Phần 2. YÊU CẦU VỀ KỸ THUẬT
Chương V. YÊU CẦU VỀ KỸ THUẬT

Mục 1. Giới thiệu chung về dự toán, gói thầu

- Tên gói thầu: Mua sắm bản quyền phần mềm tăng cường an toàn thông tin, an ninh mạng TTXVN.

- Dự toán: Kiểm tra, đánh giá rủi ro và ứng phó mở rộng nhằm tăng cường an toàn thông tin, an ninh mạng và bảo vệ bí mật nhà nước tại TTXVN

- Chủ đầu tư: Trung tâm Kỹ thuật Thông tấn

- Loại hợp đồng: Trọn gói.

- Thời gian thực hiện hợp đồng: 15 ngày kể từ ngày hợp đồng có hiệu lực.

- Địa điểm thực hiện gói thầu: Trung tâm Kỹ thuật Thông tấn.

- Nguồn vốn: Ngân sách Nhà nước

Mục 2. Yêu cầu về kỹ thuật:

I. Chỉ dẫn nhà thầu:

- Hàng hóa phải tương thích với hạ tầng hiện có của đơn vị sử dụng. Trong trường hợp Nhà thầu cần khảo sát hiện trường để có cơ sở chuẩn bị Hồ sơ dự thầu, Nhà thầu cần đề xuất đến Chủ đầu tư bằng văn bản trước thời điểm đóng thầu tối thiểu 03 ngày. Toàn bộ chi phí đi khảo sát hiện trường do nhà thầu tự chi trả.

Chủ đầu tư sẽ cho phép nhà thầu và các bên liên quan của nhà thầu tiếp cận hiện trường để phục vụ mục đích khảo sát hiện trường với điều kiện nhà thầu và các bên liên quan của nhà thầu cam kết rằng Chủ đầu tư và các bên liên quan của Chủ đầu tư không phải chịu bất kỳ trách nhiệm nào đối với nhà thầu và các bên liên quan của nhà thầu liên quan đến việc khảo sát hiện trường này. Nhà thầu và các bên liên quan của nhà thầu sẽ tự chịu trách nhiệm cho những rủi ro của mình như tai nạn, mất mát hoặc thiệt hại tài sản và bất kỳ các mất mát, thiệt hại và chi phí nào khác phát sinh từ việc khảo sát hiện trường.

- Quá trình triển khai thực hiện gói thầu, nếu có các hạng mục công việc phát sinh dẫn đến phát sinh thêm công việc, Nhà thầu báo cáo lại với Chủ đầu tư và các đơn vị liên quan cùng đề xuất phương án triển khai phù hợp nhằm đảm bảo chất lượng, tiến độ của gói thầu. Trong trường hợp cần thiết, Chủ đầu tư và Nhà thầu tiến hành thỏa thuận và báo cáo cấp có thẩm quyền Quyết định phương án triển khai.

- Nhà thầu có thể chào thầu hàng hóa có thông số đúng hoặc tương đương hoặc mới hơn yêu cầu (tương đương được hiểu theo đáp ứng toàn bộ các thông số được nêu ra trong một hàng hóa của E-HSMT, công nghệ mới hơn được hiểu là công nghệ ra sau và có những thông số tốt hơn so với các thông số được yêu cầu của một hạng mục hàng hóa trong E-HSMT).

- Trong mọi trường hợp, nếu E-HSDT của nhà thầu cung cấp thông tin, tài liệu làm giả hoặc làm sai lệch thông tin, không trung thực thì E-HSDT của nhà thầu bị loại và Nhà thầu sẽ bị coi là gian lận theo quy định tại khoản 4 Điều 16 của Luật Đấu thầu và bị xử lý theo quy định tại Điều 133 của Nghị định số 214/2025/NĐ-CP.

Nếu Nhà thầu cố tình sử dụng hàng hóa của nước ngoài và kê khai, gắn nhãn, mác xuất xứ Việt Nam trái quy định của pháp luật để tham dự thầu, ngoài việc bị xử lý theo các quy định trên còn bị xem xét chuyển vụ việc sang cơ quan chức năng để xử lý theo quy định của pháp luật về sản xuất, cung cấp, buôn bán hàng giả, hàng nhái.

