Phần 2. YÊU CẦU VỀ KỸ THUẬT

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

- Tên dự án: Trang bị hệ thống rà quét điểm yếu code ứng dụng cho EVNSPC.

- Tên gói thầu: Trang bị hệ thống rà quét điểm yếu code ứng dụng cho EVNSPC.

- Địa điểm thực hiện dự án:

+ *CN Tổng công ty Điện lực miền Nam TNHH - Công ty Công nghệ thông tin Điện lực miền Nam, Số 16 Âu Cơ, phường Tân Sơn Nhì, Tp.HCM.*

STT	Hạng mục đầu tư	ĐVT	Số lượng	Thời gian thực hiện gói thầu
1	**Bộ công cụ SAST (Phân tích tĩnh mã nguồn) và hỗ trợ chính hãng 03 năm:** - Hỗ trợ ít nhất 12 người dùng (named users hoặc concurrent users tùy theo mô hình cấp phép) cho cả tính năng SAST và SCA; - Không giới hạn số dự án quản lý và quét đồng thời. - Không giới hạn số lượng dòng code cho phân tích tĩnh. - Phải hỗ trợ đầy đủ các ngôn ngữ lập trình và framework như: Java, Python, JavaScript, C#, PHP, .NET, React, Angular, Vue,… cho phân tích tĩnh; - Cung cấp bộ quy tắc quét mạnh mẽ cho lỗi bảo mật và chất lượng mã, bao gồm các tiêu chuẩn bảo mật phổ biến (như OWASP Top 10, CWE, SANS Top 25) và khả năng tùy chỉnh quy tắc theo yêu cầu của Chủ đầu tư; - Có cơ chế phân tích chính xác và các tính năng để giảm thiểu cảnh báo sai như suppression rule hoặc tương đương; - Phải hỗ trợ các hệ sinh thái ngôn ngữ và trình quản lý gói như: Maven, Gradle, npm, NuGet, Gems,…; - Sử dụng cơ sở dữ liệu lỗ hổng bảo mật uy tín và được cập nhật thường xuyên như: CVE, NVD,…; - Cung cấp báo cáo chi tiết về các lỗ hổng bảo mật được phát hiện trong các thành phần, bao gồm mức độ nghiêm trọng, thông tin về lỗ hổng và khuyến nghị khắc phục;	Bộ	01	Trong vòng 90 ngày kể từ ngày hợp đồng có hiệu lực, trong đó: - Thời gian cung cấp, nghiệm thu VTTB: trong vòng 45 ngày kể từ ngày hợp đồng có hiệu lực. - Thời gian triển khai, nghiệm thu bàn giao sản phẩm: trong vòng 90 ngày kể từ ngày hợp đồng có hiệu lực

STT	Hạng mục đầu tư	ĐVT	Số lượng	Thời gian thực hiện gói thầu
	- Tích hợp Plugin cho các IDE phổ biến như: Visual Studio, IntelliJ, Eclipse, VS Code,… cho cả phân tích SAST và SCA; - Tích hợp Plugin hoặc API để tích hợp vào các công cụ CI/CD như: Jenkins, GitLab CI, Azure DevOps Pipelines, ,… cho cả SAST và SCA; - Cung cấp API để tích hợp với các nền tảng quản lý bảo mật ứng dụng tập trung; - Cung cấp báo cáo thống nhất về cả kết quả phân tích SAST và SCA, với khả năng lọc và sắp xếp theo mức độ nghiêm trọng, loại lỗ hổng, vị trí, v.v. Khả năng xuất báo cáo ở nhiều định dạng; - Cung cấp API để tự động hóa và tích hợp với các hệ thống khác; - Bao gồm bản quyền sử dụng và bảo hành hỗ trợ kỹ thuật chính hãng trong 03 năm.			
2	**Bộ công cụ DAST (Kiểm thử bảo mật ứng dụng động) và hỗ trợ chính hãng 03 năm:** - Hỗ trợ ít nhất 01 người dùng (named users hoặc concurrent users); - Không giới hạn số lần thực hiện quét và số lượng ứng dụng web/API; - Hỗ trợ quét các ứng dụng web, API (REST, SOAP, GraphQL), và có khả năng tùy chỉnh cấu hình quét; - Có khả năng thực hiện quét toàn diện (full crawl) và quét sâu các khu vực cụ thể; - Có khả năng phát hiện nhiều loại lỗ hổng DAST phổ biến như OWASP Top 10,…; - Có cơ chế phân tích chính xác và khả năng cấu hình để giảm thiểu cảnh báo sai; - Cung cấp báo cáo chi tiết về các lỗ hổng, mức độ nghiêm trọng, các bước tái hiện và đề xuất khắc phục; - Hỗ trợ nhiều phương pháp xác thực ứng dụng; - Cung cấp API để tự động hóa và tích hợp với các hệ thống khác; - Bao gồm bản quyền sử dụng và bảo hành hỗ trợ kỹ thuật chính hãng trong 03 năm.	Bộ	01	
3	**Gói triển khai, đào tạo, vận hành:** + Thực hiện cấu hình, cài đặt tất cả các phần mềm trang bị theo dự án; + Khảo sát và xây dựng giải pháp CI/CD tích hợp kiểm thử bảo mật (DevSecOps) phù hợp với đặc thù tại SPCIT;	Gói	01	

