ĐẠI HỌC Y DƯỢC TPHCM
BỆNH VIỆN ĐẠI HỌC Y DƯỢC

Số: ...6512.../BVĐHYD-CNTT

V/v mời chào giá

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

Thành phố Hồ Chí Minh, ngày 15 tháng 12 năm 2025

Kính gửi: Quý nhà cung cấp

Bệnh viện Đại học Y Dược Thành phố Hồ Chí Minh kính mời các đơn vị có đủ năng lực và kinh nghiệm cung cấp dịch vụ giám sát An toàn thông tin (SOC) và kiểm thử xâm nhập liên tục theo yêu cầu dưới đây vui lòng gửi hồ sơ chào giá cho Bệnh viện theo nội dung cụ thể như sau:

1. Tên dự toán: cung cấp dịch vụ giám sát An toàn thông tin (SOC) và kiểm thử xâm nhập liên tục

2. Phạm vi cung cấp: chi tiết theo phụ lục đính kèm.

3. Thời gian cung cấp dịch vụ: 36 tháng kể từ ngày hợp đồng có hiệu lực

4. Loại hợp đồng: trọn gói

5. Địa điểm thực hiện: 215 Hồng Bàng, Phường Chợ Lớn, Thành phố Hồ Chí Minh

6. Hiệu lực của hồ sơ chào giá: tối thiểu 6 tháng.

7. Yêu cầu về giá chào: giá chào đã bao gồm các loại thuế, phí, lệ phí theo luật định, chi phí vận chuyển, giao hàng và các yêu cầu khác của chủ đầu tư.

8. Thời gian nhận hồ sơ chào giá: trước 12 giờ, ngày 23/12/2025

9. Quy định về tiếp nhận hồ sơ chào giá:

- Gửi báo giá online qua website: https://bvdaihoc.com.vn/Home/ViewList/31;
- Gửi bản giấy có ký tên, đóng dấu về địa chỉ sau đây: Phòng Công nghệ thông tin, Tầng 4, Khu A, Bệnh viện Đại học Y Dược Thành phố Hồ Chí Minh – Cơ sở 1, số 215 Hồng Bàng, Phường Chợ Lớn, Thành phố Hồ Chí Minh.

Người liên hệ: Nguyễn Thị Thu Tuyết Số điện thoại: 028.39525391

10. Yêu cầu khác:

Hồ sơ chào giá của nhà thầu bao gồm các tài liệu sau:

+ Thư chào giá, bảng báo giá của nhà thầu (có ký tên, đóng dấu);

+ Hợp đồng trúng thầu còn hiệu lực đối với các mặt hàng đã trúng thầu tại các cơ sở y tế (nếu có);

+ Tài liệu kỹ thuật của hàng hóa.

Trân trọng./.

Nơi nhận:
- Như trên;
- Giám đốc (để báo cáo);
- Đơn vị Quản lý Đấu thầu (để đăng tin);
- Lưu: VT, CNTT (J23-130-ntttuyet) (2).

TUQ. GIÁM ĐỐC
TRƯỞNG PHÒNG CÔNG NGHỆ THÔNG TIN

BỆNH VIỆN ĐẠI HỌC Y DƯỢC TP. HỒ CHÍ MINH

Trần Văn Đức

BM:CVĐT.01(1)

PHỤ LỤC. PHẠM VI CUNG CẤP VÀ YÊU CẦU KỸ THUẬT

(Đính kèm Công văn số ..6512../BVĐHYD-CNTT ngày 15... tháng 12 năm 2025)

I. Phạm vi cung cấp

STT	Danh mục	ĐVT	Số lượng
1	Dịch vụ giám sát An toàn thông tin	Gói	01
2	Kiểm thử xâm nhập liên tục	Gói	01

II. Yêu cầu kỹ thuật

A. YÊU CẦU CHUNG VỀ NĂNG LỰC NHÀ THẦU

STT	Tiêu chí	Yêu cầu chi tiết
1.	Giấy phép kinh doanh dịch vụ an toàn thông tin	Nhà thầu phải cung cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng, trên Giấy phép phải ghi rõ phạm vi cung cấp dịch vụ bao gồm dịch vụ giám sát an toàn thông tin.
2.	Năng lực tổ chức	Nhà thầu phải đạt chứng nhận ISO 27001 (Quản lý ATTT) và ISO 9001 (Quản lý chất lượng) còn hiệu lực.
3.	Kinh nghiệm giám sát an toàn thông tin	Nhà thầu phải có kinh nghiệm triển khai dịch vụ SOC cho tối thiểu 03 khách hàng quy mô tương đương (trên 200 máy chủ).
4.	Kinh nghiệm đánh giá an toàn thông tin	Nhà thầu phải có kinh nghiệm triển khai dịch vụ đánh giá an toàn thông tin, kiểm thử xâm nhập cho khách hàng có quy mô tương đương hoặc các hệ thống thông tin có tính chất tương tự.
5.	Năng lực đội ngũ kỹ thuật	Nhà thầu đã từng phát hiện hơn 20 lỗ hổng được định danh CVE trong 03 năm gần đây (2023 - 2025), trong đó phải có ít nhất 05 CVE phát hiện có điểm CVSS từ 9.0 trở lên.
6.	Chứng chỉ, chứng nhận dịch vụ	Nhà thầu có chứng nhận CREST tối thiểu từ Pathway+ và còn hiệu lực.
7.	Chứng nhận kỹ sư cấp khu vực	Nhà thầu có tối thiểu 05 kỹ sư được công nhận chứng chỉ kỹ sư cấp khu vực.

B. YÊU CẦU VỀ NHÂN SỰ CHỦ CHỐT

STT	Vị trí / Vai trò	Yêu cầu về trình độ và kinh nghiệm	Yêu cầu về chứng chỉ	Số lượng
1	Trưởng dự án	- Trình độ: Tốt nghiệp Đại học trở lên thuộc các chuyên ngành: Công nghệ thông tin, Điện tử Viễn thông, An toàn thông tin, Hệ thống thông tin, Khoa học máy tính hoặc các chuyên ngành có liên quan. - Kinh nghiệm: Tối thiểu 5 năm kinh nghiệm kể từ ngày tốt nghiệp Đại học trong lĩnh vực	Có đồng thời các chứng chỉ: - CISSP (Certified Information Systems Security Professional) - CCSP (Certified Cloud Security Professional)	1 nhân sự

STT	Vị trí / Vai trò	Yêu cầu về trình độ và kinh nghiệm	Yêu cầu về chứng chỉ	Số lượng
		Công nghệ thông tin/ An toàn thông tin		
2	Chuyên gia phân tích an ninh cấp cao (Senior Security Analyst / Tier 2 Lead)	- Trình độ: Tốt nghiệp Đại học trở lên thuộc các chuyên ngành: Công nghệ thông tin, Điện tử Viễn thông, An toàn thông tin, Hệ thống thông tin, Khoa học máy tính hoặc các chuyên ngành có liên quan. - Kinh nghiệm: Tối thiểu 5 năm kinh nghiệm kể từ ngày tốt nghiệp Đại học trong ngành An toàn thông tin.	Có đồng thời các chứng chỉ: - CySA+ (CompTIA Cybersecurity Analyst) - CEH (Certified Ethical Hacker).	1 nhân sự
3	Chuyên gia ứng cứu sự cố và điều tra số (Incident Responder / Forensic Lead)	- Trình độ: Tốt nghiệp Đại học trở lên thuộc các chuyên ngành: Công nghệ thông tin, Điện tử Viễn thông, An toàn thông tin, Hệ thống thông tin, Khoa học máy tính hoặc các chuyên ngành có liên quan. - Kinh nghiệm: Tối thiểu 5 năm kinh nghiệm kể từ ngày tốt nghiệp Đại học trong lĩnh vực An toàn thông tin.	Có đồng thời các chứng chỉ: - CHFI (Computer Hacking Forensic Investigator) - ECIH (EC-Council Certified Incident Handler)	1 nhân sự
4	Chuyên gia săn lùng mối đe dọa và tấn công (Threat Hunter / Tier 3)	- Trình độ: Tốt nghiệp Đại học trở lên thuộc các chuyên ngành: Công nghệ thông tin, Điện tử Viễn thông, An toàn thông tin, Hệ thống thông tin, Khoa học máy tính hoặc các chuyên ngành có liên quan. - Kinh nghiệm: Tối thiểu 5 năm kinh nghiệm kể từ ngày tốt nghiệp Đại học. - Ghi nhận tìm ra ít nhất 1 CVE được công bố trên các sản phẩm như Microsoft, Oracle, SAP.	Có đồng thời các chứng chỉ: - CEH (Certified Ethical Hacker). - ECSA (EC-Council Certified Security Analyst) - LPT Master (Licensed Penetration Tester - Master) - GXPN (GIAC Exploit Researcher and Advanced Penetration Tester) - eCTHP (Certified Threat Hunting Professional).	1 nhân sự
5	Chuyên gia bảo mật hạ tầng và tích hợp (Infrastructure Security Lead)	- Trình độ: Tốt nghiệp Đại học trở lên thuộc các chuyên ngành: Công nghệ thông tin, Điện tử Viễn thông, An toàn thông tin, Hệ thống thông tin, Khoa học máy tính hoặc các chuyên ngành có liên quan. - Kinh nghiệm: Tối thiểu 5 năm kinh nghiệm triển khai giải	Có đồng thời các chứng chỉ: - CCIE Security (Cisco Certified Internetwork Expert) - CCNP Security.	1 nhân sự

STT	Vị trí / Vai trò	Yêu cầu về trình độ và kinh nghiệm	Yêu cầu về chứng chỉ	Số lượng
		pháp bảo mật kể từ ngày tốt nghiệp Đại học		
6	Đội ngũ giám sát ATTT	- Trình độ: Tốt nghiệp Đại học trở lên thuộc các chuyên ngành: Công nghệ thông tin, Điện tử Viễn thông, An toàn thông tin, Hệ thống thông tin, Khoa học máy tính hoặc các chuyên ngành có liên quan. - Kinh nghiệm: Tối thiểu 01 năm kinh nghiệm triển khai giải pháp bảo mật kể từ ngày tốt nghiệp Đại học		8 nhân sự
7	Trưởng nhóm triển khai kiểm thử xâm nhập liên tục	- Trình độ: Tốt nghiệp Đại học trở lên thuộc các chuyên ngành: Công nghệ thông tin, Điện tử Viễn thông, An toàn thông tin, Hệ thống thông tin, Khoa học máy tính hoặc các chuyên ngành có liên quan. - Kinh nghiệm: Tối thiểu 5 năm kinh nghiệm trong lĩnh vực Công nghệ thông tin/ An toàn thông tin. - Chuyên môn: đã từng phát hiện lỗ hổng zero-day trên sản phẩm của các tổ chức uy tín như Microsoft, Oracle, … và được công nhận.	Có đồng thời các chứng chỉ: - OSCP (Offensive Security Certified Professional) - OSCE (Offensive Security Certified Expert) - CPSA (CREST Pratitioner Security Analyst)	1 nhân sự
8	Đội ngũ triển khai kiểm thử xâm nhập liên tục	- Trình độ: Tốt nghiệp Đại học trở lên thuộc các chuyên ngành: Công nghệ thông tin, Điện tử Viễn thông, An toàn thông tin, Hệ thống thông tin, Khoa học máy tính hoặc các chuyên ngành có liên quan. - Kinh nghiệm: Tối thiểu 1 năm kinh nghiệm kể từ ngày tốt nghiệp Đại học trong lĩnh vực Công nghệ thông tin/ An toàn thông tin.	Có tối thiểu 1 trong các chứng chỉ: - CEH (Certified Ethical Hacker) - eWPTX (eXtreme Web Application Penetration Tester) - eMAPT (Mobile Application Penetration Tester) - GWAPT (GIAC Web Application Penetration Tester) - CRTA (Red Team Analyst)	8 nhân sự

PHẦN I: YÊU CẦU KỸ THUẬT: DỊCH VỤ GIÁM SÁT AN TOÀN THÔNG TIN (SOC)

I. YÊU CẦU VỀ NỀN TẢNG CÔNG NGHỆ (SOC PLATFORM)

1. Yêu cầu về thành phần công nghệ và bản quyền sản phẩm

- Nhà thầu cung cấp bản quyền công nghệ, nền tảng Trung tâm điều hành an ninh mạng hợp nhất các nguồn dữ liệu hiện có (license không phụ thuộc vào độ lớn dữ liệu).