- Khi lập danh sách trang thiết bị, hàng hóa trong Hồ sơ dự thầu, đề nghị các nhà thầu lập theo thứ tự danh mục thiết bị, hàng hóa trong Hồ sơ mời thầu.

- Tên hãng sản xuất, xuất xứ, model, ký mã hiệu của hàng hóa (nếu có) nêu trong E-HSMT chỉ mang tính chất tham khảo.

- Các nội dung do nhà thầu đề xuất chào thầu phải thể hiện rõ ràng, đầy đủ thông tin theo yêu cầu của E-HSMT. Trường hợp nhà thầu đề xuất các nội dung mang tính chung chung, không cụ thể (ví dụ: Nhà thầu cam kết đáp ứng tất cả các yêu cầu của E-HSMT, .v.v…) thì Chủ đầu tư, Tổ chuyên gia sẽ không xem xét, đánh giá là tương đương so với yêu cầu của E-HSMT.

II. Yêu cầu chung: Nhà thầu phải đề xuất hoặc cam kết trong E-HSDT các nội dung đáp ứng yêu cầu sau:

- Đối với nội dung công việc cung cấp phần mềm:

+ Cam kết phần mềm có nguồn gốc rõ ràng, hợp pháp, không vi phạm bản quyền hoặc đang có tranh chấp về bản quyền/quyền sở hữu.

+ Nhà thầu có Bảng chào kỹ thuật của hàng hóa chào thầu với đầy đủ các nội dung: Tên hàng hóa, model (hoặc ký mã hiệu nếu có), hãng sản xuất, xuất xứ (không bắt buộc đối với phần mềm, phụ kiện đi kèm), đặc tính kỹ thuật.

+ Đặc tính, thông số kỹ thuật của hàng hóa được chào thầu phải đáp ứng các yêu cầu của E-HSMT, có đầy đủ các tài liệu chứng minh theo yêu cầu tại E-CDNT 10.8 Chương II, quy định tại Chương V (nếu có) và các yêu cầu khác của E-HSMT này.

(Ghi chú:

(i) Trường hợp có sự sai khác giữa bảng chào kỹ thuật hàng hóa dự thầu so với Catalogue hoặc tài liệu kỹ thuật của hàng hóa nộp trong E-HSDT thì bảng chào kỹ thuật của nhà thầu sẽ làm cơ sở để đánh giá E-HSDT. Nhà thầu phải cung cấp đầy đủ các tài liệu do nhà sản xuất công bố để chứng minh tính đáp ứng các thông số kỹ thuật chào thầu:

+ Trường hợp Catalogue hoặc tài liệu kỹ thuật của hàng hóa do nhà thầu nộp trong E-HSDT không có xác nhận của nhà sản xuất (hoặc cơ quan/đơn vị có

thẩm quyền): Nếu thông tin trong các tài liệu này không phù hợp với thông tin được công bố trên trang thông tin điện tử (website) của nhà sản xuất thì Chủ đầu tư có quyền thực hiện các biện pháp xác thực thông tin theo quy định tại Mục 23.6 Chương I của E-HSMT này và có quyền yêu cầu nhà thầu cung cấp tài liệu chứng minh hoặc cung cấp hàng hóa thực tế để kiểm tra, đối chiếu.

+ Trường hợp Catalogue hoặc tài liệu kỹ thuật của hàng hóa do nhà thầu nộp trong E-HSDT đã được nhà sản xuất (hoặc cơ quan/đơn vị có thẩm quyền) xác nhận: Nếu thông tin trong các tài liệu này không phù hợp với thông tin được công bố trên trang thông tin điện tử của nhà sản xuất thì Chủ đầu tư sẽ căn cứ theo tài liệu đã nộp trong E-HSDT để đánh giá.

(ii) Nhà thầu tham dự thầu có trách nhiệm kiểm tra, đối chiếu và hoàn toàn chịu trách nhiệm về tính chính xác thông tin tài liệu kèm theo E-HSDT khi nộp E-HSDT so với tài liệu trên website chính thức của nhà sản xuất).

- Đối với nội dung công việc cho thuê thiết bị CNTT:

+ Nhà thầu có Bảng chào kỹ thuật của thiết bị, phần mềm cho thuê với đầy đủ các nội dung: Tên thiết bị/phần mềm; model hoặc ký mã hiệu (nếu có), hãng sản xuất; xuất xứ (nếu có); đặc tính kỹ thuật, tiêu chuẩn áp dụng (nếu có).

