SỞ Y TẾ
THÀNH PHỐ HỒ CHÍ MINH
BỆNH VIỆN UNG BƯỚU
Số: 1872 /TB-BVUB

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

Thành phố Hồ Chí Minh, ngày 15 tháng 4 năm 2026

YÊU CẦU BÁO GIÁ

Chủng loại mặt hàng: Tư vấn dịch vụ thẩm định giá

Kính Gửi: Các nhà cung cấp

Bệnh viện Ung Bướu có kế hoạch lựa chọn nhà thầu tư vấn dịch vụ thẩm định giá gói thầu: **"Dịch vụ giám sát hệ thống công nghệ thông tin và an toàn thông tin sử dụng tại 2 cơ sở của bệnh viện"**

Kính mời các đơn vị thẩm định giá quan tâm, có khả năng cung cấp báo giá theo nội dung như sau:

1. Thông tin đơn vị yêu cầu báo giá:

- Bệnh viện Ung Bướu
- Địa chỉ: Số 12, Đường 400, Phường Tăng Nhơn Phú, Thành phố Hồ Chí Minh.

2. Thành phần hồ sơ:

- Bảng báo giá còn hiệu lực, có ký và đóng dấu của đơn vị theo mẫu đính kèm.
- Hồ sơ năng lực nhà thầu (nếu có)

3. Thông tin người nhận báo giá trực tiếp:

- Họ và tên: Phan Thị Thu Huyền (Phòng Tài Chính - Kế Toán)
- Số điện thoại: 0906373626
- Địa chỉ nhận báo giá: Số 03, Đường Nơ Trang Long, Phường Gia Định, Tp. HCM
- Email: thamdinhgiabvub@gmail.com

Thời gian nhận báo giá: 05 ngày kể từ ngày đăng thông báo. Các báo giá nhận được sau thời điểm nêu trên sẽ không được xem xét.

Thời gian nhận chứng thư thẩm định giá: sau 05 ngày kể từ ngày nhận báo giá và ký kết hợp đồng tư vấn dịch vụ thẩm định giá.

Trân trọng./.

Nơi nhận:
- Các đơn vị có quan tâm.
- Lưu: VT, TC-KT (PTTH)

GIÁM ĐỐC

SỞ Y TẾ THÀNH PHỐ HỒ CHÍ MINH
BỆNH VIỆN UNG BƯỚU

DIỆP BẢO TUẤN

Địa chỉ:

Số điện thoại:

Email:

BẢNG BÁO GIÁ

Kính gửi: Bệnh viện Ung Bướu

Theo thông báo của Quý bệnh viện, Công ty chúng tôi xin gửi báo giá phí tư vấn dịch vụ thẩm định gói thầu sau:

STT	Nội dung công việc	ĐVT	Số lượng	Đơn giá (đã bao gồm VAT) (VNĐ)	Thành tiền (VNĐ)	Địa điểm thực hiện dịch vụ	Dự kiến ngày hoàn thành dịch vụ
1	Phí tư vấn dịch vụ thẩm định giá gói thầu: "**Dịch vụ giám sát hệ thống công nghệ thông tin và an toàn thông tin sử dụng tại 2 cơ sở của bệnh viện**"	Gói	01			Bệnh viện Ung Bướu	Nhận dự thảo chứng thư thẩm định giá sau 05 ngày kể từ ngày nhận báo giá và ký kết hợp đồng tư vấn dịch vụ thẩm định giá
	Tổng cộng						

Ghi chú: Báo giá này có hiệu lực từ ngày……đến ngày……

Ngày … tháng … năm …

ĐẠI DIỆN HỢP PHÁP CỦA NHÀ THẦU

(Ghi rõ chức danh, ký tên và đóng dấu)

SỞ Y TẾ THÀNH PHỐ HỒ CHÍ MINH
BỆNH VIỆN UNG BƯỚU

DANH MỤC THẨM ĐỊNH GIÁ

Dịch vụ giám sát hệ thống công nghệ thông tin và an toàn thông tin sử dụng tại 2 cơ sở của bệnh viện

