Chương V. YÊU CẦU VỀ KỸ THUẬT

Mục 1. Yêu cầu về kỹ thuật

1.1. Giới thiệu chung về dự án/dự toán mua sắm, gói thầu

- Bên mời thầu: Bộ Tư lệnh 86/BQP

- Tên gói thầu: MS-03: Bảo đảm kỹ thuật hệ thống giám sát an toàn thông tin.

- Nguồn vốn: Ngân sách nhà nước năm 2026.

- Thời gian bắt đầu tổ chức lựa chọn nhà thầu: Quý II năm 2026

- Thời gian tổ chức lựa chọn nhà thầu: 45 ngày

- Hình thức lựa chọn nhà thầu: Đấu thầu rộng rãi qua mạng

- Phương thức lựa chọn nhà thầu: Một giai đoạn một túi hồ sơ

- Loại hợp đồng: Trọn gói

- Thời gian thực hiện gói thầu: 120 ngày

1.2. Yêu cầu về kỹ thuật

a) Yêu cầu về kỹ thuật chung:

- Hàng hóa cung cấp trong gói thầu đảm bảo đáp ứng đúng chủng loại, xuất xứ, tiêu chuẩn kỹ thuật của nhà sản xuất, không có khuyết tật phát sinh.

- Khi bàn giao hàng hóa, hai bên tiến hành kiểm tra hàng hóa về số lượng, chất lượng, chủng loại, nhãn mác, xuất xứ được quy định trong hợp đồng. Nếu hàng hóa đáp ứng theo quy định thì hai bên tiến hành bàn giao (hai bên ký biên bản bàn giao hàng hóa). Trong trường hợp hàng hóa không đúng chủng loại, xuất xứ, chất lượng theo hợp đồng thì bên mua có quyền từ chối nhận hàng và yêu cầu bên bán cung cấp lô hàng mới đảm bảo chất lượng như hợp đồng quy định, quy trình kiểm tra như lần đầu. Bất kỳ hàng hóa nào sai khác so với hợp đồng, nhà thầu phải có văn bản giải trình, làm rõ gửi chủ đầu tư, nếu được chủ đầu tư chấp nhận, hai bên sẽ ký phụ lục điều chỉnh, bổ sung hợp đồng và tiến hành kiểm tra, nghiệm thu theo trình tự trên.

b) Yêu cầu cụ thể

Yêu cầu nhà thầu tóm tắt thông số kỹ thuật của hàng hóa và các dịch vụ liên quan chứng minh hàng hóa do nhà thầu chào đáp ứng các nội dung yêu cầu kỹ thuật dưới đây hoặc đáp ứng tốt hơn. Nhà thầu có thể lựa chọn dự thầu hàng hóa có nguồn

gốc, xuất xứ, nhà sản xuất, thương hiệu phù hợp với điều kiện cung cấp nhưng phải đảm bảo yêu cầu có thông số kỹ thuật, tính năng sử dụng, tiêu chuẩn "tương đương" hoặc tốt hơn so với các yêu cầu cụ thể ở dưới và cung cấp tài liệu chứng minh sự đáp ứng tốt hơn của hàng hóa chào thầu so với yêu cầu của E-HSMT.

Tóm tắt thông số kỹ thuật của hàng hóa và các dịch vụ liên quan phải tuân thủ các thông số kỹ thuật và các tiêu chuẩn sau đây:

STT	Danh mục hàng hóa	Cấu hình, tính năng kỹ thuật tối thiểu
1	Phần mềm Security Logger Standard Edition nâng cấp từ 350 EPS lên 2000 EPS - Subscription (ArcSight Logger Standard Edition)	**Yêu cầu bản quyền**: - Cung cấp bản quyền phần mềm ArcSight Logger tối thiểu 2000 Event Per Second (EPS) - Thời gian cập nhật phần mềm, hỗ trợ kỹ thuật chính Hãng 36 tháng **Tính năng tích hợp, thu thập nhật ký:** - Cho phép thu thập nhật ký từ các hệ thống CNTT bao gồm các loại: thiết bị mạng (Router, Switch...), thiết bị an ninh (Firewall, IDS/IPS, Database firewall, Antivirus...), hệ điều hành (Operating systems), ứng dụng (Application), cơ sở dữ liệu (Database) - Cung cấp các loại Connectors bao gồm: API Connectors Database Connectors File Connectors FlexConnectors Microsoft Windows Event Log Connectors Model Import Connectors Scanner Connectors SNMP Connectors Syslog Connectors - Cho phép phân tách dữ liệu thu thập từ các thiết bị trong mạng bằng lược đồ chuẩn hóa (normalized schema), tối thiểu 400 trường dữ liệu (Data Fields) - Thành phần thu thập cung cấp chức năng lưu trữ tạm thời (Caching) để đảm bảo tính toàn vẹn nhật ký trong trường hợp kết nối đến thành phần phân tích bị gián đoạn - Cho phép cấu hình cụ thể phần dung lượng ổ cứng

