Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

1. Giới thiệu chung về dự án/dự toán mua sắm, gói thầu:

- Tên gói thầu: Thuê Hệ thống phát hiện và quản lý các nguy cơ ATTT từ bên ngoài trong 3 năm

- Thời gian thực hiện gói thầu: 1095 ngày kể từ ngày hợp đồng có hiệu lực

- Địa điểm: Ngân hàng TMCP Công thương Việt Nam

- Phạm vi, quy mô:

TT	Hạng mục	Đơn vị	Số lượng
1	Thuê dịch vụ phần mềm trên Cloud (SaaS): Hệ thống phát hiện và quản lý các nguy cơ ATTT từ bên ngoài trong 3 năm	Gói	1

2. Mục tiêu công việc:

- Chủ động khám phá và dò quét các tài sản số đầy đủ và chính xác;
- Cung cấp các thông tin liên quan, đồng thời hỗ trợ kiểm thử các rủi ro;
- Xây dựng cơ chế tự động phản hồi, tích hợp với quy trình phát hiện và phản ứng rủi ro;
- Quản lý chặt chẽ việc xử lý, ngăn chặn các nguy cơ gây mất ATTT.

Từ đó giúp cho VietinBank có thể phát hiện sớm, chuẩn bị ứng phó với các nguy cơ gây mất ATTT nhằm nâng cao bảo mật cho hệ thống thông tin (HTTT) của VietinBank. Đồng thời chủ động hơn đối với các hiểm họa trên không gian mạng trong tương lai và giúp cho các nhân sự SOC, người dùng được cảnh báo về các mối nguy hại mới nhất, các rủi ro khi phải đối mặt với các tấn công này, đồng thời xây dựng được các báo cáo an ninh theo nhu cầu.

3. Yêu cầu kỹ thuật của gói thầu:

3.1 Yêu cầu kỹ thuật: Dịch vụ của nhà thầu phải đáp ứng tối thiểu các yêu cầu sau:

TT	Tính năng	Yêu cầu
1. Yêu cầu chung		

TT	Tính năng	Yêu cầu
1.1	Thuê dịch vụ phần mềm trên Cloud (SaaS): Hệ thống phát hiện và quản lý các nguy cơ ATTT từ bên ngoài trong 3 năm	• Hệ thống đáp ứng cho tối đa 2000 tài sản trực tuyến (live assets); • Quản lý các nguy cơ an toàn thông tin từ bên ngoài (Attack Surface Management); • Hỗ trợ làm giàu thông tin dựa trên các thông tin tình báo về an ninh mạng (Exploit Intelligence); • Tần suất thực hiện dò quét: 1 lần/tháng bao gồm: - Dò quét các tài sản mới, các thay đổi về tài sản. - Dò quét các vấn đề rủi ro (issue) liên quan đến các tài sản mới này.
2. Yêu cầu kỹ thuật chi tiết		
2.1	**Quản lý và tìm kiếm các tài sản số liên quan đến VietinBank**	
2.1.1	Giải pháp cung cấp đường dẫn và vị trí của tất cả các tài sản bên ngoài Internet	• Giải pháp cung cấp đường dẫn và vị trí của tất cả các tài sản bên ngoài Internet bao gồm cả tài sản được lưu trữ trên môi trường đám mây của bên thứ 3
2.1.2	Có khả năng phát hiện cơ cấu và các tài sản trực thuộc VietinBank dựa trên bằng chứng rõ ràng	• Khám phá để phát hiện các cơ cấu và tài sản được đưa ra môi trường Internet trực thuộc VietinBank. • Danh sách tài sản số liên quan
2.1.3	Phát hiện, phân nhóm và phân bổ tài sản theo cơ cấu tổ chức của VietinBank	Giải pháp có khả năng nhóm các tài sản liên kết nếu liên quan đến một ứng dụng web cụ thể: • Thông tin về tài sản bao gồm thông tin máy chủ, ngôn ngữ, dịch vụ sử dụng,... được phân bổ theo các phân nhóm dựa trên cơ cấu tổ chức, vị trí triển khai, đối tác hoặc các môi trường công ty thành viên.
2.1.4	Cho phép xác minh các công nghệ hoặc sản phẩm được sử dụng.	• Giải pháp cho phép xác minh được các công nghệ hoặc sản phẩm được sử dụng (Ví dụ: Cisco Router, VPN, Paloalto Firewall, ...)
2.1.5	Cho phép xác định mức độ rủi ro, xếp hạng và phân loại cấp độ đối với mỗi tài sản dựa trên các tiêu chí như vấn đề/lỗ hổng/cấu hình	Giải pháp cung cấp tính năng: • Xác định mức độ rủi ro. • Phân loại cấp độ của tài sản.