- Thành phần công nghệ cung cấp trong gói thầu:

  - Thành phần SIEM/SOAR
  - Thành phần SIRP
  - Thành phần NSM
  - Thành phần Threat Intelligence
  - Thành phần ASM
  - Thành phần Trợ lý ảo ATTT (AI Assistant)
  - Thành phần Dashboard
  - Thành phần FIM
  - Thành phần Vulnerability Management
  - Thành phần Threat Hunting

2. Yêu cầu nền tảng trung tâm điều hành an ninh mạng (SOC Platform)

2.1. Yêu cầu Dashboard của nền tảng trung tâm điều hành

• Cung cấp Dashboard cập nhật tức thời các vấn đề an toàn thông tin của tổ chức, phân nhóm cảnh báo theo MITRE và kèm các lớp đối tượng quan trọng của hệ thống như: Network, Database, Application, Host. Dashboard có ứng dụng trí tuệ nhân tạo tích hợp sẵn trong lõi phần mềm.

• Dashboard có tối thiểu các tính năng như: tin tức an toàn thông tin, quản lý số lượng EPS, quản lý tài sản, trạng thái online/offline của các nguồn logs, thông tin lỗ hổng bảo mật, trạng thái và kết quả xử lý các sự cố đã được ghi nhận, xuất báo cáo tức thời trên cùng 01 nền tảng ứng dụng. Cung cấp tối thiểu các Dashboard Giám sát trên cùng 1 Portal duy nhất:

- Báo cáo tổng quan về cảnh báo ứng với 04 lớp đã nêu, có áp dụng khung MITRE

- Truy vấn, tìm kiếm, cung cấp thông tin tình báo

- Dashboard quản lý và thống kê Event, Alert, Case, Abnormal Case, Incident

- Quản lý Agent on/off, thống kê sự kiện theo thời gian (EPS)

- Quản lý lỗ hổng bảo mật

- Dashboard về Threat Intelligence (bao gồm các tài khoản lộ lọt, thông tin về các chiến dịch tấn công mới xuất hiện và các lỗ hổng bảo mật có liên quan đến Bảo Minh)

-Cho phép thống kê các mối đe dọa, cảnh bảo an toàn thông tin trên giao diện đồ họa duy nhất liên kết thông tin nguồn từ các sản phẩm TI, SIEM, WAF, API, DDOS.

-Hỗ trợ tính năng ChatBot tích hợp AI.

2.2. Tính năng quản lý nhật ký và cảnh báo vi phạm ATTT

-Tích hợp không giới hạn các sự kiện, cảnh báo, tài sản cũng như tuỳ chỉnh lọc

-Parsing và chuẩn hoá các sự kiện

-Lưu giữ nhật ký cho phép mở rộng quy mô và dễ dàng thích ứng với Big data

-Tương quan sự kiện dựa trên KillChain và IOC

-Phát hiện và cảnh báo các hoạt động độc hại hoặc những rủi ro bảo mật theo thời gian thực

-Dashboard và các biểu đồ cho giám sát an toàn thông tin theo thời gian thực

-Quản lý và xử lý sự cố, sự kiện bảo mật

-Tích hợp API để tương tác hai chiều giữa các hệ thống bảo mật

-Quy trình tự động hoá phản hồi bảo mật và playbooks

-Quản lý và rà soát lỗ hổng bảo mật

2.3. Yêu cầu về năng lực xử lý dữ liệu lớn

-Hệ thống phải đảm bảo năng lực thu thập và xử lý log trung bình đạt 4.500 EPS (Events Per Second) và có khả năng chịu tải đột biến (Peak) lên đến 30% mà không làm mất log hay gián đoạn dịch vụ.

-Hỗ trợ mô hình triển khai linh hoạt (On-premise, Cloud hoặc Hybrid). Ưu tiên giải pháp cho phép mở rộng dung lượng lưu trữ (Scale-out) và năng lực xử lý bằng cách bổ sung phần cứng hoặc node xử lý mà không yêu cầu thay thế toàn bộ phần cứng/kiến trúc hiện tại.

-Hỗ trợ cấu hình High Availability (HA) và cơ chế lưu trữ dự phòng. Hệ thống phải có cơ chế nén log thô (Raw log) để tối ưu hóa chi phí lưu trữ cho đơn vị, đảm bảo tuân thủ thời gian lưu trữ tối thiểu 03 tháng trực tuyến và khả năng mở rộng lưu trữ dài hạn.

-Hệ thống không giới hạn năng lực xử lý dữ liệu (Event Per Second) hoặc khả năng xử lý nhật ký hằng ngày (Log per Day).

2.4. Khả năng thu thập và tích hợp dữ liệu

-Hệ thống phải hỗ trợ thu thập log từ đa dạng nguồn bao gồm hệ điều hành (Windows, Linux), thiết bị mạng, bảo mật và ứng dụng.

-Hệ thống phải có sẵn các bộ kết nối (Connectors) để tích hợp sâu với các giải pháp bảo mật hiện có tại Bệnh viện mà không phát sinh chi phí phát triển thêm.

-Hỗ trợ kết nối qua API native để thu thập và phân tích log hành vi người dùng trên nền tảng Microsoft Office 365 (Exchange, SharePoint, OneDrive) cho tối thiểu 3.500 người dùng.

-Có khả năng tự động nhận diện, phân tách (parsing) và chuẩn hóa các định dạng log thô về một định dạng chuẩn thống nhất. Hỗ trợ tính năng làm mờ (masking) để che giấu dữ liệu nhạy cảm trong log.

2.5. Khả năng phân tích, phát hiện và trợ lý thông minh

-Hệ thống hỗ trợ phân tích tương quan thời gian thực (Real-time Correlation) với bộ luật mẫu tối thiểu 1000+ rules bao phủ khung MITRE ATT&CK.

-Hỗ trợ khả năng phân tích hành vi người dùng và thực thể (UEBA) để phát hiện các bất thường như đăng nhập vào khung giờ lạ, truy cập dữ liệu nhạy cảm trái phép .

-Hệ thống tích hợp công nghệ Trợ lý ảo AI (AI Assistant) sử dụng Xử lý ngôn ngữ tự nhiên (NLP) để hỗ trợ đội ngũ vận hành. Trợ lý ảo này phải hỗ trợ tương tác, truy vấn (Query) và giải thích nội dung sự cố, khuyến nghị xử lý hoàn toàn bằng Tiếng Việt để đảm bảo tốc độ phản ứng nhanh nhất cho đội ngũ trực vận hành tại Việt Nam.

2.6. Tích hợp tình báo mối đe dọa và quản lý lỗ hổng

-Hệ thống phải tích hợp sẵn nguồn dữ liệu Tình báo mối đe dọa (Threat Intelligence) được cập nhật liên tục. Nguồn dữ liệu tình báo phải bao gồm các chỉ số tấn công (IOC) đặc thù.

-Hệ thống SIEM phải có khả năng hiển thị Dashboard quản lý lỗ hổng bảo mật (Vulnerability Management) ngay trên cùng một giao diện giám sát, cho phép tương quan trực tiếp giữa sự kiện tấn công và lỗ hổng tồn tại trên tài sản để đánh giá rủi ro chính xác.

2.7. Khả năng tự động hóa và hợp nhất nền tảng

-Tính năng Điều phối, Tự động hóa và Phản ứng (SOAR) phải được tích hợp sẵn trên cùng một nền tảng quản trị (Unified Dashboard).

-Cung cấp sẵn thư viện các kịch bản phản ứng tự động (Playbooks) cho các sự cố phổ biến và cho phép tùy chỉnh quy trình xử lý trực quan.

-Tính năng SOAR hỗ trợ tối thiểu 30 users truy cập hệ thống, hỗ trợ không giới hạn kịch bản có thể xây dựng.

2.8. Tính năng báo cáo

-Hệ thống cho phép xuất báo cáo định kỳ tự động theo mẫu tùy chỉnh, hỗ trợ đầy đủ font chữ và định dạng Tiếng Việt.

3. Yêu cầu về thành phần tự động hóa quy trình xử lý - SOAR

3.1. Khả năng tích hợp và hợp nhất nền tảng

-Hệ thống phải cung cấp khả năng điều phối và tự động hóa quy trình xử lý sự cố an toàn thông tin, tích hợp liền mạch với các công cụ bảo mật hiện có của Bệnh viện (Firewall, EDR, Active Directory, Email Gateway).

-Tính năng SOAR phải là một thành phần được tích hợp sẵn trên cùng một nền tảng quản trị (Unified Platform).

-Cung cấp mặc định các playbook tự động hoá bảo mật

-Tích hợp đa dạng các công cụ bảo mật và CNTT như SIEM, tường lửa, thiết bị mạng, nền tảng threat intelligence (thông tin mối đe dọa an toàn thông tin)

-Kết hợp các quy trình bảo mật và quy trình làm việc bằng cách kết nối các công cụ và hệ thống khác nhau

-Hệ thống phải tương thích hoàn toàn với các giải pháp Endpoint Security hiện hữu tại đơn vị để thực thi các lệnh ngăn chặn (như cô lập máy) ngay lập tức

3.2. Khả năng tự động hóa và quản lý kịch bản (Playbooks)

-Cung cấp thư viện kịch bản phản ứng (Playbooks) mẫu đa dạng cho các loại sự cố phổ biến như: Phishing Email, Ransomware, Brute-force, Lây nhiễm mã độc.

-Hỗ trợ giao diện thiết kế kịch bản trực quan (Visual Playbook Editor) dạng kéo-thả (Drag & Drop), cho phép đội ngũ vận hành tùy chỉnh quy trình xử lý (Workflow) mà không yêu cầu kỹ năng lập trình chuyên sâu (Low-code/No-code).

-Hỗ trợ cơ chế Human-in-the-loop, cho phép thiết lập các điểm kiểm soát để quản trị viên phê duyệt thủ công trước khi hệ thống thực thi các hành động có tính rủi ro cao (như chặn IP trên Firewall Core, khóa tài khoản).

3.3. Tích hợp trợ lý thông minh và làm giàu dữ liệu

-Hệ thống có khả năng tự động thực hiện làm giàu dữ liệu (Enrichment) bằng cách truy vấn các nguồn Tình báo mối đe dọa (Threat Intelligence) để xác minh mức độ uy tín của IP, Domain, Hash file ngay khi cảnh báo xuất hiện.