STT	Danh mục hàng hóa	Cấu hình, tính năng kỹ thuật tối thiểu
		(disk space) của mỗi Connectors dành cho việc lưu trữ nhật ký tạm thời ngay tại thành phần thu thập. - Cho phép cấu hình lọc bỏ các sự kiện không cần thiết ngay tại thành phần thu thập trước khi gửi về thành phần phân tích. Đồng thời cho phép cấu hình lọc các sự kiện theo các đặc tính cụ thể nào đó (certain characteristics) hoặc các sự kiện từ một thiết bị mạng cụ thể (specific network devices) - Cho phép cấu hình hợp nhất nhiều sự kiện (Aggregate events) nhằm giảm thiểu số lượng sự kiện cần phân tích - Cho phép cấu hình thiết lập lượng băng thông sử dụng tại thành phần thu thập khi gửi nhật ký **Tính năng lưu trữ:** - Cung cấp giải pháp quản lý nhật ký (Log management solution) - Cung cấp tính năng nén dữ liệu - Cung cấp tính năng Archive dữ liệu - Cho phép định nghĩa các nhóm lưu trữ (Storage Group) trên một không gian lưu trữ (Storage Volume) - Cho phép cấu hình chính sách lưu trữ cho mỗi Storage Group bao gồm: dung lượng lưu trữ, thời gian lưu trữ - Cho phép định nghĩa các quy tắc lưu trữ nhằm xác định loại sự kiện từ các nguồn nhật ký cụ thể sẽ được lưu trữ ở Storage Group nào. - Cho phép lưu các truy vấn để sử dụng sau này **Tính năng phân tích:** - Cho phép truy vấn nhật ký theo dạng từ khóa (full-text search), các trường đã được định nghĩa từ trước hay theo một biểu thức cụ thể. - Cung cấp sẵn các bảng theo dõi điều khiển (Dashboard) về: + Số lượng sự kiện nhận và chuyển đi + Thay đổi cấu hình và hành động xâm nhập trong hệ thống + Thông tin về việc đăng nhập và hành động kết nối trong hệ thống + Thông tin trạng thái CPU, luồng sự kiện, lưu trữ...

STT	Danh mục hàng hóa	Cấu hình, tính năng kỹ thuật tối thiểu
		- Cung cấp sẵn các bảng theo dõi điều khiển (Dashboard) về an toàn, an ninh trong hệ thống thống như: + Các hành vi của mã độc + Các sự kiện bị chặn trên tường lửa + Các hành động thay đổi cấu hình + Các hành vi tạo tài khoản trên hệ điều hành Window + Các hành vi login không thành công + Các kết nối VPN: hiển thị thông tin các người dùng đã kết nối vào VPN - Cho phép cấu hình Real-time Alerts và cho phép gửi Alerts qua Email, SNMP, hoặc Syslog - Cho phép tạo báo cáo và hỗ trợ các định dạng HTML, PDF, MS EXCEL, MS WORD **Tính năng quản trị:** - Quản trị thông qua giao diện Web
2	Phần mềm Security Logger Standard Edition nâng cấp từ 350 EPS lên 3000 EPS - Subscription (ArcSight Logger Standard Edition)	**Yêu cầu bản quyền**: - Cung cấp bản quyền phần mềm ArcSight Logger tối thiểu 3000 Event Per Second (EPS) - Thời gian cập nhật phần mềm, hỗ trợ kỹ thuật chính Hãng 36 tháng **Tính năng tích hợp, thu thập nhật ký:** - Cho phép thu thập nhật ký từ các hệ thống CNTT bao gồm các loại: thiết bị mạng (Router, Switch...), thiết bị an ninh (Firewall, IDS/IPS, Database firewall, Antivirus...), hệ điều hành (Operating systems), ứng dụng (Application), cơ sở dữ liệu (Database) - Cung cấp các loại Connectors bao gồm: API Connectors Database Connectors File Connectors FlexConnectors Microsoft Windows Event Log Connectors Model Import Connectors Scanner Connectors SNMP Connectors Syslog Connectors

