Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

Mục 1. Giới thiệu chung về gói thầu:

- Tên gói thầu: Phần mềm phòng chống Virus cho 3000 máy chủ kèm dịch vụ triển khai, 2 năm.
- Nguồn vốn: Vốn đầu tư mua sắm tài sản cố định của Ngân hàng TMCP Việt Nam.
- Tên Chủ đầu tư: Ngân hàng TMCP Công thương Việt Nam.
- Thời gian thực hiện gói thầu: 60 ngày, kể từ ngày hợp đồng có hiệu lực.
- Loại hợp đồng: Trọn gói.
- Mục tiêu công việc: Triển khai phần mềm phòng chống virus cho 3000 máy chủ chạy hệ điều hành Non-Windows tại các Trung tâm dữ liệu chính và dự phòng (DC, DR) của Ngân hàng TMCP Công thương Việt Nam (VietinBank) nhằm đảm bảo an toàn bảo mật thông tin góp phần nâng cao năng lực bảo mật và duy trì hoạt động ổn định cho toàn bộ hạ tầng công nghệ thông tin của hệ thống.
- Nội dung và quy mô mua sắm:

STT	Nội dung	Đơn vị tính	Số lượng
1	Phần mềm phòng chống virus cho 3000 máy chủ kèm dịch vụ triển khai, 2 năm	Gói	1

Mô tả yêu cầu cụ thể đối với hàng hóa, dịch vụ: chi tiết tại Mục 2 – Chương V của E-HSMT.

Mục 2. Yêu cầu về Kỹ thuật

2.1. Biểu phạm vi cung cấp:

Đáp ứng theo yêu cầu tại Mẫu số 01A - Phạm vi cung cấp hàng hóa, Chương IV.

2.2. Yêu cầu kỹ thuật chi tiết:

Phần mềm và dịch vụ đi kèm phải có tính năng tương đương hoặc cao hơn các yêu cầu sau:

STT	Tính năng	Yêu cầu
1	**Yêu cầu chung**	
1.1	Phạm vi triển khai	Có khả năng triển khai, cài đặt tối thiểu cho 3000 máy chủ tại Trung tâm dữ liệu DR và DC của VietinBank.
1.2	Thời hạn bản quyền	Tối thiểu 02 năm

STT	Tính năng	Yêu cầu
1.3	Hãng cung cấp giải pháp uy tín	Giải pháp nằm trong nhóm leader theo đánh giá của Gartner Magic Quadrant cho Endpoint Protection Platform 2023/2024
		Hãng cung cấp nằm trong top 3 về khả năng nghiên cứu, phát hiện các lỗ hổng bảo mật trên đa nền tảng dựa trên 03 báo cáo mới nhất của Omdia
		Giải pháp nằm trong nhóm leader theo đánh giá của Forrester Wave về Endpoint Security 2023/2024
2	**Tính năng bảo vệ**	
2.1	Đa module trên nền tảng 01 agent duy nhất	Đáp ứng tối thiểu các module: - Anti Malware - Firewall - Kiểm soát độ uy tín Web - Chống xâm nhập và vá ảo - Kiểm soát tính toàn vẹn của file - Kiểm soát log trên server - Kiểm soát ứng dụng được thực thi trên server
2.2	Bảo vệ khỏi các mối đe dọa ở mức File-based	Hỗ trợ theo thời gian thực hoặc quét theo yêu cầu đối với các tính năng bảo vệ File-based: - Malware - Virus - Spyware - Trojan
2.3	Bảo vệ khỏi các mối đe dọa đối với Docker	Hỗ trợ bảo vệ Docker host với các tính năng: - Phòng chống xâm nhập/tấn công khai thác lỗ hổng - Ngăn chặn mã độc - Giám sát toàn vẹn của Docker host - Giám sát ứng dụng - Firewall Hỗ trợ bảo vệ Docker container với các tính năng: - Phòng chống tấn công khai thác lỗ hổng bảo mật - Phòng chống mã độc thực thi

STT	Tính năng	Yêu cầu
2.4	Bảo vệ với Virtual Patching	Hỗ trợ vá lỗ hổng bảo mật đã biết/chưa biết đối với web, ứng dụng, hệ điều hành thông qua IPS
2.5	Kiểm soát file thực thi	Ngăn chặn việc thực thi/cài đặt các file thực thi, các file script… khi chưa được cấp phép
2.6	Kiểm soát memory	Hỗ trợ Process Memory Scanning để quét các tiến trình chạy trên RAM
2.7	Kiểm soát tính toàn vẹn	Giám sát sự thay đổi các file, dịch vụ, registry, port… Khi có thay đổi thực hiện log thông tin và gửi cảnh bảo tới quản trị hệ thống
2.8	Kiểm soát BotNet, C&C	Phát hiện và ngăn chặn botnet, các kết nối đến C&C server
3	**Tính năng phát hiện, phản hồi, tự động hóa phản hồi**	
3.1	Khả năng điều tra và phản hồi	Giải pháp cung cấp khả năng điều tra và phản hồi tổng hợp trên Endpoint, Servers, Email, Cloud Workload và Network
3.2	Nền tảng thống nhất	Giải pháp cung cấp nền tảng thống nhất cho phép các nhóm bảo mật thực hiện phản hồi ngay lập tức và theo dõi các hành động trên endpoint, email, network, container
3.3	Hỗ trợ chatbot AI	Giải pháp cần có chatbot hỗ trợ AI để hướng dẫn điều tra và tự động đưa ra câu trả lời cho mọi câu hỏi liên quan đến an ninh mạng
3.4	Tính năng playbook	Giải pháp có khả năng tự động hóa nhiều hành động khác nhau bằng Playbook để giảm tài công việc, đẩy nhanh tác vụ điều tra
4	**Yêu cầu hỗ trợ, tích hợp**	
4.1	Hỗ trợ đa dạng endpoint cho các hệ điều hành	Tối thiểu các hệ điều hành Windows Server 2012, 2016, 2019, 2022; Oracle Linux; RedHat Enterprise Linux, Ubuntu
4.2	Cơ chế license	Giải pháp cung cấp mô hình license dựa trên credit để linh hoạt và tự do triển khai các mô-đun/dịch vụ bổ sung
4.3	Tích hợp với nền tảng ảo hóa trên Cloud	Hỗ trợ tích hợp với các tền tảng áo hóa trên Cloud như Microsoft Azure, Amazon AWS, Google Cloud Platform
4.4	Tích hợp với SIEM	Hỗ trợ tích hợp với dịch vụ SIEM QRadar

STT	Tính năng	Yêu cầu
4.5	Tích hợp đa nền tảng	Giải pháp có khả năng tính hợp khả năng quản lý Endpoint, Email, Cloud, Network, XDR và Zerotrust trên một bảng điều khiển duy nhất
5	**Yêu cầu triển khai & đào tạo**	
5.1	Dịch vụ hỗ trợ và đào tạo	Cung cấp dịch vụ hỗ trợ chính hãng Tổ chức đào tạo chuyển giao công nghệ kết hợp khóa đào tạo chuyển giao công nghệ cho tối thiểu 05 cán bộ
5.2	Hỗ trợ kỹ thuật	- Dịch vụ hỗ trợ kỹ thuật chính hãng. - Có nhân sự hỗ trợ sự cố, troubleshooting, tối ưu cấu hình và policy, thực hiện đánh giá cấu hình hệ thống tối thiểu 01 lần/năm.