NGÂN HÀNG TMCP THỊNH VƯỢNG VÀ PHÁT TRIỂN

Hà nội, ngày 12 tháng 8 năm 2024

THƯ MỜI CHÀO HÀNG CẠNH TRANH

Kính gửi: Quý Công ty

Ngân hàng TMCP Thịnh vượng và Phát triển (PGBank) chuẩn bị tổ chức chào hàng cạnh tranh gói mua sắm ***"Trang bị phần mềm rà quét kiểm tra an toàn cho mã nguồn tại PGBank."*** tại Tầng 24 – Tòa Mipec - 229 Tây Sơn - Quận Đống Đa - Hà Nội. Trân trọng kính mời Quý Công ty quan tâm tham gia chào hàng cạnh tranh gói mua sắm nêu trên.

Quý Công ty sẽ được cung cấp bộ hồ sơ yêu cầu tại website Ngân hàng TMCP Thịnh vượng và Phát triển: https://www.pgbank.com.vn/.

Thời gian phát hành hồ sơ yêu cầu từ 16 giờ 00 ngày 09 tháng 8 năm 2024 đến trước 17 giờ 00 ngày 09 tháng 08 năm 2024. (giờ Việt Nam)

Hồ sơ chào hàng cạnh tranh phải được gửi đến Ngân hàng TMCP Thịnh vượng và Phát triển muộn nhất là trước 17 giờ 00, ngày 15 tháng 08 năm 2024.

Hồ sơ phải được niêm phong kín bên ngoài ghi rõ "**Trang bị phần mềm rà quét kiểm tra an toàn cho mã nguồn tại PGBank.**". Hồ sơ chào hàng cạnh tranh sẽ không hợp lệ và bị loại nếu không có niêm phong, niêm phong bị hư hại hoặc gửi tới địa chỉ trên quá giờ quy định ở trên.

PGBank thực hiện nhận HSĐX/báo giá, mở HSĐX/báo giá có thể nhiều hơn 1 lần. Sau thời hạn báo giá lần đầu, PGBank thực hiện mở HSĐX/báo giá và PGBank được quyền yêu cầu NCC đã gửi HSĐX/báo giá thực hiện đàm phán giá, điều kiện thương mại. PGBank có thể nhận HSĐX/báo giá và mở HSĐX/báo giá trong các lần tiếp theo theo thông báo bằng thư điện tử (email) của PGBank nhằm đạt được mức giá tối ưu nhất, tùy vào thực tế việc chào hàng.

Nếu Quý Công ty cần biết thêm thông tin, xin vui lòng liên hệ với đầu mối như bên dưới.

Hồ sơ đề xuất xin vui lòng gửi về địa chỉ:

Ngân Hàng TMCP Thịnh vượng và Phát triển

Tầng 24, Tòa nhà Mipec, 229 Tây Sơn, Đống Đa, Hà Nội

Người nhận: **Mr. Vũ Minh Thành - Trung tâm mua sắm** – 0914115595

ĐẠI DIỆN NGÂN HÀNG TMCP THỊNH VƯỢNG VÀ PHÁT TRIỂN

M.S.D.N: 1400116233-C.T.
NGÂN HÀNG THƯƠNG MẠI CỔ PHẦN THỊNH VƯỢNG VÀ PHÁT TRIỂN
Q. ĐỐNG ĐA - T.P HÀ NỘI

PHÓ TỔNG GIÁM ĐỐC ĐIỀU HÀNH

Trần Văn Luân

HỒ SƠ MỜI CHÀO HÀNG CẠNH TRANH

Gói mua sắm: **Trang bị phần mềm rà quét kiểm tra an toàn cho mã nguồn tại PGBank.**
Bên mời chào hàng cạnh tranh: Ngân hàng TMCP Thịnh vượng và Phát triển (PGBank)