STT	Danh mục hàng hóa	Cấu hình, tính năng kỹ thuật tối thiểu
		- Cho phép phân tách dữ liệu thu thập từ các thiết bị trong mạng bằng lược đồ chuẩn hóa (normalized schema), tối thiểu 400 trường dữ liệu (Data Fields) - Thành phần thu thập cung cấp chức năng lưu trữ tạm thời (Caching) để đảm bảo tính toàn vẹn nhật ký trong trường hợp kết nối đến thành phần phân tích bị gián đoạn - Cho phép cấu hình cụ thể phần dung lượng ổ cứng (disk space) của mỗi Connectors dành cho việc lưu trữ nhật ký tạm thời ngay tại thành phần thu thập. - Cho phép cấu hình lọc bỏ các sự kiện không cần thiết ngay tại thành phần thu thập trước khi gửi về thành phần phân tích. Đồng thời cho phép cấu hình lọc các sự kiện theo các đặc tính cụ thể nào đó (certain characteristics) hoặc các sự kiện từ một thiết bị mạng cụ thể (specific network devices) - Cho phép cấu hình hợp nhất nhiều sự kiện (Aggregate events) nhằm giảm thiểu số lượng sự kiện cần phân tích - Cho phép cấu hình thiết lập lượng băng thông sử dụng tại thành phần thu thập khi gửi nhật ký **Tính năng lưu trữ:** - Cung cấp giải pháp quản lý nhật ký (Log management solution) - Cung cấp tính năng nén dữ liệu - Cung cấp tính năng Archive dữ liệu - Cho phép định nghĩa các nhóm lưu trữ (Storage Group) trên một không gian lưu trữ (Storage Volume) - Cho phép cấu hình chính sách lưu trữ cho mỗi Storage Group bao gồm: dung lượng lưu trữ, thời gian lưu trữ - Cho phép định nghĩa các quy tắc lưu trữ nhằm xác định loại sự kiện từ các nguồn nhật ký cụ thể sẽ được lưu trữ ở Storage Group nào. - Cho phép lưu các truy vấn để sử dụng sau này **Tính năng phân tích:** - Cho phép truy vấn nhật ký theo dạng từ khóa (full-text search), các trường đã được định nghĩa từ trước hay theo một biểu thức cụ thể.

STT	Danh mục hàng hóa	Cấu hình, tính năng kỹ thuật tối thiểu
		- Cung cấp sẵn các bảng theo dõi điều khiển (Dashboard) về: + Số lượng sự kiện nhận và chuyển đi + Thay đổi cấu hình và hành động xâm nhập trong hệ thống + Thông tin về việc đăng nhập và hành động kết nối trong hệ thống + Thông tin trạng thái CPU, luồng sự kiện, lưu trữ... - Cung cấp sẵn các bảng theo dõi điều khiển (Dashboard) về an toàn, an ninh trong hệ thống thống như: + Các hành vi của mã độc + Các sự kiện bị chặn trên tường lửa + Các hành động thay đổi cấu hình + Các hành vi tạo tài khoản trên hệ điều hành Window + Các hành vi login không thành công + Các kết nối VPN: hiển thị thông tin các người dùng đã kết nối vào VPN - Cho phép cấu hình Real-time Alerts và cho phép gửi Alerts qua Email, SNMP, hoặc Syslog - Cho phép tạo báo cáo và hỗ trợ các định dạng HTML, PDF, MS EXCEL, MS WORD **Tính năng quản trị:** - Quản trị thông qua giao diện Web
3	Phần mềm Enterprise Security Manager Standard Edition nâng cấp từ 350 EPS lên 2000 EPS - New Model - Subscription (ArcSight	**Yêu cầu bản quyền:** - Cung cấp bản quyền phần mềm ArcSight Enterprise Security Manager tối thiểu 2000 Event Per Second (EPS) - Thời gian cập nhật phần mềm, hỗ trợ kỹ thuật chính Hãng 36 tháng **Tính năng tích hợp, thu thập nhật ký:** - Cho phép thu thập nhật ký từ các hệ thống CNTT bao gồm các loại: thiết bị mạng (Router, Switch...), thiết bị an ninh (Firewall, IDS/IPS, Database firewall, Antivirus...), hệ điều hành (Operating systems), ứng dụng (Application), cơ sở dữ liệu (Database) - Cung cấp các loại Connectors bao gồm:

