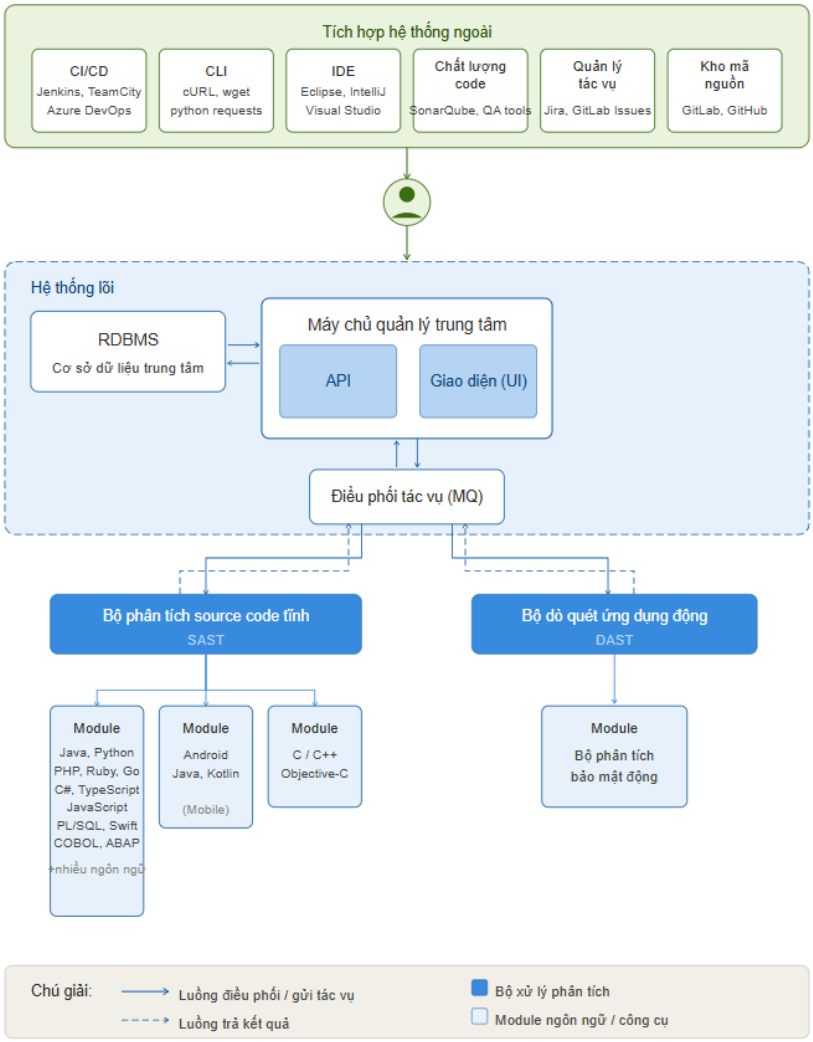
Phần 2. YÊU CẦU VỀ KỸ THUẬT
Chương V. YÊU CẦU VỀ KỸ THUẬT

1. Sơ đồ và thuyết minh chi tiết giải pháp

1.1. Mô hình kết nối, triển khai



Các thành phần triển khai

Giải pháp được triển khai theo mô hình phân tầng, bao gồm các thành phần chính sau:

- **Máy chủ quản lý trung tâm (Web Server / API + UI):** Là thành phần cốt lõi của hệ thống, cung cấp giao diện web và API để người dùng khởi tạo yêu cầu quét, theo dõi tiến trình, xem kết quả và quản trị hệ thống. Máy chủ này đảm nhận việc xác thực người dùng, kiểm soát phân quyền và điều phối toàn bộ luồng hoạt động.

- **Hệ quản trị cơ sở dữ liệu (RDBMS):** Lưu trữ tập trung toàn bộ dữ liệu của hệ thống bao gồm cấu hình dự án, lịch sử quét, kết quả phân tích và thông tin người dùng.
- **Thành phần điều phối tác vụ (Message Queue):** Đảm nhận vai trò trung gian phân phối các yêu cầu quét tới máy chủ phân tích phù hợp theo cơ chế bất đồng bộ, giúp hệ thống xử lý nhiều yêu cầu đồng thời mà không gây tắc nghẽn.
- **Máy chủ phân tích mã nguồn tĩnh (SAST):** Thực hiện phân tích tĩnh trên mã nguồn, file build hoặc binary, hỗ trợ đa ngôn ngữ lập trình và đa nền tảng. Kết quả phân tích được chuẩn hóa theo các tiêu chuẩn bảo mật phổ biến như OWASP, CWE.
- **Máy chủ phân tích bảo mật động (DAST):** Thực hiện kiểm thử bảo mật trên ứng dụng đang vận hành, mô phỏng các kịch bản tấn công thực tế để phát hiện lỗ hổng mà phân tích tĩnh không thể nhận diện.

Mô hình triển khai

Quy trình hoạt động được thiết kế theo luồng khép kín từ khởi tạo yêu cầu đến hiển thị kết quả, cụ thể như sau:

- **Khởi tạo yêu cầu quét:** Người dùng hoặc hệ thống tích hợp (CI/CD pipeline, IDE, công cụ dòng lệnh) gửi yêu cầu quét bảo mật tới hệ thống, kèm theo các tham số như loại phân tích, phạm vi ứng dụng và chính sách bảo mật áp dụng.
- **Tiếp nhận và phân phối tác vụ:** Máy chủ trung tâm xác thực yêu cầu, ghi nhận thông tin vào cơ sở dữ liệu, sau đó đưa tác vụ vào hàng đợi để phân phối tới máy chủ phân tích phù hợp.
- **Thực thi phân tích:** Các máy chủ phân tích nhận tác vụ và thực hiện quét độc lập-máy chủ SAST phân tích mã nguồn, máy chủ DAST kiểm thử ứng dụng đang chạy. Cơ chế này cho phép mở rộng năng lực xử lý linh hoạt theo nhu cầu.
- **Tổng hợp và lưu trữ kết quả:** Sau khi hoàn tất, kết quả được chuẩn hóa, lưu vào cơ sở dữ liệu và hiển thị tập trung trên giao diện quản lý dưới dạng danh sách lỗ hổng, mức độ nghiêm trọng và khuyến nghị khắc phục.
- **Tích hợp và phản hồi:** Hệ thống tự động đồng bộ kết quả sang các công cụ theo dõi lỗi và quản lý dự án (ví dụ Jira, Azure DevOps).

- **Theo dõi và kiểm soát liên tục:** Người quản trị có thể theo dõi tiến trình, lịch sử quét và hiệu quả khắc phục qua giao diện thống nhất. Hệ thống hỗ trợ lên lịch quét định kỳ hoặc kích hoạt tự động theo sự kiện build/release, đảm bảo kiểm soát bảo mật xuyên suốt vòng đời phát triển phần mềm.

2. Danh mục phần mềm và các thông số kỹ thuật.

TT	Danh mục vật tư	Yêu cầu kỹ thuật
1	**Phần mềm kiểm thử bảo mật ứng dụng tĩnh (Static Application Security Testing - SAST)**	
	Bản quyền	
		Số lượng tài khoản: Tối thiểu cho 05 tài khoản hoặc 05 lập trình viên.
		Số lượng ứng dụng: Không hạn chế số lượng ứng dụng dò quét
		Loại bản quyền: Vĩnh viễn
		Hỗ trợ và cập nhật: Thời gian cập nhật phần mềm, cơ sở dữ liệu, hỗ trợ kỹ thuật từ chính hãng 03 năm
	Tính năng phần mềm	
		Phân tích mã nguồn: Cho phép thực hiện dò quét mã nguồn (source code scanning) và xác định nguyên nhân các lỗ hổng của phần mềm.
		Xử lý kết quả: So sánh kết quả từ nhiều lần quét để xác định lỗ hổng mới, đã khắc phục, hoặc lặp lại.
		- Phân tích mã nguồn: Hỗ trợ các ngôn ngữ lập trình: ASP.NET, VB.NET, C# (.NET), C/C++, PHP, Python, Ruby, Go, Java, Javascript, Kotlin

TT	Danh mục vật tư	Yêu cầu kỹ thuật
		Phát hiện lỗ hổng: Có thể phát hiện lỗ hổng trong cả mã nguồn và tệp thực thi
		Phương pháp phân tích mã: Có thể kết hợp nhiều phương pháp, bao gồm phân tích luồng thực thi , từ đó tối đa hóa khả năng phát hiện các lỗ hổng mã nguồn.
		So sánh kết quả: So sánh kết quả của các lần phân tích đã hoàn thành. Khởi tạo nhiều dạng biểu đồ thể hiện các lỗ hổng và chức năng không chính thức mới xuất hiện hay được loại bỏ.
		Cho phép sử dụng máy học (Machine Learning) để kiểm tra kết quả dò quét
		Cung cấp sẵn các mẫu báo cáo kiểm tra khả năng tuân thủ theo một số tiêu chuẩn như: PCI DSS Compliance (Application Security Requirements), OWASP Top 10, OWASP Mobile Top 10, DISA STIG, CWE/SANS Top 25
		Cho phép tạo báo cáo theo các định dạng PDF, HTML
		Điều khiển truy cập lập trình viên: Có khả năng phân chia quyền truy cập của lập trình viên. Hỗ trợ tích hợp Microsoft Active Directory
		Tích hợp hệ thống theo dõi sự cố: Hỗ trợ các hệ thống theo dõi sự cố như Atlassian Jira
		Cho phép tạo báo cáo theo các định dạng khác nhau.
2	**Phần mềm kiểm thử bảo mật ứng dụng động Dynamic Application Security Testing (DAST)**	
	Bản quyền	
		Số lượng sử dụng : 01 tài khoản
		Bản quyền (License): Vĩnh viễn

TT	Danh mục vật tư	Yêu cầu kỹ thuật
		Thời gian cập nhật phần mềm, cơ sở dữ liệu, hỗ trợ kỹ thuật từ chính hãng 03 năm
	Tính năng phần mềm	
		Có khả năng rà quét và phát hiện các lỗ hổng trong các ứng dụng Website.
		Giải pháp phải có khả năng xác thực vào ứng dụng yêu cầu xác thực bằng các phương thức như: tên đăng nhập/mật khẩu, token, headers, biểu mẫu ủy quyền/xác thực (authorization forms), NTLM.
		Phần mềm phải có khả năng rà quét và phát hiện các lỗ hổng trong các ứng dụng Website, tối thiểu phải phát hiện được các lỗ hổng trong Top 10 OWASP, CWEs (Common Weakness Enumeration).
		Phần mềm phải có khả năng rà quét và phát hiện các lỗ hổng bảo mật đối với các ứng dụng web hiện đại, phức tạp sử dụng các công nghệ như OpenAPI (JSON)
		Phần mềm phải có chức năng xem báo cáo trên giao diện dashboard, trích xuất báo cáo ra các định dạng file PDF, HTML.
		Phần mềm phải cung cấp các API, phải có khả năng tích hợp vào với SDLC (Software Development Lifecycle) cho phép tự động rà quét trong môi trường DevOps và CI/CD pipelines.
		Phần mềm phải cho phép tạo và phân quyền tài khoản
		Phần mềm phải hỗ trợ các công cụ Issue tracker integration (bao gồm: Jira, Azure DevOps, Gitlab).

3. Yêu cầu triển khai:

a. Yêu cầu chung

- Nhà thầu phải cung cấp các tài liệu liên quan đến vận hành hệ thống: Mô hình kiến trúc hệ thống sau khi triển khai, Hướng dẫn cài đặt, cấu hình, vận hành hệ thống, hướng dẫn sử lý lỗi trong quá trình vận hành hệ thống, và các tài liệu liên quan đến quá trình triển khai hệ thống.
- Yêu cầu nhà thầu thực hiện đánh giá an toàn an ninh thông tin trước khi đi vào vận hành.
- Yêu cầu nhà thầu thực hiện cập nhật phiên bản, bản vá trong thời gian bảo hành, hỗ trợ kỹ thuật
- Đơn vị trúng thầu phải thực hiện toàn bộ công việc cung cấp, vận chuyển, lắp đặt, cấu hình và kiểm tra phần mềm đúng chủng loại, cấu hình, số lượng theo hồ sơ yêu cầu.
- Quá trình triển khai phải đảm bảo không ảnh hưởng đến hoạt động vận hành của Trung tâm dữ liệu TP Hà Nội.
- Thực hiện đầy đủ các quy trình sao lưu dữ liệu, an toàn hệ thống, đảm bảo dữ liệu không bị mất mát hoặc gián đoạn sau nâng cấp**.**
- Nhà thầu thi công có trách nhiệm lập và thông báo cho chủ đầu tư hệ thống quản lý chất lượng, mục tiêu và chính sách đảm bảo chất lượng công trình của nhà thầu. Hệ thống quản lý chất lượng của nhà thầu phải phù hợp với công trình, trong đó nêu rõ sơ đồ tổ chức và trách nhiệm của từng bộ phận, cá nhân đối với công tác quản lý chất lượng của nhà thầu.
- Nhà thầu có trách nhiệm lập và thực hiện các nội dung sau:
- Kế hoạch tổ chức hoàn thiện công tác kiểm tra, giám định xác định về số lượng, chủng loại, xuất xứ, tình trạng của các chi tiết của hàng hóa theo yêu cầu thiết kế và chỉ dẫn kỹ thuật.
- Biện pháp kiểm tra, kiểm soát chất lượng vật tư, thiết bị, phần mềm được sử dụng cho công trình; phương án biện pháp thi công, trong đó quy định cụ thể các biện pháp, bảo đảm an toàn cho người, máy, thiết bị và công trình;
- Tiến độ thi công xây dựng công trình.
- Kế hoạch triển khai, kiểm tra, nghiệm thu công việc xây dựng.
- Triển khai thực hiện kế hoạch tổng hợp về an toàn lao động trong thi công xây dựng công trình (được chủ đầu tư chấp thuận)

- Các nội dung cần thiết khác theo yêu cầu của chủ đầu tư và quy định của hợp đồng.
- Bố trí nhân lực, thiết bị thi công theo quy định của hợp đồng và quy định của pháp luật có liên quan.
- Thực hiện các công tác kiểm tra hàng hóa trước và trong khi thi công lắp đặt theo quy định của hợp đồng.
- Nhà thầu có trách nhiệm thi công triển khai theo đúng hợp đồng, thiết kế đã được duyệt. Kịp thời thông báo cho chủ đầu tư nếu phát hiện sai khác giữa thiết kế, hồ sơ hợp đồng và điều kiện hiện trường trong quá trình thi công. Tự kiểm soát chất lượng thi công xây dựng theo yêu cầu của thiết kế và quy định của hợp đồng. Hồ sơ quản lý chất lượng của các công việc lắp đặt phải được lập theo quy định và phù hợp với thời gian thực hiện thực tế tại công trường.
- Dừng thi công xây dựng đối với công việc xây dựng, hạng mục công việc khi phát hiện có sai sót, khiếm khuyết về chất lượng hoặc xảy ra sự cố công trình. Xử lý, khắc phục các sai sót, khiếm khuyết về chất lượng trong quá trình thi công (nếu có). Dừng thi công xây dựng khi phát hiện nguy cơ xảy ra tai nạn lao động, sự cố gây mất an toàn lao động và có biện pháp khắc phục để đảm bảo an toàn trước khi tiếp tục thi công; khắc phục hậu quả tai nạn lao động, sự cố gây mất an toàn lao động xảy ra trong quá trình thi công xây dựng công trình (nếu có).
- Lập nhật ký thi công công trình theo quy định.
- Lập bản vẽ hoàn công theo quy định (nếu có)
- Báo cáo chủ đầu tư về tiến độ, chất lượng, khối lượng, an toàn lao động và vệ sinh môi trường thi công xây dựng theo quy định của hợp đồng xây dựng và quy định của pháp luật khác có liên quan hoặc báo cáo đột xuất theo yêu cầu của chủ đầu tư.
- Hoàn trả mặt bằng, di chuyển vật tư, máy móc, thiết bị và những tài sản khác của mình ra khỏi phòng máy chủ của EVNHANOI tại TTDL sau khi công trình đã được nghiệm thu, bàn giao, trừ trường hợp trong hợp đồng có thỏa thuận khác.

b. Yêu cầu về tiến độ triển khai

- Thời gian hoàn thành toàn bộ công việc không quá 60 ngày kể từ ngày ký hợp đồng.
- Lập kế hoạch chi tiết triển khai, trình Chủ đầu tư phê duyệt trước khi thực hiện.

c. Yêu cầu về nhân sự kỹ thuật

- Đại học chuyên ngành Công nghệ thông tin hoặc tương đương theo quy định tại Khoản a,b Điều 2 Thông tư số 45/2017/TT-BTTTT ngày 29/12/2017 của Bộ Thông tin và Truyền thông quy định tiêu chuẩn, chức danh nghề nghiệp viên chức chuyên ngành công nghệ thông tin.
- Có chứng chỉ chuyên môn về giải pháp, có đủ năng lực triển khai cài đặt cho sản phẩm của hãng được cung cấp trong gói thầu này.

d. Yêu cầu kỹ thuật khi triển khai

- Nhà thầu thi công phải lập kịch bản kiểm tra, vận hành thử nghiệm chi tiết trong phương án kỹ thuật triển khai đối với từng hạng mục theo kế hoạch. Tiến hành kiểm tra thử nghiệm theo kịch bản đã lập cho công trình.
- Khi tiến hành nghiệm thu yêu cầu phải có đầy đủ sự xác nhận của Chủ đầu tư, Nhà thầu và đơn vị Tư vấn (nếu có). Biên bản nghiệm thu phải ghi đầy đủ các yếu tố chất lượng, tình trạng hoạt động của thiết bị và xác nhận của các thành viên có liên quan.
- Khi tiến hành nghiệm thu công việc, Chủ đầu tư và Nhà thầu tuân thủ Luật Xây dựng số 50/2014/QH13 ngày 18/6/2014; Nghị định số 06/2021/NĐ-CP ngày 26/01/2021 của Chính phủ về Quy định chi tiết một số nội dung về quản lý chất lượng, thi công xây dựng và bảo trì công trình xây dựng, các tiêu chuẩn kỹ thuật, quy phạm hiện hành và theo thông tư số: 24/2020/TT-BTTTT ngày 09/9/2020 của Bộ thông tin truyền thông.

e. Yêu cầu về an toàn dữ liệu

- Tuyệt đối không làm mất, hỏng, sai lệch dữ liệu trong quá trình triển khai.
- Yêu cầu nhà thầu thực hiện kiểm tra an toàn, an ninh cho hệ thống và có báo cáo kết quả an toàn, an ninh thông tin được sự đồng ý của chủ đầu tư trước khi đưa hệ thống vào vận hành.

4. Nguyên tắc tổ chức triển khai

- Đảm bảo không ảnh hưởng đến hoạt động của Trung tâm Dữ liệu.

- Phân chia công việc theo từng cụm máy chủ để tránh gián đoạn hệ thống đồng thời.
- Có kế hoạch tạm dừng các máy chủ hợp lý, theo từng khung giờ thấp điểm đã được thống nhất(nếu cần).

5. Biện pháp đảm bảo an toàn – dữ liệu – vận hành

- Toàn bộ quá trình, triển khai nâng cấp có sự giám sát trực tiếp của đội kỹ thuật nội bộ.