh giá mối đe dọa (Threat) - Điều phối các chức năng ứng phó sự cố	<b>Có khả năng làm được các công việc của level 3 và:</b> - Thực hiện phân tích & báo cáo xu hướng phòng thủ ATTT - Nghiên cứu & xây dựng các tài liệu hướng dẫn kỹ thuật trong lĩnh vực xử lý sự cố - Làm việc với nhân viên thực thi pháp luật với vai trò chuyên gia kỹ thuật để giải thích các chi tiết trong sự cố theo yêu cầu, trong trường hợp cần thiết
----------	---	--	---	---