ĐẠI HỌC Y DƯỢC TPHCM
BỆNH VIỆN ĐẠI HỌC Y DƯỢC

Số: 1599/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 08 tháng 5 năm 2024

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 bản quyền phần mềm phòng chống mã độc cho thiết bị đầu cuối 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 phần mềm phòng chống mã độc cho thiết bị đầu cuối

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

3. Thời gian thực hiện hợp đồng: 6 tháng kể từ ngày hợp đồng có hiệu lực

4. Loại hợp đồng: Hợp đồng theo đơn giá cố định

5. Địa điểm thực hiện: Bệnh viện Đại học Y Dược TPHCM

6. Hiệu lực của hồ sơ chào giá: tối thiểu 06 tháng kể từ ngày báo giá

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 bên mời thầu.

8. Thời gian nhận hồ sơ chào giá: trước 16 giờ, ngày 13/5/2024

9. Quy định về tiếp nhận thông tin và hồ sơ chào giá: Quý đơn vị thực hiện gửi hồ sơ chào giá online tại website của Bệnh viện và 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 11, Quận 5, TPHCM

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);

+ Hồ sơ pháp lý, hồ sơ năng lực của nhà thầu;

+ 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 (giấy chứng nhận đăng ký lưu hành, giấy chứng nhận lưu hành tự do (nếu có), catalogue sản phẩm và các tài liệu kỹ thuật liên quan khác).

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) (02).

TUQ. GIÁM ĐỐC
TRƯỞNG PHÒNG CÔNG NGHỆ THÔNG TIN

BỘ Y TẾ * BỆNH VIỆN ĐẠI HỌC Y DƯỢC TP. HỒ CHÍ MINH * 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 1599/BVĐHYD-CNTT ngày 08 tháng 5 năm 2024)

I. Phạm vi cung cấp

STT	Tên danh mục	ĐVT	Số lượng
1	Bản quyền phần mềm phòng chống mã độc cho máy trạm	Bản	2184
2	Bản quyền phần mềm phòng chống mã độc cho máy chủ	Bản	51
3	Bản quyền phần mềm phòng chống mã độc cho thiết bị di động	Bản	404
Tổng cộng			**2639**

II. Yêu cầu kỹ thuật

STT	Nội dung yêu cầu	Mô tả
I.	**Phần mềm phòng chống mã độc cho máy trạm**	
1.	Máy chủ quản trị tập trung (Centralized Management)	- Giao diện dashboard, report cảnh báo tập trung - Quản trị trên môi trường Cloud (SaaS based) - Giao diện duy nhất cho tất cả các cấu hình endpoint inventory, giám sát bảo mật, licensing, quản trị phân quyền - Thiết lập chính sách quản lý tập trung - Cập nhật các pattern, engine cho toàn bộ hệ thống tập trung - Trung tâm chia sẻ các thông tin về File, hash, IP, URL, domain nguy hiểm với các giải pháp khác của hãng đang triển khai tại Tổ chức và giải pháp của Bên thứ ba - Thu thập log tập trung, có thể chia sẻ cho hệ thống SIEM - Có cơ chế lưu log, activity data tập trung: đảm bảo tối thiểu 30 ngày
2.	Hỗ trợ các tính năng chính để bảo vệ máy tính	- Giải pháp kết hợp các công nghệ phát hiện mã dược tiên tiến: máy học (machine learning), giám sát hành vi (behavior monitoring để phát hiện và ngăn chặn nhanh chóng các mã độc chưa biết (unknown malware) có thể lây nhiễm vào hạ tầng endpoint của Tổ chức

