Chương V. YÊU CẦU VỀ KỸ THUẬT

Mục 1. Yêu cầu về kỹ thuật

Yêu cầu về kỹ thuật bao gồm các nội dung cơ bản như sau:

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

Gói thầu số 14: "Mua sắm thiết bị, phần mềm phục vụ giám sát ATTT của Ban Cơ yếu Chính phủ" thực hiện Báo cáo kinh tế kỹ thuật "Triển khai giám sát an toàn thông tin cho một số hệ thống công nghệ thông tin của Ban Cơ yếu Chính phủ"

Địa điểm thực hiện: Lô CN27, Khu nghiên cứu triển khai, Khu công nghệ cao Hòa Lạc - Hà Nội, Xã Hòa Lạc, Thành phố Hà Nội.

Nguồn vốn: Ngân sách quốc phòng – Lĩnh vực chi Cơ yếu Chính phủ.

Loại hợp đồng: Trọn gói.

Thời gian thực hiện gói thầu: 45 ngày.

1.2. Yêu cầu về kỹ thuật

Yêu cầu về kỹ thuật bao gồm yêu cầu về kỹ thuật chung và yêu cầu về kỹ thuật chi tiết đối với hàng hóa thuộc phạm vi cung cấp của gói thầu, cụ thể:

Hạng mục số	Tên hàng hóa/dịch vụ liên quan	Thông số kỹ thuật và các tiêu chuẩn
1	**Máy chủ cài đặt tại trung tâm xử lý** Số lượng: 01 Chiếc	***(Có cấu hình tương đương hoặc cao hơn)*** **-CPU:** >= Intel Xeon Gold 2.2G, 32C/64T, 16GT/s, 60M Cache, Turbo, HT (270W) DDR5-4800 - **RAM:** >= 10 x 32GB RDIMM, 5600MT/s, Dual Rank - **HDD:** >= 8 x 3.84TB SSD SATA Read Intensive 6Gbps 512e 2.5in Hot-plug AG Drive, 1 DWPD **-Power:** Dual, HotPlug,Power Supply Fault Tolerant Redundant (1+1), 800W, Mixed Mode **Network port:** Broadcom 5720 Quad Port 1GbE BASE-T Adapter, OCP NIC 3.0

Hạng mục số	Tên hàng hóa/dịch vụ liên quan	Thông số kỹ thuật và các tiêu chuẩn
		Broadcom 57414 Dual Port 10/25GbE SFP28 Adapter, PCIe Full Height, V2 - Hỗ trợ các hệ điều hành: Windows, Red Hat Enterprise Linux, VMware Vsphere. - Sản xuất: năm 2025 trở lại đây. - Bảo hành: 36 tháng.
2	**Máy chủ cài đặt thiết bị thu thập tại các hệ thống triển khai** Số lượng: 05 Chiếc	***(Có cấu hình tương đương hoặc cao hơn)*** - **CPU:** >= Intel Xeon Silver 2.4G, 12C/24T, 16GT/s, 30M Cache, Turbo, HT (150W) DDR5-440 - **RAM:** >= 4 x 32GB RDIMM, 5600MT/s, Dual Rank - **HDD:** >= 4 x 960GB SSD SATA Read Intensive 6Gbps 512e 2.5in Hot-plug AG Drive, 1 DWPD. **Network port:** Broadcom 5720 Quad Port 1GbE BASE-T Adapter, OCP NIC 3.0 Broadcom 57414 Dual Port 10/25GbE SFP28 Adapter, PCIe Low Profile, V2 - **Power:** Dual, (1+1) Fully Redundant, Hot-Plug Power Supply, 800W MM (100-240Vac). - Hỗ trợ các hệ điều hành: Windows, Red Hat Enterprise Linux, VMware Vsphere. - Sản xuất: năm 2025 trở lại đây - Bảo hành: 36 tháng.
3	**Phần mềm SIEM phục vụ giám sát an toàn thông tin** Số lượng: 01 Phần mềm	- Các thành phần hỗ trợ khả năng tích hợp với hạ tầng, thu thập hoặc làm giàu thông tin cho các sự kiện thì không yêu cầu thêm chi phí bản