+ Đặc tính, thông số kỹ thuật, các chức năng của phần mềm cho thuê phải đáp ứng các yêu cầu của E-HSMT. Trong trường hợp cần thiết, Chủ đầu tư có thể yêu cầu Nhà thầu cung cấp tài liệu chứng minh quyền sở hữu thiết bị của Nhà thầu và tài liệu kỹ thuật hoặc catalogue của thiết bị, phần mềm do Nhà sản xuất công bố để chứng minh, nếu Nhà thầu không cung cấp tài liệu hoặc tài liệu không đáp ứng yêu cầu thì E-HSDT của Nhà thầu sẽ được đánh giá là không đáp ứng yêu cầu của E-HSMT.

- Các thành phần hoặc các phụ kiện đi kèm của hàng hóa phải đảm bảo tương thích với hàng hóa chính.

- Nhà thầu phải cam kết và chịu hoàn toàn trách nhiệm về việc hàng hóa đảm bảo không cài cắm firmware, mã độc hoặc các hình thức thu thập dữ liệu trái phép khác.

- Thời gian bảo hành: tối thiểu 12 tháng cho toàn bộ hàng hóa của gói thầu (trừ các hàng hóa có yêu cầu về thời gian bảo hành riêng được quy định tại Chương V của E-HSMT này).

- Phương thức bảo hành:

+ Toàn bộ hàng hóa được bảo hành theo tiêu chuẩn của nhà sản xuất. Nhà thầu phải nộp khoản bảo lãnh bảo hành theo quy định là 5% giá trị hợp đồng.

+ Khi có yêu cầu về bảo hành, Nhà thầu phải cử cán bộ kỹ thuật (nhân sự có chuyên môn phù hợp) đến khắc phục sự cố không chậm quá 48 giờ kể từ khi được yêu cầu của Chủ đầu tư. Việc thực hiện bảo hành khi thiết bị có sự cố và quá trình khắc phục không được kéo dài quá 7 ngày làm việc trừ trường hợp phải đặt

hàng từ nước ngoài. Trong trường hợp Nhà thầu không đáp ứng được việc bảo hành thì Chủ đầu tư có quyền thuê Nhà thầu khác thực hiện và toàn bộ kinh phí này sẽ do Nhà thầu chi trả.

+ Nhà thầu phải cam kết cung cấp dịch vụ bảo hành, hỗ trợ kỹ thuật chính hãng cho toàn bộ hàng hóa của gói thầu này.

- Trừ trường hợp có thỏa thuận khác trong hợp đồng ký kết giữa Chủ đầu tư và Nhà thầu, trước khi các bên tiến hành bàn giao và nghiệm thu hàng hóa, Nhà thầu phải cung cấp cho chủ đầu tư bao gồm nhưng không giới hạn các tài liệu theo yêu cầu sau (không bắt buộc đối với vật tư tiêu hao, vật tư hoặc phụ kiện lắp đặt đi kèm thiết bị chính):

+ Tài liệu chứng minh nguồn gốc xuất xứ của hàng hóa (không bắt buộc đối với hàng hóa được sản xuất trong nước, phần mềm) do cơ quan có thẩm quyền cấp (sau đây gọi tắt là "C/O");

+ Tài liệu chứng nhận chất lượng hoặc chứng nhận xuất xưởng hợp lệ của hàng hóa, thiết bị do nhà sản xuất phát hành (sau đây gọi tắt là "C/Q");

+ Các tài liệu khác theo quy định của hợp đồng.

- Trong mọi trường hợp, nếu xảy ra tranh chấp về bản quyền hoặc quyền sở hữu liên quan đến hàng hóa của gói thầu thì nhà thầu phải chịu hoàn toàn trách nhiệm, bao gồm bồi thường các thiệt hại xảy ra do tranh chấp gây ra.

- Bàn giao và lắp đặt triển khai thiết bị

+ Địa điểm bàn giao, kiểm tra thiết bị: Trung tâm Kỹ thuật Thông tấn.

+ Nhà thầu chịu mọi trách nhiệm về tổn thất, hư hại đối với các hàng hóa cung cấp theo hợp đồng trong quá trình vận chuyển, lưu kho, giao hàng đến điểm giao hàng cuối cùng và nghiệm thu; mua bảo hiểm trong các quá trình nêu trên (nếu cần thiết).