-Tích hợp công nghệ Trợ lý ảo AI (AI Assistant) có khả năng tự động phân tích ngữ cảnh sự cố và đề xuất kịch bản phản ứng (Playbook) phù hợp nhất.

3.4. Quản lý vòng đời sự cố và báo cáo hiệu quả

-Cung cấp giao diện quản lý sự cố tập trung (Incident Management), cho phép theo dõi toàn bộ vòng đời xử lý từ lúc phát hiện, gán ticket, thực thi playbook đến khi đóng sự cố.

-Có khả năng tự động đo lường và báo cáo trực quan các chỉ số hiệu năng của trung tâm SOC như: Thời gian trung bình để phát hiện (MTTD), Thời gian điều tra (MTTI) và Thời gian trung bình để phản hồi (MTTR) ngay trên Dashboard.

-Hỗ trợ tích hợp với các hệ thống gửi thông báo (Notification) phổ biến như Email, Microsoft Teams, Telegram để cảnh báo tức thời cho đội ngũ trực ban 24/7.

4. Tình báo mối đe dọa

4.1. Nguồn dữ liệu và phạm vi thu thập

-Hệ thống phải cung cấp cơ sở dữ liệu tri thức về các mối đe dọa ATTT được cập nhật liên tục từ tối thiểu 60+ nguồn uy tín trên thế giới và trong nước.

-Nhà thầu phải cung cấp nguồn dữ liệu tình báo đặc thù tại thị trường Việt Nam, bao gồm khả năng thu thập thông tin từ hacker trong nước để phát hiện sớm các chiến dịch tấn công nhắm vào tổ chức Y tế tại Việt Nam.

-Cung cấp khả năng giám sát và thu thập dữ liệu từ các nguồn Darkweb, Deepweb, chợ đen mua bán dữ liệu để phát hiện các thông tin nhạy cảm bị rò rỉ (Leaked Data).

4.2. Quản lý bề mặt tấn công (Attack Surface Management - ASM)

-Dịch vụ phải bao gồm tính năng Quản lý bề mặt tấn công (ASM) được tích hợp sẵn trên cùng nền tảng Tình báo mối đe dọa. Tính năng này cho phép tự động rà quét

định kỳ các tài sản số công khai (IP Public, Domain, Sub-domain) của Bệnh viện để phát hiện các rủi ro như: Port nhạy cảm bị mở, Dịch vụ tồn tại lỗ hổng (CVE) chưa vá, hoặc Chứng chỉ số hết hạn.

4.3. Khả năng tích hợp và làm giàu dữ liệu tự động

-Hệ thống Threat Intelligence phải có khả năng tích hợp hai chiều (Bi-directional) với hệ thống SIEM và SOAR của Bệnh viện thông qua API để thực hiện tự động làm giàu dữ liệu (Auto-Enrichment) cho các cảnh báo.

-Tự động đối chiếu các trường thông tin trong log (IP, Domain, Hash, URL) với cơ sở dữ liệu Threat Intelligence theo thời gian thực để phát hiện các kết nối đến máy chủ điều khiển (C&C), botnet hoặc mã độc đã biết mà không cần thao tác thủ công .

-Hỗ trợ các chuẩn chia sẻ dữ liệu nguy cơ phổ biến như STIX/TAXII và OpenIOC để dễ dàng đồng bộ với các thiết bị bảo mật khác (Firewall, EDR).

4.4. Cổng thông tin tra cứu và quản lý

-Cung cấp cổng thông tin (Portal) cho phép quản trị viên tra cứu (Lookup/Search) không giới hạn các chỉ số tấn công (IOC) bao gồm: IP, Domain, URL, File Hash và thông tin chi tiết về các nhóm tấn công APT.

-Hỗ trợ API với năng lực truy vấn cao (tối thiểu 2.000 query/giờ) để đảm bảo khả năng đáp ứng cho các hệ thống an ninh khác truy xuất liên tục.

5. Thành phần Network Security Monitoring (NSM)

5.1. Khả năng thu thập và phân tích lưu lượng mạng

-Hệ thống phải có khả năng giám sát lưu lượng mạng theo thời gian thực thông qua cơ chế Out-of-band (nhận dữ liệu từ SPAN/Mirror Port) để đảm bảo không gây ảnh hưởng đến hiệu năng vận hành của hệ thống mạng Bệnh viện.

-Hỗ trợ giải mã và phân tích các giao thức mạng phổ biến để phát hiện các hành vi bất thường, bao gồm nhưng không giới hạn ở lớp 3 đến lớp 7 của mô hình OSI

5.2. Khả năng phát hiện tấn công nâng cao

-Hệ thống phải được trang bị các luật (Rules) và chữ ký (Signatures) để phát hiện các cuộc tấn công mạng đã biết, tấn công khai thác lỗ hổng (Exploits) và các hành vi vi phạm chính sách an ninh.

-Cung cấp khả năng phát hiện sớm các dấu hiệu của tấn công có chủ đích (APT) và mã độc ẩn mình trong mạng thông qua việc nhận diện các kết nối đến máy chủ điều khiển (C&C Communication), các dịch vụ bất thường hoặc hành vi truyền tải dữ liệu nhạy cảm ra ngoài (Data Exfiltration).

-Tích hợp cơ chế phát hiện dựa trên hành vi (Behavior-based) để nhận diện các bất thường về lưu lượng (Traffic Anomaly) mà các giải pháp dựa trên chữ ký truyền thống có thể bỏ qua.

5.3. Hỗ trợ săn lùng mối đe dọa (Network Threat Hunting)

-Hệ thống phải cung cấp công cụ tìm kiếm mạnh mẽ cho phép đội ngũ vận hành thực hiện Săn lùng mối đe dọa (Threat Hunting) trực tiếp trên dữ liệu mạng. Yêu cầu hỗ trợ truy vấn sâu vào siêu dữ liệu (Metadata) của các giao thức quan trọng như: SMB (phát hiện lây lan ngang hàng), HTTP/DNS (phát hiện C&C), và SSH.

-Hỗ trợ tính năng rà quét và phát hiện các tập tin nhạy cảm hoặc độc hại được truyền tải trong luồng mạng (File Transfer scanning).

5.4. Khả năng tích hợp và quản trị tập trung

-Giải pháp NSM phải có khả năng quản trị tập trung và tích hợp hai chiều với hệ thống SIEM, SOAR và Threat Intelligence của Bệnh viện. Cho phép tự động gửi cảnh báo về SIEM để tương quan dữ liệu và nhận các chỉ số tấn công (IOC) mới nhất từ Threat Intelligence để cập nhật khả năng phát hiện.

-Hỗ trợ trích xuất bằng chứng mạng (Network Evidence) nhanh chóng để đính kèm vào hồ sơ sự cố (Incident Ticket), giúp rút ngắn thời gian điều tra cho đội ngũ Ứng cứu sự cố (Tier 3).

6. Thành phần quản lý sự cố tập trung (Incident Response Platform)

6.1. Quản lý vòng đời sự cố và quy trình chuẩn hóa

-Hệ thống phải cung cấp một giao diện làm việc tập trung để quản lý toàn bộ vòng đời của sự cố an toàn thông tin, từ giai đoạn phát hiện (Detection), phân tích (Analysis), ngăn chặn (Containment), loại bỏ (Eradication) đến phục hồi (Recovery) và bài học kinh nghiệm (Post-incident) .

-Yêu cầu hỗ trợ xây dựng và tùy biến quy trình phản ứng sự cố (Workflow) linh hoạt, tuân thủ các framework chuẩn quốc tế như NIST SP 800-61 để đảm bảo tính chuyên nghiệp và nhất quán trong xử lý.

-Hỗ trợ phân loại sự cố theo mức độ nghiêm trọng (Critical, High, Medium, Low) và loại hình tấn công (Phishing, Malware, DDoS...) để tự động gán quy trình xử lý (SLA) phù hợp

6.2. Khả năng cộng tác và điều phối

-Cung cấp môi trường cộng tác thời gian thực cho đội ngũ SOC (Tier 1, Tier 2, Tier 3), cho phép phân công nhiệm vụ (Task assignment), ghi chú (Note), và chia sẻ dữ liệu điều tra ngay trên từng hồ sơ sự cố (Case) .

-Nền tảng SIRP phải được tích hợp sẵn trên cùng một giao diện quản trị với hệ thống SIEM và SOAR (Unified Platform).

-Hệ thống phải hỗ trợ tích hợp với các kênh liên lạc như Email, Ticket Portal để tự động cập nhật trạng thái xử lý cho các bên liên quan tại Bệnh viện.

6.3. Tích hợp trí tuệ nhân tạo và tự động hóa

-Tích hợp công nghệ Trợ lý ảo AI (AI Assistant) hỗ trợ quy trình ứng cứu:

+Tự động tóm tắt diễn biến sự cố (Incident Timeline) từ hàng loạt log kỹ thuật phức tạp thành ngôn ngữ tự nhiên dễ hiểu.

+Hỗ trợ soạn thảo báo cáo sự cố (Incident Report) và khuyến nghị khắc phục bằng Tiếng Việt, giúp giảm thiểu thời gian làm báo cáo thủ công cho đội ngũ kỹ thuật.

-Tự động làm giàu dữ liệu sự cố (Auto-enrichment) bằng cách kết nối với Threat Intelligence để lấy thông tin về uy tín của IP, File Hash, Domain liên quan, giúp chuyên gia phân tích ra quyết định nhanh chóng.

6.4. Quản lý tuân thủ

-Hỗ trợ theo dõi và cảnh báo tự động về thời hạn cam kết chất lượng dịch vụ (SLA) cho từng giai đoạn xử lý để đảm bảo tuân thủ cam kết với Bệnh viện .

-Cung cấp Dashboard báo cáo hiệu năng vận hành SOC trực quan, bao gồm các chỉ số KPI/SLA quan trọng như: Số lượng sự cố theo loại, Thời gian trung bình phát hiện (MTTD), Thời gian trung bình điều tra (MTTI), Thời gian trung bình xử lý (MTTR).

7. Thành phần quản lý lỗ hổng bảo mật (Vulnerability Management)

7.1. Khả năng tích hợp và quản lý tập trung trên nền tảng SOC

-Hệ thống quản lý lỗ hổng phải được tích hợp sẵn hoặc có khả năng kết nối dữ liệu liền mạch vào nền tảng giám sát an ninh chung (Unified Dashboard).

-Kết quả rà quét không chỉ được xuất dưới dạng báo cáo file (PDF/Excel) mà phải được hiển thị trực quan (Visualize) ngay trên Dashboard của hệ thống SOC theo thời gian thực. Dashboard này cần cung cấp cái nhìn tổng quan về Sức khỏe tài sản (Asset Health), cho phép quản trị viên xem được tổng số lỗ hổng, mức độ nghiêm trọng (Critical/High/Medium) và xu hướng tăng giảm theo thời gian ngay khi đăng nhập vào hệ thống giám sát.

7.2. Khả năng tương quan dữ liệu và đánh giá rủi ro động

-Hệ thống phải có khả năng tự động tương quan (Auto-Correlation) giữa dữ liệu lỗ hổng (Vulnerability Data) và dữ liệu sự kiện an ninh (Security Events/Logs) từ SIEM.

-Hệ thống phải tự động nâng mức độ ưu tiên của cảnh báo nếu phát hiện hành vi tấn công nhắm vào một máy chủ/thiết bị đang tồn tại lỗ hổng bảo mật chưa được vá.