STT	Danh mục hàng hóa	Cấu hình, tính năng kỹ thuật tối thiểu
	Enterprise Security Manager)	+ API Connectors + Database Connectors + File Connectors + FlexConnectors + Microsoft Windows Event Log Connectors + Model Import Connectors + Scanner Connectors + SNMP Connectors + Syslog Connectors - Cho phép phân tách dữ liệu thu thập từ các thiết bị trong mạng bằng lược đồ chuẩn hóa (normalized schema), tối thiểu 400 trường dữ liệu (Data Fields) - Thành phần thu thập cung cấp chức năng lưu trữ tạm thời (Caching) để đảm bảo tính toàn vẹn nhật ký trong trường hợp kết nối đến thành phần phân tích bị gián đoạn - Cho phép cấu hình cụ thể phần dung lượng ổ cứng (disk space) của mỗi Connectors dành cho việc lưu trữ nhật ký tạm thời ngay tại thành phần thu thập. - Cho phép cấu hình lọc bỏ các sự kiện không cần thiết ngay tại thành phần thu thập trước khi gửi về thành phần phân tích. Đồng thời cho phép cấu hình lọc các sự kiện theo các đặc tính cụ thể nào đó (certain characteristics) hoặc các sự kiện từ một thiết bị mạng cụ thể (specific network devices) - Cho phép cấu hình hợp nhất nhiều sự kiện (Aggregate events) nhằm giảm thiểu số lượng sự kiện cần phân tích - Cho phép cấu hình thiết lập lượng băng thông sử dụng tại thành phần thu thập khi gửi nhật ký **Tính năng theo dõi và điều tra:** - Cung cấp các công cụ cho việc theo dõi như Dashboard, Active Channel - Cho phép thực hiện chức năng Dashboard drill-down - cho phép kỹ sư thực hiện phân tích sâu vào Event Data từ Graphical Dashboard - Cung cấp chức năng Graphing Attacks - cho phép kỹ sư phân tích nhanh chóng nhận diện khối lượng lớn kẻ

STT	Danh mục hàng hóa	Cấu hình, tính năng kỹ thuật tối thiểu
		tấn công hoặc mục tiêu tấn công - Chức năng Graphing Attacks cần cho phép hiển thị dữ liệu các chế độ: + Static: đưa ra biểu đồ đối với các sự kiện được lựa chọn + Live: đưa ra biểu đồ sự kiện theo thời gian thực và liên tục được cập nhật - Cho phép giám sát theo Geographic event graphs Cung cấp chức năng Integration Commands - cho phép người quản trị thực hiện các câu lệnh phục vụ việc điều tra ngay trên giao diện quản trị của giải pháp - Chức năng Integration Commands cần hỗ trợ hai loại cơ bản như sau: + URL: câu lệnh cho phép liên kết đến Web page URLs hoặc URIs + Script: câu lệnh định nghĩa việc thực thi một Script **Tính năng phân tích sự tương quan:** - Cung cấp sẵn các gói Use-case theo dõi các mối đe dọa an ninh như: + Application Monitoring + Entity Monitoring + Host Monitoring + Malware Monitoring + Network Monitoring + Perimeter Monitoring + Vulnerability Monitoring - Cung cấp sẵn gói Use-case theo dõi các mối đe dọa dựa theo dữ liệu tình báo an ninh mạng (Threat intelligence data feed), bao gồm các Use-case: Botnet Activity + Dangerous Browsing + Internal Asset Found in Reputation List + Malware + Phishing + Ransomware + Suspicious Activity + Suspicious DNS Query