III. Yêu cầu kỹ thuật cụ thể:

STT	Danh mục thiết bị	Thông số kỹ thuật	Đơn vị tính	Số lượng
A	**Bản quyền phần mềm**			
1	**License phần mềm đánh giá xâm nhập**			
1.1	**Nền tảng đánh giá xâm nhập**	**Thời gian bản quyền: 12 tháng**	**Gói**	**01**
		Phát hiện được các mã độc tấn công có chủ đích (APT), phân tích		

		hành vi dựa trên công nghệ học máy (Machine Learning) với dữ liệu từ các tấn công APT thực tế trên thế giới.		
		Có tính năng quản trị tập trung qua nền tảng web.		
		Có tính năng tìm kiếm, lọc các thông tin của máy chủ.		
		Hoạt động dựa trên cách thức đánh giá rủi ro về các tấn công APT (risk-based context), tránh các cảnh báo giả.		
		Phát hiện được các hành vi độc hại của mã độc như: Process-injection, DLL-sideloading, Keylogging, Windows Credential Hash-dump API, PE Packers		
		Tìm kiếm, điều tra phân tích các dấu vết lây nhiễm với mã độc: memory, process, network connection, registry, eventlog, task scheduler, MBR, WMI.		
		Phát hiện các dịch vụ không có chữ ký số hoặc giả mạo chữ ký số.		
		Phát hiện được thời điểm mã độc bắt đầu phát tán, lây nhiễm.		
		Hỗ trợ triển khai hệ thống theo hình thức đặt máy chủ tại Thông Tấn Xã (on-premise).		
		Có tính năng cập nhật thêm các thông tin tình báo an ninh mạng (Hash, IP, Domain), cập nhật YARA rule để hỗ trợ rà quét.		
		Có tính năng rà quét offline (offline scanning), cho phép rà quét các mã độc mà không cần kết		

		nối tới thành phần quản lý, phục vụ cho nhu cầu điều tra truy vết và ứng cứu sự cố.		
		Phát hiện và phân tích được các tấn công dạng lây nhiễm ngang hàng (Lateral Movement), đồng thời thể hiện bằng biểu đồ kết nối (Graph)		
		Có tính năng tự động điều tra phân tích (auto-investigate) giúp phát hiện các nghi vấn về nhiễm mã độc, phát hiện nguồn gốc lây nhiễm		
		Thành phần cài đặt trên máy trạm (agent) hỗ trợ đa nền tảng :		
		- Windows 10, Windows 11, Windows server 2016, Windows server 2019		
		- Redhat 7, Redhat 8		
		- MacOS 11,12,13 (MacOS 11 and later)		
		Có khả năng phân quyền cho các tài khoản trên hệ thống.		
		Hỗ trợ báo cáo, thống kê, tìm kiếm.		
		Hỗ trợ định dạng báo cáo đa dạng như PDF, CSV, Dashboard.		
		Hỗ trợ tích hợp với hệ thống SIEM		
		Hỗ trợ tích hợp với giải pháp Threat Intelligence (TI)		
1.2	**License phần mềm đánh giá xâm nhập/node**	**Thời gian bản quyền: 12 tháng**	**Node**	**1000**
2	**License phần mềm Bảo vệ chống tấn công bề mặt**			

2.1	**Nền tảng bảo vệ chống tấn công bề mặt hỗ trợ tối đa 1000 node, bao gồm các tính năng:**	**Thời gian bản quyền: 12 tháng**	**Gói**	**01**
	Module quản lý tấn công bề mặt (ASM - Attack Surface Management)			
		Khám phá Tổ chức và Tài sản (Organizational and Asset Discovery): Sử dụng hệ thống phân tán toàn cầu (mạng lưới bot whitehat), xử lý ngôn ngữ tự nhiên (NLP) tự động, AI độc quyền, công nghệ mã nguồn mở và điều tra của chuyên gia phân tích để khám phá toàn bộ cấu trúc kinh doanh cùng với các tài sản chưa được biết và chưa được quản lý.		
		Gán thuộc tính (Attribution): Các tài sản được ánh xạ tới tổ chức/các tổ chức mà chúng thuộc về và được minh họa rõ ràng, kèm theo chi tiết và bằng chứng.		
		Phân loại (Classification): Các dịch vụ và cổng được phơi bày, hệ điều hành, ngăn xếp công nghệ đang sử dụng, v.v., được ánh xạ tới từng tài sản. Các dịch vụ được xác định theo loại môi trường (ví dụ: máy chủ web, máy chủ thư, bộ định tuyến, bộ cân bằng tải, v.v.) và nền tảng (ví dụ: Giao thức IMAP, Dịch vụ FTP Microsoft IIS, Giao thức		