Hạng mục số	Tên hàng hóa/dịch vụ liên quan	Thông số kỹ thuật và các tiêu chuẩn
		quyền (đối với các giải pháp phòng chống mã độc đang được triển khai). - Kết nối giữa các thành phần của SIEM sử dụng kênh mã hóa. Giải pháp có thể hoạt động trong mạng đóng mà không yêu cầu kết nối hoặc cập nhật trực tiếp từ Internet. Giải pháp có giao diện web để quản trị tập trung và giám sát và hỗ trợ nhiều tenant. - Giải pháp hỗ trợ RESTful API để quản lý các tài sản, làm việc với các sự kiện/nhật ký. Hỗ trợ khả năng triển khai với tính sẵn sàng cao (High Availability) mà không yêu cầu thêm phí bản quyền. - Hỗ trợ các định dạng log sau: JSON, CEF, Regexp, Syslog, CSV, Key-Value, XML, NetFlow, Sflow, Ipfix (v10). Giải pháp cung cấp khả năng tùy chỉnh lưu trữ các sự kiện thô. - Giải pháp hỗ trợ khả năng tự tùy chỉnh thêm luật để chuyển đổi các định dạng log mới sang định dạng mà giải pháp có thể đọc hiểu (normalization rule). - Giải pháp hỗ trợ chia logic tổng lưu lượng lữu trữ thành các nhóm với các yêu cầu lưu trữ khác nhau. - Hỗ trợ khả năng truy vấn sự kiện đã lưu trong cơ sở dữ liệu với ngôn ngữ giống SQL. Có khả năng tìm kiếm các sự kiện trong toàn hệ thống mà được lưu trong bộ lưu trữ sự kiện

Hạng mục số	Tên hàng hóa/dịch vụ liên quan	Thông số kỹ thuật và các tiêu chuẩn
		khác nhau và trong các tenant khác nhau. - Cung cấp mức độ lưu trữ sự kiện khác nhau để lưu trữ, nén hoặc di chuyển các sự kiện đến các vùng lưu trữ khác nhau. - Giải pháp đã bao gồm tập luật phát hiện được hãng bảo mật nghiên cứu và phát triển trên ma trận MITRE ATT&CK với hơn 450 rules phát hiện các nguy cơ tấn công mạng hoặc các mối đe dọa an ninh mạng. - Giải pháp cho phép tạo các luật phát hiện với khả năng tạo luật bằng giao diện đồ hoặc và giao diện code. - Giải pháp cho phép thực hiện truy vấn để làm giàu thông tin từ nguồn thông tin an ninh mạng, các thông tin truy vấn liên quan đến IP, mã hash, URL/domain. - Làm giàu thông tin liên quan đến vị trí thông qua MaxMind/IP2Location - Giải pháp có khả năng làm giàu thông tin cho sự kiện thông qua các nguồn/cơ chế như: từ dữ liệu thám báo an ninh mạng (data feed), từ dữ liệu tìm kiếm truy vấn từ thám báo an ninh mạng (Lookup), từ thông tin về các thiết bị đầu cuối, thông tin về lỗ hổng phần mềm và các phần mềm được cài đặt trên thiết bị đầu cuối, từ thông tin về người dùng (tài khoản) từ Active Directorty, từ thông tin về FQDN hoặc IP từ DNS, từ thông tin

Hạng mục số	Tên hàng hóa/dịch vụ liên quan	Thông số kỹ thuật và các tiêu chuẩn
		về dữ liệu địa lý của IP, từ thông tin được tạo trong từ điển. - Giải pháp hỗ trợ tích hợp trực tiếp với hệ thống quản lý bảo mật tập trung cho thiết bị đầu cuối (Security Center); Giải pháp phải có khả năng tích hợp với hạ tầng Threat Intelligence (TI) hiện đang được triển khai bao gồm: - Hỗ trợ nền tảng phân tích và chuẩn hóa các mối đe dọa, cho phép cảnh báo và phản ứng khi có sự cố (Cyber Trace) và hệ thống tra cứu thông tin lỗ hổng, mối đe dọa an ninh mạng (Threat Lookup) - Từ giao diện web quản trị của giải pháp SIEM cho phép đội ngũ an ninh mạng thực hiện các hành động phản ứng sự cố. - Có khả năng phản ứng sự cố với các kịch bản tùy chỉnh (custom script). - Tích hợp và thực hiện các tác vụ liên quan đến hệ thống phòng chống mã độc; Tích hợp và thực hiện các hành động dựa trên hệ thống EDR; Tích hợp và phản ứng với Active Directory. - Hỗ trợ triển khai trên môi trường Kubernetes. - Hỗ trợ cơ chế định tuyến sự kiện (event routing) linh hoạt, với khả năng giám sát toàn bộ đường đi của sự kiện (event path).

