Phần 2. YÊU CẦU KỸ THUẬT
Chương V. YÊU CẦU KỸ THUẬT

1. Giới thiệu chung về gói thầu

- Tên gói thầu: Dịch vụ giám sát ATTT cho hệ thống tài chính, 02 năm.
- Địa chỉ thực hiện: Ngân hàng TMCP Công thương Việt Nam
- Quy mô gói thầu:

TT	Hạng mục	Đơn vị	Số lượng	Mô tả, ghi chú
I	**Dịch vụ giám sát ATTT cho hệ thống tài chính, 02 năm**	**Gói**	**1**	
1	Dịch vụ giám sát và xử lý sự cố ATTT 24/7, 2 năm	Gói	01	Thời gian thực hiện dịch vụ 24 tháng kể từ ngày ký biên bản kích hoạt dịch vụ giám sát
2	Dịch vụ cập nhật các mối nguy hại ATTT (Threat Intelligence), 2 năm	Gói	01	Thời gian thực hiện dịch vụ 24 tháng kể từ ngày ký biên bản kích hoạt dịch vụ giám sát

- Thời gian thực hiện gói thầu 790 ngày bao gồm: 730 ngày thực hiện dịch vụ giám sát, điều hành an toàn thông tin + tối đa 60 ngày cho thời gian khảo sát, triển khai, tích hợp … trước khi tiến hành giám sát toàn phần.

2. Yêu cầu kỹ thuật của gói thầu

Yêu cầu kỹ thuật cho gói Dịch vụ giám sát ATTT cho hệ thống tài chính, 02 năm cụ thể như sau:

2.1. Yêu cầu kỹ thuật chi tiết

STT	Hạng mục dịch vụ	Nội dung dịch vụ	Đáp ứng yêu cầu dịch vụ
I	Dịch vụ giám sát 24/7, 02 năm	Triển khai tích hợp hệ thống giám sát tập trung - SOAR (Security Orchestration, Automation and	- Phạm vi giám sát: Thực hiện giám sát tối đa 2200 máy chủ ứng dụng, 200 thiết bị mạng, bảo mật liên quan đến hệ thống, dịch vụ tài chính và bao gồm nhưng không giới hạn các hệ thống hỗ trợ liên quan đến hệ thống, dịch vụ tài chính.

		Response) Platform của đơn vị cung cấp dịch vụ với các hệ thống của VietinBank	- Đơn vị cung cấp dịch vụ triển khai và hạ tầng các giải pháp giám sát ATTT cho VietinBank bao gồm nhưng không giới hạn: + Giải pháp Quản lý và phân tích sự kiện an toàn thông tin SIEM (Security Information & Event Management), đáp ứng tối thiểu khả năng xử lý 30.000 EPS (sự kiện/ giây), được lưu trực tuyến tối thiểu 03 tháng theo hình thức tập trung và có phương án sao lưu tối thiểu một năm . + Giải pháp giám sát và phát hiện bất hành vi bất thường UEBA (User and Entity Behavior Analytics), đáp ứng khả năng xử lý tối thiểu 30.000 EPS (sự kiện/ giây). - Đơn vị cung cấp dịch vụ cung cấp hệ thống SOAR Platform riêng để thực hiện giám sát ATTT cho hệ thống của VietinBank. - Yêu cầu đối với đơn vị cung cấp dịch vụ: + Công nghệ sử dụng cần tuân thủ các tiêu chuẩn hiện hành của Việt Nam. + Đáp ứng các yêu cầu, hướng dẫn của nhà nước đối với tổ chức, triển khai hoạt động giám sát an toàn thông tin tại các cơ quan, tổ chức. - Không giới hạn số lượng tài khoản để cán bộ giám sát ATTT của VietinBank (Tier 2) có thể review quá trình xử lý sự cố trên hệ thống SOAR Platform. - Thực hiện tích hợp giữa SOAR Platform của bên cung cấp dịch vụ với hệ thống SIEM, ITSM,…; và các hệ thống bảo mật của VietinBank để tự động hóa quá trình phản ứng với các nguy cơ an toàn thông tin, tối ưu hóa hiệu quả và giảm thiểu tác động của các sự cố bảo mật. - Kết nối đảm bảo có mã hóa đường truyền .và sử dụng trường truyền riêng, có dự phòng. - Sử dụng API và có xác thực.

			- Xây dựng hệ thống dashboard và cảnh báo sự kiện an toàn thông tin qua các kênh OTT như Telegram, Skype, Zalo, Viber,... và Email. - Hệ thống giám sát phải có khả năng mở rộng, phù hợp với sự phát triển của công nghệ trong tương lai, triển khai theo mô hình HA – Cluster đảm bảo tính sẵn sàng cao của hệ thống giám sát; bảo đảm khắc phục kịp thời toàn bộ hệ thống khi có sự cố; bảo đảm kế thừa tương thích kết nối an toàn và tránh xung đột với hạ tầng hiện có; bảo đảm khi triển khai các hệ thống khác của VietinBank vẫn hoạt động bình thường. - Xây dựng kế hoạch và kịch bản diễn tập định kỳ đảm bảo hoạt động liên tục cho hệ thống theo quy định của VietinBank.
		Trực giám sát 24/7 cho hệ thống VietinBank từ các thông tin trên SOC Platform. Nội dung thực hiện:	- Giám sát trạng thái và an ninh của hệ thống thông qua các luồng sự kiện, bảng điều khiển và cảnh báo an ninh. - Xử lý những sự cố An toàn thông tin được đẩy lên từ bộ phận đầu mối hỗ trợ (Helpdesk) và đầu mối phụ trách của VietinBank. - Phân loại cảnh báo, đưa ra hành động phù hợp với tính nghiêm trọng của cảnh báo. - Xử lý những cảnh báo thông thường theo quy trình thống nhất, thu thập ngữ cảnh và thông tin liên quan đến các cảnh báo. - Nâng cấp mức độ nghiêm trọng của những mối đe dọa chưa được làm rõ lên chuyên viên phân tích mức 2 (Tier 2 tại VietinBank). - Tạo các báo cáo sự cố và vận hành. - Có nhân sự đảm bảo việc thực hiện dịch vụ đáp ứng yêu cầu nhân sự theo phụ lục 03 - Yêu cầu chất lượng dịch vụ giám sát : Đáp ứng phụ lục 02 "Yêu cầu về chất lượng dịch vụ"