		SMTP, v.v.). Bao gồm vị trí, đường dẫn khám phá, dịch vụ và cổng, cùng các tài sản liên quan.		
		Đánh giá An ninh (Security grading): Điểm an ninh (A-F) được bao gồm cho mỗi tài sản.		
		Dữ liệu Nhạy cảm (Sensitive data): Bao gồm việc khám phá dữ liệu nhạy cảm, kể cả PII (Thông tin nhận dạng cá nhân).		
		Thu thập Bằng chứng (Evidence collection): CyCognito cung cấp việc thu thập bằng chứng xuyên suốt quá trình và cho phép truy cập bằng chứng thông qua giao diện người dùng (UI).		
		Ánh xạ Cấu trúc Tổ chức (Organizational structure mapping): Hiển thị đồ họa tương tác về ánh xạ tổ chức, bao gồm đánh giá an ninh ban đầu, hệ thống phân cấp, v.v..		
		Tổng quan (General): Management console: Analytics, dashboard hành động độc đáo, chế độ xem tài sản và vấn đề hoạt động, báo cáo, tài sản đám mây, v.v.. API access: Dữ liệu nền tảng CyCognito có sẵn qua REST API. Integrations: Ví dụ bao gồm SIEM, quản lý sự cố, tự động hóa quy trình làm việc, cộng tác, quản		

		lý tài sản, SOAR và Endpoint/XDR. Hỗ trợ ngoài hộp bao gồm Snow, Splunk, JIRA, Zendesk, Slack, Gmail, Teams, O365, và nhiều hơn nữa		
	Module kiểm tra bảo mật tự động (AST - Automated Security Testing)	AST là module được xây dựng trên ASM, cung cấp dữ liệu kiểm tra bảo mật trên toàn bộ mạng lưới ảo bên ngoà.		
		Kiểm tra Tài sản (Asset Testing):		
		Kiểm thử chung (General tests): CVEs (Internet, IoT, OT, v.v.), vệ sinh an ninh (cấu hình sai; RDP, FTP bị phơi bày, v.v.), cơ sở dữ liệu bị phơi bày (MongoDB, Elastic, SQL Server, v.v.), đánh giá độ nhạy cảm của các thư mục tệp bị phơi bày, CVE Thực thi Mã Từ xa, chiếm đoạt tên miền phụ và tên miền, cấu hình sai bảo mật email (SPF, DMARC, v.v.).		
		Kiểm thử Ứng dụng Web (DAST - Dynamic application security testing): Các rủi ro OWASP top 10 (tấn công Injection như XSS, SQLi, v.v.), vấn đề xác thực (crypto, thông tin xác thực mặc định, bypass), thư viện javascript (JS) dễ bị tấn công, hệ thống quản lý nội dung dễ bị tấn công (ví dụ: WordPress), nền tảng nội bộ bị phơi bày & cấu hình sai, trang web bị bỏ quên và không được duy trì		
		Tổng quan (General):		
		Lập kết hoạch khắc phục: Tính năng tương tác phong phú, xây		