STT	Nội dung yêu cầu	Mô tả
		- Tự động phát hiện và ngăn chặn các mối đe dọa mới, bao gồm fileless và ransomware. - Một Agent cung cấp đầy đủ các tính năng bảo mật cần có, các tính năng tối thiểu gồm có anti-malware realtime scan, kiểm soát ứng dụng, phòng chống xâm nhập IPS, kiểm soát thiết bị ngoại vi, DLP, ngăn chặn thất thoát các dữ liệu DLP. - Hỗ trợ bảo vệ toàn bộ thiết bị máy trạm của cán bộ nhân viên khỏi mã độc như Virus, Trojans, worms, spyware, ransomware... - Hỗ trợ "vá ảo" các lỗ hổng bảo mật đã biết và chưa biết cho Endpoint thông qua các rule IPS. Có thể bảo vệ an toàn người dùng ngay cả khi bản vá chính thức chưa phát hành hoặc triển khai. - Trực quan và quản lý tập trung: nhiều tính năng có thể được quản trị thông qua một giao diện duy nhất gồm có quản trị trực quan, licensing, kiểm soát phân quyền, inventory, policy. - Hỗ trợ nhiều công nghệ bảo vệ chống mã độc, mối đe dọa như: máy học độ tin cậy cao (high-fidelity machine learning), phân tích hành vi, ngăn ngừa các biến thể mã độc (variant protection), kiểm tra độ tin cậy của mẫu (census check), kiểm soát ứng dụng, ngăn chặn khai thác trong tài liệu (exploit prevention), độ nổi tiếng của các web (web reputation), kiểm soát kết nối tới C&C. Chặn thất thoát dữ liệu - Khả năng ngăn chặn các ransomware tinh vi mã hóa file trên các thiết bị đầu cuối, có thể chặn các hành vi mã hóa nguy hiểm, và phục hồi các file đã bị mã hóa nếu cần thiết - Cho phép nhận thông tin chia sẻ về hiểm họa (threat intelligence) từ nguồn khác thông qua: TAXII và MISP - Cho phép tùy biến dashboard phù hợp dựa trên vai trò quản trị khác nhau. - Hỗ trợ bảo vệ đa nền tảng như: Windows, Linux, MAC OS.
3.	Có đầy đủ các tính năng bảo mật nâng cao cung cấp sẵn trong phần mềm (Threat Detection Capabilities)	- Tính năng phát hiện mã độc sử dụng công nghệ máy học với độ tin cậy cao ở cả hai mức độ trước thực thi (pre-execution) và thực thi (runtime): + Pre execution machine learning (công nghệ học máy ở giai đoạn tiền thực thi)

STT	Nội dung yêu cầu	Mô tả
		+ Runtime machine learning (công nghệ học máy ở giai đoạn thực thi) - Tính năng phân tích hành vi, dùng để ngăn chặn dạng tấn công sau: + Sử dụng script khai thác + Injection + Ransomware + Memory attacks + Browser attacks - Tính năng kiểm tra độ nổi tiếng của file (File reputation), độ nổi tiếng của web (web reputation), bảo vệ phát hiện các biến thể mã độc mới... - Tính năng ngăn chặn tấn công khai thác (host firewall, exploit protection): + Host firewall + Exploit protection - Kiểm soát thiết bị ngoại vi – device control dựa trên nhiều tiêu chí: + Location awareness: theo vị trí của máy trạm + Áp dụng tới từng người dùng, nhóm người dùng, có thể kết nối với Activc Directory + Block autorun + Hỗ trợ cả mobile device, CD/DVD, Floppy disk, network drives, USB storage devices, thiết bị giao tiếp hồng ngoại, bluetooth - Chính sách cho device control hỗ trợ nhiều hành động như: + Full access + Modify + Read and execute + Read + List device content only + Block - Tính năng Update Agent: cho phép lựa chọn một số agent làm thành phần cache các thông tin cập nhật như pattern, engine. Các agent chỉ cần cập nhật từ thành phần update agent này giúp giảm lưu lượng cập nhật trực tiếp từ server
4.	Có tính năng vá ảo các lỗ hổng Bảo mật cho máy	- Hỗ trợ nhanh chóng các bản vá ảo lỗ hổng bảo mật