-Hỗ trợ đánh giá rủi ro dựa trên ngữ cảnh tài sản, cho phép định nghĩa mức độ quan trọng của từng nhóm thiết bị để ưu tiên nguồn lực khắc phục.

7.3. Quy trình quản lý vòng đời lỗ hổng khép kín

-Dịch vụ phải cung cấp quy trình quản lý lỗ hổng toàn diện theo chu trình khép kín: Phát hiện (Discover) -> Phân loại (Prioritize) -> Đánh giá (Assess) -> Báo cáo (Report) -> Khắc phục (Remediate) -> Xác minh (Verify) .

-Hỗ trợ tính năng "Xác minh lại" (Verify/Re-scan): Hệ thống cho phép theo dõi trạng thái của từng lỗ hổng (Open/Fixed) và hỗ trợ thực hiện quét kiểm tra lại ngay sau khi đội ngũ CNTT thông báo đã khắc phục, đảm bảo lỗ hổng đã được xử lý triệt để trước khi đóng Ticket xử lý.

7.4. Phạm vi rà quét và cơ sở dữ liệu tri thức

-Nhà thầu phải cung cấp năng lực và công cụ để thực hiện rà quét định kỳ (hàng tháng) hoặc đột xuất cho toàn bộ phạm vi hạ tầng CNTT bao gồm: Máy chủ (Windows/Linux), Thiết bị mạng, Thiết bị bảo mật.

-Cơ sở dữ liệu lỗ hổng (Vulnerability Database/CVE) phải được cập nhật liên tục và tự động từ các nguồn uy tín toàn cầu để đảm bảo khả năng phát hiện các lỗ hổng mới nhất ngay khi được công bố.

7.5. Báo cáo và hỗ trợ khắc phục

-Tự động tạo và gửi báo cáo định kỳ thống kê chi tiết tình hình lỗ hổng bảo mật của đơn vị.

-Báo cáo và giao diện hệ thống phải cung cấp Khuyến nghị khắc phục (Remediation Guidance) chi tiết cho từng lỗ hổng

8. Giải pháp phát hiện và phản ứng trên điểm đầu cuối

8.1. Agent hợp nhất

-Nhà thầu phải cung cấp Agent duy nhất có khả năng thực hiện đồng thời nhiều chức năng trên máy chủ/máy trạm để tối ưu hóa tài nguyên hệ thống, bao gồm:

+Thu thập nhật ký (Log Collection): Thu thập System logs, Application logs, Security logs.

+Giám sát hiệu năng (System Metrics): Thu thập thông tin về CPU, RAM, Disk I/O để hỗ trợ chẩn đoán sự cố vận hành.

+Bảo vệ an ninh (Security Protection): Có khả năng phát hiện và ngăn chặn mã độc.

8.2. Khả năng truy vấn sâu thông tin hệ thống

-Hệ thống phải cung cấp khả năng Truy vấn trạng thái hệ thống theo thời gian thực (Real-time Query) trên toàn bộ các điểm cuối được cài đặt Agent.

-Cho phép quản trị viên sử dụng cú pháp truy vấn có cấu trúc (tương tự SQL) để tìm kiếm thông tin chi tiết sâu trong hệ điều hành như: Danh sách tiến trình đang chạy (Running processes), Các kết nối mạng hiện hoạt (Active sockets), Các khóa Registry cụ thể, hoặc Các gói phần mềm đã cài đặt. Tính năng này nhằm phục vụ hoạt động Săn lùng mối đe dọa (Threat Hunting) và Điều tra số (Forensic) tức thì.

8.3. Quản lý tập trung và triển khai linh hoạt

-Cung cấp giao diện quản lý tập trung (Centralized Management Console) cho phép xem trạng thái (Health check) của toàn bộ các Agent đang hoạt động.

-Hỗ trợ cơ chế quản lý chính sách động: Cho phép đẩy cấu hình, cập nhật chính sách thu thập dữ liệu (Integration policies) hoặc nâng cấp phiên bản Agent hàng loạt từ xa mà không cần tái khởi động máy chủ hoặc can thiệp vật lý vào từng thiết bị.

8.4. Năng lực phòng vệ và tích hợp SIEM

-Agent phải có khả năng kết nối và gửi dữ liệu trực tiếp về hệ thống SIEM trung tâm của Nhà thầu thông qua các giao thức bảo mật (TLS) mà không cần qua quá nhiều tầng trung gian phức tạp, đảm bảo tính toàn vẹn và tốc độ của dữ liệu log

9. Thành phần Threat Hunting

9.1. Kiến trúc và khả năng triển khai linh hoạt

-Hệ thống phải cung cấp khả năng săn lùng mối đe dọa trên diện rộng thông qua nền tảng phần mềm chuyên dụng, hỗ trợ mô hình triển khai linh hoạt (Cloud-based hoặc On-premise).

-Cung cấp giao diện quản trị tập trung, thân thiện, cho phép kích hoạt các tác vụ rà quét và thu thập kết quả phân tích từ hàng loạt máy chủ về một Dashboard duy nhất.

9.2. Năng lực phân tích sâu thành phần hệ thống

-Hệ thống phải có khả năng phân tích sâu vào các thành phần cốt lõi của hệ điều hành Windows để phát hiện các dấu hiệu xâm nhập tinh vi mà các giải pháp diệt virus truyền thống thường bỏ qua, bao gồm:

+Rà quét bộ nhớ (Memory Scanning): Phát hiện các mã độc hoạt động trong bộ nhớ (Fileless Malware), các tiến trình bị tiêm mã (Process Injection) mà không để lại dấu vết trên đĩa cứng.

+Kiểm tra tự khởi động (Autoruns & Startup): Rà soát toàn bộ các điểm khởi chạy cùng hệ thống (Registry Run keys, Startup folders, Services, Scheduled Tasks) để phát hiện cơ chế duy trì sự tồn tại (Persistence) của mã độc.

+Phân tích tiến trình và dịch vụ: Tự động phát hiện các tiến trình giả mạo, dịch vụ lạ hoặc các tác vụ (Tasks) bất thường đang chạy ngầm.

9.3. Phương pháp phát hiện đa chiều

-Hệ thống phải tích hợp sẵn bộ luật YARA (YARA Rules) chuyên sâu, được cập nhật liên tục bởi đội ngũ chuyên gia của nhà cung cấp để rà quét và định danh các mẫu mã độc mới, các biến thể Ransomware hoặc các công cụ tấn công APT đặc thù.

-Hỗ trợ phát hiện dựa trên bất thường (Anomaly Detection) bằng cách phân tích siêu dữ liệu (Metadata) của tập tin, kiểm tra tính toàn vẹn và các dấu hiệu đáng ngờ trong thuộc tính file (như thiếu thông tin nhà phát hành, thời gian biên dịch bất hợp lý).

-Có khả năng xâu chuỗi dữ liệu từ Nhật ký sự kiện (Windows Event Logs) với các dấu hiệu thu thập được trên đĩa/bộ nhớ để tái dựng lại hành vi đáng ngờ của đối tượng.

9.4. Tích hợp đánh giá lỗ hổng và tuân thủ

-Nền tảng Threat Hunting phải tích hợp sẵn khả năng kiểm tra tình trạng bảo mật của máy chủ ngay trong quá trình săn lùng, bao gồm:

+Tự động kiểm kê phần mềm cài đặt và đối chiếu phiên bản với cơ sở dữ liệu lỗ hổng (như Exploit-DB) để cảnh báo các phần mềm tồn tại lỗ hổng đã công bố.

+Tự động kiểm tra cấu hình chính sách nhóm (GPO) của máy chủ và so sánh với các tiêu chuẩn an ninh quốc tế (như CIS Benchmarks) để phát hiện các cấu hình yếu kém có thể bị khai thác..

9.5. Tích hợp tình báo mối đe dọa

-Hệ thống phải tự động đối chiếu các Băm tập tin (File Hash), IP kết nối và Tên miền phát hiện được trên máy chủ với cơ sở dữ liệu Tình báo mối đe dọa (Threat Intelligence) từ nguồn uy tín toàn cầu và nguồn dữ liệu chỉ số tấn công (IOC) nội bộ đặc thù của nhà cung cấp (được thu thập từ các dự án giám sát tại Việt Nam).

-Ứng dụng Học máy (Machine Learning) để hỗ trợ phân loại và nhận diện mã độc chưa biết (Unknown threats) dựa trên hành vi và đặc điểm kỹ thuật.

10. Thành phần giám sát tính toàn vẹn của tệp tin (FIM)

-Giải pháp FIM phải được cung cấp dưới dạng một mô-đun hoặc tính năng kích hoạt trên cùng một Agent Giám sát duy nhất.

-Agent phải hỗ trợ đa nền tảng hệ điều hành bao gồm Windows, macOS và các bản phân phối Linux phổ biến (CentOS, RHEL, Ubuntu, Debian, SUSE) với cùng một cơ chế quản lý cấu hình.

-Hệ thống phải cung cấp khả năng giám sát thời gian thực (Real-time) đối với các sự kiện thay đổi trên hệ thống tập tin, bao gồm: Tạo mới (Created), Cập nhật nội dung (Updated), Xóa (Deleted) và Di chuyển/Đổi tên (Moved/Renamed).

-Yêu cầu bắt buộc đối với môi trường Windows: Ngoài hệ thống tập tin, giải pháp phải có khả năng giám sát sự toàn vẹn của Windows Registry. Cho phép định nghĩa các khóa Registry nhạy cảm (như Run keys, Service configurations) để phát hiện kịp thời các kỹ thuật duy trì sự tồn tại (Persistence) của mã độc hoặc hành vi thay đổi cấu hình an ninh trái phép.

-Hỗ trợ giám sát các đường dẫn (Paths) cụ thể, giám sát đệ quy (Recursive monitoring) thư mục con, và hỗ trợ sử dụng ký tự đại diện (Wildcards) để cấu hình chính sách linh hoạt.

-Khả năng phát hiện thay đổi không chỉ dựa trên nội dung tệp tin mà còn dựa trên siêu dữ liệu (Metadata), bao gồm:

+Mã băm (File Hashing): Hỗ trợ đồng thời các thuật toán băm mạnh như MD5, SHA-1, SHA-256 để xác minh tính toàn vẹn nội dung.

+Thuộc tính tệp (Attributes): Giám sát thay đổi về kích thước tệp, thời gian truy cập/chỉnh sửa (Timestamps), và các thuộc tính hệ thống.

+Quyền truy cập (Permissions & Ownership): Giám sát thay đổi về chủ sở hữu (User/Group ownership) và quyền truy cập tệp.

-Dữ liệu sự kiện FIM phải bao gồm thông tin ngữ cảnh về tiến trình (Process) và người dùng (User) đã thực hiện thay đổi.

-Dữ liệu cảnh báo FIM phải được chuẩn hóa và gửi trực tiếp về hệ thống SIEM trung tâm để lưu trữ và phân tích tương quan.

-Hỗ trợ cấu hình danh sách loại trừ (Exclusions) mạnh mẽ để loại bỏ nhiễu từ các tệp tin thường xuyên thay đổi (như tệp log, tệp tạm) giúp giảm thiểu cảnh báo giả (False Positives) cho đội ngũ vận hành.

