PHỤ LỤC 1:
TÍNH NĂNG KỸ THUẬT
THUÊ 06 THÁNG DỊCH VỤ GIÁM SÁT AN TOÀN THÔNG TIN SOC

(Kèm theo Thư mời chào giá số 1607 /RHMTW, ngày 01 /10 /2025)

STT	Tên danh mục	Tính năng kỹ thuật	ĐVT	Số lượng
1	**Thuê 06 tháng dịch vụ giám sát an toàn thông tin SOC**	*** Số lượng hệ thống, thiết bị công nghệ thông tin trong phạm vi giám sát:** - Hệ thống Cloud (bao gồm dịch vụ: Firewall Cloud, cân bằng tải): 01 - Hệ thống máy chủ: 02 + Tổng số lượng máy chủ ảo: 10 - Thiết bị chuyển mạch: 04 - Thiết bị Lưu trữ (SAN): 01 - Thiết bị tường lửa (Firewall): 01 - Thiết bị đầu cuối (Máy tính người dùng): 250 Tính năng kỹ thuật dịch vụ: *** Tiêu chí triển khai hệ thống giám sát:** - Khảo sát hiện trạng hệ thống (mô hình mạng, các phân vùng, thông tin phiên bản..) của hệ thống tại Bệnh viện đưa ra giải pháp phù hợp. - Tiếp nhận, đưa ra giải pháp theo yêu cầu từ phía Bệnh viện. - Đề xuất phương án thiết kế hệ thống giám sát, phương án triển khai - Đề xuất tính huống, nguyên tắc cài đặt giám sát - Đề xuất các nguồn dữ liệu cần thu thập và phương thức thu thập. - Cung cấp, trình bày mô hình và phương án triển khai - Cung cấp vai trò cụ thể của các bên liên quan trong hệ thống giám sát. - Nhà cung cấp dịch vụ chuẩn bị hạ tầng máy chủ vận hành hệ thống giám sát.	**Gói**	**01**

		- Mở firewall các ports cho phép cấu hình đẩy log, data về hệ thống SIEM (công cụ tổng hợp nhật ký - log). - Cài đặt và cấu hình hệ thống SIEM theo mô hình triển khai đã thống nhất. - Cấu hình thu thập các nguồn dữ liệu tiêu chuẩn (máy chủ, thiết bị mạng, thiết bị bảo mật, database...). - Chuẩn hóa các dữ liệu đã thu thập. - Cấu hình các câu lệnh tìm kiếm và cảnh báo theo mô hình dữ liệu đã chuẩn hóa. - Tinh chỉnh khả năng phát hiện và cảnh báo, giảm thiểu cảnh báo sai. - Tùy chỉnh Dashboard. - Tài liệu thiết kế, tài liệu cấu hình cài đặt, tài liệu hướng dẫn sử dụng. - Cung cấp máy chủ vận hành hệ thống giám sát. - Cài đặt cấu hình toàn bộ các thiết bị, ứng dụng trong phạm vụ giám sát. *** Tích hợp trong hệ thống giám sát:** - Hệ thống SIEM/XDR: công cụ giám sát tập trung dùng để thu thập, phân tích, giám sát nhật ký (log) và sự kiện an ninh trên toàn hệ thống công nghệ thông tin Bệnh viện trong phạm vi giám sát. - Hệ thống quản lý định danh và truy cập: quản lý định danh và truy cập, xác thực người dùng tại Bệnh viện. - Hệ thống Endpoint Protection (AV/EDR): hệ thống bảo mật toàn diện, trong đó EDR (Endpoint Detection and Response) là giải pháp tập trung vào việc giám sát liên tục các thiết bị đầu cuối để phát hiện, phân tích và ứng phó với các mối đe dọa mạng tinh vi đối với Bệnh viện. - Hệ thống quản lý lỗ hổng: có quy trình liên tục, chủ động và tự động hóa để xác định, đánh giá, ưu tiên, khắc phục và báo cáo các điểm yếu (lỗ hổng) trong hệ thống, mạng và ứng dụng. Sử dụng các công cụ quét lỗ hổng, kiểm tra thâm nhập và kiểm tra hệ thống để tìm ra các điểm yếu bảo mật trong phần cứng, phần mềm và cấu hình. - Hệ thống NAC - Network Access Control (Kiểm soát truy cập mạng): có giải pháp bảo mật mạng cho phép kiểm soát chặt chẽ quyền truy cập vào tài nguyên mạng của Bệnh viện, đảm bảo rằng chỉ những người dùng và thiết bị tuân thủ chính sách bảo mật mới được phép kết nối.		