Hạng mục số	Tên hàng hóa/dịch vụ liên quan	Thông số kỹ thuật và các tiêu chuẩn
		- Thông tin sự cố bảo mật bao gồm khả năng tùy chỉnh mức độ ưu tiên (mức độ nguy hiểm), giao sự cố bảo mật cho từng chuyên viên, thông tin các sự kiện liên quan sự cố bảo mật, thông tin thiết bị và người dùng liên quan… - Cho phép kết hợp nhiều sự kiện vào một sự cố bảo mật: cả tự động và thủ công - Thực hiện thu thập và cập nhật thông tin về thiết bị đầu cuối trong hạ tầng như: IP, MAC, danh sách phần mềm cài đặt, lỗ hổng, thông tin phần cứng… - Cho phép tùy chỉnh thêm các trường thông tin về thiết bị. - Giải pháp bao gồm tính năng kiểm toán thiết bị và theo dõi các sự kiện: khi có thiết bị được thêm vào, thay đổi các tham số của thiết bị (tên, IP, MAC, FQDN, Hệ điều hành), xóa thiết bị, thông tin về lỗ hổng được thêm vào thiết bị. - Cung cấp giao diện quản trị web với các biểu đồ thống kê, hiển thị cảnh báo, thông tin tài sản (thiết bị) - Cho phép tùy chỉnh mẫu báo cáo và mẫu giao diện dashboard. Cho phép tạo báo cáo và xuất ra định dạng HTML, CSV, XLSX. - Có khả năng hỗ trợ tự động phân tích lưu lượng lớp mạng, hỗ trợ

Hạng mục số	Tên hàng hóa/dịch vụ liên quan	Thông số kỹ thuật và các tiêu chuẩn
		không giới hạn lưu lượng mạng (network traffic flow per second). - Dịch vụ hỗ trợ kỹ thuật 24/7 (onsite), dịch vụ custom parser cho các sản phẩm, thiết bị đặc thù. - Bảo hành: 12 tháng.

1.3. Các yêu cầu khác

- Hàng hóa được bảo hành theo chính sách, tiêu chuẩn của nhà sản xuất.

- Có cam kết hỗ trợ kỹ thuật từ các chuyên gia của hãng trong quá trình triển khai và sử dụng.

- Có cam kết thực hiện việc lắp đặt, cấu hình, tích hợp hệ thống khi triển khai.

- Có cam kết hướng dẫn tập huấn cho Chủ đầu tư trong quá trình vận hành, sử dụng hàng hóa.

- Trong thời gian bảo hành, mọi sự cố của hàng hóa phải được nhà thầu cử cán bộ kỹ thuật đến xử lý khắc phục: Trong vòng 24 giờ kể từ khi nhận được thông báo của Chủ đầu tư, Nhà thầu phải có mặt để thực hiện các nghĩa vụ về bảo hành, hỗ trợ kỹ thuật, sửa chữa theo yêu cầu của Chủ đầu tư. Trường hợp không thể sửa chữa trong 48 giờ sau khi Nhà thầu đến kiểm tra sự cố thì phải có thiết bị thay thế tạm thời để không làm gián đoạn đến công việc. Nếu thiết bị phải gửi đi sửa chữa, mọi thủ tục và chi phí phát sinh khi gửi thiết bị đi và gửi trả thiết bị cho Chủ đầu tư sẽ do Nhà thầu chịu.

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: Kiểm tra về số lượng, chất lượng, chủng loại, xuất xứ, nhãn mác, năm sản xuất, thông số kỹ thuật. Sau đó tổ chức lắp đặt, cài đặt để chạy thử hàng hóa. Nhà thầu phải tiến hành kiểm tra, thử nghiệm hàng hóa trước khi nghiệm thu.