BỘ Y TẾ
BỆNH VIỆN NHI TRUNG ƯƠNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Số: 541 /TM-BVNTW

Hà Nội, ngày 18 tháng 12 năm 2024

THƯ MỜI BÁO GIÁ

Kính gửi: Quý công ty/ Nhà cung cấp

Bệnh viện Nhi Trung ương có nhu cầu tiếp nhận báo giá để tham khảo, xây dựng giá gói thầu làm cơ sở tổ chức lựa chọn nhà thầu gói thầu Mua sắm phần mềm diệt virus thế hệ mới và hệ thống phát hiện phòng chống tấn công chủ động lớp người dùng EDR với nội dung cụ thể như sau:

I. Thông tin của đơn vị yêu cầu báo giá:

1. Đơn vị yêu cầu báo giá: Bệnh viện Nhi Trung ương

2. Thông tin liên hệ của người chịu trách nhiệm tiếp nhận báo giá:

- Phòng Công nghệ thông tin, Bệnh viện Nhi Trung ương;

- Địa chỉ: Số 18, ngõ 879 đường La Thành, Đống Đa, Hà Nội;

- Số điện thoại: 024.6273.8981.

3. Cách thức tiếp nhận báo giá:

- Nhận trực tiếp tại địa chỉ: Bộ phận Văn thư - Tầng 3 nhà 15 tầng Bệnh viện Nhi Trung ương; Địa chỉ: Số 18, ngõ 879 đường La Thành, Đống Đa, Hà Nội.

- Gửi 01 bản excel/word về địa chỉ email: p.cntt@nch.gov.vn

4. Thời gian tiếp nhận báo giá: Trong vòng 07 ngày làm việc kể từ ngày thông báo.

Các báo giá nhận được sau thời điểm nêu trên có thể không được xem xét.

5. Thời gian có hiệu lực của báo giá: Tối thiểu 90 ngày kể từ ngày báo giá.

1. Danh mục mua sắm phần mềm diệt virus thế hệ mới và hệ thống phát hiện phòng chống tấn công chủ động lớp người dùng EDR mời chào giá Chi tiết tại **Phụ lục 1** đính kèm yêu cầu báo giá này.

2. Địa điểm cung cấp hàng hóa: Bệnh viện Nhi Trung ương. Địa chỉ: số 18, ngõ 879 Đường La Thành, Đống Đa, Hà Nội. Yêu cầu báo giá bao gồm chi phí vận chuyển, lắp đặt và toàn bộ các loại thuế, phí liên quan.

3. Thành phần và quy cách hồ sơ báo giá:

- Báo giá theo mẫu Báo giá tại **Phụ lục 2**.

- Tài liệu chứng minh về tính năng, thông số kỹ thuật và các tài liệu liên quan đến việc lưu hành hợp pháp của hàng hóa.

- Giấy chứng nhận đăng ký kinh doanh và xác nhận ngành nghề đăng ký kinh doanh (nếu có)

- Kèm theo kết quả trúng thầu của đơn vị trong vòng 12 tháng (nếu có) đối với các hàng hóa tương tự mà đơn vị chào giá cho Bệnh viện.

Lưu ý: Báo giá phải được người có thẩm quyền ký trực tiếp trên văn bản giấy, khi ký văn bản dùng bút có mực màu xanh, không dùng các loại mực dễ phai hoặc dùng dấu chữ ký khắc sẵn để ký báo giá.

Kính đề nghị các Công ty/ Nhà cung cấp quan tâm và có khả năng cung cấp gửi Báo giá để Bệnh viện có căn cứ xây dựng Kế hoạch lựa chọn nhà thầu cho gói thầu.

Trân trọng!