STT	Nội dung yêu cầu	Mô tả
	trạm (Vulnerability Protection)	cho máy trạm. - Ngăn chặn các khai thác lỗ hổng zero-day cho máy trạm trong mạng hoặc ngoài mạng của tổ chức - Cung cấp các bản vá ảo nghiêm trọng cho các hệ điều hành không còn được hỗ trợ bởi chính hãng thông qua các rule bảo vệ bởi module host based IPS - Nhận dạng botnet và targeted attack C&C
5.	Có tính năng giám sát Ứng dụng máy trạm (Application Control)	- Cho phép tổ chức nâng cao khả năng phòng thủ chống lại mã độc và các cuộc tấn công có chủ đích (Advanced persistent threat- APT) bằng cách ngăn chặn các ứng dụng không biết/không mong muốn thực thi trên máy trạm bằng sử dụng chính sách động kết hợp whitelist và blacklist - Ngăn chặn các tác động nguy hiểm từ các ứng dụng không mong muốn/không biết thông qua kiểm soát các file thực thi (đường dẫn file, mã hash...), danh mục các ứng dụng trên endpoint, certificate cho cả whitelist/allow list và blacklist/block list - Cơ sở dữ liệu đám mây về dữ liệu ứng dụng được phân tích và tương quan hỗ trợ trên 1 tỷ file record - Hỗ trợ cấu hình chính sách kiểm soát ứng dụng chi tiết tới mức người dùng - Hỗ trợ chính sách động cho phép người dùng cài đặt các ứng dụng cho phép dựa trên các tiêu chí về mức độ nổi tiếng (reputation-based) như prevalence, mức độ trưởng thành của ứng dụng (maturity of the application). - Cho phép lockdown hệ thống để khóa người dùng không cho phép thực thi các ứng dụng mới.
6.	Có khả năng hỗ trợ bảo mật dành cho máy hệ điều hành Mac (Security for MAC)	- Cung cấp các tính năng bảo mật cho máy Apple Mac, khả năng phát hiện mã độc tinh vi dùng machine learning - Cung cấp tính năng Device Control – kiểm soát các thiết bị ngoại vi kết nối tới máy tính Mac - Cung cấp khả năng kiểm soát, ngăn chặn kết nối tới các website nguy hiểm trên máy tính Mac
II.	**Phần mềm phòng chống mã độc cho máy chủ**	

STT	Nội dung yêu cầu	Mô tả
1.	**Tính năng bảo vệ**	
1.1.	Bảo mật bao gồm nhiều module trên một agent duy nhất	- Anti-Malware - Kiểm soát độ uy tín Web - Firewall - Chống xâm nhập và vá ảo - Kiểm soát tính toàn vẹn của các file hệ thống quan trọng - Kiểm soát log trên server - Kiểm soát ứng dụng được thực thi trên server
1.2.	Hỗ trợ đa nền tảng hệ điều hành	- Windows, Linux, SuSE, Redhat, CentOS, Ubuntu, Oracle linux, Amazon Linux
1.3.	Hỗ trợ tính năng Behaviour Control	- Có khả năng kiểm soát hành vi nhằm chống mã độc mới
1.4.	Hỗ trợ tính năng bảo vệ lỗ hỏng	- Vá ảo lỗ hổng bảo mật đã biết và chưa biết đối với web, ứng dụng doanh nghiệp, hệ điều hành thông qua IPS
1.5.	Tính năng Intrusion Prevention	- Hỗ trợ tính năng chống xâm nhập giúp bảo vệ khỏi những cuộc tấn công SQL injection, cross-site scripting, và các web application vulnerabilities
1.6.	Log Inspection	- Hỗ trợ nhận dạng và cảnh báo các thay đổi không được biết, hoặc các tấn công mã độc tinh vi, bao gồm các ransomware ngay khi nó xảy ra trên hệ thống.
1.7.	Host Firewall	- Hỗ trợ tính năng tường lửa có khả năng ngăn chặn các cuộc tấn công từ chối dịch vụ và phát hiện các hành vi dò quét: + Computer OS Fingerprint Probe + Network or Port Scan + TCP Null Scan + TCP SYNFIN Scan + TCP Xmas Scan
1.8.	Các tính năng Data Execution Prevention (DEP), Structured	- Sử dụng những kỹ thuật Data Execution Prevention (DEP), Structured Exception Handling Overwrite