1. Yêu cầu kỹ thuật

STT	Danh Mục	Đặc điểm và yêu cầu kỹ thuật
1	**Phần mềm giám sát hệ thống SIEM**	
1.1	**Tập trung hóa nhật ký (log) hệ thống**	Thu thập và lưu trữ log từ 100% hệ thống quan trọng (server, firewall, ứng dụng, endpoint, thiết bị mạng).
		Đảm bảo khả năng lưu trữ log tối thiểu 6–12 tháng phục vụ điều tra.
1.2	**Kiến trúc Open XDR**	Thiết kế mở, thu thập và tương quan dữ liệu từ mọi công cụ bảo mật hiện có (EDR, Firewall, Cloud) thay vì chỉ giới hạn trong một nhà cung cấp duy nhất.
1.3	**Sử dụng AI đa lớp**	Sử dụng AI đa lớp bao gồm Machine Learning có giám sát/không giám sát, GraphML và LLMs để tự động phát hiện, tương quan và phản ứng.
1.4	**Khả năng Đa người dùng**	Giải pháp hỗ trợ tính năng Multi-Tenancy
1.5	**Phân quyền RBAC**	Quản lý quyền truy cập chi tiết dựa trên vai trò (Super Admin, Platform Admin...) để kiểm soát chặt chẽ các đặc quyền trên hệ thống.
1.6	**Dashboard tùy chỉnh**	Cho phép thiết kế bảng điều khiển bằng cách kéo thả hơn 60 thành phần đồ họa (biểu đồ vùng, cột, tròn, bản đồ nhiệt).
		Công nghệ Interflow phân tích các dữ liệu thô thành các dữ liệu metadata có chứa các thông tin bao gồm: dữ liệu metadata được lưu theo ngữ cảnh, metadata chứa các thông tin từ layer 2-7 (Network Data, Server Data, Application Data, User Data, Syslog), L4-L7 performance metrics, UDLs, URIs, và domain names; Code signing certificates within files; Authentication failures; MD5 hashes of files downloaded;
1.7	**Giám sát trạng thái hệ thống**	Theo dõi trạng thái hoạt động theo thời gian thực của các nút xử lý, Data Lake và cảm biến thông qua chỉ báo màu sắc trực quan.
1.8	**Tính năng SIEM**	Chuẩn hóa mọi dữ liệu thô thành định dạng JSON metadata, giảm dung lượng lưu trữ trung bình 100:1 so với PCAP thô.
		Khung phân loại tấn công 5 giai đoạn giúp phân biệt rõ ràng tấn công nội bộ và bên ngoài, khắc phục nhược điểm của MITRE ATT&CK.

STT	Danh Mục	Đặc điểm và yêu cầu kỹ thuật
		Giải pháp sử dụng machine learrning: Tự động nhóm các cảnh báo rời rạc liên quan đến cùng một thực thể hoặc cuộc tấn công thành một Case duy nhất để giảm nhiễu
		Cung cấp sẵn thư viện gồm 789 luật phát hiện dựa trên quy tắc cho các môi trường Windows, AWS, Azure và OCI.
		Có khả năng phân loại các hành vi tấn công như: Abnormal Parent / Child Process, Brute Forced User Logins, Cryptojacking, DNS Tunneling Anomaly, Exploited C&C Connection, Exploited vulnerability, Mimikatz Credential Dump, PII Leaks, SQL Dumpfile Execution, SYN Flood, SMB Suspicious Copy
1.9	**Tính năng giám sát mạng**	Tích hợp sẵn IDS và Malware Sandbox ngay trên cảm biến để phân tích dữ liệu trực tiếp tại biên mạng
		Tích hợp sẵn IDS và Malware Sandbox ngay trên cảm biến để phân tích dữ liệu trực tiếp tại biên mạng
		Sử dụng AI để phát hiện các bất thường về mạng (Network Behavior Analytics) dựa trên các sai lệch hành vi
		Cho phép khả năng hiển thị mô phỏng cuộc tấn công mạng bằng giao diện web bao gồm IP nguồn và đích đến, cũng như phạm vi lây lan, loại tấn công, số lần của các cuộc tấn công.
		Có khả năng phát hiện: Ransomware, Spyware,Trojan, malware; các password Plaintext không được mã hóa trên đường truyền; các vi phạm bất thường trên WAF; các chính sách bất thường của tường lửa; hành vi đánh cắp dữ liệu qua DNS tunneling.
1.10	**Tính năng SOAR**	Cung cấp hơn 250 mẫu kịch bản tự động hóa săn tìm và phản ứng
		Giải pháp hoạt động hai chiều, có thể tích hợp với các giải pháp IT hoặc bảo mật khác để thực hiện hành động thủ công hoặc tự động từ SOAR.
		Tự động nhóm cảnh báo liên quan thành Case và cung cấp kho lưu trữ bằng chứng (Evidence Locker) để hỗ trợ điều tra tập trung
1.11	**Tính năng Threat Intellegence Feed**	Giải pháp đã bao gồm thông tin tình báo mối đe dọa an ninh mạng (Threat Intelligence).
		Dữ liệu Metadata được làm giàu với Threat Intelligence & Geo Location
		Hỗ trợ nạp IoCs hàng loạt từ tệp .csv hoặc .txt (lên đến 10.000 bản ghi mỗi lần xuất) phục vụ mục đích điều tra và chia sẻ thông tin nội bộ