11. Thành phần trợ lý ảo AI (AI Assistant)

-Hệ thống phải tích hợp Trợ lý ảo chuyên dụng cho an toàn thông tin, sử dụng công nghệ Xử lý ngôn ngữ tự nhiên (NLP) hoặc AI tạo sinh (Generative AI) để tương tác với người quản trị .

-Trợ lý ảo phải hỗ trợ tương tác hai chiều hoàn toàn bằng Tiếng Việt. Cụ thể:

+Cho phép người dùng đặt câu hỏi truy vấn dữ liệu hoặc yêu cầu thực hiện tác vụ bằng ngôn ngữ tự nhiên Tiếng Việt.

+Các câu trả lời, giải thích mã lỗi, tóm tắt sự cố và khuyến nghị xử lý phải được hiển thị bằng Tiếng Việt.

-Trợ lý AI có khả năng tự động phân tích các cảnh báo đến từ SIEM, đánh giá lại mức độ nghiêm trọng dựa trên bối cảnh thực tế của hạ tầng Bệnh viện và thông tin Tình báo mối đe dọa (Threat Intelligence), từ đó đề xuất mức độ ưu tiên xử lý (Priority).

-Cung cấp hướng dẫn xử lý theo ngữ cảnh (Contextual Guidance): Khi người dùng chọn một cảnh báo cụ thể, AI phải tự động đề xuất các bước xử lý tiếp theo hoặc gợi ý Kịch bản phản ứng (Playbook) phù hợp nhất dựa trên loại hình tấn công đang diễn ra.

-Trợ lý AI phải có khả năng tự động chuyển đổi câu hỏi ngôn ngữ tự nhiên thành các câu lệnh truy vấn kỹ thuật (Query Syntax) chính xác để chạy trên hệ thống SIEM.

-Hỗ trợ cung cấp các giả thuyết (Hypotheses) và danh sách kiểm tra (Checklist) để định hướng cho hoạt động Săn lùng mối đe dọa chủ động (Threat Hunting), giúp phát hiện các tấn công lẩn tránh.

-Hỗ trợ tóm tắt tự động diễn biến sự cố (Incident Timeline) từ hàng loạt log thành một đoạn văn bản tóm tắt ngắn gọn, dễ hiểu để phục vụ báo cáo nhanh cho Lãnh đạo.

-Hỗ trợ soạn thảo dự thảo Báo cáo sự cố (Incident Report) và Ghi chú bàn giao ca trực (Shift Handover) dựa trên dữ liệu hệ thống.

-Có khả năng phân tích dữ liệu vận hành để đưa ra các khuyến nghị tối ưu hóa hệ thống

-Tự động xác định các sự cố có nguy cơ vi phạm cam kết chất lượng dịch vụ (SLA)

II. YÊU CẦU VỀ PHẠM VI DỊCH VỤ VÀ QUY TRÌNH VẬN HÀNH

1. Phạm vi cung cấp

-Giám sát hệ thống công nghệ thông tin của Chủ đầu tư gồm có:

-220 máy chủ

-10 thiết bị mạng/bảo mật

-Microsoft Office 365 cho 3500 người dùng

-TrendMicro Endpoint Security

2. Yêu cầu về triển khai hệ thống SOC

2.1. Khảo sát hiện trạng

-Khảo sát chi tiết định danh tài sản: Nhà thầu phải thực hiện khảo sát vật lý và logic để xác định chính xác phạm vi giám sát, bao gồm: phiên bản hệ điều hành (OS Version patching level), vai trò nghiệp vụ (Business Logic) của từng máy chủ và mối quan hệ luồng dữ liệu (Data Flow) giữa các vùng mạng để tối ưu hóa việc đặt sensor giám sát.

+Thu thập và phân loại tài khoản quản trị: Yêu cầu thu thập và phân loại danh sách tài khoản quản trị, thời gian hoạt động và chu kỳ bảo trì hệ thống để thiết lập các khung thời gian giám sát (Monitoring Windows) và loại trừ cảnh báo giả (Suppression rules) chính xác ngay từ giai đoạn đầu.

+Phương án lưu trữ Log tùy biến: Đề xuất phương thức lưu trữ log phân tầng (Hot/Warm/Cold) cụ thể cho từng loại dữ liệu của Bệnh viện. Thời gian truy xuất log (Query time) đối với dữ liệu lưu trữ trên 03 tháng để đảm bảo hiệu năng điều tra số.

+Quy hoạch Tài nguyên Tại chỗ (On-premise Resource): Tính toán và yêu cầu chính xác tài nguyên (CPU, RAM, Disk) để triển khai các thành phần thu thập tại hạ tầng khách hàng, đảm bảo không ảnh hưởng đến hiệu năng hệ thống bệnh viện.

2.2. Thiết lập thành phần hạ tầng giám sát

-Triển khai Collector Đa nhiệm (Multi-function Collector):

+Yêu cầu triển khai hệ thống Collector đặt tại hạ tầng của Bệnh viện(On-premise).

+Collector phải có khả năng thực hiện đồng thời các chức năng: (1) Thu thập và đệm log (Buffering) để chống mất dữ liệu khi mất kết nối, (2) Thực hiện chuẩn hóa sơ bộ (Pre-parsing), và (3) Tích hợp module quét lỗ hổng bảo mật (Vulnerability Scanner) để thực hiện rà quét nội bộ.

-Thiết lập kênh kết nối bảo mật và riêng biệt: Thiết lập kênh kết nối VPN Site-to-Site hoặc kênh truyền riêng (Leased line/TLS) dành riêng cho luồng dữ liệu giám sát.

-Cung cấp Portal: Cấp quyền truy cập vào Customer Portal và Dashboard giám sát.

2.3. Tích hợp và kết nối nguồn dữ liệu

-Triển khai Agent hợp nhất (Unified Agent):

+Thực hiện cài đặt Agent trên toàn bộ máy chủ/VMs (Windows, Linux...).

+Agent phải có khả năng thu thập log hệ thống, log ứng dụng, giám sát tính toàn vẹn file (FIM) và có khả năng giao tiếp/thu thập thông tin ngữ cảnh từ các giải pháp EDR hiện có để làm giàu dữ liệu ngay tại điểm cuối trước khi gửi về Collector.

-Nhà thầu phải trực tiếp thực hiện tinh chỉnh cấu hình Audit Policy trên Windows/Linux và cấu hình trên thiết bị mạng để đảm bảo thu thập đúng các trường thông tin phục vụ điều tra (như Process ID, Parent Process, Command Line).

-Chuẩn hóa và xử lý lỗi (Parsing & Error Handling):

+Thực hiện chuẩn hóa log (Parsing) ngay tại Collector để giảm tải băng thông đường truyền.

+Yêu cầu xây dựng các Parser tùy chỉnh (Custom Parsers) cho các ứng dụng đặc thù.

+Thiết lập quy trình tự động kiểm tra và cảnh báo khi nguồn log bị mất kết nối hoặc thay đổi định dạng

2.4. Xây dựng nội dung và Usecase giám sát

-Xây dựng Dashboard chuyên biệt: Thiết kế các Dashboard giám sát tùy biến riêng cho từng đối tượng: Lãnh đạo Bệnh viện (Tổng quan KPI, Rủi ro), Quản trị hệ thống (Trạng thái Server, Kết nối mạng) và Đội ngũ An toàn thông tin (Chi tiết sự kiện, Threat Map).

-Thiết lập Bộ luật (Rules) và Threat Hunting:

+Kích hoạt và tinh chỉnh (Fine-tune) bộ luật phát hiện tấn công theo khung MITRE ATT&CK.

+Thiết lập sẵn các bộ kịch bản Săn lùng mối đe dọa (Threat Hunting queries) định kỳ để chủ động tìm kiếm các dấu hiệu tấn công (IOC).

-Báo cáo tuân thủ và tùy biến:

+Thiết lập hệ thống báo cáo định kỳ tự động.

+Mẫu báo cáo phải được tùy chỉnh theo nhu cầu của Bệnh viện.

-Lưu trữ phục vụ điều tra số: Cấu hình phân vùng lưu trữ log tập trung (Centralized Log Management) với khả năng đánh chỉ mục (Indexing) tốc độ cao để phục vụ truy vấn điều tra số (Forensic) tức thì khi có sự cố.

2.5. Yêu cầu về giám sát an toàn thông tin 24/7

-Nhà thầu phải thực hiện đầy đủ các công việc sau đây theo chế độ 24/7/365 (bao gồm ngày nghỉ, Lễ, Tết) nhằm đảm bảo hệ thống của Bệnh viện luôn được giám sát và bảo vệ liên tục.

2.6. Giám sát và sàng lọc sự kiện

-Trực giám sát 24x7: Nhân sự SOC phải thực hiện theo dõi liên tục các cảnh báo trên Dashboard tập trung. Đảm bảo mọi cảnh báo mức độ Cao/Nghiêm trọng đều được tiếp nhận trong vòng 15 phút.

-Tiếp nhận và Phân loại cảnh báo:

+Tiếp nhận log và cảnh báo từ toàn bộ phạm vi giám sát.

+Thực hiện theo quy trình Playbook để phân loại sơ bộ: Tách biệt sự cố thực sự (True Positive) khỏi các cảnh báo giả (False Positive) hoặc nhiễu hệ thống (Noise).

-Thông báo sự cố (Notification): Gửi thông báo cảnh báo cho Khách hàng qua Email/Hotline theo đúng biểu mẫu và quy trình đã thống nhất.

2.7. Phân tích và điều tra chuyên sâu

-Phân tích tương quan (Correlation Analysis):

+Không chỉ nhìn vào một cảnh báo đơn lẻ, Nhà thầu phải thực hiện tương quan chuỗi sự kiện từ nhiều nguồn (Ví dụ: Tương quan giữa cảnh báo Email Phishing trên O365 -> Hành vi tải file lạ trên máy trạm EDR -> Kết nối C&C trên Firewall) để vẽ lại bức tranh toàn cảnh của cuộc tấn công.

-Làm giàu dữ liệu và xác minh (Enrichment & Verification):

+Sử dụng nguồn Threat Intelligence để kiểm tra uy tín của các IP, Domain, File Hash nghi ngờ.

+Loại bỏ các cảnh báo dương tính giả (False Positive) phát sinh do các hoạt động nghiệp vụ hợp lệ của Bệnh viện (như quét lỗ hổng định kỳ, cập nhật phần mềm).

-Xác định Phạm vi ảnh hưởng (Impact Assessment): Xác định chính xác số lượng máy trạm/máy chủ bị ảnh hưởng, loại dữ liệu có nguy cơ bị rò rỉ và mức độ tác động đến hoạt động khám chữa bệnh.

2.8. Săn lùng Mối đe dọa chủ động (Proactive Threat Hunting)

-Săn lùng định kỳ (Scheduled Hunting):

+Thực hiện tối thiểu 01 đợt săn lùng/tháng trên toàn bộ hệ thống (Network & Endpoint).

+Nội dung săn lùng tập trung vào việc tìm kiếm các dấu hiệu xâm nhập (IOCs) tinh vi không kích hoạt cảnh báo tự động, các mã độc nằm vùng, hoặc các hành vi lạm dụng công cụ quản trị.

-Săn lùng theo Chiến dịch (Campaign-based Hunting):

+Ngay khi có thông tin về các chiến dịch tấn công mới hoặc lỗ hổng Zero-day nhắm vào ngành Y tế, Nhà thầu phải chủ động thực hiện rà soát trên hệ thống Bệnh viện để xác nhận an toàn.