TT	Tính năng	Yêu cầu
2.1.6	Giải pháp xếp hạng về mức độ tìm kiếm và các mối liên kết trong cấu trúc hoặc xếp hạng theo mức độ hấp dẫn của các tài sản đối với hacker	Giải pháp có khả năng xếp hạng các tài sản về mức độ tìm kiếm và các mối liên kết trong cấu trúc của Vietinbank hoặc xếp hạng theo mức độ hấp dẫn của các tài sản đối với hacker.
2.1.7	Cho phép tìm kiếm các tài sản dựa trên môi trường, các thẻ được tạo gắn với tài sản hoặc các tham số khác của ứng dụng	• Giải pháp cung cấp tính năng tìm kiếm các tài sản dựa trên môi trường, các thẻ được tạo gắn với tài sản hoặc các tham số khác của ứng dụng.
2.2	**Khả năng phát hiện các hướng tấn công (Attack Vector Detection)**	
2.2.1	Cơ chế hoạt động hệ thống giống như hacker	• Giải pháp cung cấp cơ chế hoạt động giống như hacker sử dụng các kỹ thuật "Black-box" để do thám hệ thống của Vietinbank.
2.2.2	Hỗ trợ hướng dẫn khắc phục sự cố đối với mỗi vấn đề được tìm thấy	• Giải pháp cung cấp các thông tin, các hướng dẫn khắc phục và các bằng chứng liên quan đến các vấn đề được tìm thấy.
2.2.3	Cơ chế kiểm tra chủ động, cho phép ưu tiên các vấn đề có bằng chứng rõ ràng	• Xác định và ưu tiên hóa các hành vi truy cập quan trọng từ xa mà kẻ tấn công có thể sử dụng để cài đặt phần mềm độc hại hoặc sử dụng cho các lần xâm nhập ban đầu. • Xác định và ưu tiên các rủi ro an ninh mạng liên quan đến các công ty con, công ty thành viên để lại bỏ.
2.3	**Cung cấp các gợi ý ưu tiên khắc phục sự cố**	
2.3.1	Hướng dẫn xử lý các sự cố ưu tiên	• Giải pháp phải cung cấp các hướng dẫn đối với các sự cố ưu tiên.
2.3.2	Cung cấp các đề xuất và theo dõi khắc phục sự cố	• Giải pháp có khả năng cung cấp các đề xuất và theo dõi khắc phục sự cố 1 cách chi tiết.
2.3.3	Lọc các vấn đề theo mức độ rủi ro và độ tin tưởng	• Giải pháp cung cấp có khả năng lọc và tối ưu các vấn đề cần xử lý dựa trên mức độ rủi ro (severity) và mức độ tin tưởng (confidence).
2.4	**Khả năng tích hợp và hỗ trợ quy trình làm việc (workflows)**	
2.4.1	Giải pháp có khả năng tích hợp với các ứng dụng điều phối từ bên thứ 3 của Vietinbank	• Giải pháp có khả năng tích hợp với hệ thống SIEM.