STT	Hạng mục đầu tư	ĐVT	Số lượng	Thời gian thực hiện gói thầu
	+ Đào tạo hướng dẫn sử dụng toàn bộ hệ thống; + Đào tạo hướng dẫn sử dụng công cụ cho nhóm kỹ sư phát triển và bảo mật.			

1.2. Yêu cầu về kỹ thuật: Theo Phụ lục Đặc tính kỹ thuật Dự án đầu tư: "Trang bị hệ thống rà quét điểm yếu code ứng dụng cho EVNSPC"

1.3. Các yêu cầu khác:

- Đáp ứng theo Hồ sơ yêu cầu kỹ thuật đính kèm.

- Đánh giá chất lượng VTTB trong giai đoạn vận hành: các VTTB sau khi được mua sắm, lắp đặt sẽ tiếp tục được đánh giá chất lượng theo quy định của EVN trong quá trình vận hành, bao gồm cả giai đoạn bảo hành và sau bảo hành.

Mục 2. Bản vẽ: Không có

Mục 3. Kiểm tra và thử nghiệm

Các kiểm tra và thử nghiệm cần tiến hành gồm có: Theo E-ĐKC 21.1 – Điều kiện cụ thể hợp đồng.

TỔNG CÔNG TY ĐIỆN LỰC MIỀN NAM
CÔNG TY CÔNG NGHỆ THÔNG TIN ĐIỆN LỰC MIỀN NAM

TP. Hồ Chí Minh ngày 16 tháng 11 năm 2025

BÁO CÁO KINH TẾ KỸ THUẬT

DỰ ÁN ĐẦU TƯ
Trang bị Hệ thống rà quét điểm yếu code ứng dụng cho EVNSPC

Thiết lập: Tổ Xây dựng dự án và yêu cầu kỹ thuật

- Lê Tân Tiến - Tổ trưởng Tổ Dự án
- Lê Hoàng Minh - Thành viên
- Lưu Đăng Khoa - Thành viên
- Lê Việt Quang - Thành viên
- Nguyễn Quang Huy - Thành viên

GIÁM ĐỐC

Đặng Nguyên Phương

TỔNG CÔNG TY
ĐIỆN LỰC MIỀN NAM
CÔNG TY CÔNG NGHỆ THÔNG TIN
ĐIỆN LỰC MIỀN NAM

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

BIÊN CHẾ BÁO CÁO KINH TẾ KỸ THUẬT

DỰ ÁN: "Trang bị hệ thống rà quét điểm yếu code ứng dụng cho EVNSPC"

Dự án đầu tư "Trang bị hệ thống rà quét điểm yếu code ứng dụng cho EVNSPC" là dự án đầu tư sử dụng vốn Đầu tư xây dựng, nhằm phát hiện sớm lỗi logic, mã kém chất lượng, điểm yếu bảo mật ngay từ giai đoạn lập trình để kịp thời hiệu chỉnh, có tổng mức đầu tư khoảng 2,9 tỷ VNĐ. Căn cứ theo Khoản 2 Điều 10 của 73/2019/NĐ-CP ngày 05/09/2019, hồ sơ dự án được thiết kế 01 bước.
Theo đó, Hồ sơ dự án có biên chế hồ sơ thành 03 tập như sau:

- Tập 1 : Thuyết minh Báo cáo kinh tế kỹ thuật
- Tập 2 : Dự toán
- **Tập 3 : Yêu cầu kỹ thuật và Tiêu chuẩn đánh giá**