STT	Danh mục hàng hóa	Cấu hình, tính năng kỹ thuật tối thiểu
		+ Suspicious Email + Suspicious File Hash - Cho phép thực hiện phân tích tương quan theo thời gian thực (Real-time Rules) và trong quá khứ (Scheduled rules) - Cho phép thực hiện công việc quản lý Rule như: Creating hoặc Editing Rules, Enabling và Disabling Rules Cho phép định nghĩa điều kiện trong Rule theo: điểm yếu an ninh (Vulnerability), tài sản trong hệ thống (Assest) - Cho phép định nghĩa các Action cụ thể sẽ thực hiện bởi Rule như: + Gửi thông báo (Send Notification) + Thực thi một lệnh (Execute Command) + Tạo lập hồ sơ sự cố (Case/Create New Case) + Đưa vào danh sách theo dõi (Active List), Session List" - Cung cấp tính năng cho phép kiểm tra hoạt động của các luật (test hoặc verify rules) trước khi triển khai vào hệ thống **Hỗ trợ tính năng điều phối, tự động phản ứng lại sự cố an toàn thông tin:** - Hỗ trợ chức năng SOAR (Security Orchestration Automation and Response) cho phép thực hiện điều phối, tự động hóa phản ứng lại sự cố An toàn thông tin sau khi nhận từ thành phần phân tích tương quan - Hỗ trợ chức năng SOAR cần cung cấp các chức năng chính bao gồm: Consolidation, Orchestration, Automation, Response và Case Management - SOAR cho phép tự động thực hiện các hành động bảo vệ/ngăn chặn các mối đe dọa thông qua Playbook và tích hợp với giải pháp bảo mật của bên thứ 3 - Cho phép thực hiện tạo, sửa đổi, xóa, với Playbook **Tính năng báo cáo:** - Cung cấp sẵn các báo cáo và cho phép tùy biến báo cáo

STT	Danh mục hàng hóa	Cấu hình, tính năng kỹ thuật tối thiểu
		- Cho phép lập lịch tạo báo cáo và gửi cho người quản trị - Cho phép tạo Trending Report - để đưa ra báo cáo phân tích xu hướng - Cho phép tạo báo cáo theo các định dạng báo cáo như: HTML, PDF, Excel, CSV, RTF **Triển khai & Quản trị:** - Cho phép quản lý việc truy cập của User đến các tài nguyên sử dụng Access Control Lists (ACLs). ACLs áp dụng đối với User Group, cho phép các Users trong Group có quyền Read/Write đến các tài nguyên cụ thể - Cung cấp cơ chế xác thực được xây dựng sẵn trên chính thiết bị cho người quản trị và cho phép tích hợp với các cơ chế xác thực được cung cấp bởi 3rd party như: RADIUS Authentication, Microsoft Active Directory, hoặc LDAP. - Cho phép quản trị, vận hành qua giao diện Web Interface và Console.
4	Phần mềm Enterprise Security Manager Standard Edition nâng cấp từ 350 EPS lên 3000 EPS - New Model - Subscription (ArcSight Enterprise Security Manager)	**Yêu cầu bản quyền:** - Cung cấp bản quyền phần mềm ArcSight Enterprise Security Manager tối thiểu 3000 Event Per Second (EPS) - Thời gian cập nhật phần mềm, hỗ trợ kỹ thuật chính Hãng 36 tháng **Tính năng tích hợp, thu thập nhật ký:** - Cho phép thu thập nhật ký từ các hệ thống CNTT bao gồm các loại: thiết bị mạng (Router, Switch...), thiết bị an ninh (Firewall, IDS/IPS, Database firewall, Antivirus...), hệ điều hành (Operating systems), ứng dụng (Application), cơ sở dữ liệu (Database) - Cung cấp các loại Connectors bao gồm: + API Connectors + Database Connectors + File Connectors + FlexConnectors + Microsoft Windows Event Log Connectors + Model Import Connectors

