1. GIẢI THÍCH THUẬT NGỮ, ĐỊNH NGHĨA, KHÁI NIỆM

- Sự kiện an toàn thông tin (Information security event): Là sự việc xác định liên quan đến trạng thái của một hệ thống, dịch vụ hoặc trạng thái mạng nằm ngoài việc vận hành thông thường, cho thấy có khả năng vi phạm chính sách ATTT hay lỗi kiểm soát ATTT, hoặc một tình huống không lường trước liên quan đến ATTT. Không phải tất cả các sự kiện ATTT đều là sự cố ATTT.
- Sự cố an toàn thông tin (Information security incidient): Là một hoặc một loạt các sự kiện ATTT không mong muốn hoặc không dự tính có khả năng ảnh hưởng đáng kể đến các hoạt động nghiệp vụ và đe dọa ATTT.
- SOC (Security Operation Center): được giao nhiệm vụ giám sát, điều phối, ứng cứu, xử lý sự cố ATTT và đảm bảo ATTT cho Công ty.
- Tier 1: bộ phận thuộc Phòng Vận hành dịch vụ số của Trung tâm Dịch vụ hạ tầng số/TT VHKT làm đầu mối chịu trách nhiệm thực hiện giám sát hệ thống. an
- Tier 2: bộ phận trực SOC thuộc BU MSSP- Trung tâm Hợp tác kinh doanh làm đầu mối chịu trách nhiệm thực hiện tiếp nhận các ticket từ Tier 1, tiến hành xác minh, phối hợp với SO xử lý ticket.
- Tier 3: bộ phận SOC thuộc BU MSSP- Trung tâm Hợp tác kinh doanh làm đầu mối thực hiện xử lý, trong trường hợp Tier 2 không thể xử lý được hoặc đã xử lý nhưng không thành công. Trường hợp Tier 3- Viettel IDC không thể xử lý thì chuyển lên SOC manager để tiếp tục xử lý.
- SLA: thời gian xử lý cảnh báo
- Ticket: Ticket sự cố ATTT được tạo và đưa lên hệ thống SOAR để điều phối luồng xử lý sự cố ATTT.
- SOAR (Security Orchestration, Automation and Response): là giải pháp điều phối, tự động hóa phản ứng an ninh thông tin tập trung giúp xác định, ưu tiên và tiêu chuẩn hóa cho các chức năng ứng phó sự cố, lỗ hổng, vấn đề ATTT.
- SOC manager: làm nhiệm vụ điều hành xử lý sự cố, phê duyệt yêu cầu về thời gian xử lý sự cố của SO (nếu có); phê duyệt yêu cầu hỗ trợ xử lý ticket của SO (nếu có) và đóng ticket.
- Ban lãnh đạo: Ban lãnh đạo quản lý sự cố ATTT chịu trách nhiệm xác nhận hoặc phê duyệt kế hoạch ứng cứu sự cố ATTT ATTT và chủ trì xử lý sự cố ATTT nghiêm trọng.