TẬP 3 – YÊU CẦU KỸ THUẬT VÀ TIÊU CHUẨN ĐÁNH GIÁ

MỤC LỤC

Yêu cầu chung

1. Giới thiệu chung

a. Nội dung

Công ty CNTT Điện lực miền Nam cần trang bị hệ thống rà quét điểm yếu code ứng dụng cho việc kiểm tra, đánh giá chất lượng và bảo mật mã nguồn trong toàn bộ quá trình phát triển phần mềm nội bộ dùng chung trong EVNSPC nhằm phát hiện sớm lỗi logic, mã kém chất lượng, điểm yếu bảo mật ngay từ giai đoạn lập trình để kịp thời hiệu chỉnh.

b. Địa điểm thực hiện

Công ty CNTT Điện lực miền Nam tại Số 16 Âu Cơ, phường Tân Sơn Nhì, Tp.HCM.

c. Quy mô

STT	Hạng mục đầu tư	Đơn vị tính	Số lượng
1	Bộ công cụ SAST (Phân tích tĩnh mã nguồn)	Bộ	1
2	Bộ công cụ DAST (Kiểm thử bảo mật ứng dụng động)	Bộ	1
3	Gói triển khai, đào tạo, vận hành	Gói	1

2. Yêu cầu kỹ thuật

STT	Đặc tính kỹ thuật	Mô tả chi tiết
I	**Bộ công cụ SAST (Phân tích tĩnh mã nguồn)**	
1	Số lượng người dùng	Hỗ trợ ít nhất 12 người dùng (named users hoặc concurrent users tùy theo mô hình cấp phép) cho cả tính năng SAST (Static Application Security Testing) và SCA (Software Composition Analysis).
2	Số lượng dự án quản lý	Không giới hạn số dự án quản lý và quét đồng thời.
3	Số lượng dòng code phân tích	Không giới hạn số lượng dòng code cho phân tích tĩnh.
4	Hỗ trợ ngôn ngữ lập trình	Phải hỗ trợ đầy đủ các ngôn ngữ lập trình và framework như: Java, Python, JavaScript, C#, PHP, .NET, React, Angular, Vue, Python… cho phân tích tĩnh.
5	Bộ quy tắc quét	Cung cấp bộ quy tắc quét mạnh mẽ cho lỗi bảo mật và chất lượng mã nguồn, bao gồm các tiêu chuẩn bảo mật phổ biến (như OWASP Top 10, CWE, SANS Top 25) và khả năng tùy chỉnh quy tắc theo yêu cầu của Chủ đầu tư;.
6	Cơ chế phân tích	Có cơ chế phân tích hiệu quả để tối ưu tỷ lệ phát hiện lỗ hổng thực tế (True Positives) và giảm thiểu cảnh báo sai (False Positives); đồng thời phải cung cấp khả năng cấu hình linh hoạt (ví dụ: thông qua quy tắc loại trừ - exclusion rules, quy tắc trấn áp - suppression rules, hoặc các bộ lọc tùy chỉnh) để tinh chỉnh kết quả và phù hợp với đặc thù ứng dụng.
7	Hỗ trợ	Phải hỗ trợ các hệ sinh thái ngôn ngữ và trình quản lý gói như: Maven, Gradle, npm, NuGet, Gems,…
8	Cơ sở dữ liệu sử dụng	Sử dụng cơ sở dữ liệu lỗ hổng bảo mật được cập nhật thường xuyên từ: CVE, NVD,…
9	Báo cáo	Cung cấp báo cáo chi tiết về các lỗ hổng bảo mật được phát hiện trong các thành phần, bao gồm mức độ nghiêm trọng, thông tin về lỗ hổng và khuyến nghị khắc phục.
10	Tích hợp Plugin cho các IDE	Tích hợp Plugin cho các IDE phổ biến như: Visual Studio, IntelliJ, Eclipse, VS Code,… cho cả phân tích SAST và SCA.