STT	Danh mục hàng hóa	Cấu hình, tính năng kỹ thuật tối thiểu
		+ Scanner Connectors + SNMP Connectors + Syslog Connectors - Cho phép phân tách dữ liệu thu thập từ các thiết bị trong mạng bằng lược đồ chuẩn hóa (normalized schema), tối thiểu 400 trường dữ liệu (Data Fields) - Thành phần thu thập cung cấp chức năng lưu trữ tạm thời (Caching) để đảm bảo tính toàn vẹn nhật ký trong trường hợp kết nối đến thành phần phân tích bị gián đoạn - Cho phép cấu hình cụ thể phần dung lượng ổ cứng (disk space) của mỗi Connectors dành cho việc lưu trữ nhật ký tạm thời ngay tại thành phần thu thập. - Cho phép cấu hình lọc bỏ các sự kiện không cần thiết ngay tại thành phần thu thập trước khi gửi về thành phần phân tích. Đồng thời cho phép cấu hình lọc các sự kiện theo các đặc tính cụ thể nào đó (certain characteristics) hoặc các sự kiện từ một thiết bị mạng cụ thể (specific network devices) - Cho phép cấu hình hợp nhất nhiều sự kiện (Aggregate events) nhằm giảm thiểu số lượng sự kiện cần phân tích - Cho phép cấu hình thiết lập lượng băng thông sử dụng tại thành phần thu thập khi gửi nhật ký **Tính năng theo dõi và điều tra:** - Cung cấp các công cụ cho việc theo dõi như Dashboard, Active Channel - Cho phép thực hiện chức năng Dashboard drill-down - cho phép kỹ sư thực hiện phân tích sâu vào Event Data từ Graphical Dashboard - Cung cấp chức năng Graphing Attacks - cho phép kỹ sư phân tích nhanh chóng nhận diện khối lượng lớn kẻ tấn công hoặc mục tiêu tấn công - Chức năng Graphing Attacks cần cho phép hiển thị dữ liệu các chế độ: + Static: đưa ra biểu đồ đối với các sự kiện được lựa chọn + Live: đưa ra biểu đồ sự kiện theo thời gian thực và

STT	Danh mục hàng hóa	Cấu hình, tính năng kỹ thuật tối thiểu
		liên tục được cập nhật - Cho phép giám sát theo Geographic event graphs Cung cấp chức năng Integration Commands - cho phép người quản trị thực hiện các câu lệnh phục vụ việc điều tra ngay trên giao diện quản trị của giải pháp - Chức năng Integration Commands cần hỗ trợ hai loại cơ bản như sau: + URL: câu lệnh cho phép liên kết đến Web page URLs hoặc URIs + Script: câu lệnh định nghĩa việc thực thi một Script **Tính năng phân tích sự tương quan:** - Cung cấp sẵn các gói Use-case theo dõi các mối đe dọa an ninh như: + Application Monitoring + Entity Monitoring + Host Monitoring + Malware Monitoring + Network Monitoring + Perimeter Monitoring + Vulnerability Monitoring - Cung cấp sẵn gói Use-case theo dõi các mối đe dọa dựa theo dữ liệu tình báo an ninh mạng (Threat intelligence data feed), bao gồm các Use-case: Botnet Activity + Dangerous Browsing + Internal Asset Found in Reputation List + Malware + Phishing + Ransomware + Suspicious Activity + Suspicious DNS Query + Suspicious Email + Suspicious File Hash - Cho phép thực hiện phân tích tương quan theo thời gian thực (Real-time Rules) và trong quá khứ (Scheduled rules) - Cho phép thực hiện công việc quản lý Rule như:

STT	Danh mục hàng hóa	Cấu hình, tính năng kỹ thuật tối thiểu
		Creating hoặc Editing Rules, Enabling và Disabling Rules Cho phép định nghĩa điều kiện trong Rule theo: điểm yếu an ninh (Vulnerability), tài sản trong hệ thống (Assest) - Cho phép định nghĩa các Action cụ thể sẽ thực hiện bởi Rule như: + Gửi thông báo (Send Notification) + Thực thi một lệnh (Execute Command) + Tạo lập hồ sơ sự cố (Case/Create New Case) + Đưa vào danh sách theo dõi (Active List), Session List" - Cung cấp tính năng cho phép kiểm tra hoạt động của các luật (test hoặc verify rules) trước khi triển khai vào hệ thống **Hỗ trợ tính năng điều phối, tự động phản ứng lại sự cố an toàn thông tin:** - Hỗ trợ chức năng SOAR (Security Orchestration Automation and Response) cho phép thực hiện điều phối, tự động hóa phản ứng lại sự cố An toàn thông tin sau khi nhận từ thành phần phân tích tương quan - Hỗ trợ chức năng SOAR cần cung cấp các chức năng chính bao gồm: Consolidation, Orchestration, Automation, Response và Case Management - SOAR cho phép tự động thực hiện các hành động bảo vệ/ngăn chặn các mối đe dọa thông qua Playbook và tích hợp với giải pháp bảo mật của bên thứ 3 - Cho phép thực hiện tạo, sửa đổi, xóa, với Playbook **Tính năng báo cáo:** - Cung cấp sẵn các báo cáo và cho phép tùy biến báo cáo - Cho phép lập lịch tạo báo cáo và gửi cho người quản trị - Cho phép tạo Trending Report - để đưa ra báo cáo phân tích xu hướng - Cho phép tạo báo cáo theo các định dạng báo cáo như: HTML, PDF, Excel, CSV, RTF