		Điều tra số, phân tích mã độc, hỗ trợ điều tra số, xử lý sự cố chuyên sâu (Tier 3):	- Xác định mức độ xâm nhập, các đặc tính của mã độc và khả năng dữ liệu bị đánh cắp. - Phân tích cơ bản và nâng cao về mạng, máy tính lây nhiễm, tệp tin, registry, bộ nhớ và nhật ký hệ thống. - Kiểm tra các mẫu hình lưu lượng truy cập tới máy chủ điều khiển mã độc đã biết hoặc tệp nhị phân đã tải xuống. - Duy trì chuỗi chứng cứ (phục vụ quá trình điều tra). - Tóm tắt các phát hiện trong báo cáo kỹ thuật để có thể sử dụng như một phần chứng cứ hợp pháp. - Có nhân sự đảm bảo việc thực hiện dịch vụ đáp ứng yêu cầu nhân sự theo phụ lục 03. - Thời gian xử lý đáp ứng yêu cầu chất lượng dịch vụ theo phụ lục 02.
		Thực hiện săn tìm các dấu hiệu tấn công, mã độc (hunting) trên hệ thống VietinBank	- Thực hiện hunting định kỳ nhằm phát hiện các hành vi tấn công thông qua hình thức nghiên cứu, phân tích, tổng hợp hệ thống lưu trữ log trên SIEM, EDR và trực tiếp trên máy chủ cho tối đa 400 máy chủ/năm. - Tần suất thực hiện 01 quý/lần, mỗi lần 100 máy chủ. - Có nhân sự đảm bảo việc thực hiện dịch vụ đáp ứng yêu cầu nhân sự theo phụ lục 03. - Thời gian xử lý đáp ứng yêu cầu chất lượng dịch vụ theo phụ lục 02.
		Tối ưu rule hệ thống SIEM	- Tối ưu SIEM Rule nhằm nâng cao khả năng nhận biết và cảnh báo khi có sự cố (bao gồm các rule theo MITRE ATT&CK Framework, Signature-Based Detection, User Behavior Analytics (UBA) và Anomaly-Based Detection, Threat Intelligence, Business Context, …) - Tối ưu logsource: review cấu hình lấy log đưa ra đề xuất, hỗ trợ VietinBank thực hiện

			parser logsource đối với các ứng dụng mới, hoặc các logsource đã thu thập log nhưng thiếu các trường thông tin. - Tần suất thực hiện review và tối ưu rule tối thiểu 01 tháng / 01 lần và có phụ lục trong báo cáo tháng. - Đối với logsource: hỗ trợ parser log đối với những log hệ thống không thể tự động parser hoặc parser nhưng không lấy đủ các trường thông tin. - Có nhân sự đảm bảo việc thực hiện dịch vụ đáp ứng yêu cầu nhân sự theo phụ lục 03. - Thời gian xử lý đáp ứng yêu cầu chất lượng dịch vụ theo phụ lục 02.
		Xây dựng báo cáo định kỳ hoạt động giám sát an toàn thông tin.	+ Báo cáo sự cố. + Báo cáo định kỳ công tác giám sát ATTT (hàng tháng, quý, năm)
		Yêu cầu hướng dẫn, đào tạo và tài liệu chuyển giao	Đào tạo hướng dẫn sử dụng, cung cấp tài liệu, chuyển giao toàn bộ hệ thống dịch vụ cung cấp cho đội ngũ chuyên trách về an toàn thông tin của VietinBank: - Đào tạo: + Hình thức đào tạo: Trực tiếp. + Phạm vi đào tạo: mô hình triển khai, các tính năng, giải pháp, dịch vụ trong phạm vi đã triển khai, dịch vụ cung cấp ,cách thức quản trị, vận hành dịch vụ. + Số lượng học viên: tối thiểu 10 nhân viên. + Thời gian đào tạo: tối thiểu 02 buổi. - Tài liệu, sản phẩm bàn giao: + Tài liệu phân tích và thiết kế hệ thống; + Tài liệu hướng dẫn sử dụng; + Tài liệu hướng dẫn cài đặt quản trị vận hành; + Tài liệu các báo cáo liên quan thuộc phạm vi cung cấp dịch vụ ; + Tài liệu khác (nếu có)