M.S.D.N: 1400116233 - C.T.C.P
NGÂN HÀNG THƯƠNG MẠI CỔ PHẦN THỊNH VƯỢNG VÀ PHÁT TRIỂN
Q. ĐỐNG ĐA - T.P HÀ NỘI

PHÓ TỔNG GIÁM ĐỐC ĐIỀU HÀNH
Trần Văn Luận

ĐẠI DIỆN BÊN CHÀO HÀNG CẠNH TRANH

PHẦN A. TỪ NGỮ VIẾT TẮT

PGBANK	Ngân hàng TMCP Thịnh vượng và Phát triển
CHCT	Chào hàng cạnh tranh
HSYC	Hồ sơ yêu cầu
HSĐX	Hồ sơ đề xuất
HSĐXKT	Hồ sơ đề xuất kỹ thuật
HSĐXTC	Hồ sơ đề xuất tài chính
VND	Đồng Việt Nam

PHẦN B. CHỈ DẪN ĐỐI VỚI NHÀ CUNG CẤP

Mục 1. Nội dung mời chào hàng cạnh tranh

1. PGBank mời nhà cung cấp tham gia chào hàng cạnh tranh gói CHCT được mô tả bắt đầu từ **Mục 2** của phần này.
2. Tên gói CHCT: **Trang bị phần mềm rà quét kiểm tra an toàn cho mã nguồn tại PGBank.**
3. Loại hợp đồng: trọn gói

Mục 2. Thời hạn triển khai

Thời gian triển khai – Tối đa 30 ngày.

Đào tạo và bàn giao tài liệu – Tối đa 10 ngày. Áp dụng kể từ thời điểm bàn giao hoặc có email xác nhận license dịch vụ từ nhà sản xuất.

Mục 3. Hiện trạng và mục tiêu đầu tư

1. **Hiện trạng**

PGBank đang có nhu cầu **"Trang bị phần mềm rà quét kiểm tra an toàn cho mã nguồn tại PGBank"**

2. **Mục tiêu đầu tư**

Trang bị phần mềm rà quét kiểm tra an toàn cho mã nguồn tại PGBank để kiểm soát được an toàn cho mã nguồn và ứng dụng, phát hiện ra các điểm yếu nghiêm trọng để kịp thời khắc phục trước khi đưa ra ngoài cho các đơn vị sử dụng tránh được các điểm yếu nghiêm trọng ảnh hưởng đến dịch vụ của Ngân hàng.

Mục 4. Nội dung của HSĐX

HSĐX do nhà cung cấp chuẩn bị phải bao gồm:

1. Đơn chào hàng;
2. Tài liệu chứng minh tư cách hợp lệ của nhà cung cấp;
3. Hồ sơ đề xuất kỹ thuật đáp ứng các yêu cầu của PGBank;
4. Hồ sơ đề xuất tài chính;
5. Các tài liệu khác mà nhà cung cấp thấy cần thiết để làm rõ năng lực và kinh nghiệm của mình trong việc triển khai Gói chào hàng.
6. Cam kết của NCC:
   - Cam kết của NCC về việc tham gia chào giá minh bạch, trung thực, không đưa hối lộ cho nhân sự liên quan của PGBank dưới mọi hình thức (quà, tiền mặt, tiền chuyển khoản, lợi ích khác,…) trước, trong và sau khi công bố kết quả Chào hàng cạnh tranh.
   - Cam kết bảo mật thông tin cho PGBank nếu được PGBank lựa chọn là NCC
   - Cam kết chất lượng các sản phẩm tốt nhất và tiến độ giao hàng/thực hiện theo thỏa thuận

Mục 5. Làm rõ HSYC

1. **Làm rõ HSYC**

Trong trường hợp cần làm rõ HSYC, nhà cung cấp gửi đề nghị làm rõ đến bên mời chào hàng muộn nhất trước thời điểm đóng chào hàng. Khi nhận được đề nghị làm rõ HSYC của nhà cung cấp, bên mời chào hàng sẽ trả lời cho nhà cung cấp có yêu cầu làm rõ và tất cả các nhà cung cấp khác đã nhận HSYC từ bên mời chào hàng, trong đó mô tả nội dung yêu cầu làm rõ nhưng không nêu tên nhà cung cấp đề nghị làm rõ. Trường hợp việc làm rõ dẫn đến phải sửa đổi HSYC thì bên mời chào hàng tiến hành sửa đổi HSYC theo thủ tục quy định tại Khoản 2 Mục này.

