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

a. Giới thiệu về dự toán:

- Tên dự án : Hệ thống quản lý và phân tích sự kiện an toàn thông tin tập trung cho hệ thống Egov.

- Chủ đầu tư: Trung tâm Chuyển đổi số và Công nghệ chiến lược Đà Nẵng.

- Địa điểm thực hiện: Thành phố Đà Nẵng.

- Nguồn vốn: Ngân sách nhà nước năm 2025 (Theo Quyết định số 1602/QĐ-UBND ngày 22/5/2025 của UBND thành phố Đà Nẵng và Quyết định số 324/QĐ- SKHCN ngày 28/5/2025 của Giám đốc Sở Khoa học và Công nghệ thành phố Đà Nẵng).

b. Giới thiệu về gói thầu:

- Tên gói thầu: Mua sắm

- Giá gói thầu: 2.822.557.944 đồng.

- Nguồn vốn: Ngân sách nhà nước năm 2025 (Theo Quyết định số 1602/QĐ-UBND ngày 22/5/2025 của UBND thành phố Đà Nẵng và Quyết định số 324/QĐ- SKHCN ngày 28/5/2025 của Giám đốc Sở Khoa học và Công nghệ thành phố Đà Nẵng).

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

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

- Thời gian bắt đầu tổ chức lựa chọn nhà thầu: Quý IV năm 2025.

- Loại hợp đồng: Hợp đồng trọn gói.

- Thời gian thực hiện hợp đồng: 30 ngày

c. Mục tiêu công việc:

- Đầu tư Hệ thống quản lý và phân tích sự kiện an toàn thông tin tập trung cho hệ thống Egov (Lisence/03 năm);

- Mua sắm 01 bộ máy chủ SIEM hoặc tương đương và 04 thiết bị TAP Quang 10GB SFP+.

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:

1.2.1 Yêu cầu về kỹ thuật chung:

STT	Nội dung, yêu cầu
1.2.1.1	***Chủng loại, tiêu chuẩn, đặc điểm hàng hóa:*** - Thiết bị đồng bộ chính hãng, mới 100%, chưa qua sử dụng, nguyên đai, nguyên kiện và hoạt động tốt. - Tài liệu kỹ thuật, phụ kiện kèm theo và hướng dẫn sử dụng: theo tiêu chuẩn của nhà sản xuất. - Năm sản xuất: Sản xuất từ năm 2025 trở về sau. - Đáp ứng các yêu cầu cơ bản, tuân thủ và phù hợp với các quy định của Nhà nước, Bộ thông tin và truyền thông bao gồm: + Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015; + Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; + Thông tư 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông về việc quy định hoạt động giám sát an toàn hệ thống thông tin; + Quyết định Số 1127/QĐ-BTTTT ngày 30/7/2021 ban hành yêu cầu kỹ thuật cơ bản đối với sản phẩm quản lý và phân tích sự kiện an toàn thông tin; + Và các quy định liên quan khác. - Triển khai hệ thống quản lý và phân tích sự kiện an toàn thông tin tập trung nhằm đáp ứng quy định hệ thống thông tin cấp độ 3 trở lên theo hướng dẫn của Bộ Thông tin và Truyền thông tại Thông tư số 12/2022/TT-BTTTT và Công văn số 708/BTTTT-CATTT, đảm bảo tối thiểu các chức năng sau: - Thu thập, phân tích và quản lý log của các thiết bị mạng, bảo mật máy chủ, ứng dụng, thiết bị đầu cuối - Có chức năng quản trị: Chức năng phân tích tương quan (Correlation); Chức năng lọc (Filters), Tạo các luật (Rules), Chức năng hiển thị (Dashboards), Chức năng cảnh báo và báo cáo (Alerts and Reports), Chức năng cảnh báo thời gian thực (Real Time Alert). - Có chức năng nhận log: Cho phép nhận log từ các nguồn với nhiều định dạng khác nhau từ các thiết bị mạng, máy chủ và ứng dụng;

	định dạng, chuẩn hóa log nhận được theo các trường thông tin tùy biến theo nhu cầu sử dụng - Hệ thống kết nối, chia sẻ dữ liệu giám sát hệ thống mạng của thành phố đến Trung tâm giám sát an toàn không gian mạng Quốc gia NCSC. - Thành phần của giải pháp gồm 1 máy chủ và 1 phần mềm bản quyền 3 năm. Sau 3 năm vẫn hoạt động bình thường , không cập nhật các tính năng mới. - Thiết bị trích xuất lưu lượng mạng băng thông 1Gbps, tích hợp vào hệ thống quản lý. - Hệ thống đảm bảo cho hoạt động của chính quyền địa phương 02 cấp sắp đến và sẵn sàng cho sáp nhập 02 tỉnh, thành phố. - Phần mềm có bản quyền bản quyền 3 năm. Sau 3 năm vẫn hoạt động bình thường.
1.2.1.2	***Kiểm tra, thử nghiệm, đóng gói, vận chuyển:*** - Vận chuyển, lắp đặt, hướng dẫn sử dụng và bàn giao tại rung tâm Dữ liệu, thành phố Đà Nẵng, tầng 19, 02 Quang Trung, phường Hải Châu, thành phố Đà Nẵng; - Cung cấp đầy đủ tài liệu kỹ thuật, phụ kiện kèm theo và hướng dẫn dử dụng.
1.2.1.3	Tiến độ giao hàng, ngày hoàn thành dịch vụ: Theo yêu cầu tại Mẫu số 01A Chương IV.
1.2.1.4	Thời gian bảo hành theo tiêu chuẩn nhà sản xuất nhưng không thấp hơn 12 tháng đối với hàng hóa là "Máy chủ hệ thống" và "Thiết bị TAP Quang"; cam kết về Dịch vụ bảo trì theo chính sách bảo trì của hãng cung cấp đối với "Phần mềm quản lý và phân tích sự kiện an toàn thông tin tập trung cho hệ thống Egov"