		- Hệ thống quản lý Truy cập đặc quyền (PAM): có kỹ thuật và chiến lược bảo mật mạng, tập trung vào việc kiểm soát, giám sát và bảo vệ các tài khoản, thông tin đăng nhập và hoạt động có quyền truy cập cao (đặc quyền) vào các hệ thống và dữ liệu quan trọng của Bệnh viện. Mục tiêu là giới hạn quyền truy cập, ngăn chặn việc lạm dụng và giảm thiểu rủi ro từ các cuộc tấn công mạng và lỗi nội bộ, thông qua việc áp dụng nguyên tắc đặc quyền tối thiểu. - Hệ thống Threat Intelligence (TI) thông tin tình báo về mối đe dọa an ninh mạng: có hệ thống TI tự động tìm các nguồn tấn công thông qua các biện pháp theo dấu, tìm kiếm phân tích dữ liệu trên không gian mạng. Sau khi có kết quả, dữ liệu về mối đe dọa sẽ được gửi cho Bệnh viện để Bệnh viện sẽ có những biện pháp tăng cường bảo mật, vá lỗ hổng nguy hiểm. - Hệ thống UEBA (User and Entity Behavior Analytics): có giải pháp an ninh mạng có áp dụng máy học và AI để phát hiện các hành vi bất thường của người dùng và các thực thể như máy chủ, ứng dụng, thiết bị mạng trong hệ thống trong phạm vi giám sát của Bệnh viện. - Tích hợp hệ thống điều phối và xử lý tự động SOAR (Security Orchestration, Automation & Response) bao gồm: + Tự động hóa điều phối xử lý. + Quản lý sự cố, tùy chỉnh theo từng trường hợp. + Phản ứng thích ứng theo tình huống (cô lập máy, khóa tài khoản, chặn IP...). - Tích hợp phản ứng tự động. *** Đội ngũ và quy trình giám sát:** Dịch vụ đảm bảo cung cấp quy trình, đội ngũ giám sát, đánh giá và xử lý chuyên nghiệp; quy trình xử lý sự cố phải phân chia cấp độ cụ thể đáp ứng các tiêu chí sau: - Giai đoạn 1 (Giám sát): Thu thập dữ liệu từ nhiều nguồn trong hệ thống giám sát để phân tích, đánh giá dữ liệu đưa ra hướng xử lý nếu có hoặc xử lý các cảnh báo sai từ hệ thống để điều chỉnh hệ thống trở nên hiệu quả. - Giai đoạn 2 (Xử lý sự cố): Sự cố được xác nhận đã xảy ra tại giai đoạn 1 sẽ chuyển qua giai đoạn 2 để xử lý, cụ thể như sau: + Tiếp nhận thông tin, dữ liệu liên quan đến sự cố tại giai đoạn 1. + Phân tích chuyên sâu các dữ liệu đã thu thập được.		