II	Dịch vụ cập nhật các mối nguy hại ATTT (Threat Intelligence), 2 năm	Cung cấp các thông tin liên quan các mối đe dọa	- Có hệ thống Threat Intelligence Platform - Nguồn Threat Intelligence: 03 nguồn (Nguồn opensource ví dụ như: Phishtank, AlienVault…, nguồn từ các tổ chức, đối tác quốc tế như: APWG, FIRST, VirusTotal, ThreatConnect, Recorded Future, Mandiant, GroupIB, Crowdstrike… và nguồn tổng hợp của đơn vị cung cấp trong quá trình thực hiện giám sát) - Thông tin Threat Intelligence cung cấp bao gồm nhưng không giới hạn: + Thông tin IOC: IP Address, Domain, URL, file hash, CIDR, Mutex, Hashtag, User Agent, Registry Key + Thông tin Group: Threat, Adversary, Incident, Campaign, Signature, Intrusion Set + Khuyến nghị phương án xử lý lỗ hổng: cài đặt bản vá, workaround, phát hiện, ngăn chặn hành vi khai thác lỗ hổng - Có khả năng tích hợp với các hệ thống SIEM/SOAR như IBM Qradar, Splunk…
		Hỗ trợ takedown, ngăn chặn truy cập đến các trang giả mạo brandname của VietinBank	- Hỗ trợ Takedown (vô hiệu hoá) các trang web, bài viết giả mạo, lừa đảo, lạm dụng thương hiệu và chứa nội dung, văn bản nhạy cảm, mật của VietinBank sở hữu. - Hỗ trợ VietinBank làm việc với cơ quan chức năng để xử lý các trang đặt tại Việt Nam, có hành vi vi phạm pháp luật gây ảnh hưởng đến quyền và lợi ích hợp pháp của VietinBank.
		Xây dựng các báo cáo về cảnh báo ATTT, xu hướng tấn công khi có cảnh báo về các lỗ hổng bảo mật hoặc định kỳ báo cáo theo tháng	- Các cảnh báo chi tiết về các lỗ hổng bảo mật, IOC, group. - Các báo cáo, đánh giá, dự báo về xu hướng, nguy cơ tấn công đối với VietinBank.

		Yêu cầu hướng dẫn, đào tạo và tài liệu chuyển giao	Đào tạo hướng dẫn sử dụng, cung cấp tài liệu, chuyển giao toàn bộ hệ thống dịch vụ cung cấp cho đội ngũ chuyên trách về an toàn thông tin của VietinBank: - Đào tạo: + Hình thức đào tạo: Trực tiếp + Phạm vi đào tạo: Các tính năng, giải pháp, dịch vụ , dịch vụ cung cấp và cách thức quản trị, vận hành dịch vụ + Số lượng học viên: tối thiểu 10 nhân viên + Thời gian đào tạo: tối thiểu 01 buổi - Tài liệu, sản phẩm bàn giao: + Tài liệu hướng dẫn sử dụng; + Tài liệu hướng dẫn cài đặt quản trị vận hành; + Tài liệu các báo cáo liên quan thuộc phạm vi cung cấp dịch vụ; + Tài liệu khác (nếu có)

2.2. CAM KẾT CHẤT LƯỢNG DỊCH VỤ

2.2.1. Đối với Dịch vụ giám sát và xử lý sự cố ATTT 24/7

STT	Hạng mục công việc	Mô tả	Cách tính thời gian xử lý	Trách nhiệm đơn vụ cung cấp dịch vụ	Trách nhiệm VietinBank	Mục tiêu cam kết
I	**Quản lý các sự kiện ATTT**					
	Giám sát cảnh báo ATTT					
1	Tỷ lệ xử lý cảnh báo đúng hạn	- Là tỉ lệ giữa số lượng cảnh báo ATTT đã hoàn thành xử lý với Tổng số lượng cảnh báo trên hệ thống SOC. - Thời gian xử lý cảnh báo ATTT đúng hạn, cụ thể như sau: + Nghiêm trọng: ≤ 30 phút + Thông thường: ≤ 01 giờ	Từ thời điểm cảnh báo được tạo trên hệ thống Đến khi cảnh báo được gán vào 1 Case (hoặc chuyển trạng thái False Positive)	R		95%

STT	Hạng mục công việc	Mô tả	Cách tính thời gian xử lý	Trách nhiệm đơn vụ cung cấp dịch vụ	Trách nhiệm VietinBank	Mục tiêu cam kết
II	**Xử lý sự cố ATTT**					
	Phân tích xử lý sự cố theo hướng dẫn					
1	Tỉ lệ sự cố ATTT đã có hướng dẫn hoàn thành xử lý trong hạn	- Là tỷ lệ giữa số lượng sự cố ATTT đã có hướng dẫn hoàn thành xử lý trong thời gian quy định với Tổng số sự cố ATTT được cảnh báo. - Sự cố ATTT đã có hướng dẫn được quản lý trên hệ thống SOC (của VietinBank) được tạo và gắn cho VietinBank (01 sự cố ATTT tương ứng với 01 ticket)	Từ thời điểm ticket sự cố có trạng thái OPEN đến khi ticket chuyển trạng thái CLOSE	S	R	95%

STT	Hạng mục công việc	Mô tả	Cách tính thời gian xử lý	Trách nhiệm đơn vụ cung cấp dịch vụ	Trách nhiệm VietinBank	Mục tiêu cam kết
		- Thời gian xử lý sự cố ATTT quy định theo loại sự cố ATTT, cụ thể như sau: + Nghiêm trọng:≤ 24 giờ + Thông thường:≤ 72 giờ				
	Phân tích và xử lý sự cố chưa có hướng dẫn					
2	Tỉ lệ sự cố ATTT chưa có hướng dẫn hoàn thành xử lý trong hạn	- Là tỷ lệ giữa số lượng sự cố ATTT chưa có hướng dẫn hoàn thành xử lý trong thời gian quy định với Tổng số sự cố ATTT chưa có hướng dẫn. - Sự cố ATTT chưa có hướng dẫn được quản lý trên hệ thống SOC (của VietinBank) được	Từ thời điểm case sự cố có trạng thái OPEN đến khi case chuyển trạng thái CLOSE	R	S	95%