2.9. Phân tích mã độc và kỹ thuật (Malware Analysis)

-Thu thập mẫu và phân tích: Khi phát hiện tệp tin nghi ngờ, Nhà thầu phải tiến hành thu thập mẫu an toàn và thực hiện phân tích:

+Phân tích Tĩnh (Static Analysis): Kiểm tra mã băm, chuỗi string, header của file.

+Phân tích Động (Dynamic Analysis): Chạy mẫu trong môi trường Sandbox cô lập để quan sát hành vi kết nối mạng, thay đổi registry/file system.

+Dịch ngược mã (Reverse Engineering): Yêu cầu bắt buộc đối với các sự cố nghiêm trọng: Chuyên gia Tier 3 phải thực hiện dịch ngược để hiểu rõ cơ chế hoạt động của mã độc nhằm đưa ra phương án gỡ bỏ triệt để

2.10. Hỗ trợ xử lý và khắc phục (Remediation Support)

-Khởi tạo Ticket và Hướng dẫn: Đối với các sự cố thực sự (True Positive), Nhà thầu phải khởi tạo vé xử lý (Ticket) và cung cấp Hướng dẫn khắc phục chi tiết (Step-by-step Remediation Plan) bằng Tiếng Việt.

-Phối hợp Ngăn chặn (Containment Coordination):

+Hỗ trợ đội ngũ IT Bệnh viện thực hiện ngăn chặn từ xa (Block IP, Isolate Host).

+Có mặt trực tiếp (Onsite Support): Cử chuyên gia đến hiện trường trong vòng 02 giờ để hỗ trợ xử lý các sự cố nghiêm trọng (Ransomware, tấn công phá hoại dữ liệu).

2.11. Công tác báo cáo và tinh chỉnh hệ thống (Reporting & Tuning)

-Báo cáo Định kỳ (Monthly Reporting):

+Lập báo cáo tháng bao gồm: Thống kê tình hình an ninh, Phân tích xu hướng tấn công, Kết quả xử lý sự cố và Đánh giá tuân thủ SLA.

+Báo cáo phải có phần "Nhận định và Khuyến nghị của Chuyên gia" về các điểm yếu cần khắc phục trong hệ thống.

-Tinh chỉnh Chính sách (Policy Tuning):

+Dựa trên dữ liệu giám sát, Nhà thầu phải liên tục thực hiện tinh chỉnh (Fine-tune) các tập luật (Rule Base) để giảm thiểu cảnh báo giả.

+Đề xuất các thay đổi cấu hình (Configuration hardening) cho thiết bị mạng/máy chủ của Bệnh viện để nâng cao khả năng phòng vệ

3. Vai trò của các nhân sự trong SOC

Mô hình vận hành SOC phải được tổ chức theo cấu trúc phân tầng (Tiered Structure) chuẩn quốc tế, đảm bảo sự phối hợp chặt chẽ giữa con người, quy trình và công nghệ để xử lý các sự cố từ đơn giản đến phức tạp nhất.

3.1. Tier 1: Giám sát viên An toàn thông tin (Security Analyst Tier 1)

-Vai trò: Là tuyến phòng thủ đầu tiên, hoạt động liên tục 24/7/365 theo ca trực (Shift)

-Nhiệm vụ và yêu cầu công việc:

+Trực chiến 24/7: Theo dõi liên tục các cảnh báo thời gian thực trên màn hình Dashboard giám sát hợp nhất (Unified Dashboard).

+Sàng lọc ban đầu (Triage): Tiếp nhận cảnh báo và xử lý theo các Playbook:

o Xác định cảnh báo sai (Noise/False Positive) để đóng ticket.

o Xác định cảnh báo thực sự (True Positive) để leo thang (Escalate) lên Tier 2.

+Thông báo sự cố (Notification): Đảm bảo cam kết thời gian thông báo (SLA) dưới 15 phút đối với các cảnh báo mức Nghiêm trọng cho Khách hàng qua các kênh Hotline/Email.

+Thực thi ngăn chặn cơ bản: Thực hiện các hành động ngăn chặn sơ cấp theo quy trình đã được phê duyệt trước (ví dụ: Block IP trên Firewall, Cô lập máy trạm qua EDR) khi có dấu hiệu tấn công rõ ràng.

3.2. Tier 2: Chuyên viên phân tích chuyên sâu (Security Analyst Tier 2)

-Vai trò: Là tuyến phân tích chính, chịu trách nhiệm điều tra sâu, xác minh sự cố và đưa ra phương án xử lý cụ thể.

-Nhiệm vụ và yêu cầu công việc:

+Điều tra và Tương quan (Deep Dive Investigation):

o Phân tích sâu các vé sự cố (Ticket) được Tier 1 chuyển lên.

o Thực hiện tương quan dữ liệu từ nhiều nguồn (SIEM, EDR, Network Logs) để xác định phạm vi ảnh hưởng (Scope of Impact): Có bao nhiêu máy bị nhiễm? Dữ liệu nào bị truy cập?

+Xác minh qua Threat Intel: Sử dụng các nguồn Tình báo mối đe dọa để kiểm tra các chỉ số tấn công (IP, Hash, Domain) có thực sự nguy hiểm hay không.

+Đề xuất biện pháp khắc phục (Remediation): Tier 2 phải cung cấp hướng dẫn xử lý từng bước (Step-by-step) bằng Tiếng Việt cho đội ngũ IT của Bệnh viện.

+Tinh chỉnh hệ thống (Fine-tuning): Chịu trách nhiệm phân tích các cảnh báo giả (False Positive) để tinh chỉnh lại luật (Rule) và ngưỡng (Threshold) trên hệ thống SIEM, đảm bảo hệ thống ngày càng chính xác.

3.3. Chuyên gia săn lùng và ứng cứu (Expert Hunter/Responder Tier 3)

-Vai trò: Là tuyến chuyên gia cao cấp nhất, xử lý các sự cố phức tạp (APT, Zero-day), thực hiện săn lùng chủ động và đảm bảo sự hiện diện tại hiện trường (Onsite).

-Nhiệm vụ và yêu cầu công việc:

+Săn lùng Mối đe dọa Chủ động (Proactive Threat Hunting):

o Không chờ cảnh báo, Tier 3 phải chủ động định kỳ thực hiện các truy vấn săn lùng trên hệ thống dựa trên các giả thuyết về các nhóm tấn công APT đang nhắm vào ngành Y tế.

o Phát hiện các mối đe dọa nằm vùng mà hệ thống tự động bỏ qua.

+Phân tích Mã độc Nâng cao (Advanced Malware Analysis):

o Thực hiện kỹ thuật Dịch ngược mã (Reverse Engineering) để phân tích hành vi các mẫu mã độc mới bắt được.

o Xác định cơ chế lây lan và đích đến của mã độc để chặn đứng tận gốc.

+Điều tra số (Digital Forensics) & RCA:

o Thu thập và phân tích chứng cứ số (Disk/Memory Forensics) để xác định Nguyên nhân gốc rễ (Root Cause Analysis - RCA) của sự cố.

o Dựng lại toàn bộ kịch bản tấn công (Kill Chain) để báo cáo Lãnh đạo.

+Cam kết ứng cứu tại chỗ (Onsite Response):

o Trong trường hợp sự cố nghiêm trọng (Ransomware diện rộng, rò rỉ dữ liệu lớn), Tier 3 phải có mặt trực tiếp tại Data Center của Bệnh viện trong vòng 02 giờ để trực tiếp chỉ huy và thực hiện khôi phục hệ thống, hỗ trợ làm việc với các cơ quan chức năng nếu cần.

4. Yêu cầu về giám sát bảo mật ứng dụng

4.1. Khảo sát hiện trạng và thiết kế kiến trúc

-Khảo sát Luồng dữ liệu và Nghiệp vụ: Nhà thầu có trách nhiệm khảo sát và xây dựng sơ đồ luồng dữ liệu (Data Flow Diagram) của ứng dụng, xác định rõ các thành phần trọng yếu (Critical Assets).

-Thiết kế Kiến trúc Giám sát (Monitoring Topology): Đề xuất kiến trúc thu thập dữ liệu đảm bảo tính sẵn sàng và tuyệt đối không gây ảnh hưởng đến hiệu năng vận hành (Performance) hoặc trải nghiệm người dùng của ứng dụng thực tế (Production).

-Định danh và Phân loại tài sản: Thực hiện phân loại mức độ quan trọng của ứng dụng.

4.2. Cài đặt và quản trị dữ liệu

-Thu thập nhật ký: Hệ thống phải có khả năng thu thập đầy đủ các loại nhật ký ứng dụng bao gồm:

+Access Logs: Ghi nhận mọi truy cập thành công/thất bại.

+Error Logs: Ghi nhận lỗi hệ thống và ngoại lệ (Exceptions).

+Audit Trails: Ghi nhận thay đổi cấu hình hoặc hành vi của quản trị viên.

-Chuẩn hóa dữ liệu (Normalization & Parsing): Hệ thống phải có khả năng tự động phân tách (Parsing) và chuẩn hóa các định dạng log thô (Raw logs) từ nhiều nền tảng khác nhau (IIS, Nginx, Apache, Tomcat, WebLogic...) về một định dạng chuẩn thống nhất JSON, CEF) để phục vụ phân tích.

-Làm sạch và Bảo vệ dữ liệu (Data Sanitization): Cung cấp tính năng làm mờ (Masking) hoặc mã hóa các trường dữ liệu nhạy cảm ngay tại nguồn thu thập hoặc trước khi lưu trữ, đảm bảo tuân thủ các quy định bảo mật.

-Quản lý Vòng đời Dữ liệu (Data Lifecycle): Cho phép thiết lập chính sách lưu trữ phân tầng (Hot/Warm/Cold) linh hoạt theo từng loại log ứng dụng để tối ưu hóa chi phí và đáp ứng yêu cầu truy vết dài hạn.

4.3. Tích hợp nguồn dữ liệu (Integration)

-Khả năng tương thích đa nền tảng: Hỗ trợ tích hợp sâu (Native Integration) hoặc thông qua API/Agent với các nền tảng ứng dụng phổ biến (Java, .NET, PHP, Node.js) và các cơ sở dữ liệu (SQL, NoSQL).

-Tích hợp Ngữ cảnh (Contextual Integration): Có khả năng liên kết dữ liệu log ứng dụng với các nguồn dữ liệu khác như WAF (Web Application Firewall), Load Balancer và Database Activity Monitoring (DAM) để cung cấp góc nhìn toàn cảnh về chuỗi truy cập.

4.4. Hiển thị và báo cáo (Visualization & Reporting)

-Dashboard giám sát thời gian thực: Cung cấp các Dashboard trực quan, cho phép theo dõi trạng thái sức khỏe (Health Check), lưu lượng truy cập (Traffic) và các chỉ số an ninh (Security Metrics) của ứng dụng theo thời gian thực.

-Báo cáo Tùy biến (Customizable Reporting): Hệ thống cho phép tạo và xuất các báo cáo định kỳ hoặc đột xuất theo mẫu tùy chỉnh, tập trung vào các thông số quan trọng: Top hành vi tấn công, Top người dùng vi phạm, Tần suất lỗi ứng dụng.

-Cảnh báo Đa kênh thông minh: Hỗ trợ thiết lập ngưỡng cảnh báo (Threshold) linh hoạt và gửi thông báo tức thời qua đa kênh (Email, OTT). Hỗ trợ cơ chế gộp cảnh báo (Aggregation) để tránh spam thông báo (Alert Fatigue).