TT	Tính năng	Yêu cầu
2.4.2	Cung cấp quy trình làm việc tự động trên chính phần mềm	• Giải pháp cung cấp quy trình làm việc tự động trên chính phần mềm (ví dụ cho phép thay đổi trạng thái của quá trình điều tra sự cố hoặc thêm các ý kiến (comments) trên tài sản và các vấn đề).
2.4.3	Tích hợp REST API	• Giải pháp hỗ trợ tích hợp REST API để trích xuất thông tin các tài sản và các dữ liệu trên Endpoint.
2.4.4	Hỗ trợ xuất dữ liệu về các vấn đề và tài sản	• Giải pháp cung cấp tính năng xuất dữ liệu về các vấn đề và tài sản theo định dạng CSV.
3.	**Các yêu cầu quản trị**	
3.1	Hỗ trợ giao diện quản trị qua web-based, hoặc có thể truy cập thông qua API	• Giải pháp cung cấp tính năng truy cập thông qua các API.
3.2	Lưu trữ log truy cập của quản trị	• Giải pháp cho phép kiểm toán các log truy cập của người dùng quản trị.
4. Thời gian cung cấp dịch vụ		
4.1	Thuê dịch vụ phần mềm trên Cloud (SaaS): Hệ thống phát hiện và quản lý các nguy cơ ATTT từ bên ngoài trong 3 năm	• Thời hạn thuê dịch vụ phần mềm trên Cloud trong vòng 03 năm. Hệ thống có bản quyền sử dụng dịch vụ chính hãng. • Hỗ trợ VietinBank trong quá trình sử dụng, hỏi đáp, thắc mắc. • Hỗ trợ tham gia cùng khách hàng trong các phiên meeting với hãng. Xây dựng báo cáo đánh giá 6 tháng 1 lần về: - Báo cáo tổng quan các rủi ro; - Các tài sản mới, các rủi ro liên quan đến tài sản mới; - Phân tích rủi ro ở mức cao, hỗ trợ xác minh cùng khách hàng.

3.2 Yêu cầu khác:

Nhà thầu phải cam kết:

- Không có thông tin vi phạm về kết quả thực hiện hợp đồng của nhà thầu theo quy định tại Điều 19 và Điều 20 của Nghị định số 214/2025/NĐ-CP.

- Không sao chép, thay đổi, sử dụng hay cung cấp dữ liệu của VietinBank cho cá nhân, tổ chức khác (dưới bất kỳ hình thức nào) nếu không được sự đồng ý của VietinBank.

- Trong phạm vi cung cấp dịch vụ cho VietinBank, phải hỗ trợ, hợp tác điều tra trong trường hợp có yêu cầu từ các cơ quan chức năng có thẩm quyền thực hiện xử lý các sự cố vi phạm an toàn thông tin mạng theo quy định của pháp luật. Trường hợp bắt buộc phải cung cấp dữ liệu của VietinBank cho cơ quan có thẩm quyền (như cơ quan điều tra, phòng chống tội phạm, …) phải thông báo cho VietinBank.

- Tiêu hủy dữ liệu khi kết thúc hợp đồng.

4. Quy định trả lời yêu cầu kỹ thuật:

Để trả lời đối với từng yêu cầu, đề nghị Nhà thầu sử dụng Bảng mẫu Trả lời dưới đây.

Stt	Yêu cầu	Mức độ đáp ứng (Chọn Có/Không)	Dẫn chứng trong E-HSDT
[Yêu cầu trong E-HSMT]	Yêu cầu: [đưa phần mô tả yêu cầu từ E-HSMT]		Chỉ dẫn tới dẫn chứng trong E-HSDT

Nhà thầu phải nêu rõ đã giải thích/dẫn chứng tại phần nào, mục nào, tài liệu nào của E-HSDT, đáp ứng yêu cầu kỹ thuật gì trong E-HSMT, để bên mời thầu dễ dàng tham chiếu khi xem xét E-HSDT.

Trường hợp E-HSDT thiếu các tài liệu theo yêu cầu, hoặc nhà thầu chỉ dẫn, dẫn chiếu không đúng, hoặc thông tin trong E-HSDT được trích dẫn không chính xác, hoặc thông tin trong E-HSDT không được tìm thấy trên các địa chỉ của chính hãng cung cấp sản phẩm, dịch vụ, hoặc không có cơ sở để cho rằng sản phẩm, dịch vụ dự thầu có cấu hình tương đương hoặc đáp ứng yêu cầu kỹ thuật trong E-HSMT thì yêu cầu đó coi như trả lời không hợp lệ và chấm không đạt.