2. **Sửa đổi HSYC**

Trường hợp sửa đổi HSYC, chủ đầu tư sẽ gửi quyết định sửa đổi kèm theo những nội dung sửa đổi đến tất cả các nhà cung cấp đã nhận HSYC không muộn hơn tối thiểu 02 ngày làm việc trước ngày có thời điểm cuối nhận HSĐX, trường hợp không đủ 02 ngày làm việc thì chủ đầu tư sẽ gia hạn thời điểm cuối nhận HSĐX tương ứng.

Mục 6. Đơn chào hàng cạnh tranh

Đơn chảo hàng cạnh tranh phải có chữ ký của người đại diện hợp pháp của nhà cung cấp (người đại diện theo pháp luật của NCC hoặc người được ủy quyền kèm theo giấy ủy quyền hợp lệ)

Mục 7. Giá chào hàng cạnh tranh

Giá chào cạnh tranh bằng VNĐ, là giá đã bao gồm các loại thuế/phí theo quy định và tất cả các chi phí phát sinh liên quan mà PGBank không phải chịu thêm bất kỳ 1 chi phí nào khác.

Mục 8. Thời gian có hiệu lực của HSĐX

Thời gian có hiệu lực của HSĐX là tối thiểu 30 ngày, kể từ ngày có thời điểm hết hạn nộp hồ sơ chào giá. HSĐX nào có thời hạn hiệu lực ngắn hơn quy định sẽ không được tiếp tục xem xét, đánh giá.

Mục 9. Chuẩn bị và nộp HSĐX

1. Nhà cung cấp phải chuẩn bị 01 bản gốc, túi đựng HSĐX phải được niêm phong và ghi rõ tên gói chào giá, tên nhà cung cấp. Bên chủ đầu tư có trách nhiệm bảo mật thông tin trong HSĐX của nhà cung cấp.

2. Nhà cung cấp nộp trực tiếp hoặc gửi HSĐX theo đường bưu điện địa chỉ của bên chủ đầu tư nhưng phải đảm bảo bên chủ đầu tư nhận được trước thời hạn nộp hồ sơ trước … giờ ngày ….. tháng …….năm…. theo địa chỉ như sau:

   a) Ngân Hàng TMCP Thịnh vượng và Phát triển
   b) Tầng 24, Tòa nhà Mipec, 229 Tây Sơn, Đống Đa, Hà Nội
   c) Người liên hệ : Mr. Vũ Minh Thành
   d) Email: thanhvm@pgbank.com.vn
   e) Điện thoại: (+84) 914.115.595

Đồng thời, gửi bản mềm của HSĐX (đã mã hóa bằng mật khẩu - khác nhau cho HSĐXKT và HSĐXTC) tới hòm thư điện tử: hienntt3@pgbank.com.vn trước thời hạn nộp hồ sơ. Mật khẩu chỉ được cung cấp cho bên mời chào hàng khi được yêu cầu bởi bên mời chào hàng. Nhà cung cấp cam kết tính đồng nhất thông tin giữa bản mềm và bản cứng của HSĐX đã gửi.

3. Bên chủ đầu tư sẽ tiếp nhận HSĐX của tất cả nhà cung cấp nộp HSĐX trước thời hạn nộp hồ sơ. Trường hợp nhà cung cấp nộp HSĐX sau thời hạn thì HSĐX bị loại và được trả lại nguyên trưng cho nhà cung cấp.

Mục 10. Làm rõ HSĐX

Sau khi mở báo giá, nhà cung cấp có trách nhiệm làm rõ hồ sơ đề xuất theo yêu cầu của bên mời chào giá.

Việc làm tỏ phải bảo đảm không làm thay đổi bản chất của nhà cung cấp, không làm thay đổi nội dung cơ bản của hồ sơ đề xuất đã nộp.

Mục 11. Mở báo giá

- Việc mở báo giá không phụ thuộc vào sự có mặt hay vắng mặt của đại diện nhà cung cấp tham dự chào hàng.
- Việc mở chào giá được thực hiện theo trình tự sau đây:

  + Kiểm tra niêm phong hoặc mở bản mềm với mật khẩu được cung cấp bởi nhà cung cấp.

  + Mở bản chào giá và đọc to, rõ tối thiểu những thông tin sau: tên nhà cung cấp, giá, thời gian có hiệu lực của chào giá và các thông tin khác mà bên mời chào hàng thấy cần thiết.