4.5. Năng lực phát hiện tấn công (Detection Capabilities)

-Phát hiện Tấn công theo OWASP Top 10: Hệ thống phải có bộ luật (Ruleset) tích hợp sẵn để phát hiện các kỹ thuật tấn công ứng dụng phổ biến như: SQL Injection, XSS (Cross-Site Scripting), Command Injection, Path Traversal.

-Phát hiện Bất thường Nghiệp vụ (Business Logic Anomaly): Ứng dụng công nghệ phân tích hành vi (Behavioral Analysis) để phát hiện các gian lận nghiệp vụ.

-Giám sát Phiên làm việc (Session Monitoring): Khả năng phát hiện các hành vi chiếm quyền phiên (Session Hijacking) hoặc leo thang đặc quyền (Privilege Escalation).

5. Yêu cầu về Đánh giá mức độ xâm phạm (Compromised Assessment Service)

5.1. Rà soát mã độc

-Phạm vi rà quét: Nhà thầu phải thực hiện rà quét trên toàn bộ các thành phần của thiết bị (Máy chủ, Máy trạm).

-Năng lực phát hiện: Hệ thống/Công cụ sử dụng phải có khả năng phát hiện các loại mã độc đã biết (Signature-based) và chưa biết (Unknown).

-Phát hiện mã độc: Đặc biệt yêu cầu năng lực phát hiện các loại mã độc chuyên dụng nhằm trốn tránh sự phát hiện.

5.2. Săn tìm mối đe dọa chủ động (Active Threat Hunting)

-Đối soát chỉ số tấn công (IoC Sweeping): Thực hiện rà quét toàn bộ hệ thống dựa trên cơ sở dữ liệu Tình báo mối đe dọa (Threat Intelligence) mới nhất để tìm kiếm các dấu vết xâm nhập (Indicators of Compromise - IoC) như: Hash file độc hại, IP/Domain của máy chủ điều khiển (C2).

-Phát hiện kết nối C2: Phân tích các kết nối mạng hiện hoạt (Active Connections) và lịch sử kết nối để phát hiện các liên lạc bí mật ra máy chủ điều khiển (Command & Control - C2 Server) của kẻ tấn công.

-Phát hiện di chuyển ngang hàng (Lateral Movement): Nhận diện các dấu hiệu kẻ tấn công sử dụng công cụ quản trị hợp pháp (như PsExec, WMI, RDP) hoặc khai thác lỗ hổng (SMB/RPC) để lây lan từ máy này sang máy khác trong mạng nội bộ.

5.3. Phân tích hành vi và kỹ thuật trốn tránh

-Phát hiện tấn công không tệp tin (Fileless Malware): Nhà thầu phải có phương án kỹ thuật để phát hiện các mã độc hoạt động hoàn toàn trên bộ nhớ RAM hoặc sử dụng các script độc hại (PowerShell, VBScript, Bash) mà không ghi file lên ổ cứng.

-Kỹ thuật duy trì hiện diện (Persistence Mechanisms): Rà soát toàn bộ các điểm khởi động của hệ điều hành (Startup folders, Registry Run Keys, Scheduled Tasks, Services, Cron jobs) để tìm kiếm các cơ chế tự động kích hoạt lại của mã độc sau khi khởi động lại máy.

-Phát hiện kỹ thuật ẩn mình: Nhận diện các kỹ thuật tiêm mã vào tiến trình sạch (Process Injection/Hollowing) hoặc giả mạo tên tiến trình hệ thống (Masquerading) để qua mặt các giải pháp Antivirus truyền thống.

5.4. Đánh giá và phân loại rủi ro

-Xác minh & Loại bỏ Nhiễu (False Positive Filtering): Kết quả rà quét thô (Raw data) phải được thẩm định thủ công bởi chuyên gia bảo mật để loại bỏ các cảnh báo dương tính giả (False Positives), đảm bảo báo cáo cuối cùng chỉ chứa các mối đe dọa thực sự.

-Phân loại Mức độ Nghiêm trọng: Các thiết bị phải được dán nhãn phân loại rõ ràng dựa trên tình trạng an ninh:

+Nghiêm trọng (Compromised): Đã bị kiểm soát, có mã độc hoạt động, cần cách ly ngay.

+Nghi ngờ (Suspicious): Có dấu hiệu bất thường, cần theo dõi thêm.

+An toàn (Clean): Không phát hiện dấu hiệu xâm nhập tại thời điểm rà soát.

5.5. Báo cáo và khuyến nghị khắc phục

-Báo cáo hiện trạng chi tiết: Cung cấp danh sách định danh cụ thể (IP, Hostname, OS) của các thiết bị đã bị xâm nhập kèm theo bằng chứng kỹ thuật (Evidence) rõ ràng cho từng trường hợp.

-Phương án bóc gỡ và khắc phục:

+Cung cấp công cụ hoặc hướng dẫn chi tiết (Step-by-step) để đội ngũ CNTT nội bộ có thể tự bóc gỡ mã độc.

+Đối với các máy chủ bị nhiễm nặng (Rootkit/Ransomware), phải đưa ra khuyến nghị cụ thể.

-Khuyến nghị phòng ngừa: Đề xuất các biện pháp vá lỗ hổng (Hardening) để ngăn chặn kẻ tấn công quay trở lại qua con đường cũ.

6. Yêu cầu về đào tạo và diễn tập An toàn thông tin

6.1. Đào tạo kỹ năng phản ứng sự cố

Nhà thầu có trách nhiệm cung cấp khóa đào tạo chuyên sâu nhằm trang bị kiến thức và kỹ năng thực chiến cho đội ngũ vận hành, bao gồm các nội dung sau:

-Kỹ năng phát hiện và phân loại Sự cố (Detection & Analysis):

+Phân tích Log chuyên sâu: Hướng dẫn kỹ thuật đọc hiểu và phân tích log từ các nguồn quan trọng (Windows Event Logs, Linux Syslog, Web Server Logs, Firewall Logs).

+Khai thác IoC & Threat Intel: Hướng dẫn cách sử dụng các chỉ số xâm nhập (IoC - Indicators of Compromise) như Hash, IP, Domain độc hại để rà soát trên hệ thống giám sát (SIEM/EDR).

+Sử dụng công cụ giám sát: Đào tạo kỹ năng viết câu truy vấn (Query) để săn tìm mối đe dọa và phân biệt giữa sự cố thực (True Positive) và cảnh báo giả (False Positive).

-Kỹ năng điều tra và phân tích (Investigation & Forensics):

+Phân tích Endpoint: Hướng dẫn sử dụng các công cụ để kiểm tra các tiến trình lạ, key khởi động (Autoruns), và các kết nối mạng bất thường trên máy chủ/máy trạm.

+Phân tích Lưu lượng mạng: Hướng dẫn sử dụng Wireshark/TCPDump để phân tích gói tin (Pcap), phát hiện dấu hiệu máy chủ điều khiển (C2) hoặc hành vi dò quét mạng.

+Phân tích Mã độc cơ bản: Trang bị kỹ năng trích xuất mẫu mã độc và thực hiện phân tích tĩnh (Static Analysis) để xác định hành vi cơ bản mà không cần kích hoạt mã độc.

-Kỹ năng xử lý và khôi phục (Containment, Eradication & Recovery):

+Chiến lược Ngăn chặn: Hướng dẫn các phương pháp cô lập hệ thống bị nhiễm (ngắt mạng, đóng port, isolate host) mà không làm mất dữ liệu điều tra.

+Loại bỏ và Khôi phục: Quy trình bóc gỡ mã độc triệt để (xóa file, registry, service độc hại) và các bước kiểm tra an ninh trước khi đưa hệ thống vận hành trở lại.

6.2. Diễn tập kịch bản xử lý sự cố

Tổ chức diễn tập nhằm đánh giá khả năng phản ứng của quy trình và con người trước các cuộc tấn công giả lập sát với thực tế.

-Xây dựng kịch bản diễn tập:

+Nhà thầu phải khảo sát và xây dựng kịch bản tấn công

+Kịch bản phải bao gồm đầy đủ các giai đoạn của chuỗi tấn công (Kill Chain): Từ xâm nhập ban đầu, leo thang đặc quyền đến hành động phá hoại/đánh cắp dữ liệu.

-Tổ chức theo hình thức Capture the Flag (Blue Team/Purple Team CTF):

+Mô hình: Diễn tập phòng thủ chủ động. Hệ thống sẽ sinh ra các đợt tấn công giả lập theo thời gian thực.

+Nhiệm vụ: Đội ngũ tham gia diễn tập (Blue Team) phải sử dụng các công cụ đã được đào tạo để tìm ra các dấu vết của cuộc tấn công.

-Thực hiện giả lập tấn công (Attack Simulation):

+Nhà thầu đóng vai trò tấn công giả lập theo kịch bản có kiểm soát.

+Các hành vi tấn công phải để lại dấu vết log giống như tấn công thật để học viên thực hành phân tích.

-Tổ chức và hậu cần:

+Thời lượng: 01 ngày (Onsite tại trụ sở).

+Thành phần: Bao gồm phiên hướng dẫn, phiên diễn tập và phiên tổng kết rút kinh nghiệm.

+Báo cáo sau diễn tập: Nhà thầu phải cung cấp báo cáo đánh giá năng lực đội ngũ, đề xuất cải tiến.

-Cấp Giấy chứng nhận kết quả diễn tập An toàn thông tin

7. Yêu cầu về ứng cứu sự cố (Incident Response)

Nhà thầu phải cung cấp dịch vụ ung cứu sự cố trọn gói, bao trùm toàn bộ vòng đời sự cố theo chuẩn NIST SP 800-61, bao gồm các đầu việc cụ thể sau:

-Tiếp nhận và phân loại sự cố (Preparation & Triage)

+Kênh tiếp nhận đa dạng: Duy trì kênh tiếp nhận sự cố 24/7 qua Hotline, Email, Portal và các công cụ chat (OTT) chuyên dụng.

+Đánh giá mức độ nghiêm trọng (Severity Assessment):

o Ngay khi tiếp nhận thông tin, chuyên gia Ứng cứu (Tier 3) phải thực hiện đánh giá sơ bộ để xác định mức độ nghiêm trọng (Critical, High, Medium, Low) dựa trên ma trận rủi ro đã thống nhất với Bệnh viện.

o Cam kết SLA: Phải đưa ra phương án phản hồi ban đầu trong vòng 15 phút đối với sự cố mức nghiêm trọng.

7.1. Điều tra và phân tích chứng cứ số (Analysis & Digital Forensics)

Đây là giai đoạn yêu cầu năng lực kỹ thuật chuyên sâu để xác định nguyên nhân gốc rễ (Root Cause Analysis):

-Thu thập chứng cứ (Evidence Collection): Thực hiện thu thập dữ liệu phục vụ điều tra từ các nguồn: Ổ cứng (Disk image), Bộ nhớ đệm (RAM dump), Nhật ký mạng (Network PCAP) và Log hệ thống.

-Phân tích mã độc nâng cao (Advanced Malware Analysis):

+Nhà thầu phải thực hiện Dịch ngược mã độc (Reverse Engineering) để phân tích các mẫu mã độc mới, mã độc được thiết kế riêng (Targeted Malware).

+Xác định rõ: Mã độc làm gì? Nó giao tiếp với ai (C&C Server)? Nó đã lây lan như thế nào?