STT	Danh Mục	Đặc điểm và yêu cầu kỹ thuật
		Nền tảng hỗ trợ nạp lên tới 50.000 IoCs cho mỗi chu kỳ quét từ nguồn SOCRadar
1.12	**Tính năng UEBA**	Tính năng Real ID liên kết nhiều danh tính khác nhau của một người dùng vào một thực thể duy nhất dựa trên SID
		Có khả năng phát hiện: command trên linux và windows; hành vi cài đặt phần mềm; Potential DLL Injection; PowerShell Startup; Windows New Processes; Windows Registry Persistence; hành vi leo thang đặc quyền trong Linux; hành vi leo thang đặc quyền trong Window.
		Tự động tính toán điểm rủi ro thực thể mỗi 10 phút dựa trên các sự kiện bảo mật trong vòng 24 giờ
		Machine Learning tự động học hành vi người dùng để phát hiện các truy cập hoặc hoạt động bất thường
1.13	**Thời hạn phần mềm**	Sử dụng tối thiểu 24 tháng
2	**Dịch vụ giám sát ATTT cho hệ thống (SIEM)**	
2.1 Giám sát, phát hiện, cảnh báo (Security Monitoring)		
2.1.1	Đăng nhập, login/logout	- Đăng nhập sai nhiều lần - Đăng nhập thời điểm bất thường (Ngày nghỉ, lễ, ngoài giờ, ban đêm..) - Đăng nhập từ vị trí bất thường (từ IP nước ngoài, từ các đơn vị khác nhau,…) - Đăng nhập từ account không hợp lệ (nghỉ việc, hết hạn,…) - Đăng nhập từ nhiều IP vào 01 nguồn - Đăng nhập từ nhiều nguồn vào 01 IP
2.1.2	Scan/Crawler/Brute force hệ thống	- Dùng các script/tool thực hiện scan - Sử dụng các payload độc hại scan tấn công hệ thống - Sử dụng các script/payload tấn công brutefoce - Các hành vi bất thường như dò quét mạng, dò quét tài khoản mật khẩu mặc định, mật khẩu yếu...
2.1.3	Thay đổi cấu hình thiết bị, hệ thống	- Thay đổi khởi tạo user mới - Password change thành công - Thay đổi xóa, sửa file cấu hình - Các audit hệ thống với trạng thái success - Thay đổi vào thời điểm bất thường - Thay đổi tính toàn vẹn file/thư mục (được giám sát) - Sự thay đổi trái phép của các tệp tin hệ thống; - Các tiến trình có dấu hiệu bất thường về hành vi và việc sử dụng tài nguyên máy chủ; - Tấn công dò quét, vét cạn mật khẩu, thư mục và khai thác thông tin; - Tấn công Phishing và cài cắm mã độc trên ứng dụng;
2.1.4	Các kết nối bất thường, tấn công DDoS	- Các kết nối tới IP nước ngoài nằm trong blacklist - Các kết nối qua giao thức samba, port 135, 137,