1.2.2 Yêu cầu cụ thể về tính năng phần mềm:

STT	Giải pháp	Số lượng	Yêu cầu kỹ thuật tối thiểu
1.2.2.1	Hệ thống quản lý và phân tích sự kiện an toàn	1	Giải pháp Quản lý và phân tích sự kiện an toàn thông tin tập trung có các chức năng chính: 1. Thu thập, phân tích và quản lý log - Các thiết bị mạng, thiết bị bảo mật như: Router,

	thông tin tập trung cho hệ thống Egov		Switch, Firewall/IPS/IDS, Sandbox, WAF, Network APT... - Các máy chủ hệ thống (cả máy chủ vật lý và ảo hóa) trên các nền tảng khác nhau: Windows, Linux, Unix… - Các ứng dụng: (1) Ứng dụng phục vụ hoạt động của hệ thống: DHCP, DNS, NTP, VPN, Proxy Server…; (2) Ứng dụng cung cấp dịch vụ: Web, Mail, FPT, TFTP và các hệ quản trị cơ sở dữ liệu Oracle, SQL, MySQL... - Các thiết bị đầu cuối: Máy tính người sử dụng, máy in, máy fax, IP Phone, IP Camera… - Điểm giám sát trên đường truyền: Điểm giám sát biên tại giao diện kết nối của thiết bị định tuyến biên với các mạng bên ngoài; điểm giám sát tại mỗi vùng mạng của hệ thống 2. Tự động chuẩn hóa log - Tự động chuẩn hóa các dạng log nhận được từ các thiết bị, ứng dụng - Tự động cập nhật các định dạng log mới từ Cloud 3. Phát hiện tấn công mạng - Phát hiện tấn công mạng dựa vào phân tích log truy cập ứng dụng Web - Phát hiện truy vấn tên miền độc hại dựa vào phân tích log truy vấn DNS - Phát hiện kết nối tới các địa chỉ IP độc hại dựa vào phân tích log kết nối của các thiết bị và hệ điều hành - Dấu hiệu Phát hiện tấn công ứng dụng Web, danh sách tên miền và địa chỉ độc hại được cập nhật tự động từ Cloud 4. Tích hợp Threat Intelligence

			- Tích hợp Chức năng Threat Intelligence - Cập nhật dữ liệu Threat Intelligence từ Cloud - Tự động cập nhật BlackList (IP, Domain, Hash) Cho SIEM từ dữ liệu Threat Intelligence - Cho phép chia sẻ thông tin với các hệ thống Threat Intelligence khác 5. Tích hợp các tính năng quản lý các điểm yếu về bảo mật (Vulnerability Management) - Tích hợp Chức năng Quản lý điểm yếu an toàn thông tin (lớp hệ điều hành, lớp ứng dụng…) - Tự động cảnh báo khi Phát hiện điểm yếu an toàn thông tin trong hệ thống - Cho phép thiết lập chính sách bản vá ảo để bảo vệ hệ thống - Tích hợp Chức năng tra cứu thông tin lỗ hổng, điểm yếu (CVE) 6. Quản lý Ticket và tự động hóa quy trình xử lý sự cố - Tự động tạo Ticket, Quản lý, cảnh báo tới từng Tier - Tự động thu thập, phân tích, tổng hợp thông tin và thực thi chính sách chặn tấn công 7. Xử lý, phân tích tương quan - Behavior Detection - Cho phép thiết lập các luật phân tích tương quan giữa các nguồn log khác nhau để phát hiện tấn công mạng phức tạp, có chủ đích. - Cho phép phát hiện các hành vi tấn công có chủ đích của tin tặc thông qua phân tích các hành động mà tin tặc tác động vào hệ thống. - Cho phép thực biện các Play Book của SOAR để tự động xác minh và xử lý sự cố. - Cho phép cập nhật tri thức về các hành vi dị thường,

			tấn công mạng có chủ đích - Cho phép cập nhật tri thức về các hành vi dị thường, tấn công mạng có chủ đích từ Cloud - Chuẩn hóa các dạng tấn công mạng theo các kỹ thuật Mitre ATT&CK 8. Cảnh báo và tự động ngăn chặn tấn công - Tự động cảnh báo tấn công qua SMS, Email… - Hệ thống cung cấp khả năng tương tác với thiết bị mạng (Router Cisco – Juniper, Firewall Cisco PIX – ASA, Firewall Check-Point, Firewall Forgtinet,..), Thiết bị bảo mật (Firewall, NAC, IDS, IPS) và hệ điều hành (Windows Server 2008, 2012, 2019, 2022, Linux Centos, Fedora, Ubuntu, Debian, Linux Transparent Firewall …) để thực hiện ngăn chặn tấn công mạng - Khả năng này cho phép hệ thống có thể ngăn chặn tấn công mạng mà không làm ảnh hưởng tới hoạt động và hiệu năng của hệ thống và không yêu cầu cài đặt Agent trên các thiết bị hay máy chủ 9. Điều tra và phân tích sự cố - Cho phép phân tích log mức sâu theo từng tường thông tin - Cho phép viết luật tương quan để phát hiện và điều tra tấn công, sự cố - Cho phép phân tích và điều tra sự cố thông qua giao diện trực quan 10. Chức năng quản trị hệ thống - Chức năng Dashboard cho phép người quản trị có thông tin tổng quan về hệ thống - Chức năng Event Map cho phép hiển thị trực quan theo thời gian thực tấn công mạng

			- Chức năng tạo báo cáo cho phép người quản trị tạo ra các báo cáo tùy biến theo từng điều kiện cụ thể theo các định dạng khác nhau - Quản lý cấu hình hệ thống - Quản lý các tài khoản quản trị hệ thống - Quản lý cập nhật phần mềm hệ thống từ Cloud - Thông tin trạng thái hệ thống - Quản lý logs hoạt động trên hệ thống - Shutdown và Restart hệ thống - Quản trị hệ thống thông qua giao diện Console và SSH 11. Chức năng quản lý và cảnh báo máy tính trong mạng botnet - Quản lý thời gian thực các máy tính trong mạng có kết nối đến máy chủ C&C trong mạng botnet - Quản lý các đối tượng trong mạng theo IP Objects - Quản lý cảnh báo tự động các IP Objects trong mạng botnet - Tự động xác minh, làm giàu thông tin và điều tra sự cố 12. Quản lý Logs và chia sẻ dữ liệu - Chức năng chia sẻ, quản lý log tập trung trên SIEM của các hãng khác nhau - Chức năng chia sẻ, quản lý log tập trung trên NOC - Quản lý Log Offline và tự động xử lý Log theo chính sách thiết lập - Chia sẻ dữ liệu về hệ thống Giám sát không gian mạng quốc gia 13. Năng lực xử lý: Năng lực xử lý tối thiểu 05 Gbps trên 1 ngày vẫn hoạt động bình thường.

1.2.3 Yêu cầu danh mục thiết bị đầu tư

STT	Giải pháp	Số lượng	Yêu cầu kỹ thuật tối thiểu
1.2.3.1	Thiết bị phần cứng máy chủ cài đặt giải pháp	1	Mua sắm máy chủ có cấu hình (hoặc tương đương): Thiết bị phần cứng máy chủ SIEM - Máy chủ rackmount 1U - Bộ vi xử lý CPU: **+ Số lượng**: Tối thiểu 2 bộ xử lý. **+ Số lõi và luồng**: Mỗi bộ xử lý có tối thiểu **16 lõi (cores)** và **32 luồng (threads)** để xử lý đa nhiệm hiệu quả. + **Tần số xử lý**: Tần số cơ bản tối thiểu **2.8 GHz**, có khả năng tăng tốc (turbo boost) lên tần số cao hơn để xử lý các tác vụ nặng. + **Bộ nhớ đệm (Cache)**: Tối thiểu **30 MB** trở lên trên mỗi bộ xử lý để tăng tốc độ truy cập dữ liệu. - Bộ nhớ truy cập ngẫu nhiên RAM: + **Dung lượng**: Tối thiểu **128GB**. + **Số lượng thanh**: Bao gồm 4 thanh bộ nhớ, mỗi thanh có dung lượng **32GB**. + **Loại bộ nhớ**: Sử dụng công nghệ **DDR5** với tốc độ bus tối thiểu **5600 MT/s** (Mega Transfers per second) hoặc cao hơn. + **Cấu trúc thanh**: **Dual Rank** (x8), cho phép tăng hiệu quả truyền dữ liệu. - Ổ cứng SSD: ≥ 3 x 960GB (960GB SATA 6G Mixed Use SFF BC Multi Vendor SSD) - Ổ cứng HDD: ≥ 5 x 2.4TB (2.4TB SAS 12G Mission Critical 10K SFF BC 3-year Warranty