2. QUY TRÌNH XỬ LÝ SỰ CỐ

Bước	Hoạt động	Mô tả chi tiết	Vai trò	Đầu vào	Đầu ra	Thời gian thực hiện
1	Tiếp nhận và xác minh thông tin cảnh báo về sự cố	1. Tiếp nhận thông tin cảnh báo về sự cố ATTT từ: - Cảnh báo của các giải pháp ATTT: SIEM, - Email, điện thoại của Phòng/Ban, cá nhân phát hiện sự cố ATTT báo cho bộ phận ATTT qua email: idc.attt@123com.vn; - Đe dọa Hungting, Pentest 2. Thực hiện xác minh thông tin cảnh báo: - Cảnh báo đúng: Chuyển bước 2a. Phân loại, đánh giá mức độ - Cảnh báo sai: cảnh báo nhầm nghiệp vụ quản trị, nghiệp vụ đơn vị, tác động có kế hoạch... Chuyển bước 2b. Cập nhật trạng thái cảnh báo REJECT-False Positive, đóng case.	Tier 1	- Dấu hiệu sự cố ATTT được nhận diện từ: - Cảnh báo của các giải pháp ATTT - Email, điện thoại của các Chi nhánh, Phòng/ban cá nhân phát hiện sự cố ATTT - Săn lùng mối đe dọa, Pentest	Cảnh báo về ATTT được báo cáo	Ngay khi phát hiện cảnh báo từ các nguồn tương ứng
2a	Phân loại sự cố ATTT	Phân loại, đánh giá mức độ nguy hiểm của cảnh báo gồm 2 mức độ: nghiêm trọng và thông thường (PL 01: Hướng dẫn phân loại mức độ sự cố ATTT). Với các sự cố xử lý qua ticket trên hệ thống SOAR thì thực hiện tiếp bước 3. Với các sự cố cần thông báo cho SO xử lý luôn thì liên hệ SO hệ thống theo Phụ lục 02. Danh sách liên lạc ứng cứu sự cố ATTT và	Tier 1	Cảnh báo/thông báo	Cảnh báo ATTT được phân loại	

		thực hiện theo Quy trình quản lý và xử lý sự cố				
2b	Đóng cảnh báo về sự cô ATTT	Trường hợp là cảnh báo giả: Cập nhật trạng thái cảnh báo REJECT-False Positive, đóng cảnh báo trên hệ thống SOAR		Cảnh báo về sự cố ATTT được đánh giá không phải là sự cố	Cảnh báo được đóng	Ngay sau khi có kết quả đánh giá cảnh báo
3	Tạo ra các sự cố	Tier 1 tạo case sự cố (Status = OPEN) trên SOAR Case sự sự cố được gán cho: Tier 1 đối với case đã có hướng dẫn xử lý. Chuyển bước 4b thực hiện nhiệm vụ Case Management điều hành xử lý sự cố Tier 2 đối với case sự cố chưa có hướng dẫn xử lý (Bước 4a)	Tier 1	Case chưa được xử lý	Case được gán cho Tier 1	Ngay sau bước 2a
4a	Tier 2 tiếp nhận sự cố	Tier 2 tiếp nhận case sự cố, trạng thái case là OPEN. Thực hiện xác minh thông tin cảnh báo: Cảnh báo sai chuyển bước 5 và cập nhật trạng thái cảnh báo REJECT - False Positive, đóng case. Cảnh báo đúng: + Cảnh báo đã biết hướng xử lý chuyển sang bước 4b thực hiện nhiệm vụ Case Management điều hành xử lý. Cảnh báo không xác minh được hướng xử lý gán sự cố cho Tier 3 (bước 6)	Tier 2	Case chưa được xử lý	Case được gán cho Tier 2	Ngay sau bước 3

4b	Case Management điều hành xử lý case	Case Management thực hiện điều hành xử lý case: Tạo các ticket nghiệp vụ cho System Owner/IT Admin A Nêu Tier 1 hoặc Tier 2 thực hiện theo hướng dẫn nhưng không xử lý thành công hoặc xác định mức độ sự cố Nghiêm trọng, chuyển case cho Tier 3 điều hành xử lý (Bước 6) Nếu xử lý thành công: Đóng case. Trạng thái Case là CLOSE. Nếu cần xác minh nghiệp vụ cần tạo Ticket cho SO/IT Admin	Tier 1, Tier 2, Tier 3	Ticket chưa được xử lý	Ticket đã được xử lý	
5	Cập nhật trạng thái Reject – False positive	Cảnh báo sai chuyển bước 5 và cập nhật trạng -thái cảnh báo REJECT – False Positive, đóng case.	Tier 2	Cảnh báo sai	Đóng case	
6	Tier 3 tiếp nhận case	OPEN. Tier 3 tiếp nhận case sự cố, trạng thái case là Chuyển bước 4b thực hiện nhiệm vụ CaseManagement điều hành xử lý sự cố.	Tier 3	Case sự cố		
7a	Xác minh thông tin ticket nhận được	SO/IT admin xác minh thông tin ticket nhận được:	SO, IT Admin	Ticket trên SOAR		