STT	Danh mục hàng hóa	Cấu hình, tính năng kỹ thuật tối thiểu
		Triển khai & Quản trị: - Cho phép quản lý việc truy cập của User đến các tài nguyên sử dụng Access Control Lists (ACLs). ACLs áp dụng đối với User Group, cho phép các Users trong Group có quyền Read/Write đến các tài nguyên cụ thể - Cung cấp cơ chế xác thực được xây dựng sẵn trên chính thiết bị cho người quản trị và cho phép tích hợp với các cơ chế xác thực được cung cấp bởi 3rd party như: RADIUS Authentication, Microsoft Active Directory, hoặc LDAP. - Cho phép quản trị, vận hành qua giao diện Web Interface và Console.
5	Ổ cứng máy chủ	- Dung lượng: 1,2TB - Giao diện: SAS - Kiểu dáng ổ đĩa: SFF - Tốc độ quay ổ đĩa (RPM): 10K - Thời gian bảo hành: 24 tháng

1.3 Yêu cầu khác

a) Nhà thầu phải cam kết:

- Cam kết có mặt trong vòng 48 giờ kể từ khi nhận được thông báo của chủ đầu tư về khắc phục sự cố hỏng hóc, lỗi (trong thời gian bảo hành) của hàng hóa cung cấp;

- Cam kết cung cấp hàng hóa là phần cứng mới, sản xuất từ năm 2025 trở lại đây; đối với phần mềm là phiên bản mới nhất của hãng sản xuất tính đến thời điểm dự thầu;

- Cam kết thu hồi hàng hóa trong trường hợp hàng hóa không đảm bảo yêu cầu chất lượng mà không do lỗi của bên mời thầu.

- Cam kết hỗ trợ kỹ thuật (lắp đặt, khai báo cấu hình, chạy thử, nghiệm thu) hàng hóa, đảm bảo yêu cầu kỹ thuật của gói thầu.

- Cam kết hỗ trợ chủ đầu tư trong đào tạo triển khai, khai thác sử dụng hàng hóa do nhà thầu cung cấp.

b) Các tài liệu chứng minh tính hợp lệ của hàng hoá:

Nhà thầu phải có văn bản cam kết sẽ cung cấp các tài liệu kèm theo khi bàn giao hàng hóa (không bắt buộc đối với các vật tư, phụ kiện lắp đặt) để chứng minh

tính hợp lệ của hàng hoá đú.ng như nhà thầu chào trong hồ sơ dự thầu về kỹ thuật, chất lượng và nguồn gốc xuất xứ*:*

- Hóa đơn GTGT.

- Bản gốc hoặc bản sao được chứng thực chứng nhận nguồn gốc hàng hoá (CO) do cơ quan có thẩm quyền cấp, chứng nhận chất lượng (CQ) đối với hàng hóa nhập khẩu.

- Giấy chứng nhận chất lượng hoặc chứng nhận xuất xưởng đối với hàng hóa trong nước.

- Giấy chứng nhận bản quyền đối với phần mềm.

- Bản gốc hoặc bản sao y vận đơn, phiếu đóng gói, hóa đơn thương mại, tờ khai hàng hóa nhập khẩu đối với các hạng mục hàng hóa đối với hàng hóa nhập khẩu (nếu có).

- Bộ Catalogue kỹ thuật, tài liệu hướng dẫn sử dụng bằng tiếng Việt và các tài liệu kỹ thuật khác của phần mềm nâng cấp.

Mục 2. Bản vẽ: Không có bản vẽ

Mục 3. Kiểm tra và thử nghiệm

Các kiểm tra và thử nghiệm cần tiến hành gồm có:

+ Hàng hóa phải được bên mời thầu giám định chất lượng, kiểm tra an toàn thông tin, an ninh (nếu có) đạt yêu cầu theo quy định của Nhà nước và Bộ Quốc phòng.

+ Trong trường hợp kiểm tra nghiệm thu thiết bị của Nhà thầu không đảm bảo đúng như hợp đồng quy định thì Chủ đầu tư không tiếp nhận hàng, đồng thời Nhà thầu cung cấp lô hàng mới đảm bảo chất lượng theo như hợp đồng quy định.