STT	Hạng mục công việc	Mô tả	Cách tính thời gian xử lý	Trách nhiệm đơn vụ cung cấp dịch vụ	Trách nhiệm VietinBank	Mục tiêu cam kết
		tạo và gắn cho Tier 3 (01 sự cố ATTT tương ứng với 01 case) - Thời gian xử lý sự cố ATTT quy định theo loại sự cố ATTT, cụ thể như sau: + Nghiêm trọng:≤ 24 giờ + Thông thường:≤ 72 giờ				
III	**Xử lý các lỗ hổng, vi phạm ATTT**					
1	Tỉ lệ ticket lỗ hổng, xử lý trong hạn	- Là tỷ lệ giữa số lượng lỗ hổng ATTT hoàn thành xử lý trong thời gian quy định với Tổng số lượng lỗ hổng ATTT được cảnh báo.	Từ thời điểm ticket lỗ hổng có trạng thái OPEN đến khi ticket chuyển trạng thái CLOSE	S	R	90%

STT	Hạng mục công việc	Mô tả	Cách tính thời gian xử lý	Trách nhiệm đơn vụ cung cấp dịch vụ	Trách nhiệm VietinBank	Mục tiêu cam kết
		- Lỗ hổng ATTT được quản lý trên hệ thống SOC của VietinBank (01 lỗ hổng ATTT tương ứng với 01 ticket). - Thời gian xử lý lỗ hổng ATTT quy định theo loại lỗ hổng ATTT, cụ thể như sau: + Nghiêm trọng:≤ 24 giờ + Cao:≤ 120 giờ + Trung bình:≤ 240 giờ + Thấp:≤ 360 giờ				
IV	**Tối ưu cảnh báo**					

STT	Hạng mục công việc	Mô tả	Cách tính thời gian xử lý	Trách nhiệm đơn vụ cung cấp dịch vụ	Trách nhiệm VietinBank	Mục tiêu cam kết
1	Tỷ lệ ticket tối ưu xử lý đúng hạn	- Là tỷ lệ giữa số lượng ticket tối ưu hoàn thành xử lý trong thời gian quy định với Tổng số lượng tickets tối ưu được tạo, gán cho nhóm Content Analyst trên hệ thống SOC. - Thời gian xử lý ticket tối ưu quy định theo loại ticket tối ưu, cụ thể như sau: + Cao:≤ 24 giờ + Trung bình:≤120 giờ + Thấp:≤360 giờ Trong đó: - Mức CAO: với các yêu cầu chỉnh sửa tối ưu cảnh báo gấp	Từ thời điểm ticket tối ưu có trạng thái OPEN đến khi ticket chuyển trạng thái CLOSE	R	S	95%

STT	Hạng mục công việc	Mô tả	Cách tính thời gian xử lý	Trách nhiệm đơn vị cung cấp dịch vụ	Trách nhiệm VietinBank	Mục tiêu cam kết
		do các cảnh báo phát sinh sai, hoặc lặp lại nhiều gây nhiễu, ảnh hưởng gây gián đoạn việc vận hành giám sát ATTT. - Mức TRUNG BÌNH: với các yêu cầu chỉnh sửa tối ưu cảnh báo nhằm nâng cao tính chính xác dù hiện tại việc vận hành giám sát chưa bị ảnh hưởng trực tiếp, whitelist các trường hợp ngoại lệ. - Mức THẤP: Các góp ý, yêu cầu bổ sung các tính năng công cụ hỗ trợ việc vận hành giám sát, phân tích, xử lý cảnh báo ATTT.				

STT	Hạng mục công việc	Mô tả	Cách tính thời gian xử lý	Trách nhiệm đơn vụ cung cấp dịch vụ	Trách nhiệm VietinBank	Mục tiêu cam kết
V	**Các hoạt động liên quan việc vận hành cung cấp dịch vụ**					
1	Tỷ lệ báo cáo tháng toàn diện công tác ATTT của VietinBank đúng hạn	- Là tỷ lệ báo cáo hàng tháng gửi VietinBank đúng hạn với Tổng số báo cáo tháng gửi VietinBank. - Thời gian báo cáo đúng hạn, gửi vào ngày thống nhất giữa hai bên.	Tỷ lệ báo cáo hàng tháng gửi VietinBank đúng hạn với Tổng số báo cáo tháng gửi VietinBank (Thời gian báo cáo đúng hạn, gửi vào ngày thống nhất giữa hai bên)	R	I	95%
VI	**Chất lượng của hệ thống giám sát cảnh báo**					
1	Số lượng cảnh báo mức Nghiêm trọng mà hệ	Số lượng cảnh báo mức Nghiêm trọng được gửi từ Tier 2 – SOC (VietinBank) mà hệ thống không phát hiện được và	Đo bằng số lượng cảnh báo được Tier 2 VietinBank gửi đến Đơn vị cung cấp dịch vụ theo đúng "Quy trình phối hợp xử lý sự cố ATTT" và được Tier 1	R	I	0 cảnh báo