			512e Multi Vendor HDD) - Card điều khiển ổ cứng hỗ trợ Raid: 0,1 - Card mạng: **+ Kết nối tốc độ cao**: Một **card mạng 2 cổng tốc độ 10 Gigabit Ethernet (GbE)** sử dụng giao diện **SFP+**. Mỗi cổng này đều đi kèm một bộ thu phát quang **10Gb SFP+ SR**, cho phép máy chủ kết nối với hạ tầng mạng tốc độ cao, lý tưởng cho việc truyền tải lượng lớn dữ liệu một cách nhanh chóng. **+ Kết nối đa cổng**: Một **card mạng 4 cổng tốc độ 1 Gigabit Ethernet (GbE)** sử dụng chuẩn **BASE-T** (cổng RJ45). Card này có chuẩn **OCP3**, cho phép lắp đặt trực tiếp lên bo mạch chủ, giúp tiết kiệm không gian và tối ưu hóa luồng khí bên trong máy chủ. Các cổng này phù hợp cho việc kết nối với các thiết bị quản lý hoặc các mạng nội bộ thông thường. - Bảo hành 36 tháng theo tiêu chuẩn nhà sản xuất
1.2.3.1	Thiết bị TAP	4	Thiết bị TAP Quang có cấu hình hoặc tương đương: 10GB SFP+ Optical TAP, 1 Link MM 850/1300nm LC, 2 Monitor Ports LC; ½ 19” rackmount housing, splitting ratio 50%/50% (rackmount kit not included) Bảo hành 12 tháng.

1.2.4 Mặt bằng và vị trí triển khai tại Trung tâm dữ liệu Đà Nẵng

- Thiết bị SIEM sẽ được lắp đặt trong tủ rack chuyên dụng, bố trí tại khu vực trung tâm phòng máy, nơi có sẵn các kết nối mạng nội bộ với các thiết bị bảo mật (Firewall, IDS/IPS), thiết bị mạng (switch/router) và các máy chủ ứng dụng. Vị trí

lắp đặt đảm bảo thuận tiện cho việc thu thập log từ các hệ thống liên quan và dễ dàng tích hợp với các thiết bị mạng hiện có thông qua các cổng kết nối mạng (LAN, SPAN port hoặc mirror port).

- Bổ sung thiết bị NAS để lưu trữ log tập trung khi cần thiết: Hệ thống hiện đã trang bị sẵn 05 thiết bị NAS, mỗi thiết bị có dung lượng khả dụng 100TB. Tổng dung lượng lưu trữ hiện tại đạt 500TB. Dung lượng này đáp ứng nhu cầu lưu trữ hiện tại và trong tương lai gần.

- Hệ thống được bố trí tại khu vực Trung tâm dữ liệu có đầy đủ các điều kiện về:

- Nguồn điện: được cấp nguồn liên tục từ hệ thống UPS và máy phát điện dự phòng.

- Điều hòa nhiệt độ: nằm trong vùng có luồng gió lạnh trực tiếp từ hệ thống điều hòa chính (CRAC), đảm bảo thiết bị hoạt động trong môi trường nhiệt độ ổn định.

- Quản lý cáp và truy xuất bảo trì: thiết bị được kết nối qua hệ thống quản lý cáp mạng, cáp nguồn đảm bảo tiêu chuẩn, thuận tiện trong công tác giám sát, vận hành và bảo trì hệ thống.

1.2.5 Yêu cầu giải pháp công nghệ

a) Giải pháp công nghệ triển khai Dự án:

Giải pháp công nghệ được xây dựng nhằm triển khai hệ thống quản lý và phân tích sự kiện an toàn thông tin tập trung (SIEM) cho hệ thống Egov. Các chức năng chính bao gồm:

- Thu thập Log: Từ thiết bị mạng, máy chủ, ứng dụng, và thiết bị đầu cuối thông qua các giao thức chuẩn như Syslog, SNMP, và Agent-based

- Phân tích log: Xử lý, chuẩn hóa và tương quan dữ liệu để phát hiện các nguy cơ tiềm ẩn.

- Cảnh báo và báo cáo: Tự động phát hiện các hành vi bất thường, đưa ra cảnh báo theo thời gian thực và cung cấp báo cáo chi tiết theo yêu cầu.

b) Phương án lựa chọn:

Trước tình hình an toàn thông tin và những mối rủi ro tiềm ẩn và đe dọa hằng ngày, hệ thống mạng của các doanh nghiệp cũng thay đổi liên tục không ngừng. Bất cứ tổ chức doanh nghiệp nào hoặc bất kể ngành công nghiệp nào cũng đều cần phải đảm bảo rằng tài sản công nghệ và dữ liệu của họ đang được bảo vệ một cách hiệu quả. Tuy nhiên điều này không thể được đảm bảo hoàn toàn bằng việc chỉ quan tâm đầu tư các sản phẩm an ninh phòng thủ một mình mà việc đảm bảo an ninh phải được triển khai kết hợp giữa các sản phẩm phòng thủ và giám sát an ninh một cách chặt chẽ, theo một chiến lược an ninh thông tin toàn diện, và được thiết kế theo mô hình chuẩn để giảm thiểu rủi ro thông tin một cách tổng thể.

Bên cạnh việc triển khai các giải pháp phòng thủ truyền thống, việc giám sát, đánh giá và nhận diện sớm các nguy cơ mất an toàn thông tin là yếu tố then chốt trong chiến lược bảo mật toàn diện của mỗi tổ chức, doanh nghiệp. Trong quá trình xây dựng và vận hành hệ thống CNTT, không thể đảm bảo tuyệt đối rằng hệ thống sẽ luôn an toàn trước các mối đe dọa đang ngày càng tinh vi và liên tục biến đổi. Do đó, việc triển khai một hệ thống quản lý và phân tích sự kiện an toàn thông tin tập trung (SIEM) cho hệ thống Egov là rất cần thiết.

Hệ thống SIEM cho Egov cho phép tổ chức giám sát liên tục các hoạt động trong hệ thống, đồng thời thu thập và phân tích dữ liệu log từ nhiều nguồn khác nhau, nhằm phát hiện các hành vi bất thường hoặc tiềm ẩn nguy cơ mất an toàn. Thông qua các cơ chế cảnh báo thông minh và khả năng phân tích tương quan sự kiện, hệ thống giúp xác định chính xác các rủi ro bảo mật và lỗ hổng trong hệ thống, từ đó hỗ trợ các bộ phận kỹ thuật đưa ra hành động khắc phục kịp thời.

Bên cạnh đó, với việc tích hợp các công cụ đánh giá tự động và công nghệ học máy (machine learning), hệ thống SIEM cho Egov còn giúp đánh giá toàn diện mức độ nghiêm trọng của từng lỗ hổng, phân loại nguy cơ và hỗ trợ quá trình ưu tiên xử lý. Điều này không chỉ tăng cường hiệu quả vận hành hệ thống mà còn giảm thiểu đáng kể thiệt hại do các sự cố an toàn thông tin gây ra

1.2.5.2 Yêu cầu giải pháp:

STT	Nội dung yêu cầu	Yêu cầu tối thiểu

1.2.5.2.1	Thu thập và quản lý log theo tời gian thực	Thu thập, phân tích và quản lý log của các thiết bị mạng, bảo mật máy chủ, ứng dụng, thiết bị đầu cuối
1.2.5.2.2	Chức năng quản trị	Chức năng phân tích tương quan (Correlation)
		Chức năng lọc (Filters)
		Tạo các luật (Rules)
		Chức năng hiển thị (Dashboards)
		Chức năng cảnh báo và báo cáo (Alerts and Reports)
		Chức năng cảnh báo thời gian thực (Real Time Alert)
1.2.5.2.3	Có chức năng nhận log	Cho phép nhận log từ các nguồn với nhiều định dạng khác nhau từ các thiết bị mạng, máy chủ và ứng dụng; định dạng, chuẩn hóa log nhận được theo các trường thông tin tùy biến theo nhu cầu sử dụng
1.2.5.2.4	Chia sẻ dữ liệu	Hệ thống kết nối, chia sẻ dữ liệu giám sát hệ thống mạng của thành phố đến Trung tâm giám sát an toàn không gian mạng Quốc gia NCSC.
1.2.5.2.5	Bản quyền	Thành phần của giải pháp gồm 1 máy chủ và 1 phần mềm bản quyền 3 năm. Sau 3 năm vẫn hoạt động bình thường.
1.2.5.2.6	Phân tích lưu lượng mạng	Thiết bị trích xuất lưu lượng mạng băng thông 1Gbps, tích hợp vào hệ thống quản lý
1.2.5.2.7	Khả năng nâng cấp	- Hệ thống đảm bảo cho hoạt động của chính quyền địa phương 02 cấp sắp đến và sẵn sàng cho sáp nhập 02 tỉnh, thành phố

1.3. Các yêu cầu khác

1.3.1 Phương án thi công đảm bảo ATTT

Hệ thống quản lý và phân tích sự kiện an toàn thông tin tập trung (SIEM) cho hệ thống Egov đề xuất triển khai trên hạ tầng Trung tâm dữ liệu. Khi triển khai cài đặt và cấu hình hệ thống SIEM, cần đảm bảo giải pháp có khả năng thu thập, phân tích và tương quan sự kiện bảo mật từ các thành phần trong toàn bộ hệ thống Egov tại thời điểm thực tế. Mục tiêu chính là phát hiện sớm các hành vi tấn công, các dấu hiệu bất thường và hỗ trợ xử lý sự cố an toàn thông tin một cách kịp thời và chính xác.

Hệ thống đảm bảo khả năng thu thập nhật ký (log) từ các thiết bị và máy chủ tại từng phân vùng mạng. Việc cấu hình tích hợp sẽ được thực hiện với các thiết bị mạng, máy chủ ứng dụng, hệ điều hành, hệ thống firewall, IDS/IPS và các nền tảng giám sát khác.

Toàn bộ dữ liệu log sau khi thu thập sẽ được chuẩn hóa, lưu trữ tập trung, đồng thời áp dụng các quy tắc phân tích và tương quan nhằm phát hiện các mối đe dọa tiềm ẩn hoặc dấu hiệu tấn công trong hệ thống. Ngoài ra, giải pháp SIEM cũng hỗ trợ hiển thị dữ liệu theo thời gian thực thông qua giao diện dashboard trực quan và cung cấp báo cáo hỗ trợ công tác giám sát và điều tra số sau sự cố.

Hệ thống SIEM cho hệ thống Egov được thiết kế triển khai tại Trung tâm Dữ liệu với kiến trúc tập trung, đảm bảo khả năng thu thập, xử lý, phân tích và cảnh báo các sự kiện an toàn thông tin một cách toàn diện và kịp thời. Kiến trúc tổng thể bao gồm các thành phần chính như sau:

a) Các nguồn sinh log (Log Sources)

Đây là các thành phần trong hệ thống của Trung tâm dữ liệu tạo ra dữ liệu nhật ký (log), bao gồm:

Thiết bị mạng: Firewall, Switch, Router, Load Balancer…

Thiết bị bảo mật: IDS/IPS, WAF, Anti-virus, DLP…

Máy chủ hệ điều hành: Windows Server, Linux Server…

Ứng dụng: Web Server, Database Server, Email Server…

Thiết bị đầu cuối (Endpoint): Máy trạm người dùng, Laptop…

Hệ thống ảo hóa và Cloud (nếu có)

Các thiết bị này được cấu hình để gửi log về hệ thống SIEM thông qua các giao thức chuẩn như Syslog, Agent-based hoặc Log Forwarder.

b) Hệ thống thu thập log (Collector/Forwarder/Agent)

Các agent được cài đặt trên các máy chủ và thiết bị đầu cuối để thu thập log hệ thống và gửi về SIEM.

Log Forwarder được triển khai tại các phân vùng mạng để chuyển tiếp log đến hệ thống SIEM, hỗ trợ cả log dạng plaintext và định dạng chuẩn hóa (JSON, CEF,…).

Hệ thống có thể hỗ trợ trích xuất dữ liệu lưu lượng mạng từ thiết bị NetFlow hoặc TAP để phân tích hành vi.

c) Máy chủ phân tích SIEM (SIEM Core Server)

Đây là trung tâm của giải pháp, gồm các chức năng:

Thu thập và chuẩn hóa log: Các log nhận được sẽ được xử lý, định dạng thống nhất và lưu trữ có tổ chức.

Phân tích tương quan (Correlation Engine): So sánh các sự kiện từ nhiều nguồn để xác định hành vi tấn công phức tạp, như brute force, lateral movement, data exfiltration,...

Cảnh báo thời gian thực (Real-time Alerting): Khi phát hiện các sự kiện nghi ngờ, hệ thống sẽ gửi cảnh báo ngay qua email, SMS, dashboard hoặc tích hợp ITSM.

Giao diện trực quan (Dashboard): Cung cấp giao diện web hiển thị biểu đồ, thống kê, bản đồ sự kiện an ninh.

Báo cáo định kỳ và tức thời: Tạo báo cáo theo mẫu hoặc theo yêu cầu của người dùng.

Lưu trữ log dài hạn (Log Archive): Đảm bảo đáp ứng yêu cầu về pháp lý, điều tra, kiểm toán và phục hồi sự cố.

d) Hệ thống tích hợp giám sát quốc gia (NCSC)

Hệ thống SIEM có tích hợp gửi dữ liệu log và cảnh báo đến Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) theo định dạng yêu cầu.

Đảm bảo tuân thủ chính sách chia sẻ dữ liệu và an toàn bảo mật thông tin quốc gia.

e) Quản trị và phân quyền người dùng

Người dùng được phân quyền theo vai trò (admin, analyst, viewer,...).

Hệ thống có chức năng xác thực mạnh (multi-factor authentication), ghi nhận nhật ký truy cập và thao tác người dùng.

f) Hạ tầng triển khai và an toàn hệ thống

Hệ thống SIEM được cài đặt trên một máy chủ riêng biệt tại Trung tâm dữ liệu, có tính toán dung lượng lưu trữ, sử dụng phần mềm bản quyền có hiệu lực trong 3 năm.

Hạ tầng mạng giữa các thành phần được bảo mật qua các VLAN riêng, VPN hoặc tunneling khi cần gửi log từ xa.

Các giải pháp backup và HA có thể được tích hợp nếu yêu cầu độ sẵn sàng cao.

1.3.2. Phương án tổ chức thực hiện, đưa vào vận hành khai thác

1.3.2.1. Hệ thống quản lý và phân tích sự kiện an toàn thông tin tập trung (SIEM) cho hệ thống Egov sẽ được sử dụng như một công cụ chủ lực trong công tác giám sát, phát hiện sớm và điều tra các sự cố an toàn thông tin trên hệ thống Egov tại Trung tâm dữ liệu. Cụ thể, phương án sử dụng giải pháp SIEM bao gồm các nội dung chính sau:

a) Giám sát tập trung:

Toàn bộ log từ các thiết bị mạng (router, switch), thiết bị bảo mật (firewall, IDS/IPS), máy chủ, máy trạm và các hệ thống ứng dụng sẽ được chuyển về hệ thống SIEM theo thời gian thực.

Các agent hoặc log forwarder sẽ được triển khai tại các thiết bị/ứng dụng cần giám sát nhằm đảm bảo khả năng thu thập log chính xác và đầy đủ.

b) Phân tích và tương quan dữ liệu:

Hệ thống SIEM sẽ tiến hành phân tích tự động các log thu thập được, thực hiện việc tương quan các sự kiện từ nhiều nguồn để xác định các hành vi đáng ngờ, dấu hiệu tấn công hoặc các rủi ro bảo mật tiềm ẩn.

Sử dụng các luật phát hiện mặc định kết hợp với các luật tùy chỉnh theo đặc thù hệ thống nhằm nâng cao hiệu quả giám sát.

c) Cảnh báo và phản ứng:

Thiết lập hệ thống cảnh báo tự động qua email/SMS khi phát hiện các sự kiện an ninh nghiêm trọng, giúp cán bộ quản trị kịp thời nắm bắt và xử lý.

Cảnh báo được phân loại theo mức độ ưu tiên (thấp, trung bình, cao, nghiêm trọng), hỗ trợ quy trình xử lý theo từng cấp độ.

d) Báo cáo và truy vết:

Hệ thống hỗ trợ tạo báo cáo định kỳ (ngày/tuần/tháng) và báo cáo theo yêu cầu, phục vụ công tác kiểm tra, đánh giá và lập hồ sơ tuân thủ.

Cung cấp khả năng truy vết sự kiện, giúp cán bộ kỹ thuật điều tra nguyên nhân và phạm vi ảnh hưởng khi xảy ra sự cố.

e) Tích hợp với các hệ thống hiện có:

Hệ thống SIEM có thể tích hợp với các hệ thống Kaspersky Endpoint hoặc các nền tảng bảo mật khác để nâng cao hiệu quả vận hành và phản ứng sự cố.

Hỗ trợ chia sẻ dữ liệu với Trung tâm Giám sát An toàn không gian mạng quốc gia (NCSC) nhằm đảm bảo tuân thủ và phối hợp trong công tác phòng chống tấn công mạng.

f) Đào tạo và vận hành:

Sau khi triển khai, cán bộ kỹ thuật sẽ được đào tạo sử dụng hệ thống, từ quản trị, cấu hình đến xử lý cảnh báo.

Xây dựng quy trình vận hành tiêu chuẩn (SOP) nhằm đảm bảo hệ thống SIEM hoạt động liên tục, ổn định và hiệu quả.

1.3.2.2. Triển khai cài đặt đưa vào sử dụng

a) Khảo sát hệ thống và xác định yêu cầu

- Thu thập thông tin về hạ tầng mạng, các thiết bị bảo mật, hệ điều hành, máy chủ, ứng dụng cần giám sát.

- Xác định số lượng log source, dung lượng log trung bình/ngày để thiết kế kiến trúc phù hợp.

- Phân tích yêu cầu bảo mật và phân loại mức độ ưu tiên giám sát.

b) Lập kế hoạch triển khai

- Xác định kiến trúc hệ thống SIEM (triển khai tập trung hoặc phân tán).

- Lập sơ đồ triển khai: vị trí máy chủ SIEM, log forwarder, agent thu thập log.

- Lên kế hoạch thời gian, nhân sự, phân vùng mạng, tài nguyên máy chủ phục vụ cài đặt.

c) Chuẩn bị hạ tầng

- Cài đặt hệ điều hành và chuẩn bị môi trường cho máy chủ SIEM (vật lý hoặc ảo hóa).

- Cấu hình mạng, phân quyền truy cập, thiết lập firewall rule cho các cổng cần thiết.

- Kiểm tra khả năng kết nối giữa máy chủ SIEM và các nguồn log.

d) Cài đặt hệ thống SIEM

- Tiến hành cài đặt phần mềm SIEM

- Cấu hình các thành phần: bộ xử lý log, cơ sở dữ liệu, dashboard quản trị, công cụ phân tích.

- Thiết lập các rule mặc định để phát hiện sự kiện an ninh.

e) Cấu hình thu thập log

- Cài đặt và cấu hình các agent hoặc log forwarder trên máy chủ, thiết bị mạng, thiết bị bảo mật.

- Thiết lập định dạng log, tần suất gửi log, phương thức truyền log (Syslog, Filebeat, Winlogbeat...).

- Kiểm tra việc gửi log và xác minh dữ liệu thu thập chính xác.

f) Xây dựng các rule phát hiện sự kiện

- Tùy chỉnh các rule cảnh báo theo yêu cầu của chủ đầu tư.

- Thiết lập các mốc cảnh báo theo độ nghiêm trọng, kịch bản tấn công, hành vi bất thường.

- Tích hợp các nguồn IOC (Indicators of Compromise) nếu có.

g) Thiết lập dashboard và cảnh báo

- Xây dựng các bảng điều khiển trực quan theo nhóm thiết bị, loại log, tình trạng sự kiện.

- Thiết lập cảnh báo qua email, SMS hoặc tích hợp với hệ thống quản lý sự cố.

- Kiểm thử các cảnh báo để đảm bảo hoạt động chính xác.

h) Kiểm thử và hiệu chỉnh

- Kiểm tra hệ thống hoạt động ổn định, đầy đủ các chức năng theo yêu cầu.

- Hiệu chỉnh cấu hình, tối ưu hiệu suất và độ chính xác của cảnh báo.

- Ghi nhận log mẫu để huấn luyện hệ thống và giảm thiểu cảnh báo giả.

i) Đào tạo, bàn giao và vận hành

- Đào tạo đội ngũ cán bộ kỹ thuật cách sử dụng, giám sát và xử lý cảnh báo.

- Bàn giao tài liệu cài đặt, cấu hình, hướng dẫn sử dụng và quy trình vận hành chuẩn.

- Thiết lập lịch bảo trì, cập nhật định kỳ và giám sát thường xuyên.

1.3.3. Biện pháp tổ chức thi công

a) Trước khi thi công

- Đơn vị thi công phải lập kế hoạch thi công để đảm bảo thi công đúng thiết kế, quy trình, quy phạm. Thi công đúng tiến độ, khối lượng và kỹ thuật yêu cầu.

- Tất cả các loại vật tư, thiết bị, dụng cụ, vật liệu trước khi sử dụng phải được nghiệm thu về chất lượng và số lượng đúng thiết kế. Quá trình lưu kho phải phân công người quản lý và bảo dưỡng theo quy trình, quy phạm bảo quản vật tư thiết bị.

- Phải thực hiện quy trình kiểm thử trước khi thi công.

- Chuẩn bị đầy đủ nhân lực (có phân công nhiệm vụ cụ thể), các phương tiện, dụng cụ thi công chuyên dùng và các vật liệu phù hợp trước khi thi công.

- Đảm bảo đầy đủ các biện pháp an toàn trước giờ thi công: phiếu công tác, đồ bảo hộ lao động và các thủ tục đăng ký công tác khác theo quy định hiện hành.

b) Trong quá trình thi công

- Khi thi công cần có phương án đảm bảo an toàn công trình, an toàn lao động, chú ý bảo vệ tài sản của nhân dân và của Nhà nước tại những vị trí thi công.

- Khi thi công phải liên hệ chặt chẽ với đơn vị quản lý tài sản, cơ sở vật chất trên tuyến và các cơ quan hữu quan.

- Đơn vị thi công phải cử người hướng dẫn các khu vực đông người qua lại. Phải có biển báo công trường đang thi công, người giám sát tại nơi tập kết vật tư.

c) Sau khi thi công

- Tổ chức nghiệm thu

- Lập hồ sơ hoàn công theo đúng biểu mẫu quy định.

1.3.4. An toàn lao động

Ngoài việc chấp hành quy định an toàn với những quy định của các đơn vị liên quan đến công trình này, đơn vị thi công cần lưu ý:

- Đơn vị thi công phải khảo sát kỹ hiện trường và nghiên cứu kỹ hồ sơ Thiết kế thi công và dự toán kinh phí sau đó có phương án thi công hợp lý mới tiến hành thi công.

- Trong suốt quá trình thi công phải liên hệ chặt chẽ với các đơn vị có liên quan nhằm đảm bảo an toàn về người, vật tư thiết bị cho công trình và các công trình khác có liên quan.

- Bố trí nhân lực hợp lý cho từng phần việc, đặc biệt lắp đặt cáp trong những khu vực phức tạp.

- Khi thi công phải có biển cảnh báo và người cảnh giới an toàn.

1.3.5. Hướng dẫn, bàn giao quản trị các hệ thống

1.3.5.1. Mục tiêu

Hướng dẫn và chuyển giao công nghệ cho đơn vị quản lý, vận hành hệ thống luôn là công việc hết sức hệ trọng trong mỗi dự án. Các dự án lớn và quan trọng thì việc hướng dẫn và chuyển giao công nghệ là cực kỳ cần thiết và không thể thiếu trong dự án. Với các nhà thầu uy tín, có đội ngũ kỹ sư triển khai, có kinh nghiệm Hướng dẫnchuyên nghiệp, kỹ năng trình bày tốt sẽ giúp đơn vị tiếp nhận chuyển giao bổ sung tốt kiến thức, công nghệ, qua đó giảm chi phí bảo hành, bào trì và khắc phục sự cố đối với hệ thống.

Đối với các thiết bị trong dự án này, việc hướng dẫn tập trung chủ yếu kỹ năng cho các quản trị hệ thống và cán bộ phụ trách CNTT.

Mục tiêu cụ thể:

+ Cung cấp kiến thức, công nghệ dựa trên việc cài đặt.

+ Giúp đội ngũ vận hành tham gia có thể nắm bắt tính năng, nguyên tắc hoạt đột của việc cấu hình và cài đặt thiết bị.

+ Nâng cao kỹ năng cài đặt, nâng cấp và cấu hình những tính năng cơ bản trên thiết bị.

+ Có khả năng quản trị hệ thống, khắc phục một số lỗi cơ bản trên thiết bị và hệ thống.

Hướng dẫn tại chỗ:

+ Trong quá trình cài đặt, cấu hình và xử lý hệ thống, các cán bộ kỹ thuật của nhà thầu sẽ trực tiếp hướng dẫn thao tác cấu hình, thiết lập và kết nối từng thiết bị, qua đó học viên sẽ được tiếp thu trực tiếp kiến thức, nguyên lý hoạt động và thực hành trên thiết bị, đảm bảo mang lại kiến thức sâu sát nhất đối với hệ thống.

+ Khóa học sẽ được thực hiện trên mỗi hệ thống.

Hướng dẫn cán bộ:

+ Các chuyên gia đã được hướng dẫn cấu hình theo các thiết bị của nhà sản xuất, đảm bảo đủ kiến thức để cấu hình, quản trị thiết bị trong dự án.

1.3.5.2. Phương pháp

Tùy thuộc vào quy mô và hạng mục công nghệ trong dự án mà nhà thầu đưa ra khóa hướng dẫn phù hợp. Trong dự án này tư vấn đề xuất khóa hướng dẫn như sau:

- Hình thức đào tạo: Hướng dẫn tập trung;

- Vị trí: tại Trung tâm Dữ liệu, thành phố Đà Nẵng, tầng 19, 02 Quang Trung, phường Hải Châu, thành phố Đà Nẵng;

- Tài liệu giảng dạy: Tài liệu giảng dạy được chuẩn bị theo mỗi khóa

- Giảng viên: Người có kinh nghiệm trong lĩnh vực quản trị mạng và có chứng chỉ chứng chỉ về ATTT như CEH, CHFI, CISM hoặc chứng chỉ khác tương đương trở lên

- Yêu câu cầu đối với học viên:

+ Có kiến thức về hệ thống mạng máy tính;

+ Có kiến thức về hệ thống mạng và hệ thống viễn thông;

+ Có kiến thức về quản trị mạng;
+ Đọc và hiểu tiếng anh kỹ thuật;
+ Kỹ năng sử dụng máy tính;

1.3.5.3. Nội dung hướng dẫn

- Đào tạo đội ngũ cán bộ kỹ thuật cách sử dụng, giám sát và xử lý cảnh báo.

- Bàn giao tài liệu cài đặt, cấu hình, hướng dẫn sử dụng và quy trình vận hành chuẩn.

- Thiết lập lịch bảo trì, cập nhật định kỳ và giám sát thường xuyên.

1.3.6. Yêu cầu về giải pháp kỹ thuật, biện pháp tổ chức cung cấp, lắt đặt hàng hóa:

Trong Hồ sơ dự thầu Nhà thầu phải lập biện pháp tổ chức cung cấp và lắp đặt hàng hóa đảm bảo tính hợp lý, hiệu quả đáp ứng các yêu cầu cơ bản sau:

- Thuyết minh giải pháp kỹ thuật rõ ràng, hợp lý, chi tiết và có đầy đủ các tài liệu kỹ thuật, mô hình kết nối theo đúng quy định;

- Cam kết cung cấp đầy đủ các tài liệu chứng nhận hàng hóa đủ tiêu chuẩn chất lượng. Có hướng dẫn vận hành sử dụng, tài liệu kỹ thuật, bảo hành chính hãng;

- Nhà thầu phải cam kết sẽ xuất trình bản gốc của tất cả giấy tờ yêu cầu trong Hồ sơ mời thầu nêu trên để đối chiếu nếu được Chủ đầu tư yêu cầu.

1.3.7. Tiến độ cung cấp, lắp đặt hàng hóa :

- Tiến độ cung cấp, lắp đặt hàng hóa đáp ứng yêu cầu của E-HSMT: Trong vòng 30 ngày kể từ ngày ký hợp đồng.

1.3.8. Bảo hành, bảo trì :

- Thiết bị phải được hỗ trợ kỹ thuật, bảo hành từ nhà cung cấp cũng như đánh giá toàn bộ hệ thống trong quá trình thay thế, đáp ứng khả năng cung cấp dịch vụ bảo hành 24x7 trong thời hạn ≥ 3 năm kể từ ngày đưa hệ thống mới vào hoạt động.

- Cam kết phải sữa chữa mọi sai sót, khiếm khuyết do lỗi của nhà thầu gây ra trong quá trình cung cấp và nhà thầu sẽ chịu mọi phí tổn để thay mới hoặc khắc phục hư hỏng đó. Nếu quá thời hạn theo yêu cầu của chủ đầu tư mà nhà thầu không khắc phục sửa chữa thì chủ đầu tư thuê một nhà thầu khác (bên thứ ba) thực hiện các công việc này và toàn bộ chi phí cho việc sửa chữa

khắc phục để chi trả cho bên thứ ba sẽ do nhà thầu chịu và sẽ khấu trừ vào tiền bảo hành của nhà thầu.quy định của E-HSMT.

- Có cam kết chi tiết về thời gian bảo hành như sau:

+ Nhà thầu cam kết sẽ hỗ trợ kỹ thuật trong suốt thời gian dự án tính từ ngày hai bên ký biên bản nghiệm thu hợp đồng. Trong suốt thời gian dự án, nhân sự thi công có trình độ chuyên môn và kinh nghiệm sẽ được cử đến địa điểm lắp đặt có mặt kịp thời để hỗ trợ và phối hợp khắc phục sự cố trong vòng 04h kể từ khi nhận được thông báo về sự cố.

+ Định kỳ hàng tháng, nhân sự của nhà thầu có trình độ chuyên môn và kinh nghiệm sẽ được cử đến có mặt tại địa điểm lắp đặt để kiểm tra tình trạng hoạt động và bảo trì hệ thống. Tư vấn cho chủ đầu tư về tình trạng sử dụng hệ thống và hướng dẫn các biện pháp khắc phục nếu cần thiết.

+ Thực hiện dịch vụ quản lý, hỗ trợ các đơn vị khai thác, sử dụng hệ thống để triển khai các nghiệp vụ xử lý nội bộ và dịch vụ đảm bảo hệ thống luôn đáp ứng đủ, đúng quy định, đúng quy trình đã được ban hành.

+ Theo dõi hoạt động vật lý, tình trạng sử dụng của các thiết bị trong sơ đồ hạ tầng.

+ Theo dõi tải hoạt động các thiết bị, ứng dụng, có biện pháp tối ưu, nâng cấp khi cần thiết để đảm bảo hiệu năng hệ thống, luôn đáp ứng cho người dùng.

+ Theo dõi hoạt động an toàn thông tin, chống tấn công, tác động thay đổi dữ liệu.

+ Xử lý các sự cố và yêu cầu phát sinh khác trong quá trình vận hành.

+ Thực hiện bố trí nhân sự có chuyên môn và kinh nghiệm trực, tiếp nhận sự cố, hỗ trợ đơn vị thực hiện các chức năng nghiệp vụ trong suốt thời gian duy trì dịch vụ.

+ Đơn vị trúng thầu phải tiến hành kiểm tra năng lực của thiết bị, kiểm tra các kết nối ban đầu của thiết bị sau khi đã được cấu hình, cài đặt.