Mục 12. Điều kiện đối với nhà cung cấp được chọn

Nhà cung cấp được xem xét, đề nghị trùng chào giá kín khi đáp ứng đủ các điều kiện sau đây:

- Có Hồ sơ đề xuất hợp lệ.
- Có năng lực và kinh nghiệm đáp ứng yêu cầu.
- Có giá đề nghị chào hàng không vượt quá ngân sách được phê duyệt.

Mục 13. Thông báo kết quả

Kết quả lựa chọn nhà cung cấp sẽ được gửi đến tất cả cung cấp tham dự chào hàng qua thư điện tử.

Mục 14. Thương thảo, hoàn thiện và ký kết hợp đồng.

1. Thương thảo về những nội dung chưa đủ chi tiết, chưa rõ hoặc chưa phù hợp, thống nhất giữa Hồ sơ yêu cầu và Hồ sơ đề xuất, giữa các nội dung khác nhau trong Hồ sơ đề xuất có thể dẫn đến các phát sinh, tranh chấp hoặc ảnh hưởng đến trách nhiệm của các bên trong quá trình thực hiện hợp đồng.
2. Thương thảo về các sai lệch do chủ đầu tư phát hiện và đề xuất trong hồ sơ đề xuất (nếu có).
3. Thương thảo về các vấn đề phát sinh trong quá trình lựa chọn nhà cung cấp (nếu có) nhằm mục tiêu hoàn thiện các nội dung chi tiết của gói CHCT.

Phần C. YÊU CẦU VỀ NĂNG LỰC KINH NGHIỆM

Mục 1: Yêu cầu về năng lực tài chính

STT	Yêu cầu chi tiết	Bắt buộc/ Tùy chọn	Mức độ đáp ứng của Bên chào hàng	
			Đạt	Không đạt
1	**Năng lực tài chính kể từ khi thành lập hoặc trong 3 năm gần nhất (2021, 2022, 2023)**			
1.1	Đính kèm Báo cáo tài chính hàng năm kể từ khi thành lập hoặc trong 3 năm gần nhất (2021, 2022, 2023), đã nộp cơ quan thuế hoặc báo cáo tài chính đã được kiểm toán và biên lai nộp thuế các năm (bản photo). Lợi nhuận sau thuế (Bắt buộc phải có lãi) trong năm gần nhất. Ưu tiên nhà cung cấp có báo cáo tài chính hàng năm.	Bắt buộc	Có	Không
2	**Năng lực cung cấp bản quyền giải pháp, dịch vụ**			
2.1	Nhà thầu cung cấp giấy phép hoặc thư ủy quyền bán hàng của nhà sản xuất, hoặc nhà phân phối hoặc nhà bán lẻ được nhà sản xuất ủy quyền tại khu vực châu á.	Bắt buộc	Có	Không
2.2	Nhà thầu có đủ 2 chứng nhận ISO9001 và ISO27001	Bắt buộc	Có	Không

Mục 2: Yêu cầu về kinh nghiệm triển khai

STT	Yêu cầu chi tiết	Bắt buộc/ Tùy chọn	Mức độ đáp ứng của Bên chào hàng	
			Đạt	Không đạt
1	Số năm thành lập: Trên 5 năm	Bắt buộc	Có	Không
2	Bản sao có công chứng Giấy chứng nhận đăng ký kinh doanh hoặc Giấy chứng nhận đăng ký đầu tư hoặc tài liệu tương đương được cấp theo quy định của pháp luật Việt Nam	Bắt buộc	Có	Không
3	Nhà thầu có kinh nghiệm triển khai tối thiểu 2 hợp đồng cung cấp giải pháp an toàn thông tin hoặc mật mã dân sự có giá trị tối thiểu 2 tỷ đồng hoặc hợp đồng cung cấp giải pháp rò quét điểm yếu mã nguồn tương tự với giá trị tối thiểu là 1,5 tỷ đồng.	Bắt buộc	Có	Không
4	Nhà cung cấp **cam kết về việc đảm bảo đầy đủ nhân sự** trong cơ cấu tổ chức tham gia triển khai dự án. Tối thiểu 1 nhân sự có chứng chỉ DevOps, 1 nhân sự có chứng chỉ CSSLP hoặc đã tham gia khóa học uy tín cao trên thế giới do pcmag đánh giá.	Bắt buộc	Có	Không