		dựng kế hoạch cải thiện tư thế an ninh có thể hành động và hoạt động.		
		Chấm điểm và đánh giá lại bảo mật: Chi tiết vấn đề an ninh cung cấp chi tiết chấm điểm; tùy chọn revalidate issues (tức là kiểm tra ngoài chu kỳ quét đã chọn)		
		Quản lý rủi ro: Quét liên tục bề mặt tấn công ở quy mô lớn (không tài sản không xác định nào bị bỏ sót), bao gồm cả quét thụ động và chủ động		
		Evidence and remediation steps (Bằng chứng và các bước khắc phục)		
		Full integration (Tích hợp đầy đủ) với bảng điều khiển ASM, API và các tích hợp gốc		
	Module: Exploit Intelligence (EI-Exploit Intelligence)	EI là module được xây dựng trên AST, cung cấp thông tin chi tiết và chính xác hơn vào các rủi ro quan trọng nhất cho tổ chức của bạn bằng cách sử dụng thông tin tình báo khai thác.		
		Khuyến nghị về mối đe dọa mới nổi (Emergent threat advisories): Nhận lời khuyên bảo mật chi tiết từ các nguồn đáng tin cậy, như CISA, kết hợp với các nguồn cấp dữ liệu tình báo về mối đe dọa khác		
		Tình báo về mối đe dọa và rủi ro (Threat and risk intelligence): Ánh xạ thông tin tình báo về hoạt động của kẻ tấn công đang diễn ra với		

		các lỗ hổng dễ bị tấn công trên bề mặt tấn công của bạn		
		Xác thực vấn đề an ninh (Security issue validation): Hướng dẫn từng bước để khai thác an toàn các lỗ hổng và mô phỏng các vi phạm. Các nhóm bảo mật có thể xác thực rủi ro bằng cách làm theo hướng dẫn khai thác mô phỏng các cuộc tấn công một cách an toàn và thực thi các biện pháp đối phó bảo mật của bạn.		
2.1	**Hỗ trợ kỹ thuật**	**Thơi gian hỗ trợ: 12 tháng**	**Gói**	**1**
3	**License phần mềm Phát hiện và Phản hồi mở rộng XDR Endpoint Security**	**Thời gian bản quyền: 12 tháng**	**User**	**1000**
3.1		**Kiến trúc triển khai**		
		- Hệ thống quản trị/ phân tích tập trung của giải pháp hỗ trợ triển khai tại chỗ (On-premise)		
		- Hỗ trợ triển khai theo mô hình Cluster;		
		- Có cơ chế kiểm tra phần cứng, hệ điều hành, phần mềm, môi trường mạng trước triển khai các thành phần của hệ thống (Deployment Toolkit) để đảm bảo đáp ứng yêu cầu		
3.2		**Khả năng tích hợp, mở rộng**		
		- Cho phép tích hợp thu thập sự kiện với các giải pháp khác thông qua giao thức: TCP, UDP, Netflow, sflow, FTP, NFS, SNMP,		

		Diode, SQL (Oracle, MS SQL,Firebird…)		
		- Giải pháp có khả năng tích hợp/bổ sung các giải pháp của cùng hãng sản xuất để nâng cao khả năng bảo vệ khi có nhu cầu như: chống tấn công APT lớp mạng (NDR), tham báo an ninh mạng (threat intelligence), đào tạo nhận thức (Security Awareness Platform), máy chủ Mail (Mail Server)...		
		- Giải pháp cho phép tích hợp với thành phần quản trị tập trung Antivirus sẵn có của Thông Tấn Xã Việt Nam và thực hiện khả năng phản hồi tự động như: Cập nhật cơ sở dữ liệu, dò quét mã độc		
		- Giải pháp cho phép đồng bộ thông tin tài sản (các thiết bị máy tính đang được quản lý bởi thành phần quản trị tập trung Antivirus sẵn có của Thông Tấn Xã Việt Nam) để nâng cao khả năng kiểm soát như: Tên tài sản, OS, địa chỉ MAC, thông tin phần mềm đang cài đặt, thông tin phần cứng của thiết bị, trạng thái Real-time protection, các lỗ hổng bảo mật của tài sản, trạng thái bảo mật của thiết bị, trạng thái mã hóa...		
3.3		**Công cụ tương quan chéo:**		
		- Kết nối của bên thứ ba + Khả năng tích hợp với các giải pháp bảo mật khác (ví dụ: Tường lửa, SIEM, EDR của nhà cung cấp khác) để thu thập dữ liệu và thực hiện hành động.		