11	Tích hợp vào các công cụ CI/CD	Tích hợp Plugin hoặc API để tích hợp vào các công cụ CI/CD như: Jenkins, GitLab CI, Azure DevOps Pipelines, ,… cho cả SAST và SCA.
12	Khả năng cung cấp API để tích hợp	Cung cấp API để tích hợp với các nền tảng quản lý bảo mật ứng dụng tập trung.
13	Khả năng cung cấp báo cáo	Cung cấp báo cáo thống nhất về cả kết quả phân tích SAST và SCA, với khả năng lọc và sắp xếp theo mức độ nghiêm trọng, loại lỗ hổng, vị trí, … Khả năng xuất báo cáo ở nhiều định dạng.
14	Khả năng cung cấp API cho các hệ thống khác	Công cụ cần cung cấp API toàn diện (ưu tiên RESTful API với định dạng dữ liệu JSON) để tự động hóa việc quét và tích hợp liền mạch vào các quy trình DevSecOps (CI/CD). API cần hỗ trợ các tác vụ như: kích hoạt quét, truy vấn trạng thái, thu thập kết quả quét và quản lý cấu hình.
15	Thời gian bản quyền	Bản quyền phần mềm và dịch vụ hỗ trợ kỹ thuật chính hãng 03 năm.
II	**Bộ công cụ DAST (Kiểm thử bảo mật ứng dụng động)**	
1	Số lượng người dùng hỗ trợ	Hỗ trợ ít nhất 01 người dùng (named users hoặc concurrent users).
2	Số lần quét	Không giới hạn số lần thực hiện quét và số lượng ứng dụng web/API.
3	Hỗ trợ quét ứng dụng	Hỗ trợ quét các ứng dụng web, API (REST, SOAP, GraphQL), và có khả năng tùy chỉnh cấu hình quét.
4	Khả năng quét	Có khả năng thực hiện quét khám phá ứng dụng toàn diện (full crawl) và thực hiện kiểm thử chuyên sâu tại các khu vực/chức năng được chỉ định (ví dụ: các luồng nghiệp vụ quan trọng, các trang yêu cầu xác thực, các API).
5	Khả năng phát hiện lỗ hổng	Có khả năng phát hiện nhiều loại lỗ hổng DAST (Dynamic Application Security Testing) phổ biến như OWASP Top 10,…
6	Cơ chế phân tích	Có cơ chế phân tích hiệu quả để tối ưu tỷ lệ phát hiện lỗ hổng thực tế (True Positives) và giảm thiểu cảnh báo sai (False Positives); đồng thời phải cung cấp khả năng cấu hình linh

		hoạt (ví dụ: thông qua quy tắc loại trừ - exclusion rules, quy tắc trấn áp - suppression rules, hoặc các bộ lọc tùy chỉnh) để tinh chỉnh kết quả và phù hợp với đặc thù ứng dụng
7	Báo cáo	Cung cấp báo cáo chi tiết về các lỗ hổng, mức độ nghiêm trọng, các bước tái hiện và đề xuất khắc phục.
8	Xác thực ứng dụng	Hỗ trợ nhiều phương pháp xác thực ứng dụng.
9	Khả năng cung cấp API cho các hệ thống khác	Công cụ DAST phải cung cấp đầy đủ API (ưu tiên RESTful với định dạng JSON) để hỗ trợ tự động hóa và tích hợp liền mạch với các hệ thống bên ngoài.
10	Thời gian bản quyền	Bản quyền phần mềm và dịch vụ hỗ trợ kỹ thuật chính hãng 03 năm.
III	**Gói triển khai, đào tạo, vận hành**	
	Khi cung cấp license Bộ công cụ SAST và DAST, Nhà thầu phải kèm theo dịch vụ tư vấn và triển khai xây dựng giải pháp CI/CD tích hợp kiểm thử bảo mật (DevSecOps) phù hợp với đặc thù của Chủ đầu tư. Phạm vi hạng mục dịch vụ này bao gồm:	
1	Khảo sát và thiết kế	Phân tích nhu cầu, nguồn lực hiện có và thiết kế phương thức, kịch bản dò quét tối ưu (SAST/DAST) để tích hợp vào quy trình CI/CD (Tích hợp Liên tục-Continuous Integration/Chuyển giao Liên tục-Continuous Delivery).
2	Triển khai và cấu hình cài đặt	Thực hiện cài đặt, cấu hình các công cụ SAST/DAST và tích hợp chúng vào các công cụ CI/CD hiện có của chủ đầu tư (ví dụ: Jenkins, GitLab CI/CD, Azure DevOps Pipelines) theo thiết kế.
3	Kiểm thử nghiệm thu	Thực hiện các bài kiểm thử nghiệm thu (Acceptance Tests) để xác nhận toàn bộ giải pháp CI/CD tích hợp bảo mật hoạt động hiệu quả theo yêu cầu đã định.
4	Đào tạo và chuyển giao công nghệ	Đào tạo chuyên sâu cho đội ngũ vận hành và phát triển của Chủ đầu tư về cách sử dụng, quản lý và duy trì giải pháp DevSecOps đã triển khai.