STT	Hạng mục công việc	Mô tả	Cách tính thời gian xử lý	Trách nhiệm đơn vụ cung cấp dịch vụ	Trách nhiệm VietinBank	Mục tiêu cam kết
	thống không phát hiện được	được Tier 1 xác minh chính xác trong tháng	xác minh chính xác là sự cố mức Nghiêm trọng và hệ thống không phát hiện được.			
2	Số lượng cảnh báo mức thông thường mà hệ thống không phát hiện được	Số lượng cảnh báo mức Thông thường được gửi từ Tier 2 – SOC (VietinBank) mà hệ thống không phát hiện được và được Tier 1 xác minh chính xác trong tháng	Đo bằng số lượng cảnh báo được Tier 2 VietinBank gửi đến Đơn vị cung cấp dịch vụ và được Tier 1 xác minh chính xác là sự cố mức Thông thường và hệ thống không phát hiện được.	R	I	05 cảnh báo

Ghi chú:

Phân loại trách nhiệm theo mô hình RASCI:

- ✓ R – Responsible: Trách nhiệm thực hiện chính.
- ✓ A – Approval: Trách nhiệm phê duyệt, đồng ý nội dung thực hiện
- ✓ S – Support: Trách nhiệm hỗ trợ Bên thực hiện chính.
- ✓ C – Consulted: Trách nhiệm dựa vào kiến thức, kinh nghiệm chuyên môn tư vấn giải pháp thực hiện.

✓ I – Informed: Trách nhiệm được cung cấp thông tin.

Các thức xác định mức độ của sự cố ATTT

- Sự cố an toàn thông tin: là việc thông tin, hệ thống thông tin bị tấn công hoặc gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.
- Phân loại mức độ sự cố ATTT: Được chia thành 2 loại NGHIÊM TRỌNG & THÔNG THƯỜNG tùy theo 'Mức độ ảnh hưởng' và 'Khả năng tấn công thành công'

Mức độ ảnh hưởng

Mức độ ảnh hưởng của sự cố sử dụng để đánh giá phạm vi ảnh hưởng, tính chất nghiêm trọng của sự cố. Mức độ ảnh hưởng của một sự cố ATTT được phân làm 04 (bốn) mức sau:

Mức độ ảnh hưởng	**Điều kiện phân loại mức độ ảnh hưởng**
Nghiêm trọng	***Tiêu chí phân loại cho Tier 1 (Đơn vị cung cấp dịch vụ giám sát)*** - Cảnh báo ATTT phát sinh từ hệ thống CoreBanking, InternetBanking, Hệ thống thẻ, hệ thống public ra internet của VietinBank ***Tiêu chí phân loại cho Tier 2 – SOC (VietinBank)*** - Đối với hệ thống thông tin quan trọng và thỏa mãn 1 trong các điều kiện sau: o Gây **gián đoạn** hầu hết các tính năng chính o Mất/ hỏng dữ liệu - Đối với hệ thống thông tin thông thường: Gây gián đoạn toàn bộ dịch vụ, người dùng phải tạm dừng công việc do không có giải pháp thay thế
Cao	***Tiêu chí phân loại cho Tier 1 (Đơn vị cung cấp dịch vụ giám sát)*** - Cảnh báo ATTT phát sinh từ hệ thống quản lý CNTT tập trung (các hệ thống xác thực, AD, Password Manager, update tập trung WSUS, máy chủ Antivirus, File server, …) của VietinBank ***Tiêu chí phân loại cho Tier 2 - SOC (VietinBank)*** - Với hệ thống thông tin quan trọng: Tính năng chính bị gián đoạn hoặc hoạt động không ổn định vào giờ dịch vụ; - Với hệ thống thông tin thông thường: Gây **gián đoạn** toàn bộ dịch vụ nhưng có giải pháp thay thế
Trung bình	***Tiêu chí phân loại cho Tier 1 (Đơn vị cung cấp dịch vụ giám sát)*** - Cảnh báo ATTT phát sinh từ hệ thống máy chủ cung cấp các dịch vụ nội bộ của VietinBank

Mức độ ảnh hưởng	Điều kiện phân loại mức độ ảnh hưởng
	Tiêu chí phân loại cho Tier 2 – SOC (VietinBank) - Với hệ thống thông tin quan trọng: Tính năng chính bị gián đoạn hoặc hoạt động không ổn định vào ngoài giờ dịch vụ - Với hệ thống thông tin thông thường và thỏa mãn 1 trong các điều kiện sau: o Gây gián đoạn một tính năng của dịch vụ o Tính năng của dịch vụ hoạt động không đúng hoặc không ổn định, gây ảnh hưởng tới một nhóm người dùng (không phải trường hợp đơn lẻ)
Thấp	***Tiêu chí phân loại cho Tier 1 (Đơn vị cung cấp dịch vụ giám sát)*** - Cảnh báo ATTT phát sinh từ máy tính người dùng của VietinBank ***Tiêu chí phân loại cho Tier 2 - SOC (VietinBank)*** - Các sự cố xảy ra đơn lẻ và không thuộc phân loại mức độ ảnh hưởng Nghiêm trọng, Cao, Trung bình nêu trên.