		- Quản lý nhật ký & Hồ dữ liệu + Khả năng thu thập, lưu trữ và xử lý nhật ký (log) và hồ sơ dữ liệu từ toàn bộ hệ thống		
		- Phát hiện mối đe dọa và tương quan chéo + Chức năng cốt lõi để xác định các hoạt động độc hại bằng cách tìm kiếm mối liên hệ giữa các sự kiện khác nhau.		
		- Quản lý tài sản + Cung cấp thông tin về các thiết bị của hệ thống		
		- Bảng điều khiển & Báo cáo + Dashboards & Reporting Bảng điều khiển & Báo cáo Cung cấp giao diện trực quan để giám sát trạng thái an ninh, xu hướng mối đe dọa và tạo báo cáo tổng hợp.		
3.4		**Các thành phần XDR:**		
		- Quản lý trường hợp (case) bảo mật		
		- Tự động hóa và điều phối phản hồi (sổ tay hướng dẫn) + Khả năng thiết lập các quy tắc tự động hóa để thực hiện các hành động phản hồi mà không cần can thiệp thủ công, sử dụng các quy trình đã định trước.		
		- Điều tra bảo mật + Các công cụ chuyên sâu để phân tích chi tiết các sự kiện bảo mật, tìm kiếm gốc rễ và phạm vi của một cuộc tấn công		
		- Có bộ công cụ triển khai		

		- Hỗ trợ API mở		
3.5		**Quản lý, điều tra và phản hồi**		
		- Phản hồi thông qua Active Directory theo một trong các phương thức sau: Từ chi tiết cảnh báo, từ sự kiện đo xa (telemetry event), từ biểu đồ điều tra. Các hành động có thể được thực hiện như: khoá, thay đổi mật khẩu hoặc xoá user.		
		- Trang bị khả năng phát hiện các mối đe dọa và tương quan chéo. Hỗ trợ tối thiểu 300 quy tắc tương quan có sẵn, có khả năng ánh xạ với MITRE ATT&CK		
		- Playbook hỗ trợ các chế động hoạt động như: Tự động, thủ công, đào tạo		
		- Cho phép tra cứu thông tin về URL, domain, IP address, file hash thông qua cổng thông tin về mối đe dọa - Threat Intelligence Portal (bản quyền có sẵn mà không cần mua thêm)		
B	**Thuê thiết bị CNTT**			**Số lượng**
1	**Máy chủ lưu trữ log** **02 Intel® Xeon® Scalable Processors** **16 cores; 128 Gb RAM; 10x1,2Tb HDD**	**Thời gian thuê: 12 tháng**	**Chiếc**	**2**
	Số lượng	≥ 02 bộ		
	Loại thiết bị	Máy chủ rack		

	Bộ xử lý chính (CPU)	02 Intel® Xeon® Scalable Processors		
	Tốc độ xung nhịp	2.0GHz		
	Số lượng core/CPU	16 cores		
	Bộ nhớ (RAM)	128 Gb		
	Ổ đĩa cứng	10 Tb HDD		
2	**Máy chủ quản lý ứng dụng 02 Intel® Xeon® Scalable Processors 8 cores; 64 Gb RAM; 4x480GB SSD + 4x1Tb HDD**	**Thời gian thuê: 12 tháng**	**Chiếc**	**5**
	Loại thiết bị	Máy chủ rack		
	Bộ xử lý chính (CPU)	02 Intel® Xeon® Scalable Processors		
	Tốc độ xung nhịp	2.0GHz		
	Số lượng core/CPU	8 cores		
	Bộ nhớ (RAM)	64Gb		
	Ổ đĩa cứng	4 x 480Gb SSD + ≥ 4 x 1Tb HDD		
3	**Thiết bị chuyển mạch 10/40Gbps**	**Thời gian thuê: 12 tháng**	**Chiếc**	**2**
	Loại thiết bị	10/40G Data Center Switches		
	Bộ xử lý chính (CPU)	Dual-Core x86		
	System Memory	4 Gigabytes		
	Flash Storage Memory	2 Gigabytes		
	Packet Buffer Memory	9MB (Dynamic Buffer Allocation)		