		+ Áp dụng các quy trình xử lý sự cố phù hợp theo từng trường hợp. + Chuyển sang giai đoạn 3 nếu sự cố có tính chất nguy hiểm hơn. - Giai đoạn 3 (áp dụng khi các sự cố có dấu hiệu nguy hiểm hơn, có cả năng ảnh hưởng đến dữ liệu, khả năng vận hành của hệ thống Bệnh viện): + Tiếp nhận thông tin từ giai đoạn 1 và 2. + Thực hiện điều tra số: thu thập, phân tích và bảo quản bằng chứng số từ máy tính, thiết bị mạng và các hệ thống lưu trữ nhằm phục vụ cho mục đích pháp lý hoặc bảo mật. + Săn tìm các mối đe dọa (Threat hunting): tìm kiếm và xác định các mối đe dọa, lỗ hổng và dấu hiệu xâm phạm ẩn giấu trong hệ thống mạng và dữ liệu của bệnh viện mà các công cụ bảo mật truyền thống có thể đã bỏ sót. + Phân tích mã độc: nghiên cứu chi tiết mã độc để hiểu rõ cách thức hoạt động, mục tiêu, và phương pháp tấn công của mã độc. + Phản ứng sự cố: Phát hiện và xác định sự cố; Hạn chế sự lây lan của cuộc tấn công, giảm thiểu thiệt hại cho hệ thống và dữ liệu ; Khắc phục nguyên nhân; Đưa các hệ thống trở lại trạng thái hoạt động bình thường một cách nhanh chóng. Phân tích sự cố để cải thiện chiến lược phòng ngừa và nâng cao năng lực bảo mật tổng thể cho Bệnh viện. + Làm sạch các mối đe dọa trên hệ thống bị sự cố và xây dung cơ chế phòng ngừa từ sự cố. Yêu cầu về trình độ đội ngũ giám sát đảm nhiệm xử lý theo giai đoạn gồm: - Đối với giai đoạn 1: + Có các kiến thức, kinh nghiệm về: Phân tích các loại nhật ký, giám sát lỗ hổng, Kỹ sư an ninh mạng (như các hệ thông: Cloud, Firewall, NAC, PAM, SIEM,...) + Chứng chỉ yêu cầu: SIEM Admin, Firewall, NAC, AWS - Đối với giai đoạn 2: + Có kiến thức, kinh nghiệm về: Phân tích các loại nhật ký, phân tích mối đe dọa và lỗ hổng, xử lý sự cố nâng cao, Threat Intelligence (thông tin tình báo), phân tích mã độc (malware forensic). + Chứng chỉ yêu cầu: SIEM Admin, Cybersecurity Analyst+ (Cysa+), Threat Intelligence, Microsoft Security Architect, AWS Security. - Đối với giai đoạn 3:		

		+ Có các kiến thức, kinh nghiệm về: Threat hunter (săn tìm mối đe dọa), Advanced threat (mối đe dọa nâng cao, tinh vi), Threat Intelligence (Thông tin tình báo), ứng phó sự cố nâng cao, phân tích mã độc (Malware Reverse) + Chứng chỉ yêu cầu: OSCP, OSWE, CHFI, Burp Suite Practitioner, CEH. - Đối với người quản lý đội ngũ SOC: + Có kiến thức, kinh nghiệm về: Kiến trúc an ninh (Security Architecture), xây dựng và chịu trách nhiệm chiến lược SOC. + Chứng chỉ yêu cầu: SIEM Architect, Enterprise Security. *** Cảnh bào và báo cáo từ hệ thống:** Việc cảnh bảo sẽ được gửi đến bệnh viện thông qua Email, phải đảm bảo tối yếu các yêu cầu sau đây: - Nội dung chi tiết cảnh báo sự cố ATTT - Có tương tác để thu thập, Phân tích - Có tương tác phản ứng tự động (Block/Unblock User/IP) - Có thông tin khuyến nghị xử lý - Cung cấp các Bảng tin tình báo về các lỗ hỏng thu thấp được (hàng tuần) Các báo cáo hiển thị, thông kê đảm báo có các loại báo cáo sau đây: - Báo cáo quản lý định danh và truy cập. - Báo cáo giám sát theo từng khoa, phòng khác nhau. - Báo cáo về hiện trạng hệ thống. - Báo cáo về xu hướng các sự cố bảo mật. - Báo cáo tổng thể tấn công các lớp hệ thống. - Báo cáo tổng hợp các sự kiện ATTT. - Báo cáo chi tiết các sự kiện theo từng lớp. *** Phạm vi dữ liệu được thu thập:** - Máy tính, máy trạm, máy chủ. - Thiết bị mạng (switch, firewall). - Máy chủ ảo. - Hệ quản trị cơ sở dữ liệu. - Nhật ký hệ thống, ứng dụng, bảo mật. - Cấu hình hệ thống, thiết bị. - Tin nhắn, thông báo hệ thống. - Dữ liệu hành vi người dùng trên web.		