GIÁM ĐỐC

BỆNH VIỆN NHI TRUNG ƯƠNG

Trần Minh Điển

PHỤ LỤC 1

DANH MỤC, SỐ LƯỢNG, TÍNH NĂNG KỸ THUẬT CƠ BẢN, TỐI THIỂU MUA SẮM PHẦN MỀM DIỆT VIRUS THẾ HỆ MỚI VÀ HỆ THỐNG PHÁT HIỆN PHÒNG CHỐNG TẤN CÔNG CHỦ ĐỘNG LỚP NGƯỜI DÙNG EDR

(Kèm theo thư mời số ..541../TM-BVNTW ngày 18/12/2024)

1. Yêu cầu về kỹ thuật chung:

- Yêu cầu về chất lượng sản phẩm mới 100%, có nguồn gốc, xuất xứ rõ ràng, đúng chủng loại, đảm bảo chất lượng theo yêu cầu của Bên mời thầu.

- Thời hạn bản quyền: 02 năm.

- Quản lý tập trung tất cả các máy trạm, thiết bị; phần mềm bảo mật đầu cuối; chính sách bảo mật; theo dõi giám sát và tự động phản ứng

- Hỗ trợ agent cài đặt, khả năng quản lý các hệ điều hành sau: Windows, MacOS, Linux, Android, iOS

- Có cơ chế tích hợp xác thực SSO cho quản trị viên qua SAML

- Tích hợp cảnh báo thông qua syslog, Slack chat, email

- Giải pháp phải có sẵn các dashboard để giám sát như Agent Management Dashboard, Incident Management Dashboard, Network Traffic Analysis (NTA) Dashboard, Risk Management Dashboard và có thể tạo thêm các dashboard theo nhu cầu thực tế

- Có cơ chế chia sẻ file cập nhật giữa các máy trạm để giảm tải cho hệ thống mạng

2. Yêu cầu về kỹ thuật cụ thể:

- Trường hợp mô tả chi tiết hàng hóa theo đặc tính kỹ thuật, thiết kế công nghệ, tiêu chuẩn công nghệ có nêu nhãn hiệu của một sản phẩm cụ thể chỉ để tham khảo, minh họa cho yêu cầu về kỹ thuật của hàng hóa, nhà thầu có thể chào hàng hoá tương đương, hoặc ưu việt hơn về đặc tính kỹ thuật, tính năng sử dụng, tiêu chuẩn công nghệ và các nội dung khác (nếu có).

- Yêu cầu hàng hóa có thông số kỹ thuật tương đương hoặc cao hơn các yêu cầu trong bảng dưới đây:

STT	Tên hàng hóa	Thông số kỹ thuật và các tiêu chuẩn	Đơn vị tính	Số lượng	Thời hạn bản quyền
1	**Hệ thống diệt virus thế hệ mới**	❖ **Năng lực bảo vệ thiết bị đầu cuối** - Chống virus, mã độc, tấn công	License	1.510	24 tháng

STT	Tên hàng hóa	Thông số kỹ thuật và các tiêu chuẩn	Đơn vị tính	Số lượng	Thời hạn bản quyền
	và phát hiện phòng chống tấn công chủ động lớp người dùng EDR	khai thác điểm yếu bảo vệ máy tính - Hỗ trợ chế độ bảo vệ liên tục và lập lịch rà quét cho các hệ thống máy tính được bảo vệ -Tường lửa bảo vệ máy chủ/máy trạm cùng khả năng quản lý thiết bị truy cập gắn ngoài như USB - Hỗ trợ sẵn và cung cấp khả năng tạo mới các hồ sơ bảo mật – Danh sách bảo mật để áp dụng xuống hệ thống máy tính được bảo vệ. Tối thiểu các security profiles có sẵn bao gồm: + Malware profile: định nghĩa các loại hình mã độc tấn công + Exploit profile: định nghĩa các hình thức tấn công khai thác lỗ hổng + Restriction profile: giới hạn các kết nối mạng, tệp tin, thiết bị gắn ngoài, ổ đĩa... - Khả năng ngăn chặn tấn công khai thác lỗ hổng ở mức OS kernel - Cung cấp sẵn tính năng máy học để ngăn chặn các tấn công dựa trên hành vi - Behavior-based threat prevention - Ngăn chặn hiệu quả hành vi tấn công mã hóa dữ liệu ransomware và có các file bẫy được để phát hiện các hành vi mã hoá dữ liệu - decoy files - Có khả năng ngăn chặn các hình thức tấn công như Reverse Shell, Cryptominers, Dylib Hijacking, Container Escaping, Brute Force,			

STT	Tên hàng hóa	Thông số kỹ thuật và các tiêu chuẩn	Đơn vị tính	Số lượng	Thời hạn bản quyền
		DLL Hijacking, Browser Exploits - Có khả năng phân tích các file nghi ngờ trong môi trường sandbox - Có khả năng kiểm tra và ngăn chặn mã độc trên nhiều định dạng file đặc biệt như: + ELF Files + Office Files + Mach-O + DMG + APK - Có tính năng tường lửa cho máy cá nhân như: Windows và Mac ❖ **Khả năng thu thập dữ liệu từ thiết bị đầu cuối** - Có khả năng thu thập dữ liệu về các tập tin trên thiết bị đầu cuối bao gồm: + Thông tin tập tin tạo mới, ghi, truy cập, mở, đổi tên hoặc xóa tập tin + Đường dẫn đầy đủ của tập tin đã sửa đổi trước và sau khi sửa đổi + Hàm băm SHA256 và MD5 cho tập tin sau khi sửa đổi - Có khả năng thu thập dữ liệu về các tiến trình: + ID của tiến trình (PID) cha (parent process) + ID của tiến trình + Đường dẫn đầy đủ + Đối số dòng lệnh + Hàm băm (SHA256 và MD5) + Chi tiết thông tin về chứng chỉ và chữ ký - Có khả năng thu thập dữ liệu về các hoạt động của registry như tạo, sửa đổi khóa, xóa và đổi tên key + Registry path của giá trị hoặc khóa bị thay đổi + Tên của các giá trị hoặc khóa bị thay đổi			

STT	Tên hàng hóa	Thông số kỹ thuật và các tiêu chuẩn	Đơn vị tính	Số lượng	Thời hạn bản quyền
		+ Dữ liệu của giá trị bị thay đổi - Có khả năng thu thập thông tin về các giao thức mạng như: + DNS request and UDP response + HTTP connect + HTTP disconnect + HTTP proxy parsing - Có khả năng thu thập thông tin về các event logs trên thiết bị đầu cuối ❖ **Khả năng điều tra, xử lý sự cố** - Có khả năng kết hợp các dữ liệu thu thập từ networks, endpoint, log authentication để xây dựng baseline về các hoạt động của các đối tượng và phát hiện các hành vi bất thường - Tích hợp sẵn nguồn Threat Intelligence để ngăn chặn các kết nối tới các địa chỉ độc hại (Malicious IP/Domain) - Cho phép theo tác từ xa trực tiếp đến hệ thống máy chủ/máy trạm được bảo vệ để thực hiện phản ứng, điều tra chuyên sâu thông qua Live Terminal - Có khả năng cô lập hệ thống máy chủ/máy trạm bị tấn công để tránh lây lan trong hệ thống - Có khả năng liên kết với các loại chiến thuật và kỹ thuật MITRE ATT & CK của từng cảnh báo - Có khả năng xem các tiến trình, các sự kiến dẫn đến cảnh báo với mô hình trực quan, có khả năng tương tác, di chuyển, mở rộng để phục vụ quá trình điều tra. Các dữ liệu được phân tích có thể bao gồm các dữ liệu từ lớp mạng - Khả năng phát hiện tấn công máy chủ/máy trạm dựa trên đa dạng dấu hiệu: + IOC (Indicator of Compromise): IP address, hash, domain, signature...			

STT	Tên hàng hóa	Thông số kỹ thuật và các tiêu chuẩn	Đơn vị tính	Số lượng	Thời hạn bản quyền
		+ BIOC (Behavioral Indicator of Compromise): hành vi hoạt động trên máy tính + Correlation: tương quan từ nhiều nguồn kết hợp - Có khả năng định nghĩa các rule phản ứng tự động cho một cảnh báo theo các điều kiện cụ thể. Các phản ứng có thể như gửi email, Assign incident, Isolate endpoint, Run malware scan, Retrieve File - Cố định cung cấp khả năng tìm kiếm và xem dữ liệu thô trên điểm cuối hoặc từ nguồn của bên thứ ba như process, file, network, registry, event log, network connection - Có khả năng thu thập file từ thiết bị cuối, máy trạm phục vụ điều tra - Có khả năng định nghĩa các rule BIOC dựa trên các hành vi thỏa hiệp (Behavioral indicators of compromise - BIOCs) dựa trên các thông tin như network, process, file, hoặc registry activity - Có giao diện đồ họa giúp truy cập vào thiết bị đầu cuối từ xa để truy cập các file, kiểm tra các tiến trình và thực thi các câu lệnh của hệ điều hành hay Python script - Có khả năng Terminate, Suspend, Resume các processs. Có khả năng check các process với Virustotal, lấy file hash, tải file binary. - Có khả năng gửi yêu cầu chặn các IP botnet, C2C xuống thiết bị tường lửa thế hệ mới qua External Dynamic List (EDL) ❖ **Có Khả năng phân tích mở rộng các cảnh báo từ tường lửa, các loại log khác** - Có khả năng nâng cấp tính năng tiếp nhận log, cảnh báo từ các giải pháp tường lửa thế hệ mới như			

STT	Tên hàng hóa	Thông số kỹ thuật và các tiêu chuẩn	Đơn vị tính	Số lượng	Thời hạn bản quyền
		Cisco, Checkpoint, Fortinet, Palo Alto Networks ❖ **Khả năng mở rộng, nâng cấp các tính năng bảo mật nâng cao** - Có khả năng nâng cấp bổ sung thêm các tính năng nâng cao + Host inventory: cung cấp các thông tin về các ứng dụng, Autoruns, Users, Disk của các máy endpoint cài đặt agent + Các lỗ hổng bảo mật trên các máy endpoint + Thu thập các thông tin phục vụ quá trình điều tra xử lý sự cố như: Browser History, File Access, Process Execution, Command History, Remote Access, Memory Collections - Có khả năng tìm và xóa các file malware trên các máy endpoint - Có khả năng nâng cấp tính năng tích hành vi người dùng - Identity analytics để phát hiện các rủi ro từ người dùng nguy hại. Đánh điểm rủi ro từng người dùng trong hệ thống ❖ **Yêu cầu về bản quyền** - Bản quyền cho thiết bị đầu cuối - Bản quyền tiếp nhận và phân tích các cảnh báo từ tường lửa và các nguồn log khác			

Phụ lục 2 - Mẫu báo giá

BÁO GIÁ

Kính gửi: Bệnh viện Nhi Trung ương

Trên cơ sở yêu cầu báo giá của Bệnh viện Nhi Trung ương, chúng tôi .... *[ghi tên, địa chỉ của hãng sản xuất, nhà cung cấp; trường hợp nhiều hãng sản xuất, nhà cung cấp cùng tham gia trong một báo giá (gọi chung là liên danh) thì ghi rõ tên, địa chỉ của các thành viên liên danh]* báo giá cho danh mục hàng hóa như sau:

1. Báo giá hàng hóa và dịch vụ liên quan:

STT	Tên hàng hóa	Tính năng kỹ thuật	Thời gian bảo hành	Hãng sản xuất	Nước sản xuất	Đơn vị tính	Số lượng	Đơn giá đã bao gồm VAT (VND)	Thành tiền (VND)
1									
.....									

2. Báo giá này có hiệu lực trong vòng: 90 ngày, kể từ ngày tháng năm .

3. Chúng tôi cam kết:

- Không đang trong quá trình thực hiện thủ tục giải thể hoặc bị thu hồi Giấy chứng nhận đăng ký doanh nghiệp hoặc Giấy chứng nhận đăng ký hộ kinh doanh hoặc các tài liệu tương đương khác; không thuộc trường hợp mất khả năng thanh toán theo quy định của pháp luật về doanh nghiệp.
- Giá trị của các tài sản, hàng hóa nêu trong báo giá là phù hợp, không vi phạm quy định của pháp luật về cạnh tranh, bán phá giá.
- Những thông tin trong báo giá là trung thực.

Hà Nội, ngày ..... tháng.....năm……

Đại diện hợp pháp của hãng sản xuất, nhà cung cấp

Ký tên, đóng dấu (nếu có)