STT	Danh Mục	Đặc điểm và yêu cầu kỹ thuật
		139, 445,.. - Kết nối qua các port quản trị, port dữ liệu: 3389, 22, 23, 1521, 3306,… - Kết nối đồng thời từ nhiều IP nội bộ tới NTP, DNS server quốc tế - Nhiều kết nối đồng thời, số lượng lớn
2.1.5	Các tấn công theo chuẩn OWASP (XSS, SQL injection, CSRF, Path traversal, RFI/LFI,….)	- Các sự kiện liên quan có payload, signature theo chuẩn OWASP 10
2.1.6	Thống kê liên quan đến Malware/Botnet.	- Các kết nối, truy vấn tới các máy chủ điều khiển mạng botnet (C&C Server); - Source IP contain virus - Các file mã độc, URL nguy hiểm được truyền qua môi trường mạng - Các Shellcode, payload tấn công khai thác lỗ hổng phần mềm, dịch vụ
2.1.7	Phát hiện các điểm yếu, lỗ hổng trên hệ thống	Các hệ thống, server, dịch vụ tồn tại lỗ hổng
2.1.8	Giám sát tính tuân thủ của các endpoint trong mạng (cài đặt antivirus/enable firewall/phần mềm bản quyền…)	Các endpoint không tuân thủ quy định
2.2 Ứng cứu xử lý sự cố (Incident response)		
2.2.1	Xác định phạm vi ảnh hưởng đối với mỗi sự cố	Số lượng dịch vụ, hệ thống, server,... bị ảnh hưởng: - Xác định các tài sản (server, network, ứng dụng, endpoint,…), phân loại phạm vi ảnh hưởng của hệ thống bị tấn công - Xác định đầu mối phối hợp, liên lạc, điều phối
2.2.2	Xác định mức độ ảnh hưởng đối với mỗi sự cố	Đánh giá mức độ ảnh hưởng của sự cố - Xác định các tài sản (server, network, ứng dụng, endpoint,…), phân loại mức độ quan trọng của hệ thống bị tấn công - Xác định đầu mối phối hợp, liên lạc, điều phối
2.2.3	Đánh giá khả năng bị lặp lại của sự cố	Dựa trên hiện trạng, phân tích đánh giá khả năng có thể lặp lại của sự cố (chưa có bản vá, chưa có trang thiết bị,..)
2.3 Điều tra số		
2.3.1	Xác định nguyên nhân sự cố	Tìm ra nguyên nhân (root cause) sự cố đã xảy ra
2.3.2	Tìm ra nguyên nhân (root cause) sự cố đã xảy ra	Thông tin các điểm yếu được sử dụng để khai thác, tấn công hệ thống, dịch vụ của khách hàng
2.3.3	Xác định cách thức/vector tấn công	Thông tin kịch bản, các bước thực hiện, khai thác có thể được dùng để tấn công
2.3.4	Đề xuất, khuyến nghị thực hiện các giải pháp tăng cường ATTT	Khuyến nghị giải pháp, biện pháp thực hiện
2.4 Yêu cầu về giám sát		- Giám sát 24/7

STT	Danh Mục	Đặc điểm và yêu cầu kỹ thuật
		- Thời hạn tối thiểu 24 tháng
3	**Đào tạo nhận thức người dùng**	- Tối thiểu: 2 lớp/12 tháng. - Chuyên đề đào tạo phải đảm bảo đầy đủ các nội dung chính: • Kiến thức và Kỹ năng về ATTT cho người dùng trên môi trường số • Nâng cao nhận thức về an toàn thông tin, các mối nguy khi sử dụng internet, lộ lọt thông tin cá nhân trên môi trường mạng xã hội. • Phòng ngừa, xử lý các nguy cơ về an toàn thông tin trong quá trình sử dụng - Nội dung đào tạo cập nhật bổ sung các quy định mới (nếu có) - Địa điểm đào tạo: tại địa chỉ doanh nghiệp, cơ sở vật chất do doanh nghiệp cung cấp; hoặc tại bệnh viện (nếu bệnh viện yêu cầu) - Cấp chứng nhận hoàn thành - Tần suất: thực hiện tối thiểu 24 tháng
4	**Diễn tập an toàn thông tin**	- Tối thiểu : 1 lần/12 tháng - Thời gian: 4 ngày, gồm 1 ngày huấn luyện, 2 ngày diễn tập, 1 ngày đánh giá kết quả, kết thúc và chia sẻ sau diễn tập - Hình thức diễn tập: diễn tập theo hình thức thực chiến (triển khai trên 1 hệ thống thông tin đang hoạt động / vận hành), tại địa điểm của đơn vị được huấn luyện - Đội chuyên gia tham gia hỗ trợ huấn luyện, hỗ trợ trong diễn tập: 4-5 người. Đội chuyên gia sẽ vừa tham gia hỗ trợ cho các đội/nhóm tham gia vai trò redteam, đồng thời sẽ cử 1 nhóm tham gia redteam để tham gia phát hiện và khai thác điểm yếu của hệ thống diễn tập - Đội chuyên gia sẽ hỗ trợ đánh giá kết quả sau diễn tập, hỗ trợ khắc phục các điểm yếu bảo mật phát hiện được trong diễn tập, hướng dẫn trao đổi, chia sẻ của các đội và chuyên gia khi tổng kết diễn tập - Bên tổ chức triển khai có trách nhiệm: xây dựng tài liệu huấn luyện, cử chuyên gia tham gia diễn tập, đánh giá kết quả và tổ chức buổi tổng kết diễn tập - Hỗ trợ của bên được huấn luyện: địa điểm huấn luyện, phòng diễn tập, máy chiếu, âm thanh, máy tính cho các thành viên tham gia diễn tập, quản lý danh sách thành viên tham gia diễn tập - Cấp chứng nhận hoàn thành