Mục 3: Yêu cầu về kỹ thuật

Nhà cung cấp phải cung cấp được các văn bản, tài liệu, chứng chỉ... để chứng minh đạt đáp ứng các tiêu chuẩn, tiêu chí lựa chọn, những yêu cầu **"PGBank chỉ chấp nhận đáp ứng toàn bộ"** nếu Đáp ứng 1 phần hoặc Không đáp ứng thì **bị loại.**

STT	Yêu cầu chi tiết	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
I	**Yêu cầu cơ bản bắt buộc phải đáp ứng**				
1	Số lượng License cho người sử dụng: - 25 License cho mã nguồn mở SCA (Software Composition Analysis), bao gồm cả Docker Container Security. - 25 License cho mã nguồn tĩnh SAST (Static Application Security Testing). Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
2	Điều kiện License của sản phẩm phải đảm bảo đầy đủ các thành phần sau: - Có đầy đủ tính năng theo số lượng nhà phát triển (Developers) và người quản trị. - Không giới hạn số lượng dự án được quản lý (project) - Không giới hạn số lượng dự án được quét đồng thời. - Không giới hạn số lượng kho lưu trữ được quản lý (repositories) và được cập nhật cảnh báo lỗ hổng. Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
3	Ứng dụng hoạt động trong môi trường lai ghép (hybrid) - Scan Engine đặt tại máy chủ nhà cung cấp dịch vụ - Máy chủ lưu trữ source code đặt tại PGBank và do nhân sự PGBank quản lý. - Ứng dụng không được phép upload code ra ngoài môi trường internet. - Hành vi quét mã nguồn gồm (tĩnh và mở) đều thực hiện trên máy chủ quản lý mã nguồn của PGBank. Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				

STT	Yêu cầu chi tiết	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
4	Bắt buộc ứng dụng được nằm trong danh TOP 5 những nhà phát triển (Developers) được The Forrester Wave hoặc Gartner đánh giá cao nhất cho ít nhất 1 hạng mục SCA hoặc SAST kể tại thời điểm năm 2023 hoặc 2024. Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
II	**Yêu cầu về cài đặt, Triển khai, phương pháp tính license**				
5	Yêu cầu bắt buộc ứng dụng cho phép nhà phát triển (Developers) quét mã nguồn trực tiếp từ máy tính. - Thông qua (windows command prompt) không cần sử dụng thông qua IDE - Không upload code lên môi trường internet dưới mọi hình thức				
III	**Yêu cầu chung về công nghệ và khả năng tích hợp**				
III.1	**Yêu cầu chung**				
6	Hỗ trợ cho nhiều loại trình quản lý gói - Cho phép chọn ngôn ngữ sẽ được quét - Nền tảng lập trình và các tác nhân khởi tạo ứng dụng từ các ngôn ngữ sau: ABAP | Android Java | APEX | ASP Classic/VB Basic/VBScript | C/C++ (beta) | COBOL | C# | ColdFusion | Go | Groovy | Java |iOS Objective C | JavaScript / Node.js | Kotlin / Kotlin Mobile | PHP | PLSQL | Python | R | Ruby| Swift | TypeScript | VB.Net | VBScript | Visual Basic | Xamarin C#				
7	Có khả năng phát hiện các tệp tin độc hại hoặc các đoạn mã nhị phân chứa mã độc Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
8	Cho phép nhà phát triển (Developers) tiếp cận đến các thông tin về những rủi ro của thư viện, và khuyến nghị ưu tiên cập nhật rủi ro này.				