STT	Nội dung yêu cầu	Mô tả
	Exception Handling Overwrite Protection (SEHOP), và Heap Spray	Protection (SEHOP), và heap spray prevention để phát hiện tiến trình nghi ngờ và ngắt những tiến trình đó
1.9.	Application Control	- Ngăn chặn việc thực thi/cài đặt các file thực thi, các file script khi chưa được cấp phép
1.10.	File Integrity Monitoring	- Giám sát sự thay đổi các files, thư viện, và dịch vụ ... Lúc có một sự thay đổi từ các file, thư viện, dịch vụ .. hệ thống sẽ log và cảnh báo tới nhà quản trị
1.11.	Process Memory Scanning	- Hỗ trợ Process Memory Scanning quét các process đang chạy trên RAM
1.12.	Recommendation Scanning	- Rà soát và phát hiện các lỗ hổng và phần mềm nhằm bảo vệ chủ động và hiệu quả. Nếu máy chủ đã vá lỗi (patched), giải pháp có khả năng quét và tự gỡ bỏ rule mà không cần nhà quản trị can thiệp.
1.13.	Tính năng Predictive Machine Learning	- Sử dụng mô hình Machine Learning với tính kỹ thuật cao cấp digital DNA fingerprinting, API mapping nhằm phát hiện những hiểm họa mới
1.14.	Ransomware protection	- Có khả năng chống thao tác mã hóa dữ liệu trái phép
1.15.	Hỗ trợ Windows AMSI	- Hỗ trợ quét tích hợp với Windows AMSI
1.16.	Firewall hỗ trợ đầy đủ các IP-based frame:	- ICMP - ICMPV6 - IGMP - GGP - TCP - UDP - TCP+UDP
1.17.	Hỗ trợ vá nhanh các lỗ hổng	- Hỗ trợ kiểm soát packet vào/ra hệ thống để phát hiện và ngăn chặn các hành vi khai thác lỗ hổng bảo mật. Hỗ trợ tự động cập nhật các rule mới và tự động vá ngay lập tức vào hệ thống
1.18.	Hỗ trợ tăng tốc đáp ứng	- Hỗ trợ đáp ứng nhiều yêu cầu tuân thủ bao gồm

STT	Nội dung yêu cầu	Mô tả
	các tuân thủ bảo mật	GDPR, PCI DSS, HIPAA, NIST ...
1.19.	SSL Inspection	- Hỗ trợ SSL Inspection giúp phân tích các traffic SSL
1.20.	Tạo Schedule scan	- Rà soát có thể được lập lịch và tự động áp đặt rule vá khi có thể nhằm loại bỏ rủi ro
1.21.	Phát hiện botnet, C&C	- Phát hiện và ngăn chặn các botnet, các kết nối C&C
1.22.	Hỗ trợ nền tảng ảo hóa trên cloud	- Hỗ trợ tích hợp với các nền tảng ảo hóa trên cloud: VMWare Cloud Microsoft Azure, Amazon AWS
1.23.	Hỗ trợ nhiều cơ chế triển khai agent	- Chef, Puppet, Ansible, AWS OpsWorks, ...
1.24.	Đồng bộ dữ liệu với Amazon AWS, Microsoft Azure, Google Cloud Platform	- Có thể đồng bộ danh sách các máy tính để triển khai bảo vệ từ cloud của Amazon AWS, Microsoft Azure, Google Cloud Platform
1.25.	Hỗ trợ REST Web Services API, DevOps, tự động hóa	- Hỗ trợ REST (REpresentational State Transfer) Web Services API. Hỗ trợ tự động hóa với công cụ DevOps tối thiểu các tác vụ sau: + Cấu hình chính sách và bảo vệ máy chủ + Tìm kiếm các lỗ hổng bảo mật và vá ảo các lỗ hổng bảo mật đó + Thực hiện các tác vụ định kỳ
1.26.	Phân quyền account	- Phân quyền cho các account quản trị tùy theo chức năng và phạm vi của từng vị trí
1.27.	Phân quyền theo nhóm	- Có thể phân quyền cho từng nhóm máy tính cần bảo vệ
1.28.	Quản lý event theo tag	- Có cơ chế quản lý các sự kiện liên quan đến bảo mật hệ thống thông qua các thẻ (tag) nhằm đơn giản hóa công tác phân tích
1.29.	Automatic tag event	- Có thể thực hiện gắn thẻ tự động cho các sự kiện bảo mật
1.30.	Filter theo tag	- Có cơ chế áp dụng lọc theo thẻ thông tin khi tạo báo cáo giúp thông tin được chuẩn xác hơn
1.31.	Report	- Báo cáo có thể được trích xuất dưới dạng file PDF

STT	Nội dung yêu cầu	Mô tả
		hoặc RTF, và phải bao gồm các loại report như sau: + Attack Report + Anti-malware report + Firewall Report + Integrity Monitoring Report + Instrusion Prevention report + Forensic Report
1.32.	Tính kế thừa	- Cơ chế quản lý các chính sách bảo mật dưới dạng phân cấp, có tính kế thừa
1.33.	Single console	- Tất cả các đối tượng được bảo vệ đều có thể được quản trị trên một màn hình quản trị duy nhất, bất kể đối tượng được bảo vệ đó là máy ảo, máy vật lý hay trên đám mây
1.34.	Quản trị trên đám mây (dạng SaaS)	- Doanh nghiệp không cần cài đặt thành phần quản trị trong DC. Quản trị tập trung một giao diện cùng với endpoint security
1.35.	Hỗ trợ tính năng gửi sự kiện đến Amazon SNS	- Hỗ trợ gửi event tới Amazon SNS để chuyển tiếp sự kiện
1.36.	Update theo nhóm	- Cơ chế update phân mức và có thể được bố trí theo từng nhóm cập nhật khác nhau nhằm giảm lưu lượng qua WAN và tăng tính Redundancy
1.37.	Hỗ trợ Multi-Factor Authentication	- Truy cập vào Giao diện quản trị có thể được xác thực với sự kết hợp giữa thiết bị mobile device (iOS, Android) và time-based one time password
1.38.	Hỗ trợ Single Sign-On SAML	- Hỗ trợ tính năng SSO SAML
1.39.	Hỗ trợ cơ chế tự bảo vệ agent	- Agent self protection
1.40.	Hỗ trợ kết nối thông qua proxy	- Hỗ trợ agent kết nối đến cloud quản trị thông qua proxy. Hỗ trợ proxy HTTP/SOCKS4/SOCKS5, PAC file
1.41.	Nhà cung cấp dịch vụ SaaS phải cung cấp chi tiết SLA	- Dịch vụ cung cấp 24/7, cung cấp thông tin về dự phòng của hệ thống, thông tin về lịch bảo trì hệ thống

STT	Nội dung yêu cầu	Mô tả
1.42.	Hỗ trợ tích hợp với SIEM	- Hỗ trợ chuyển tiếp logs đến hệ thống SIEM
2.	**Hỗ trợ tính năng XDR**	
2.1.	Hỗ trợ điều tra XDR	- Hỗ trợ liên kết với dịch vụ điều tra và phản hồi mở rộng (XDR) cho máy chủ và các thành phần khác gồm có: + Email security (Office365, Google Workspace) + Web security + Endpoint security + Network Sensor + IPS + Mobile security
2.2.	Hỗ trợ phản hồi nhanh chóng (Response)	- Hỗ trợ các phản hồi gồm có: + Thêm /bỏ đối tượng nguy hiểm vào/ra khỏi block list + Gửi vào sandbox phân tích + Thu thập file để điều tra + Dump process memory + Isolate endpoint + Chạy custom script (powershell hoặc shell) + Remote shell
2.3.	Cảnh báo và thông báo về incident	- Khi phát hiện cảnh báo mới, XDR có thể gửi thông báo qua email cho nhà quản trị.
2.4.	Detection Model (mô hình phát hiện - cảnh báo)	- Mô hình phát hiện phải kết hợp nhiều quy tắc và bộ lọc bằng cách sử dụng các kỹ thuật như học máy và xếp chồng dữ liệu. Mô hình phát hiện có thể sử dụng một hoặc nhiều bộ lọc để phát hiện các hành vi hoặc sự kiện đáng ngờ và giảm cảnh báo sai (false positive)
2.5.	Phân tích Root-Cause analysis và phản hồi cảnh báo nhanh chóng	- Bảng điều khiển XDR có thể giúp điều tra cảnh báo thông qua giao diện đồ hoạ phân tích root-cause chuyên sâu và đánh giá ảnh hưởng, cho phép tổ chức hiểu sự nghiêm trọng của cảnh báo và đưa ra các quyết định tương ứng với cảnh báo đó
2.6.	Forensic và Analysic	- Hỗ trợ đội điều tra thu thập bằng chứng từ các điểm cuối, tạo không gian làm việc để sắp xếp bằng chứng đã thu thập và tiến hành điều tra sự cố bảo mật.

STT	Nội dung yêu cầu	Mô tả
2.7.	Threat Intelligence	- Thu thập và hiển thị các thông tin về tấn công có chủ đích trên toàn cầu. Các thông tin tình báo này phải luôn được cập nhật về các mối đe doạ (APT) đang diễn ra, và chuyên gia của nhà cung cấp theo dõi sát sao. TỔ chức có thể tìm kiếm các thông tin về tấn công APT dựa trên các trường thông tin như: + Ứng hợp tên (Matched result) + Kiểu (Type) + Nhắm vào phân khúc nào (targeted industry) + Nhắm vào vùng địa lý nào (targeted region)
2.8.	Custom Threat Intelligence	- Hệ quản trị XDR cho phép tổ chức làm giàu thông tin tình báo (custom intelligence) bằng cách nhập thông tin thủ công (import) hoặc tự động từ bên thứ ba. Các loại thông tin được hỗ trợ gồm có + Domain + File (SHA-1, SHA-256, MD5) + File name + IP address + Sender address (email address) + URL + Command line + User account
2.9.	Định kỳ quét và tìm kiếm dấu hiệu xâm nhập	- Định kỳ quét và tìm kiếm các dấu hiệu xâm nhập (Indicator of Compromise)
2.10.	Hỗ trợ quét sandboxing	- Hỗ trợ quét file và URL (submit) sử dụng sandboxing
2.11.	Hỗ trợ tự động phản hồi với playbook	- Hỗ trợ tự động phản hồi cảnh báo với Playbook. Nhà quản trị có thể tự tạo hoặc sử dụng từ mẫu playbook sẵn có của nhà cung cấp
2.12.	Tích hợp XDR với bên thứ ba	- Hỗ trợ tích hợp XDR với ứng dụng của bên thứ ba. Tối thiểu gồm có + Microsoft Acitive Directory + Azure AD + Azure Sentinel Integration

STT	Nội dung yêu cầu	Mô tả
		+ PaloAlto Panorama + Nessux Pro/Tenable.io + OpenLDAP + Splunk XDR + Service Now (ITSM) + Checkpoint Firewall + Vmware Workspace One UEM + Syslog connector
2.13.	MITRE ATT&CK™ mapping	- Ánh xạ các phát hiện với MITRE ATT&CK framework cho phép tổ chức nhanh chóng hiểu được tình huống sự cố đang xảy ra trong mạng. Các phát hiện được liên kết với tài liệu chính thức của MITRE ATT&CK framework
2.14.	API mở rộng	- Hỗ trợ API mở rộng để tổ chức có thể chủ động tích hợp với các công cụ bảo mật bên ngoài chẳng hạn như SIEM và SOAR. - Các API hỗ trợ tối thiểu gồm: + Quản trị account + Quản trị event và alert + Quản trị các sensor được kết nối + Quản trị thông báo và webhook + Quản trị response + Quản trị threat intelligence + SAML
2.15.	Hỗ trợ datalake dạng SaaS	- Datalake dạng SaaS để tận dụng sức mạng của công nghệ đám mây
III.	**Phần mềm phòng chống mã độc cho thiết bị di động**	
1.	Máy chủ quản trị tập trung (Centralized Management)	- Giao diện dashboard, report cảnh báo tập trung - Quản trị trên môi trường Cloud (SaaS based). Chung với quản trị server và endpoint - Giao diện duy nhất cho tất cả các cấu hình, giám sát bảo mật