Khả năng tấn công thành công

Khả năng tấn công thành công	Điều kiện phân loại khả năng tấn công thành công
Cao	Cảnh báo ATTT phát sinh từ các luật (rule) phát hiện tấn công sau: - Phát hiện các tấn công thông qua dấu hiệu IOC (Indicator Of Compromise) trên tất cả các giải pháp ATTT - Phát hiện các hành vi bất thường trên Endpoint liên quan đến khai thác lỗ hổng phần mềm (Microsoft office, adobe reader, winrar, 7zip, mssql, …)
Trung bình	Cảnh báo ATTT phát sinh từ các luật (rule) còn lại, bao gồm: - Phát hiện các hành vi bất thường khác mức Cao, xuất hiện trên lớp Endpoint, Network, Gateway - Phát hiện thay đổi tài nguyên quan trọng trên máy chủ (User, File trong thư mục Website, Port, Service, …) - Phát hiện vi phạm tiêu chuẩn ATTT (Baseline)

Mức độ ưu tiên

Mục đích của việc phân chia mức độ ưu tiên là để: phân loại sự cố ATTT từ đó xác định thời gian cam kết xử lý tương ứng.

Có các mức độ ưu tiên được xác định theo bảng sau:

MA TRẬN THIẾT LẬP GIÁ TRỊ ƯU TIÊN CỦA SỰ CỐ			
Giá trị ưu tiên = Mức độ ảnh hưởng X Khả năng tấn công thành công		**Khả năng tấn công thành công**	
		Cao (1)	**Trung bình (2)**
Mức độ ảnh hưởng	**Nghiêm trọng (1)**	1	2
	Cao (2)	2	4
	Trung bình (3)	3	6
	Thấp (4)	4	8

Mức độ ưu tiên được xác định như sau:

- Mức 1: bao gồm các giá trị trong ma trận là 1, 2
- Mức 2: bao gồm các giá trị trong ma trận là 3, 4
- Mức 3: bao gồm các giá trị trong ma trận là 6
- Mức 4: bao gồm các giá trị trong ma trận là 8

Nếu tại cùng một thời điểm có nhiều sự cố xảy ra mà không đủ nguồn lực thực hiện, việc xử lý sự cố được thực hiện theo thứ tự các mức ưu tiên từ mức 1 đến mức 4.

Trong trường hợp tại một thời điểm có nhiều sự cố có cùng một mức ưu tiên xảy ra, việc xử lý sẽ được ưu tiên theo phạm vi ảnh hưởng (ưu tiên xử lý trước các trường hợp mức độ ảnh hưởng lớn hơn).

Trong trường hợp tại một thời điểm có nhiều sự cố có cùng mức ưu tiên, cùng mức độ ảnh hưởng, khi đó sẽ xử lý theo thứ tự thời gian ghi nhận sự cố.

Dựa trên bảng ưu tiên như trên, sự cố ATTT sẽ được phân loại thành 02 loại:

- Sự cố nghiêm trọng: là sự cố có mức 1.
- Sự cố thông thường: là sự cố có mức ưu tiên 2, 3, 4.

2.2.2. Đối với dịch vụ cập nhật các mối nguy hại ATTT (Threat Intelligence)

<table>
<tr><th>STT</th><th>Hạng mục</th><th>Yêu cầu</th><th>Cách tính thời gian xử lý</th><th>Mục tiêu cam kết</th></tr>
<tr><td>1</td><td>Cung cấp thông tin nguy cơ (theo chủ đề)</td><td></td><td></td><td></td></tr>
<tr><td>1.1</td><td>Tỉ lệ cảnh báo đúng hạn về các lỗ hổng an ninh bảo mật (vulnerability)</td><td>Là tỉ lệ cảnh báo nguy cơ đúng hạn trên tổng số cảnh báo tới VietinBank.
- Các cảnh báo nguy cơ cung cấp cho VietinBank dựa trên:
+ Danh sách các phần mềm, các hãng mà VietinBank cung cấp
+ Danh sách các hãng nổi tiếng trên thế giới: Microsoft, Google, Cisco, Adobe, Oracle, VMware,...
- Mức độ nghiêm trọng của nguy cơ cảnh báo sẽ được đánh giá dựa trên thang đo quốc tế CVSS.
-Thông tin cảnh báo bao gồm:
+ Tổng quan
+ Phiên bản bị ảnh hưởng</td><td>Thời gian cảnh báo được tính từ khi hãng cung cấp, công bố thông tin về lỗ hổng/bản vá cho đến khi dịch vụ TI cảnh báo cho VietinBank
<table><tr><th>Mức độ nguy cơ</th><th>Thời gian cảnh báo</th></tr><tr><td>CAO/Nghiêm trọng</td><td><= 24 giờ</td></tr><tr><td>TRUNG BÌNH/THẤP</td><td><=72 giờ</td></tr></table></td><td>95%</td></tr>
</table>

<table>
<tr><th>STT</th><th>Hạng mục</th><th>Yêu cầu</th><th>Cách tính thời gian xử lý</th><th>Mục tiêu cam kết</th></tr>
<tr><td></td><td></td><td>+ Cách khắc phục
+ Nhận định, đánh giá của TI
+ Cách khắc phục tạm thời (nếu có)
+ Khả năng khai thác (nếu có)
+ Các rule kèm theo (nếu có)</td><td></td><td></td></tr>
<tr><td>1.2</td><td>Tỉ lệ cảnh báo đúng hạn về các mã độc mới, hoạt động của nhóm APT</td><td>- Là tỷ lệ cảnh báo nguy cơ đúng hạn trên tổng số cảnh báo tới VietinBank. .
• Thông tin cảnh báo bao gồm:
+ Tổng quan
+ Dòng mã độc (nếu có)
+ Nhận định, đánh giá của hệ thống TI
+ Dấu hiệu nhận biết
Các cảnh báo mã độc cung cấp cho VietinBank dựa trên:</td><td>Thông tin phải có trên hệ thống TI trước hoặc sau khi các phương tiện thông tin đại chúng hoặc báo chí nhắc đến không quá:
<table><tr><th>Mức độ nguy cơ</th><th>Thời gian cảnh báo</th><th>Thông tin</th></tr><tr><td>Cao/Nghiêm trọng</td><td><=24h</td><td>Các chiến dịch đang hoạt động tấn công trực tiếp vào Việt Nam</td></tr></table></td><td>100%</td></tr>
</table>