	Tốc độ chuyển mạch (Throughput)	1.2 Tbps		
	Packets/Second	960Mpps		
	Số lượng cổng QSFP+ tối đa	4 ports		
	Số lượng cổng SFP+ tối đa	48 ports		
	Số lượng bộ nguồn	2 (1+1 redundant)		
4	**Thiết bị quản lý và phân tích lưu lượng mạng**	**Thời gian thuê: 12 tháng**	**Chiếc**	**2**
	Loại thiết bị	Edge Traffic Aggregation and Distribution Visibility		
	Network and Traffic Access	Port configurability: • Full flexibility in selecting ports as ingress, intermediate, interconnect, or egress functions • Unidirectional and bi-directional ports • Tunnel termination (e.g. L2GRE, VXLAN)		
	Core Intelligence	Flow Mapping, including: • Aggregation and replication – Selective any-to-any port mapping • Filtering – Layer 2 to 7 rules – Aggregate and egress • Load-balancing – Layers 2 to 4 hashing criteria – Session stickiness VLAN port tagging Device and Link discovery with ARP and LLDP		
	Management	User access: • Role-based Access Control		

		(RBAC) – Multi-tenant user access – Flexible user/role defined privileges, screen views and access • AAA security with local and remote authentication (RADIUS, TACACS+)		
	Field replaceable hardware	• Power supplies • Fan trays		
	Tốc độ chuyển mạch (Throughput)	1.2 Tbps		
	Số lượng cổng QSFP+ tối đa	32 ports		
	Số lượng bộ nguồn	02 load-sharing power supplies		

Mục 3. Các yêu cầu khác

1. Yêu cầu về vận hành chạy thử.

Tất cả hàng hóa, thiết bị đều phải được vận hành chạy thử trước khi nghiệm thu và Nhà thầu phải chịu tất cả các chi phí vật tư tiêu hao trong quá trình vận hành chạy thử.

2. Yêu cầu về đào tạo, hướng dẫn sử dụng.

- Sau khi lắp đặt hàng hóa, thiết bị và vận hành chạy thử, Nhà thầu phải tổ chức đào tạo, hướng dẫn sử dụng cho Chủ đầu tư tại nơi lắp đặt theo tiêu chuẩn của nhà sản xuất. Việc đào tạo hướng dẫn sử dụng được thực hiện bởi chuyên gia của hãng sản xuất hoặc nhân sự có trình độ chuyên môn, kinh nghiệm của Nhà thầu.

- Trong E-HSDT, nhà thầu phải trình bày kế hoạch đào tạo cụ thể, trình tự hướng dẫn sử dụng/vận hành phù hợp với đề xuất về kỹ thuật và tiến độ thực hiện gói thầu. Đồng thời nhà thầu phải cam kết kết thúc quá trình đào tạo thì cán bộ được đào tạo sẽ sử dụng thành thạo toàn bộ hàng hóa của gói thầu.

Mục 4. Bản vẽ: Không có.

Mục 5. Kiểm tra và thử nghiệm: Hàng hóa của gói thầu phải được kiểm tra và thử nghiệm theo yêu cầu sau đây:

- Trước khi đưa hàng hóa vào lắp đặt, hàng hóa phải được Chủ đầu tư nghiệm thu về mặt số lượng, chủng loại (model, ký mã hiệu, xuất xứ, hãng sản xuất) so

với hợp đồng. Nhà thầu chịu trách nhiệm bàn giao các tài liệu liên quan đến hàng hóa để phục vụ công tác nghiệm thu.

- Trong quá trình lắp đặt, cài đặt hàng hóa, Chủ đầu tư sẽ tổ chức nghiệm thu các công việc thành phần theo đề xuất của nhà thầu đảm bảo phù hợp với các quy định hiện hành của nhà nước.

- Sau khi nhà thầu hoàn thành toàn bộ các công việc được giao theo hợp đồng, Chủ đầu tư sẽ tổ chức nghiệm thu hoàn thành bàn giao đưa vào sử dụng. Nhà thầu phải chịu trách nhiệm bàn giao tất cả các tài liệu có liên quan đến hàng hóa và hoàn thiện các nội dung còn tồn tại trước khi được nghiệm thu.

- Trong quá trình kiểm tra và thử nghiệm, nếu Chủ đầu tư có sự nghi ngờ về chất lượng hàng hóa, sản phẩm của nhà thầu cung cấp, Chủ đầu tư có thể giao cho một đơn vị độc lập có chức năng để tiến hành đánh giá, kiểm tra, thử nghiệm. Nhà thầu sẽ phải chịu trách nhiệm chi trả toàn bộ các chi phí có liên quan nếu bị kết luận chất lượng hàng hóa, sản phẩm do nhà thầu cung cấp không đáp ứng yêu cầu theo quy định của E-HSMT và hợp đồng đã ký kết