STT	Nội dung yêu cầu	Mô tả
		- Thiết lập chính sách quản lý tập trung - Có cơ chế lưu log, activity data tập trung: đảm bảo tối thiểu 30 ngày
2.	Có thể bảo mật cho Thiết bị di động (Mobile Security)	- Khả năng thực thi các chính sách về mobile, thiết bị, ứng dụng và bảo mật trên các nền tảng iOS và Android - Malware detection: Chủ động phát hiện các ứng dụng phần mềm độc hại, ứng dụng rò rỉ quyền riêng tư và ứng dụng có lỗ hổng bảo mật - Wifi Protection: Phát hiện các kết nối Wi-Fi có các cuộc tấn công trung gian (Man-in-the-middle attack), loại bỏ HTTPS và mã hóa kém bằng các cảnh báo trên bảng điều khiển và thiết bị - Configuration manager: Kiểm tra cài đặt thiết bị để phát hiện các vi phạm bảo mật có thể xảy ra - Web reputation: Bảo vệ thiết bị di động khỏi các mối đe dọa dựa trên web và các lỗ hổng hệ điều hành tiềm ẩn - Có thể tương quan XDR
IV.	**Yêu cầu về cài đặt triển khai**	
1.	Cài đặt, triển khai phần mềm phòng chống mã độc cho các thiết bị đầu cuối (máy chủ và máy trạm)	Cài đặt, triển khai phần mềm phòng chống mã độc cho các thiết bị đầu cuối (máy chủ và máy tính) tại cơ sở của Bệnh viện Đại học Y Dược TP. Hồ Chí Minh gồm: • Cơ sở 1: 215 Hồng Bàng, Phường 11, Quận 5, TPHCM. • Cơ sở 2: 201 Nguyễn Chí Thanh, Phường 12, Quận 5, TPHCM. • Cơ sở 3: 221B Hoàng Văn Thụ, P.8, Quận Phú Nhuận, TP.HCM.
		Phần mềm Endpoint security cài đặt phải có bản quyền hợp pháp của hãng sản xuất
2.	Cài đặt, triển khai công cụ quản trị tập trung để quản lý các thiết bị đầu cuối	Cài đặt, triển khai công cụ quản trị tập trung để quản lý các thiết bị đầu cuối cho máy chủ tại cơ sở của Bệnh viện Đại học Y Dược TP. Hồ Chí Minh gồm: • Cơ sở 1: 215 Hồng Bàng, Phường 11, Quận 5, TPHCM.

STT	Nội dung yêu cầu	Mô tả
		• Cơ sở 2: 201 Nguyễn Chí Thanh, Phường 12, Quận 5, TPHCM. • Cơ sở 3: 221B Hoàng Văn Thụ, P.8, Quận Phú Nhuận,TP.HCM.
3.	Đào tạo và hướng dẫn cho nhân sự quản trị hệ thống	Đào tạo, hướng dẫn cho nhân sự phòng Công nghệ thông tin cho 3 cơ sở
4.	Thời gian bản quyền phần mềm	Thời gian sử dụng bản quyền phần mềm mua mới: ≥ 36 tháng

CÔNG TY: .....

ĐỊA CHỈ: .....

SỐ ĐIỆN THOẠI: .....

BẢNG BÁO GIÁ

Kính gửi: Bệnh viện Đại học Y Dược TPHCM

Địa chỉ: 215 Hồng Bàng, Phường 11, Quận 5, TPHCM

Theo công văn mời chào giá số 1599.../BVĐHYD-CNTT của Bệnh viện, Công ty chúng tôi báo giá như sau:

TT	Tên hàng hóa	Tên thương mại	Mã HS	Đặc tính kỹ thuật	Nhà sản xuất	Nước sản xuất	ĐVT	Số lượng	Đơn giá	Thành tiền	Ghi chú
1.	Bản quyền phần mềm phòng chống mã độc cho máy trạm										
2.	Bản quyền phần mềm phòng chống mã độc cho máy chủ										
3.	Bản quyền phần mềm phòng chống mã độc cho thiết bị di động										

❖ Yêu cầu báo giá:

- Báo giá này có hiệu lực tối thiểu 6 tháng kể từ ngày báo giá.
- *Chúng tôi cam kết về đơn giá chào hàng bằng hoặc thấp hơn giá trên thị trường của cùng nhà cung ứng hoặc cùng chủng loại.*
- Các yêu cầu khác: .....

Ngày ... tháng .... năm ....

ĐẠI DIỆN THEO PHÁP LUẬT

(Ký tên và đóng dấu)