STT	Hạng mục	Yêu cầu	Cách tính thời gian xử lý			Mục tiêu cam kết
		+ Các chiến dịch tấn công trực tiếp vào Việt Nam của các nhóm APT đã biết. + Hoạt động của các nhóm APT tấn công vào các tổ chức, quốc gia trong khu vực Đông Nam Á, hoạt động của các nhóm APT đã từng có tiền lệ tấn công vào Việt Nam. + Các dòng mã độc, coin miner, ransomware, được ghi nhận thực tế tấn công vào các ngành tài chính ngân hàng, an ninh quốc phòng, cơ quan chính phủ trên thế giới, phá hủy hệ thống máy chủ, làm mất dữ liệu, gây ảnh hưởng trên diện rộng. Các dòng mã độc sử dụng các kỹ thuật tấn công mới. Lưu ý, các cảnh báo liên quan đến các dòng mã độc, TI gửi thông tin cơ bản và cung cấp IoC.	Trung bình	<=72h	Hoạt động của các nhóm APT tấn công vào các tổ chức, quốc gia trong khu vực Đông Nam Á, hoạt động của các nhóm APT đã từng có tiền lệ tấn công vào Việt Nam. Các chiến dịch cũ tấn công trực tiếp vào Việt Nam, hạ tầng đã không còn hoạt động.	

<table>
<tr><th>STT</th><th>Hạng mục</th><th>Yêu cầu</th><th>Cách tính thời gian xử lý</th><th>Mục tiêu cam kết</th></tr>
<tr><td></td><td></td><td>+ Hoạt động của các nhóm APT, các dòng mã độc cụ thể được VietinBank cung cấp.
Danh sách các nhóm APT dưới đây (sẽ cập nhật liên tục): APT32, Mustang Panda, Globin Panda, Winnti</td><td><table><tr><td>Thấp</td><td><=72h</td><td>Các dòng mã độc, coin miner, ransomware</td></tr></table>• Báo chí có ảnh hưởng lớn:
+ Báo Dân trí
+ Báo VnExpress
+ Báo Vietnamnet
+ Báo Tuổi trẻ online
+ Báo Thanh niên
• Tổ chức có thẩm quyền:
+ NCSC</td><td></td></tr>
<tr><td>1.3</td><td>Nhóm thông tin về dữ liệu bị đánh cắp, rò rỉ (compromised/leak data) trên các diễn đàn, forum, chợ đen, deep/dark web,</td><td>- Dữ liệu về các tài khoản và mật khẩu của các dịch vụ giao dịch trực tuyến như Internet Banking, Mobile Banking, chứng khoán…: tên miền/địa chỉ đăng nhập, tên tài khoản, mật khẩu (nếu có)</td><td>Báo cáo xác nhận khối lượng/số lượng thông tin đã cung cấp
- Đối với các thông tin từ darknet, VietinBank sẽ nhận được thông báo trước</td><td>95%</td></tr>
</table>

STT	Hạng mục	Yêu cầu	Cách tính thời gian xử lý	Mục tiêu cam kết
	mạng xã hội, trang chia sẻ dữ liệu, kho mã nguồn (source code) liên quan đến VietinBank	- Dữ liệu thẻ ngân hàng, mã số thẻ, loại thẻ - Các file bị hacker/mã độc đánh cắp có thông tin liên quan đến VietinBank như các log file, tin nhắn, certificates, mã nguồn (source code), …	khi cơ quan có thẩm quyền hoặc báo chí nhắc đến. - Đối với các thông tin khác, thông tin sẽ có trên TI không quá **1 ngày** khi các phương tiện thông tin đại chúng hoặc báo chí nhắc đến. • Danh sách báo chí có ảnh hưởng lớn: + Báo Dân trí + Báo VnExpress + Báo Vietnamnet + Báo Tuổi trẻ online + Báo Thanh niên • Tổ chức có thẩm quyền: + NCSC	

STT	Hạng mục	Yêu cầu	Cách tính thời gian xử lý	Mục tiêu cam kết
1.4	Nhóm thông tin về các nguy cơ lạm dụng thương hiệu	- Cung cấp các tên miền/domain trên Internet có liên quan đến việc sử dụng thương hiệu của VietinBank: domain, địa chỉ IP, ngày phát hiện và hình ảnh của trang đi kèm. - Cung cấp các website lừa đảo có khả năng lạm dụng thương hiệu hoặc giả mạo giao diện để đánh cắp tài khoản VietinBank: domain, địa chỉ IP, ngày phát hiện và hình ảnh của trang.	Báo cáo xác nhận khối lượng/số lượng thông tin đã cung cấp - Thông tin phải có trên Threat Intelligence trước hoặc sau không quá **24 giờ** khi các phương tiện thông tin đại chúng, báo chí hoặc cơ quan có thẩm quyền nhắc đến. • Danh sách báo chí có ảnh hưởng lớn: + Báo Dân trí + Báo VnExpress + Báo Vietnamnet + Báo Tuổi trẻ online + Báo Thanh niên • Tổ chức có thẩm quyền: + NCSC	95%
1.5	Nhóm thông tin về các lỗ hổng dịch vụ, các port	Cung cấp thông tin về các lỗ hổng dịch vụ, các port mở bất thường của domain/IP công	Báo cáo xác nhận khối lượng/số lượng thông tin đã cung cấp	