		Nếu ticket gán đúng nghiệp vụ cho nhóm: Cập nhật trạng thái ticket IN PROGRESS để bắt đầu công việc (Bước 8a); Nếu ticket gán sai: Cập nhật trạng thái ticket AWAITING REASSIGNMENT để Case Management thực hiện gán lại (Bước 8b).				
7b	Đóng case	Đóng case khi tất cả các ticket điều hành đã được xử lý xong.	Case management	Ticket trên SOAR	Ticket được xử lý	Ngay sau bước 2b
8a	Bắt đầu xử lý công việc theo chức năng, nghiệp vụ của nhóm	Bắt đầu xử lý công việc theo chức năng, nghiệp vụ của nhóm A Nếu cần hỗ trợ từ Case Management chuyển sang bước 9a; thêm thời gian để xử lý hoặc cần ngoại Nếu cần lệ cho ticket. Cập nhật trạng thái A WAITING PENDING (Bước b) Xử lý xong ticket: Cập nhật thông tin xử lý và trạng thái CLOSE cho ticket (Bước 9c).	SO, IT Admin	Ticket trên SOAR	Ticket được xử lý	Ngay sau bước 6
8b	Case Management tiếp nhận ticket	Case Management thực hiện gán lại ticket có trạng thái AWATING REASSIGNMENT về đúng nhóm, người xử lý. Cập nhật lại trạng thái OPEN cho ticket.	Tier 1, Tier 2, Tier 3	Ticket trên SOAR	Ticket được cập nhật trạng thái	Ngay sau bước 6
9a	Tiếp nhận hỗ trợ	Case Management xác minh yêu cầu hỗ trợ: Nếu yêu cầu hỗ trợ sai (hoặc đã có hướng dẫn, Case Management không có quyền) thì từ chối hỗ trợ;	SOC Manager	Ticket trên SOAR	Ticket được cập nhật trạng thái	Ngay sau bước 8a

		- Nếu yêu cầu hỗ trợ đúng (SO chưa có hướng dẫn, không có quyền...) thì chuyển sang bước 4b cho Case Management tiếp tục điều hành xử lý sự cố. - Thông báo lại cho SO/IT Admin sau khi hoàn thành yêu cầu hỗ trợ.				
9b	Tiếp nhận ticket trạng thái AWAITING PENDING	Case Management xác minh yêu cầu hỗ trợ: -Nếu yêu cầu hỗ trợ sai (hoặc đã có hướng dẫn, Case Management không có quyền) thì từ chối hỗ trợ; -Nếu yêu cầu hỗ trợ đúng (SO chưa có hướng dẫn, không có quyền...) thì chuyển sang bước 4b cho Case Management tiếp tục điều hành xử lý sự cố. - Thông báo lại cho SO/IT Admin sau khi hoàn thành yêu cầu hỗ trợ.	Tier 1, Tier 2, Tier 3			
9c	Cập nhật thông tin xử lý ticket	Cập nhật thông tin xử lý và đóng ticket khi: Ticket sự vụ được xử lý thành công. TicKet trùng do đã nhận được ticket tương tự trước đó và đã xử lý thành công. Thông báo kết quả cho Case Management	SO, IT Admin	Ticket trên SOAR	Ticket được xử lý	Ngay sau bước 8a
10	Đồng ý pending	Đồng ý xét duyệt thêm thời gian xử lý ticket hoặc ngoại lệ cho ticket. Trạng thái ticket PENDING.	Tier 1, Tier 2, Tier 3	Ticket trên SOAR	Ticket pending	Ngay sau bước 9c