-Dựng lại chuỗi tấn công (Kill Chain Reconstruction): Vẽ lại toàn bộ kịch bản tấn công theo dòng thời gian (Timeline), chỉ ra chính xác điểm xâm nhập đầu tiên (Patient Zero) và các kỹ thuật hacker đã sử dụng (theo khung MITRE ATT&CK).

7.2. Ngăn chặn và kiểm soát thiệt hại (Containment)

-Ngăn chặn từ xa (Remote Containment):

+Phối hợp với công cụ SOAR và EDR để thực hiện cô lập máy nhiễm, chặn kết nối mạng, dừng tiến trình độc hại ngay lập tức.

-Ứng cứu tại chỗ (Onsite Emergency Response):

+Đối với các sự cố mức độ nghiêm trọng (ví dụ: Ransomware mã hóa dữ liệu, tấn công phá hoại diện rộng, hoặc nghi ngờ gián điệp nằm vùng): Nhà thầu bắt buộc phải cử chuyên gia cấp cao (Tier 3) có mặt tại Trung tâm dữ liệu của Bệnh viện trong vòng 02 giờ.

7.3. Loại bỏ và phục hồi (Eradication & Recovery)

-Làm sạch hệ thống (System Cleaning):

+Cung cấp công cụ và hướng dẫn chi tiết để đội ngũ IT Bệnh viện thực hiện quét và gỡ bỏ hoàn toàn mã độc, rootkit, backdoor khỏi hệ thống.

+Rà soát lại toàn bộ hệ thống để đảm bảo không còn Backdoor nào bị bỏ sót.

-Hỗ trợ khôi phục (Recovery Support):

+Tư vấn lộ trình khôi phục dịch vụ theo thứ tự ưu tiên để giảm thiểu tác động đến hoạt động khám chữa bệnh.

+Hỗ trợ kiểm tra an ninh (Security Check) lần cuối trước khi đưa hệ thống vận hành trở lại (Go-live).

7.4. Báo cáo và đóng sự cố (Post-Incident Activity)

-Báo cáo sự cố chi tiết (Incident Report):

+Nhà thầu phải cung cấp báo cáo điều tra toàn diện bằng Tiếng Việt, bao gồm: Tóm tắt cho lãnh đạo (Executive Summary), chi tiết kỹ thuật, bằng chứng số và kết luận nguyên nhân.

-Họp rút kinh nghiệm (Lessons Learned):

+Tổ chức buổi họp với các bên liên quan để trình bày kết quả điều tra.

+Đưa ra các khuyến nghị khắc phục dài hạn (Hardening Recommendations): Cần vá lỗ hổng nào? Cần thay đổi chính sách gì? Cần đào tạo nhân viên ra sao để tránh lặp lại sự cố tương tự.

-Cập nhật tri thức: Cập nhật các chỉ số tấn công (IOCs) mới phát hiện vào hệ thống giám sát và Threat Intelligence để ngăn chặn các cuộc tấn công tương tự trong tương lai.

7.5. Khả năng sẵn sàng và cam kết phản ứng (SLA)

-Nhà thầu phải cung cấp dịch vụ ứng cứu sự cố hoạt động liên tục 24/7/365, bao gồm cả ngày nghỉ, lễ, Tết. Đội ngũ chuyên gia phải luôn trong trạng thái sẵn sàng tiếp nhận yêu cầu và xử lý ngay lập tức khi sự cố xảy ra .

-Nhà thầu phải có đội ngũ chuyên gia ứng cứu sẵn sàng có mặt trực tiếp tại hiện trường (Onsite) của Bệnh viện để xử lý các sự cố mức độ Nghiêm trọng (Critical) hoặc khi có yêu cầu đặc biệt trong vòng tối đa 02 giờ kể từ khi xác nhận yêu cầu.

-Cam kết thời gian phản hồi từ xa (Remote Response) ban đầu dưới 15 phút cho các sự cố nghiêm trọng

III. YÊU CẦU VỀ BÁO CÁO VÀ CHUYỂN GIAO

1. Khả năng hiển thị hợp nhất (Unified Visibility)

-Hệ thống phải cung cấp giao diện Dashboard tập trung cho phép hiển thị đồng thời dữ liệu từ nhiều phân hệ khác nhau bao gồm: Giám sát sự kiện (SIEM), Quản lý lỗ hổng (VM), Tình báo mối đe dọa (TI) và Trạng thái phản ứng sự cố (SIRP).

-Hỗ trợ hiển thị trực quan sơ đồ chuỗi tấn công (Kill Chain) và ánh xạ các kỹ thuật tấn công theo khung MITRE ATT&CK theo thời gian thực.

2. Phân quyền và Tùy biến Dashboard (Customization)

-Hệ thống phải cung cấp thư viện Widget phong phú và công cụ thiết kế Dashboard dạng kéo-thả (Drag & Drop), cho phép tùy biến giao diện linh hoạt theo nhu cầu của từng đối tượng sử dụng tại Bệnh viện.

-Cung cấp sẵn các Dashboard chuyên biệt theo vai trò (Role-based Views):

-Dashboard Lãnh đạo (Executive View): Hiển thị các chỉ số cấp cao như Điểm rủi ro (Risk Score), Xu hướng tấn công.

-Dashboard Vận hành (Analyst View): Hiển thị chi tiết log, lưu lượng mạng, Top nguồn tấn công, Top máy chủ bị ảnh hưởng.

-Dashboard Chuyên đề: Dành riêng cho việc giám sát các ứng dụng trọng yếu của Bệnh viện và dịch vụ Microsoft O365.

3. Hệ thống báo cáo tự động và chuẩn hóa

-Hỗ trợ xuất báo cáo định kỳ (Ngày/Tuần/Tháng) và đột xuất với đa dạng định dạng: PDF (bản in), Excel/CSV (xử lý số liệu), Word (chỉnh sửa nội dung).

-Hệ thống báo cáo phải hỗ trợ tùy biến biểu mẫu (Template)

-Nội dung báo cáo phải tự động tổng hợp số liệu từ các công cụ bảo mật hiện có để cung cấp cái nhìn toàn diện về hiệu quả của toàn bộ hệ thống

4. Giám sát Hiệu năng và SLA (SLA Monitoring)

-Dashboard phải hiển thị thời gian thực các chỉ số cam kết chất lượng dịch vụ (SLA) và hiệu năng vận hành SOC (SOC KPIs), bao gồm:

-Thời gian trung bình phát hiện sự cố (MTTD).

-Thời gian trung bình phản hồi và xử lý (MTTR).

-Hệ thống tự động gửi cảnh báo qua Email/App nếu các chỉ số SLA có nguy cơ bị vi phạm.

5. Yêu cầu về thời gian triển khai

-Nhà thầu phải hoàn thành toàn bộ công việc triển khai, tích hợp và đưa hệ thống vào vận hành chính thức (Go-live) trong vòng tối đa 08 tuần (56 ngày) kể từ ngày ký hợp đồng.

-Thực hiện khảo sát trực tiếp tại hiện trường (Onsite Survey) để xác định topo mạng và danh sách tài sản.

-Nhà thầu phải hoàn thành việc xây dựng và tinh chỉnh các bộ phân tách log (Custom Parsers).

-Hoàn thành việc thiết kế và tùy biến các mẫu Báo cáo (Report Templates) và Dashboard theo đúng yêu cầu.

-Tổ chức đào tạo chuyển giao công nghệ trực tiếp (Offline/Onsite) tại trụ sở Bệnh viện trong tối thiểu 03 buổi.

-Chủ đầu tư có quyền yêu cầu chứng minh chức năng của sản phẩm tham gia thông qua Demo, POC.

PHẦN II: DỊCH VỤ KIỂM THỬ XÂM NHẬP LIÊN TỤC

1. Phạm vi cung cấp

-Đánh giá, kiểm thử xâm nhập liên tục cho hệ thống công nghệ thông tin của Chủ đầu tư gồm có:

+13 ứng dụng web và 04 ứng dụng mobile công khai

+100 repo mã nguồn ứng dụng

+3 container image

+Hạ tầng máy chủ, mạng – bảo mật

+5 ứng dụng web nội bộ

2. Yêu cầu về triển khai hệ thống

-Thành phần dò quét lỗ hổng mã nguồn, container image (Scanner) phải được đặt tại hạ tầng của Bệnh viện (on-premise)

-Scanner phải có khả năng kết nối đến các hệ thống quản lý mã nguồn và container image, đảm bảo không sao chép/ di dời mã nguồn và image khỏi hệ thống quản lý.

-Scanner phải có khả năng phát hiện và thực hiện dò quét mã nguồn, container image ngay khi có thay đổi/ cập nhật trên hệ thống quản lý

-Scanner đồng thời phải có khả năng tích hợp vào quy trình phát triển CI/CD.

3. Yêu cầu về triển khai dịch vụ

Nhà thầu phải thực hiện đầy đủ các công việc sau đây nhằm đảm bảo hệ thống ứng dụng của Bệnh viện luôn được đánh giá và kiểm thử xâm nhập liên tục.

-Theo dõi tài sản: nhà thầu thực hiện kiểm tra liên tục các ứng dụng công khai từ bên ngoài và thông báo khi có thay dổi, bao gồm tối thiểu: các cổng dịch vụ, các thành phần của ứng dụng, các endpoint truy cập, ...

-Theo dõi bề mặt tấn công:

+Kiểm tra liên tục lỗ hổng bảo mật trên các ứng dụng công khai từ bên ngoài.

+Thông báo và kiểm tra mức độ khai thác đối với các CVE mới được công bố có liên quan đến các ứng dụng công khai.

-Đánh giá ứng dụng trong quá trình phát triển:

+Thực hiện đánh giá mã nguồn ứng dụng khi có cập nhật/ thay đổi

+Thực hiện đánh giá container image của các ứng dụng khi có cập nhật/ thay đổi

-Kiểm thử xâm nhập: Thực hiện kiểm thử xâm nhập cho các ứng dụng công khai toàn diện theo tiêu chuẩn OWASP tối thiểu 01 lần

4. Yêu cầu về tần suất báo cáo và triển khai dịch vụ

-Nhà thầu đảm bảo thực hiện đầy đủ phạm vi công việc và cung cấp các báo cáo định kỳ theo tần suất như sau:

+Báo cáo về hiện trạng các ứng dụng công khai: 01 lần/tuần.

+Báo cáo về lỗ hổng bảo mật trên các ứng dụng công khai: 01 lần/tháng.

+Báo cáo về các CVE mới được công bố có liên quan đến các ứng dụng công khai: trong vòng 05 ngày làm việc kể từ ngày công bố.

+Báo cáo về hiện trạng các ứng dụng công khai: 01 lần/tháng.

+Báo cáo về lỗ hổng bảo mật trên các ứng dụng công khai: 01 lần/ quý

+Báo cáo kiểm thử xâm nhập cho hạ tầng máy chủ, mạng – bảo mật: tối thiểu 2 lần/năm

+Báo cáo đánh giá mã nguồn ứng dụng khi có cập nhật/ thay đổi: trong vòng 03 ngày làm việc kể từ ngày cập nhật/ thay đổi.

+Báo cáo đánh giá container image khi có cập nhật/ thay đổi: trong vòng 03 ngày làm việc kể từ ngày cập nhật/ thay đổi.

+Báo cáo kiểm thử xâm nhập cho các ứng dụng công khai: tối thiểu 01 lần cho từng ứng dụng.