STT	Hạng mục	Yêu cầu	Cách tính thời gian xử lý	Mục tiêu cam kết
	mở bất thường của Khách hàng	khai của tổ chức. Thông tin bao gồm: Thời gian mở, mức độ nguy hiểm, Domain/IP. Danh sách Domain/IP dựa theo thông tin VietinBank cung cấp		
1.6	Nhóm thông tin về IP của VietinBank có kết nối đến cơ sở hạ tầng của mã độc (nếu Khách hàng sử dụng đường truyền của Viettel)	- Cung cấp thông tin về các IP của VietinBank có kết nối đến cơ sở hạ tầng của mã độc: IP của VietinBank, thời gian kết nối, thông tin C&C (domain, Categories, Malware name)	Báo cáo xác nhận khối lượng/số lượng thông tin đã cung cấp - Thông tin phải có trên TI trước hoặc sau không quá **24 giờ** khi các phương tiện thông tin đại chúng hoặc báo chí nhắc đến. • Báo chí có ảnh hưởng lớn: + Báo Dân trí + Báo VnExpress + Báo Vietnamnet + Báo Tuổi trẻ online + Báo Thanh niên • Tổ chức có thẩm quyền:	95%

STT	Hạng mục	Yêu cầu	Cách tính thời gian xử lý	Mục tiêu cam kết
			+ NCSC	
1.7	Hỗ trợ xử lý nguy cơ • Gỡ bỏ website lừa đảo VietinBank	- Hỗ trợ xử lý, gỡ bỏ (takedown) website lừa đảo lợi dụng thương hiệu của VietinBank, tối thiểu cho phép: Gửi yêu cầu xử lý website giả mạo thương hiệu + Theo dõi trạng thái xử lý + Phản hồi kết quả	Báo cáo xác nhận khối lượng/số lượng thông tin đã cung cấp - Thời gian phản hồi yêu cầu không quá **04 giờ.** - Thời gian phản hồi kết quả/trạng thái xử lý không quá **24 giờ** đối với các yêu cầu VietinBank đã gửi (thông qua email hoặc portal). - Thời gian hoàn thành ngăn chặn/ gỡ bỏ không quá **03 ngày**.	95%
1.8	Hỗ trợ phân tích nguy cơ • Phân tích thông tin bổ sung lỗ hổng và cách khắc phục	• Hỗ trợ phân tích nguy cơ theo yêu cầu của VietinBank, thông tin tối thiểu bao gồm: ○ Đối với bổ sung thêm thông tin: ▪ Cách khắc phục tạm thời (nếu có)	Báo cáo xác nhận khối lượng/số lượng thông tin đã cung cấp - Thời gian phản hồi kết quả/trạng thái xử lý không quá **24 giờ** đối với các yêu cầu VietinBank đã gửi (thông qua email)	95%

STT	Hạng mục	Yêu cầu	Cách tính thời gian xử lý	Mục tiêu cam kết
		▪ Khả năng khai thác (nếu có) ▪ Các rule kèm theo (nếu có) ○ Đối với lỗ hổng mới: ▪ Tổng quan ▪ Phiên bản bị ảnh hưởng ▪ Cách khắc phục		
1.9	Hỗ trợ phân tích nguy cơ các dòng mã độc, APT	• Hỗ trợ phân tích nguy cơ mã độc theo yêu cầu của VietinBank, thông tin tối thiểu bao gồm: ○ Đối với mẫu mã độc, APT: + Tổng quan ▪ Dòng mã độc (nếu có) ▪ Dấu hiệu nhận biết	Báo cáo xác nhận khối lượng/số lượng thông tin đã cung cấp - Thời gian phản hồi kết quả/trạng thái xử lý không quá **24 giờ** đối với các yêu cầu VietinBank đã gửi (thông qua email)	95%

3. Quy định về kiểm tra, nghiệm thu sản phẩm:

- Nhà thầu thực hiện tổng hợp phân tích an ninh thông tin định kỳ theo các mức tuần/tháng/quý/năm, trong đó đánh giá các mối đe dọa, xu hướng tấn công liên quan đến các giải pháp mà VietinBank đang sử dụng.
- Báo cáo định kỳ từ cấp tháng trở lên cần ghi nhận các sự cố, hành động xử lý, các hệ thống liên quan ảnh hưởng và các khuyến nghị cần cải thiện để cung cấp cơ sở cho việc nâng cấp/điều chỉnh và ra quyết định liên quan đến rủi ro an toàn thông tin của VietinBank

4. Các yêu cầu khác

- Nhà thầu cam kết cảnh báo chuyên sâu nguy cơ lỗ hổng ATTT; cảnh báo ỗ hổng ATTT; cảnh báo chuyên sâu nguy cơ mã độc, tấn công có chủ đích; cảnh báo tài khoản lộ lọt; cảnh báo dữ liệu lộ lọt; cảnh báo lừa đảo giả mạo thương hiệu.. đáp ứng SLA ở mức 100% và gửi báo cáo định kỳ đáp ứng yêu cầu theo quy định tại Chương V, Mục 3. Quy định về kiểm tra, nghiệm thu sản phẩm.