II. Tiêu chuẩn đánh giá

1. Phương pháp đánh giá

Tiêu chuẩn đánh giá về kỹ thuật: Phương pháp đánh giá **Đạt/ Không đạt.**

Theo đó:

- Đánh giá về kỹ thuật được kết luận **Đạt** khi **tất cả** đặc tính, thông số kỹ thuật của hàng hóa đáp ứng Đạt yêu cầu của HSMT.
- Đánh giá về kỹ thuật được kết luận **Không Đạt** khi có từ **Một** trở lên đặc tính, thông số kỹ thuật của hàng hóa không đáp ứng (Không Đạt) yêu cầu của HSMT.

2. Tiêu chí đánh giá kỹ thuật

STT	Đặc tính kỹ thuật	Mô tả chi tiết	Tiêu chí đánh giá		
			Đạt	Chấp nhận được	Không đạt
I	**Bộ công cụ SAST (Phân tích tĩnh mã nguồn)**				
1	Số lượng người dùng	Hỗ trợ ít nhất 12 người dùng (named users hoặc concurrent users tùy theo mô hình cấp phép) cho cả tính năng SAST (Static Application Security Testing) và SCA (Software Composition Analysis).	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
2	Số lượng dự án quản lý	Không giới hạn số dự án quản lý và quét đồng thời.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
3	Số lượng dòng code phân tích	Không giới hạn số lượng dòng code cho phân tích tĩnh.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
4	Hỗ trợ ngôn ngữ lập trình	Phải hỗ trợ đầy đủ các ngôn ngữ lập trình và framework như: Java, Python, JavaScript, C#, PHP, .NET, React, Angular, Vue, Python… cho phân tích tĩnh.	Như yêu cầu.		Không như yêu cầu.

			Viện dẫn chương, trang, mục tham chiếu		Không viện dẫn chương, trang, mục tham chiếu
5	Bộ quy tắc quét	Cung cấp bộ quy tắc quét mạnh mẽ cho lỗi bảo mật và chất lượng mã nguồn, bao gồm các tiêu chuẩn bảo mật phổ biến (như OWASP Top 10, CWE, SANS Top 25) và khả năng tùy chỉnh quy tắc theo yêu cầu của Chủ đầu tư;.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
6	Cơ chế phân tích	Có cơ chế phân tích hiệu quả để tối ưu tỷ lệ phát hiện lỗ hổng thực tế (True Positives) và giảm thiểu cảnh báo sai (False Positives); đồng thời phải cung cấp khả năng cấu hình linh hoạt (ví dụ: thông qua quy tắc loại trừ - exclusion rules, quy tắc trấn áp - suppression rules, hoặc các bộ lọc tùy chỉnh) để tinh chỉnh kết quả và phù hợp với đặc thù ứng dụng.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
7	Hỗ trợ	Phải hỗ trợ các hệ sinh thái ngôn ngữ và trình quản lý gói như: Maven, Gradle, npm, NuGet, Gems,…	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
8	Cơ sở dữ liệu sử dụng	Sử dụng cơ sở dữ liệu lỗ hổng bảo mật được cập nhật thường xuyên từ: CVE, NVD,…	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu

9	Báo cáo	Cung cấp báo cáo chi tiết về các lỗ hổng bảo mật được phát hiện trong các thành phần, bao gồm mức độ nghiêm trọng, thông tin về lỗ hổng và khuyến nghị khắc phục.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
10	Tích hợp Plugin cho các IDE	Tích hợp Plugin cho các IDE phổ biến như: Visual Studio, IntelliJ, Eclipse, VS Code,… cho cả phân tích SAST và SCA.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
11	Tích hợp vào các công cụ CI/CD	Tích hợp Plugin hoặc API để tích hợp vào các công cụ CI/CD như: Jenkins, GitLab CI, Azure DevOps Pipelines, ,… cho cả SAST và SCA.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
12	Khả năng cung cấp API để tích hợp	Cung cấp API để tích hợp với các nền tảng quản lý bảo mật ứng dụng tập trung.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
13	Khả năng cung cấp báo cáo	Cung cấp báo cáo thống nhất về cả kết quả phân tích SAST và SCA, với khả năng lọc và sắp xếp theo mức độ nghiêm trọng, loại lỗ hổng, vị trí, … Khả năng xuất báo cáo ở nhiều định dạng.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu

14	Khả năng cung cấp API cho các hệ thống khác	Công cụ cần cung cấp API toàn diện (ưu tiên RESTful API với định dạng dữ liệu JSON) để tự động hóa việc quét và tích hợp liền mạch vào các quy trình DevSecOps (CI/CD). API cần hỗ trợ các tác vụ như: kích hoạt quét, truy vấn trạng thái, thu thập kết quả quét và quản lý cấu hình.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
15	Thời gian bản quyền	Bản quyền phần mềm và dịch vụ hỗ trợ kỹ thuật chính hãng 03 năm.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
II	**Bộ công cụ DAST (Kiểm thử bảo mật ứng dụng động)**				
1	Số lượng người dùng hỗ trợ	Hỗ trợ ít nhất 01 người dùng (named users hoặc concurrent users).	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
2	Số lần quét	Không giới hạn số lần thực hiện quét và số lượng ứng dụng web/API.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
3	Hỗ trợ quét ứng dụng	Hỗ trợ quét các ứng dụng web, API (REST, SOAP, GraphQL), và có khả năng tùy chỉnh cấu hình quét.	Như yêu cầu.		Không như yêu cầu.

			Viện dẫn chương, trang, mục tham chiếu		Không viện dẫn chương, trang, mục tham chiếu
4	Khả năng quét	Có khả năng thực hiện quét khám phá ứng dụng toàn diện (full crawl) và thực hiện kiểm thử chuyên sâu tại các khu vực/chức năng được chỉ định (ví dụ: các luồng nghiệp vụ quan trọng, các trang yêu cầu xác thực, các API).	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
5	Khả năng phát hiện lỗ hổng	Có khả năng phát hiện nhiều loại lỗ hổng DAST (Dynamic Application Security Testing) phổ biến như OWASP Top 10,…	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
6	Cơ chế phân tích	Có cơ chế phân tích hiệu quả để tối ưu tỷ lệ phát hiện lỗ hổng thực tế (True Positives) và giảm thiểu cảnh báo sai (False Positives); đồng thời phải cung cấp khả năng cấu hình linh hoạt (ví dụ: thông qua quy tắc loại trừ - exclusion rules, quy tắc trấn áp - suppression rules, hoặc các bộ lọc tùy chỉnh) để tinh chỉnh kết quả và phù hợp với đặc thù ứng dụng	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
7	Báo cáo	Cung cấp báo cáo chi tiết về các lỗ hổng, mức độ nghiêm trọng, các bước tái hiện và đề xuất khắc phục.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu

8	Xác thực ứng dụng	Hỗ trợ nhiều phương pháp xác thực ứng dụng.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
9	Khả năng cung cấp API cho các hệ thống khác	Công cụ DAST phải cung cấp đầy đủ API (ưu tiên RESTful với định dạng JSON) để hỗ trợ tự động hóa và tích hợp liền mạch với các hệ thống bên ngoài.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
10	Thời gian bản quyền	Bản quyền phần mềm và dịch vụ hỗ trợ kỹ thuật chính hãng 03 năm.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
III	**Gói triển khai, đào tạo, vận hành**				
	Khi cung cấp license Bộ công cụ SAST và DAST, Nhà thầu phải kèm theo dịch vụ tư vấn và triển khai xây dựng giải pháp CI/CD tích hợp kiểm thử bảo mật (DevSecOps) phù hợp với đặc thù của Chủ đầu tư. Phạm vi hạng mục dịch vụ này bao gồm:				
1	Khảo sát và thiết kế	Phân tích nhu cầu, nguồn lực hiện có và thiết kế phương thức, kịch bản dò quét tối ưu (SAST/DAST) để tích hợp vào quy trình CI/CD (Tích hợp Liên tục-Continuous Integration/Chuyển giao Liên tục-Continuous Delivery).	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu

2	Triển khai và cấu hình cài đặt	Thực hiện cài đặt, cấu hình các công cụ SAST/DAST và tích hợp chúng vào các công cụ CI/CD hiện có của chủ đầu tư (ví dụ: Jenkins, GitLab CI/CD, Azure DevOps Pipelines) theo thiết kế.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
3	Kiểm thử nghiệm thu	Thực hiện các bài kiểm thử nghiệm thu (Acceptance Tests) để xác nhận toàn bộ giải pháp CI/CD tích hợp bảo mật hoạt động hiệu quả theo yêu cầu đã định.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
4	Đào tạo và chuyển giao công nghệ	Đào tạo chuyên sâu cho đội ngũ vận hành và phát triển của Chủ đầu tư về cách sử dụng, quản lý và duy trì giải pháp DevSecOps đã triển khai.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu