ĐẠI HỌC Y DƯỢC TPHCM
BỆNH VIỆN ĐẠI HỌC Y DƯỢC

Số: .6301...../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 04 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 giải pháp giám sát và tình báo các mối đe dọa trên không gian mạng (Threat Intelligence) 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 giải pháp giám sát và tình báo các mối đe dọa trên không gian mạng (Threat Intelligence)

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

3. Thời gian cung cấp hàng hóa: 30 ngày 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 16. giờ, ngày 14./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 ..6301../BVĐHYD-CNTT ngày ..04.. tháng 12 năm 2025)

I. Phạm vi cung cấp

STT	Danh mục	ĐVT	Số lượng
1	Giải pháp giám sát và tình báo các mối đe dọa trên không gian mạng (Threat Intelligence)	Gói	01

II. Yêu cầu kỹ thuật

STT	Nội dung yêu cầu	Mô tả
I.	**Yêu cầu kỹ thuật**	
1.	Tính năng giám sát an toàn thông tin mạng: mạng lưới thông tin về các mối đe dọa trên không gian mạng	- Cung cấp tối thiểu 10 tài khoản truy cập - Tất cả các tính năng đều được quản lý tập trung trong một giao diện, bao gồm tối thiểu: + Theo dõi thông tin tình báo liên quan đến các mối đe dọa trên môi trường mạng (threat intelligent) + Theo dõi thông tin tình báo về tội phạm mạng và các thông tin lộ lọt dữ liệu trên hệ thống web đen (darkweb/deepweb) + Theo dõi và quản lý bề mặt tấn công của tổ chức (Attack Surface Management) + Theo dõi và quản lý thông tin tình báo liên quan đến thương hiệu của tổ chức (Brand Management) + Giám sát lãnh đạo bằng hình ảnh và thông tin trên mạng xã hội. (Executive Monitoring) + Theo dõi và quản lý thông tin các lỗ hổng bảo mật (Vulnerability Intelligence)
2.	Tính năng Theo dõi thông tin tình báo liên quan đến các mối đe dọa trên môi trường mạng (threat intelligent)	Hãng cung cấp dịch vụ phải có mạng lưới Cảm biến Toàn cầu (Global Sensor) và mạng Honeypots để thu thập các mối đe dọa toàn cầu mới, kết hợp với các nguồn tình báo mối đe dọa cao cấp.
		Cung cấp dữ liệu về các lĩnh vực, quốc gia mà nhóm tội phạm nhắm tới, Bao gồm nhưng không giới hạn ở địa chỉ IP độc hại, tên miền, URL, tên tệp, hash tệp, địa chỉ email, máy chủ C&C (Command and Control) đã biết, và các nguồn dữ liệu vị trí địa lý như tọa độ, số AS, quốc gia,….
		Cung cấp tính năng tra cứu nguồn dữ liệu OSINT và các dấu hiệu tấn công (IOC Lookup), trong đó khách hàng có thể nhận được điểm rủi ro của IOC (IOC Risk Score), điểm tin cậy (Confidence Score), thông tin nguồn (Source details), hồ

STT	Nội dung yêu cầu	Mô tả
		sơ tác nhân đe dọa (TA profile) và các chỉ báo tấn công (IOA - Indicators of Attack).
		Giải pháp cung cấp các thông tin cảnh báo nguy cơ an ninh mạng bao gồm các chiến dịch ransomware và TTPs, các tổ chức tội phạm (threat actors) và TTPs của chúng, các nhóm tấn công APT, các sự cố rò rỉ dữ liệu, phân tích các lỗ hổng và chiến dịch phát tán mã độc...
		Giải pháp cung cấp khả năng cảnh báo nhanh nhất về những vi phạm/ những cuộc tấn công theo ngành nghề và theo khu vực/ quốc gia qua chức năng New Flash trên giao diện.
		Cung cấp thông tin tình báo về các mối đe dọa liên quan đến OT/ICS và hiển thị trên dashboard.
		Cung cấp khả năng theo dõi và giám sát các nhóm hoạt động hactivitsts, các chiến dịch tấn công được tài trợ.
		Nền tảng phải có phần thư viện phần mềm độc hại và mối đe dọa, cung cấp thông tin chi tiết về các nhóm tấn công APT toàn cầu, Các nhóm tấn công ransomware, tác nhân đe dọa và công cụ chúng sử dụng, bí danh, IOC, quốc gia xuất xứ, MITRE ATT&CK, đối tượng ngành mục tiêu và khu vực mục tiêu để giám sát và theo dõi hiệu quả.
		Cung cấp khả năng tích hợp API dựa trên STIX 2.0 và tích hợp với các công cụ bảo mật để cung cấp thông tin tình báo về mối đe dọa và cảnh báo
		Giải pháp cung cấp thông tin theo thời gian thực về Các cuộc tấn công DDoS xảy ra trên thế giới, hoặc theo từng Quốc gia, thông tin C2 (Command & Control): - Cung cấp giao diện giám sát cụ thể cho tổ chức qua việc cấu hình thông tin địa chỉ IP address/ dải IP cụ thể - Đưa ra cảnh báo (Alert) về DDoS và Botnet và một số thông tin về tình trạng, quãng thời gian, loại hình tấn công... - Cung cấp bản đồ tấn công, nguồn – đích, thời gian cập nhật, và lịch sử trong khoảng thời gian, - Cung cấp chi tiết về các dòng Malware liên quan đến cuộc tấn công, thông tin C2, Bot Ips, Target Ips - Cho phép tìm kiếm theo IP address hoặc theo quốc gia.
3.	Tính năng theo dõi thông tin tình báo về tội phạm mạng và các thông tin lộ lọt trên hệ thống web	Cung cấp dữ liệu từ Dark Web về các bài viết thảo luận có đề cập đến doanh nghiệp hoặc các thông tin lộ lọt tài khoản, dữ liệu liên quan.
		Cung cấp cảnh báo sớm về các máy trạm (endpoint) bị xâm phạm, cookies và session của ứng dụng nội bộ khách hàng bị rao bán trên chợ Dark Web.

STT	Nội dung yêu cầu	Mô tả
	đen (darkweb/deepweb)	Nền tảng phải tích hợp các dịch vụ giám sát đa tầng và kỹ thuật phân tích, đồng thời tương quan dữ liệu từ nhiều nguồn, bao gồm: - Các trang .onion, I2P và mạng ẩn danh khác - Blog, diễn đàn, phòng chat trên Dark Net - Chợ mua bán Infostealer, Logs và Cookies - Hội thoại trên IRC - Các trang Chợ đen và đấu giá tội phạm - Diễn đàn ransomware - Telegram - Discord - Paste sites
		Giải pháp có khả năng cung cấp thông tin liên quan đến hệ thống truy cập bị xâm phạm đang được rao bán trên chợ Dark Web, bao gồm: - Chi tiết ứng dụng - Tên người dùng (Username) - Địa chỉ IP - Loại hệ điều hành (OS Type) - Tệp tin tự động điền (Autofill files)
		Có khả năng phân biệt rõ ràng giữa tài sản nội bộ hoặc nhân viên nội bộ với các bên liên quan khác như khách hàng và đối tác trong trường hợp thông tin xác thực bị lộ.
		Phát hiện và thông báo việc lộ lọt các mã code/ API token trong kho lưu trữ mã code (GitHub, Bitbucket, v.v.), các trang paste site
		Cung cấp dữ liệu về các tài khoản của doanh nghiệp bị xâm phạm, rò rỉ ... Dữ liệu bao gồm tên miền/địa chỉ đăng nhập, tên tài khoản, mật khẩu (nếu có), ngày phát hiện
		Có khả năng tạo, giám sát, tự động cảnh báo và báo cáo về các mối đe dọa trên dark web, bao gồm nhưng không giới hạn: - Thông tin đăng nhập của nhân viên bị xâm phạm - Thông tin nhạy cảm bị rò rỉ (Tên người dùng, Mật khẩu, Secret Token, Access Keys) - Thông tin định danh cá nhân (PII) bị xâm phạm như (Email, Số điện thoại, Địa chỉ) - Thông tin về hệ thống bị xâm phạm (Device ID, Hostname, IP) để hỗ trợ điều tra pháp y - Mã độc và hạ tầng độc hại liên quan đến tên miền khách hàng

STT	Nội dung yêu cầu	Mô tả
		- Tài liệu riêng tư/ nhạy cảm của doanh nghiệp - Tài liệu/công cụ tấn công nhắm mục tiêu vào khách hàng - Mã nguồn bị rò rỉ - Tài sản trí tuệ bị rò rỉ - Xâm phạm bản quyền/thương hiệu - Các thông tin kỹ thuật hay dữ liệu có thể bị lợi dụng để tấn công hệ thống doanh nghiệp - Các thông tin đề cập đến địa chỉ IP và hạ tầng của khách hàng - Sử dụng thông tin định danh ngân hàng (BIN) và số nhận dạng PII để xác định tài khoản và thông tin xác thực liên quan đến khách hàng - Thông tin về tài khoản và thông tin đăng nhập của khách hàng bị đánh cắp - Lộ dữ liệu từ các vụ vi phạm bảo mật của bên thứ ba - Thông tin tình báo cung cấp phải có tham chiếu đến nguồn gốc, bao gồm Dark Web, Deep Web và Paste sites, dưới dạng liên kết trực tiếp đến nguồn hoặc bản sao lưu (cached copy), giúp khách hàng có thể xác thực thông tin mà không cần trực tiếp truy cập Dark Web để tìm bằng chứng.
4.	Tính năng theo dõi và quản lý bề mặt tấn công của tổ chức (Attack Surface Management)	Số lượng tài nguyên được quản lý giám sát (liên quan đến domain, sub-domain, IP Address, SSL) của doanh nghiệp: không giới hạn.
		Liên tục theo dõi, giám sát và đánh giá chủ động các lỗ hổng, các điểm xâm nhập tiềm ẩn mà tội phạm mạng có thể lợi dụng để xâm nhập trái phép vào tổ chức.
		Cung cấp khả năng phát hiện và giám sát toàn bộ các thông tin của tổ chức, không giới hạn về: - Cloud Buckets (Kho lưu trữ đám mây) - Domains (Tên miền) - IPs (Địa chỉ IP) Ipv4, Ipv6 - IP Ranges (Dải IP) - Subdomains (Tên miền phụ) - DNS Records (Bản ghi DNS: A, AAAA, CNAME, SOA, MX, NS, TXT, v.v.) - Digital Certificates (Chứng chỉ số) - Trackers (Trình theo dõi) - Keywords (Từ khóa) - Technologies (Công nghệ sử dụng) - Emails (Địa chỉ email) - Executives (Cxx / VPs) (Thông tin lãnh đạo cấp cao)
		Cung cấp khả năng tự động xác định và lập bản đồ các tài sản số của tổ chức, bao gồm tên miền, tên miền phụ, địa chỉ

STT	Nội dung yêu cầu	Mô tả
		IP, chứng chỉ số SSL, v.v. giúp người dùng có cái nhìn toàn diện về bề mặt tấn công, kể cả những tài sản bị lãng quên hoặc không được giám sát thường xuyên, từ đó tăng cường khả năng bảo vệ hệ thống.
		Hãng cung cấp phải có hệ thống quét Internet và quy trình xử lý dữ liệu riêng để giám sát bề mặt tấn công của khách hàng, không được phụ thuộc vào bên thứ ba để cung cấp dịch vụ này.
		Cung cấp thông tin về tài sản công khai của khách hàng, bao gồm: - Ảnh chụp màn hình (Screenshot) - Chi tiết ứng dụng web (Web Applications details) - Thông tin WAF and CDN - Biểu tượng của website (Favicon) - Phát hiện và đánh giá các rủi ro bảo mật như: - Lỗ hổng và cổng quan trọng đang mở - Máy chủ ảo không dùng (Shadow IT Asset) - Lỗ hổng bảo mật Local File Inclusion (LFI) - Lỗ hổng bảo mật khai thác đường dẫn Path Traversal - Thông tin đăng nhập mặc định - Cấu hình sai trên ứng dụng web - Thiết kế kém an toàn (Insecure Design) - Xác thực bị phá vỡ (Broken Authentication) và hơn 7.000 đánh giá bảo mật khác
		Có khả năng giám sát các mã nguồn bị lộ lọt trên các nền tảng: - Github - BitBucket - Postman - Docker Hub
		Hỗ trợ quét bảo mật ứng dụng web để phát hiện các lỗ hổng thuộc OWASP Top 10 và cung cấp khả năng giám sát, phát hiện Botnet.
5.	Tính năng giám sát, bảo vệ thương hiệu (Brand Monitoring)	Giải pháp cung cấp màn hình dashboard hiển thị các thông tin liên quan đến tên miền độc hại, ảnh hưởng đến thương hiệu của tổ chức, các thông tin cung cấp bao gồm: thông tin bản ghi DNS, bản ghi WHOIS, ảnh chụp màn hình, đối chiếu logo và nội dung trang web.
		Giải pháp cho phép theo dõi thông tin trao đổi liên quan đến thương hiệu tổ chức trên các nền tảng xã hội, bao gồm nhưng không giới hạn:

STT	Nội dung yêu cầu	Mô tả
		Facebook, Instagram, Linkedin, Reddit, RSS, Tiktok, Twitter, Youtube, Pinterest, Telegram, RSS, Blogspot, Vk.com, Ok.ru, Dailymotion, Discord, Quora, Flickr, Threads
		Giải pháp cần giám sát và thực hiện gỡ bỏ (Takedown) các nội dung sau: - Các trang web và chiến dịch lừa đảo (Phishing sites và Campaigns) - Tên miền gần giống (typo-squatted Domains) - Ứng dụng giả mạo trên App Store, Play Store và các kho ứng dụng bên thứ ba - Thông tin liên hệ dịch vụ khách hàng giả mạo - Tài khoản mạng xã hội giả mạo - Tên miền/URL và trang web giả mạo - Chiến dịch tuyển dụng giả và lừa đảo việc làm - Video hoặc hình ảnh giả mạo sử dụng logo của khách hàng
		Giải pháp hỗ trợ ≥ 100 lần takedown trong 1 năm
		- Giải pháp phải cung cấp tính năng theo dõi danh sách tên miền (Domain Watchlisting), để gửi cảnh báo tức thì mỗi khi có sự thay đổi về trạng thái của tên miền. - Cho phép tìm kiếm và giám sát theo IP, keyword, hình ảnh.
6.	Tính năng Giám sát thông tin liên quan đến lãnh đạo cấp cao của tổ chức (Executive Monitoring)	Nền tảng cần có khả năng giám sát và báo cáo các nội dung sau: - Tài khoản mạng xã hội giả mạo của các lãnh đạo cấp cao (CXOs), bao gồm: bài đăng, trang, nhóm liên quan — đồng thời cho phép thực hiện gỡ bỏ (takedown) khi phát hiện. - Thông tin đăng nhập (credentials) bị lộ của các lãnh đạo cấp cao. - Các đề cập, thảo luận liên quan đến lãnh đạo trên Dark Web.
		Cần cung cấp khả năng phân tích deepfake để giám sát và bảo vệ các lãnh đạo cấp cao trong tổ chức.
		Giải pháp cung cấp màn hình dashboard riêng cho việc giám sát thông tin tình báo liên quan đến lãnh đạo cấp cao
		Giải pháp cần có khả năng phát hiện việc lộ lọt dữ liệu nhạy cảm của các lãnh đạo cấp cao trên các diễn đàn công khai hoặc thông tin lộ lọt trên deep/dark web, các thông tin liên quan đến PII (Thông tin định danh cá nhân) của các lãnh đạo VIP quan trọng, bao gồm:

STT	Nội dung yêu cầu	Mô tả
		Thông tin cá nhân, số định danh (CMND/CCCD, hộ chiếu, mã số thuế...)
		Giải pháp cần xác định và thông báo về việc lộ lọt thông tin nhạy cảm của các lãnh đạo cấp cao, chẳng hạn như thông tin đăng nhập bị xâm phạm của tài khoản doanh nghiệp cũng như tài khoản cá nhân.
		Giải pháp cần cung cấp phân tích hình ảnh bao gồm phân tích thay thế khuôn mặt và thay thế cử động môi để giám sát deepfake.
		Giám sát cho tối đa 02 lãnh đạo cao cấp.
		Hỗ trợ không giới hạn số lần takedown
7.	Tính năng Theo dõi và quản lý các lỗ hổng bảo mật của tổ chức (Vulnerability Intelligence)	Giải pháp cần cung cấp thông tin tình báo về lỗ hổng bảo mật (Vulnerability Intelligence) bao gồm: a) Thông tin nguồn của lỗ hổng, các tài liệu tham khảo chi tiết, liên kết đến mã khai thác thử nghiệm (Proof of Concept – PoC) và giải pháp khắc phục. b) Tình báo về lỗ hổng trong các sản phẩm phần mềm của bên thứ ba (3rd party software). c) Ưu tiên lỗ hổng dựa trên mức độ nghiêm trọng, khả năng khai thác và mức độ ảnh hưởng thực tế.
		Bảng điều khiển hiển thị các lỗ hổng và rủi ro được phát hiện trong một giao diện thân thiện, đi kèm với thông tin chi tiết và khuyến nghị xử lý. Cho phép người dùng truy cập báo cáo chi tiết, mô tả của lỗ hổng và hướng dẫn khắc phục, giúp xử lý các vấn đề bảo mật một cách hiệu quả.
		Giám sát toàn bộ các hạ tầng được public ra của khách hàng và cung cấp các báo cáo bằng cách cho phép khách hàng: - Nhập thông tin hãng, thiết bị, phần mềm, OS, phiên bản để giám sát lỗ hổng - Có giao diện Dashboard riêng để truy xuất thông tin - Có khả năng tạo cảnh báo (Alert) về lỗ hổng liên quan đến khách hàng
		Khả năng tích hợp liên kết thông tin, báo cáo về lỗ hổng từ nguồn darkweb về lỗ hổng qua New Flash hoặc Advisories
8.	Tính năng Báo cáo, cảnh báo	Cung cấp giao diện portal cho người dùng với các chức năng: Executive Dashboard, phân tích, tìm kiếm, ...
		Cảnh báo khi có các thông tin liên quan trực tiếp đến doanh nghiệp: thất thoát dữ liệu, mã độc có chủ đích, tấn công mạng, ...

STT	Nội dung yêu cầu	Mô tả
		Cho phép tùy chọn tạo báo cáo theo một thời gian cụ thể từ bảng điều khiển để cung cấp tổng quan về các phát hiện quan trọng và khuyến nghị liên quan trong một khoảng thời gian
		Có khả năng tích hợp để gửi thông báo đến các kênh: Whatsapp, SMS, Slack, Email
9.	Các tính năng khác	Giải pháp không giới hạn số lượng keywords liên quan đến doanh nghiệp, không giới hạn số lượng tài sản như số lượng Domain, số lượng IP Address…liên quan đến doanh nghiệp
		Giải pháp phải có chứng nhận ISO 27001:2022
		Giải pháp phải đạt cấp độ SOC2 Type2 từ năm 2024 tới hiện tại
		Giải pháp phải có tích hợp AI trong việc: - Tổng hợp dựa trên AI - Hỗ trợ chuyển ngôn ngữ tự động bằng AI - Hỗ trợ quản lý, cảnh báo, gắn thẻ (tag) bằng AI
		Giải pháp phải có chứng nhận còn hiệu lực về tiêu chuẩn SOC2 Compliance
		Khả năng tích hợp và chia sẻ dữ liệu cho bên thứ ba như các giải pháp SIEM/ SOAR, EDR qua giao thức STIX, TAXII, hoặc qua API
		Các dữ liệu Intelligence cung cấp trên hệ thống được phân loại theo chuẩn quốc tế về giới hạn chia sẻ các thông tin nhạy cảm (Traffic Light Protocol - TLP)
		Hỗ trợ xác thực 2 lớp cho các tài khoản truy cập
		Hỗ trợ phân quyền tài khoản Role Base Access Control
		Hãng cung cấp giải pháp phải cung cấp tài liệu cam kết mức độ dịch vụ (SLA) cho dịch vụ takedown
		Hãng cung cấp giải pháp phải là thành viên của nhóm International Anti-Phishing Working Group (APWG).
10.	Thời gian bản quyền, bảo hành và hỗ trợ kỹ thuật từ nhà sản xuất	≥ 3 năm kể từ ngày bàn giao tài khoản
II	**Yêu cầu khác**	

STT	Nội dung yêu cầu	Mô tả
1.	Triển khai cài đặt, cấu hình thiết bị	- Triển khai tích hợp vào hệ thống mạng Bệnh viện - Tích hợp với các hệ thống SIEM, firewall của Bệnh viện
2.	Đào tạo hướng dẫn	- Đào tạo sau triển khai - Đào tạo vận hành hệ thống cho quản trị viên - Nhà thầu lập kế hoạch đào tạo cho các cán bộ quản trị, vận hành hệ thống do chủ đầu tư cung cấp danh sách. - Nhà thầu có trách nhiệm xây dựng tài liệu các quy trình cài đặt, triển khai hệ thống, quy trình quản trị vận hành hệ thống. - Nhà thầu sẽ cung cấp nội dung và tài liệu hướng dẫn cài đặt/ sử dụng cho các đối tượng tham gia đào tạo. - Nội dung đào tạo: Nhà thầu soạn thảo tài liệu đào tạo và trình cho Chủ đầu tư xem xét trước khi tổ chức đào tạo. Đào tạo tất cả các tính năng theo yêu cầu tại mục I. Yêu cầu kỹ thuật