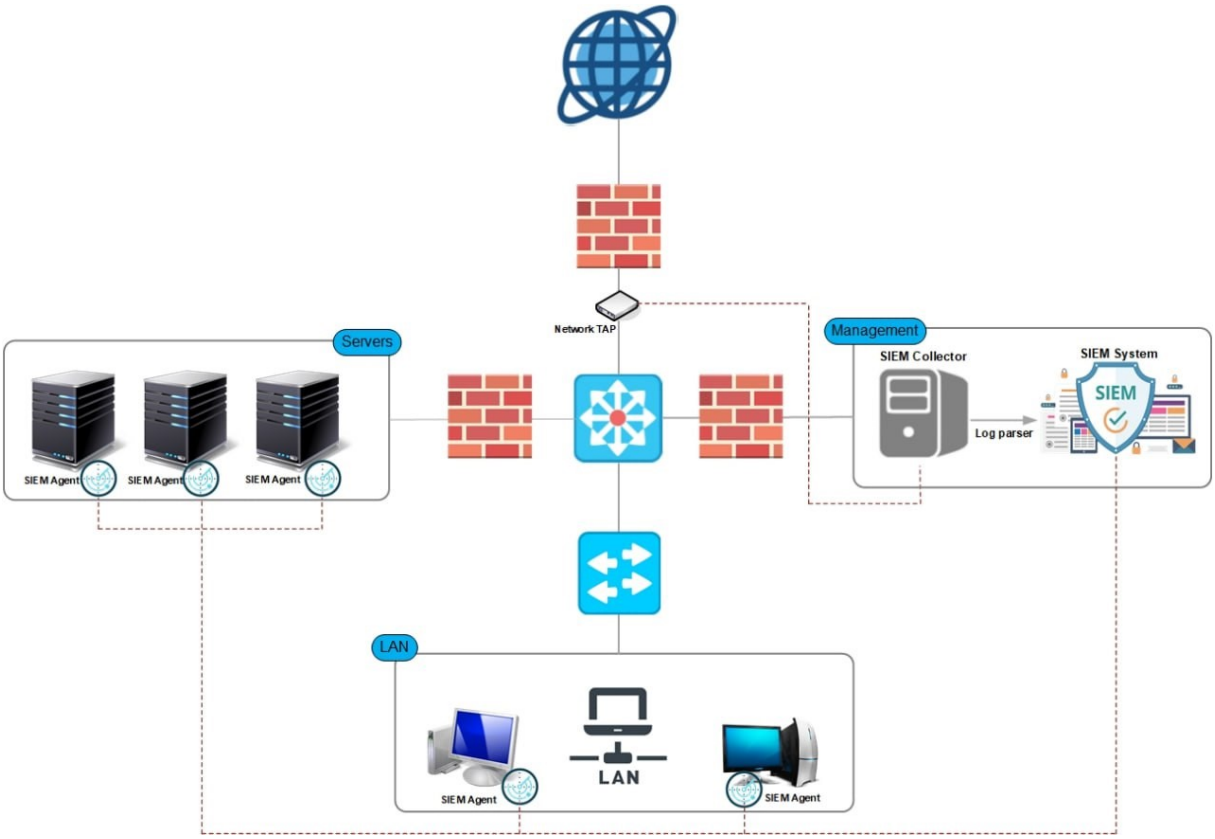
+ Trong suốt thời gian dự án, trường hợp thiết bị phát sinh sự cố hoặc bị hỏng hóc. Nhà cung cấp dịch vụ, thực hiện sửa chữa, khắc phục sự cố phát sinh hoặc thay thế thiết bị phần cứng cho thiết bị trong vòng 24 giờ và thực hiện 24/7.

+ Cam kết hỗ trợ vận hành trong suốt thời gian dự án.

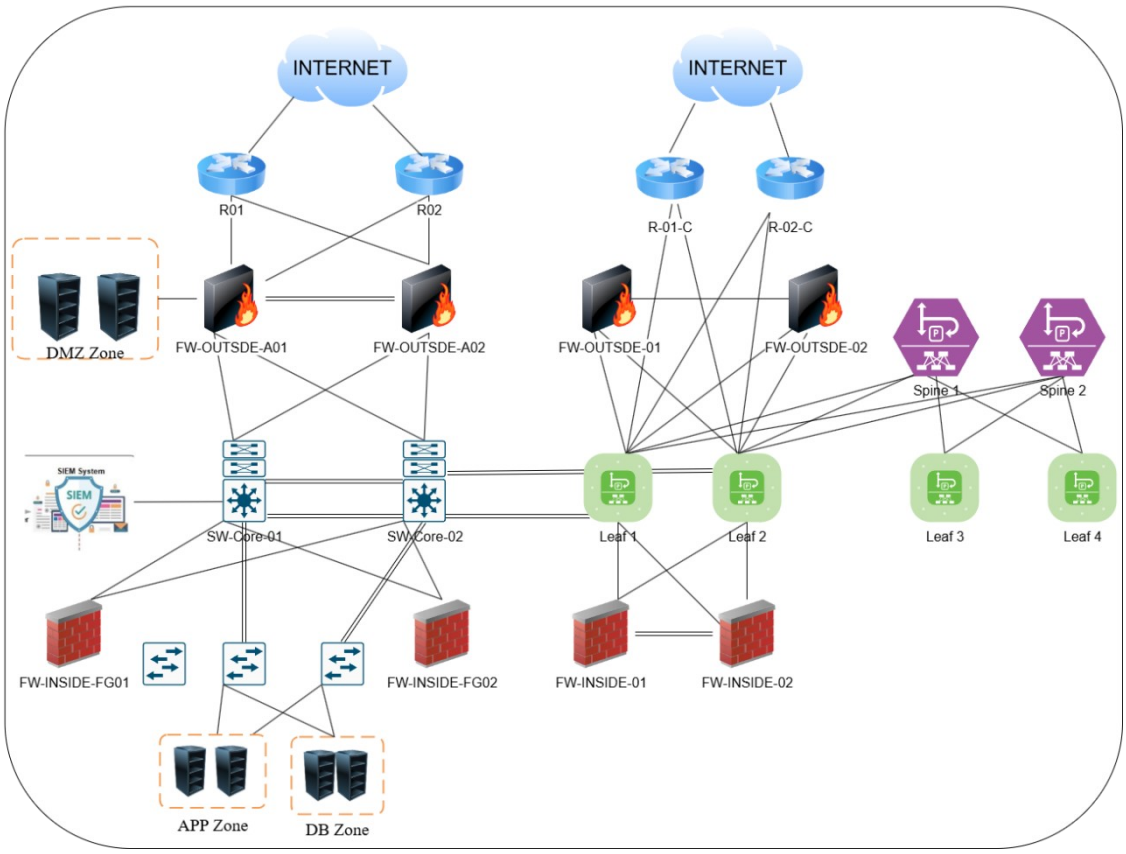
+ Hỗ trợ kỹ thuật hệ thống và bảo hành sẽ bắt đầu ngày sau khi hệ thống đi vào vận hành thực tế và kiểm tra hoạt động của hệ thống được ký và

phê duyệt. Thời gian hỗ trợ dựa vào những yêu cầu của chủ đầu tư và điều kiện trong hợp đồng.

Mục 2. Bản vẽ



Hình 1: Sơ đồ tổng thể giải pháp sau khi thực hiện dự án



Hình 2: Sơ đồ triển khai giải pháp sau khi dự án được duyệt

Mục 3. Kiểm tra và thử nghiệm

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

- Hệ thống trước khi đưa vào cài đặt sẽ được kiểm tra, nghiệm thu về số lượng, chủng loại, tiêu chuẩn và xuất xứ;

- Các hạng mục bổ sung sau khi cài đặt tại mỗi vị trí sẽ được kiểm tra, nghiệm thu thông điện, cấu hình, kết nối, tình trạng hoạt động của thiết bị.

- Nhà thầu phải cử nhân sự phối hợp với Chủ đầu tư, đơn vị Quản lý dự án để thực hiện nghiệm thu và chịu các chi phí liên quan đối với phía Nhà thầu.

- Sau khi hoàn thành việc cài đặt tại các địa điểm sẽ tiến hành nghiệm thu khối lượng, chất lượng, tiến độ thực hiện Gói thầu.