STT	Danh Mục	Đặc điểm và yêu cầu kỹ thuật
		- Tần suất: thực hiện tối thiểu 24 tháng
5	**Xây dựng quy trình ứng cứu sự cố an toàn thông tin cho bệnh viện**	- Hỗ trợ bệnh viện khảo sát hiện trạng, xây dựng và hoàn thiện quy trình ứng cứu sự cố an toàn thông tin phù hợp với mô hình tổ chức; xác định vai trò, trách nhiệm của các đơn vị liên quan; xây dựng biểu mẫu, đầu mối phối hợp; tổ chức hướng dẫn, đào tạo, bàn giao đầy đủ tài liệu quy trình và hồ sơ liên quan.
6	**Dịch vụ triển khai SIEM**	
6.1	**Cung cấp hạ tầng máy chủ**	- vCPU: ≥ 16 core - RAM: ≥ 1128 GB - OS SSD Disk Space GB: ≥ 1500GB - SSD Disk Space TB: ≥ 12TB **Đạt chuẩn (hoặc tương đương trở lên):** - Uptime Tier III Design TCDD - Uptime Tier III Facility TCCF - Uptime Tier III Operation TCOS - Hệ thống quản lý chất lượng ISO 9001:2015 - Hệ thống quản lý năng lượng ISO 50001:2018 - PCI DSS level 2 (Service Provider IDC CENTER) - PCI DSS level 2 (Service Provider CLOUD) - Hệ thống quản lý an toàn thông tin ISO/IEC 27001:2022 - Hệ thống tiêu chuẩn quản lý kinh doanh liên tục ISO 22301 - Hệ thống tiêu chuẩn về quản lý môi trường ISO 14001 - Hệ thống tiêu chuẩn về quản lý sức khỏe và an toàn nghề nghiệp - ISO 45001 Thời hạn cung cấp: tối thiểu 24 tháng
6.2	**Cài đặt hạ tầng**	- Chuẩn bị các máy chủ cho hệ thống theo thiết kế được phê duyệt. - Chuẩn bị các gói cài đặt cho các thành phần của hệ thống - Chuẩn kết nối đảm bảo kết nối cho các thành phần DA, DL, MDS - Chuẩn bị các yêu cầu về tài nguyên theo tài liệu của hãng để cài đặt hệ thống.
6.3	**Cài đặt phần mềm**	- Cài đặt khởi tạo hệ thống, cấu hình các thông số cơ bản (địa chỉ ip,dns,...), theo tài liệu đã được chuẩn hóa phê duyệt . - Cài đặt các thành phần trong giải pháp Stellar - Active license cho giải pháp Stellar - Cấu hình các tính năng nhận Log và Network Traffic trong hệ thống (Dựa theo nhu cầu sử dụng tính năng của khách hàng) - Cấu hình cài đặt các agent thu thập log cho các máy chủ windows và linux (nếu có)

STT	Danh Mục	Đặc điểm và yêu cầu kỹ thuật
		- Cấu hình Backup hệ thống, lưu trữ cold storage (nếu có)
6.4	**Cài đặt quản trị**	- Tích hợp với hệ thống xác thực sử dụng AD, LDAP (nếu có) - Tích hợp với hệ thống Email Server (nếu có) - Cấu hình xác thực đa nhận tố 2FA - Tạo các user/tenants trong hệ thống, thực hiện phân quyền theo khảo sát, tài liệu thiết kế.
6.4.1	Cấu hình các hành động (action) cảnh báo trong hệ thống	Thiết lập cấu hình các hành động (action) đưa ra khi có các cảnh báo trong hệ thống: + Thiết lập luật tương quan sự kiện cảnh báo về mail khi có các sự kiện bất thường được định nghĩa trước + Thiết lập các hành động như disable user, block ip, run script,... khi có các sự kiện bất thường được định nghĩa trước
6.4.2	Cấu hình các luật (rule) tự động phát hiện các sự kiện trong hệ thống	Cấu hình các luật (rule) tự động phát hiện các sự kiện trong hệ thống
6.4.3	Cấu hình giao diện Dashboards	Cấu hình giao diện Dashboards
6.4.4	Cấu hình theo dõi các sự kiện từ giao diện XDR	Cấu hình theo dõi các sự kiện từ giao diện XDR