STT	Yêu cầu chi tiết	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
9	Có khả năng tích hợp với kho lưu trữ như GitHub, GitLab, Azure DevOps và Bitbucket, Google DevOp				
10	Có khả năng Tích hợp với các IDE phổ biến, như IntelliJ, Eclipse, Visual Studio, Mã Visual Studio, PyCharm và WebStorm.				
11	Bắt buộc tích hợp với các trình duyệt phổ biến để các nhà phát triển (Developers) có thể xem trước các thông tin chi tiết về một thành phần, như phiên bản, giấy phép, và các lỗ hổng bảo mật đã biết, ngay từ trình duyệt trước khi quyết định tải nó về.				
12	Cho phép tích hợp CI/CD tất cả các giai đoạn trong vòng đời phát triển ứng dụng. Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
III.2	**Yêu cầu đáp ứng khả năng mở rộng**				
13	Có tính năng mở rộng để hỗ trợ quét ảnh Docker/ Quét container. Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
14	Ứng dụng có thể xác định và nhận dạng các mô hình AI - Có nguồn gốc từ Hugging Face, một nền tảng và kho lưu trữ phổ biến dành cho các mô hình AI được đào tạo trước - Phát hiện trong bối cảnh của một ứng dụng mà các mô hình AI này đang được sử dụng hoặc tích hợp.				
15	Hệ thống đánh giá và báo cáo mọi lỗ hổng bảo mật liên quan đến các mô hình AI và xác định các rủi ro hoặc điểm yếu bảo mật tiềm ẩn có thể bị khai thác. Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
16	Phần mềm phải có khả năng scan mở rộng về giấy phép các mô hình AI				

STT	Yêu cầu chi tiết	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
17	Khả năng mở rộng khi cần thiết để kích hoạt chức năng quét cơ sở hạ tầng phổ biến dưới dạng Trình quản lý mã (IaC) để tìm các cấu hình sai, bao gồm Terraform, CloudFormation, Kubernetes, Mẫu ARM, Mô hình không có máy chủ và Helm.				
IV	**Áp dụng chung cho nền tảng SAST và SCA**				
IV.1	**Quản lý và giảm thiểu rủi ro**				
18	Cho phép đánh dấu hoặc làm nổi bật những điểm yếu tố không tuân thủ trong souce code về điều kiện giấy phép mã nguồn. Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
19	Định nghĩa chính sách với tùy chỉnh thuộc tính. - Cho phép định nghĩa chính sách quét ứng dụng. - Định nghĩa chính sách trong phát hiện và phân loại lỗ hổng - Cho phép định nghĩa các chính sách ưu tiên cảnh báo lỗ hổng (có thể lựa chọn theo mức độ nghiêm trọng của lỗ hổng) liên quan đến ứng dụng và nhân sự tiếp nhận thông tin				
20	Có khả năng phân tích đầy đủ các thông tin như: - Metadata (siêu dữ liệu chứa toàn bộ thông tin của source code) - Phân tích các phụ thuộc giữa các thư viện trong source code để đánh giá được các rủi ro liên quan đến source code. Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
21	Cho phép bỏ qua file/thư mục mã nguồn mà bộ phận phát triển nội bộ thực hiện khi được yêu cầu.				
22	Có khả năng bỏ qua và kích hoạt lại chính sách vi phạm nếu ứng dụng vẫn chưa được khắc phục lỗ hổng.				

STT	Yêu cầu chi tiết	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
23	Khả năng đảm bảo rằng các thay đổi mã nguồn được đánh giá theo các quy tắc và tiêu chuẩn cụ thể, đồng thời có thể ngăn chặn việc hợp nhất hoặc triển khai mã nguồn không tuân thủ, từ đó duy trì chất lượng và tính bảo mật của mã nguồn				
24	Có thể tích hợp theo dõi vấn đề với hệ thống ITS để tự động mở ticket theo dõi vấn đề/đóng thẻ Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
25	Phải có chức năng thông báo tự động liên quan đến lỗ hổng mới qua hệ thống mail Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
IV.2	**Báo cáo, giám sát và đo lường**				
26	Cung cấp kết quả quét tổng hợp và báo cáo về lỗ hổng mới trong giao diện người dùng (GUI) và khả năng tạo báo cáo cụ thể theo từng nhóm chức năng.				
27	Lập danh sách phần mềm tài liệu được kiết xuất ở nhiều định dạng khác nhau (ít nhất 04 loại định dạng) Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
28	Có thể xuất báo cáo lỗ hổng phần mềm theo nhiều định dạng kèm CVE chi tiết và dường dẫn tham khảo của hãng công nghệ, và nguồn công khai khác. Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
29	Khả năng đảm bảo rằng dự án vẫn tuân thủ các giấy phép - Giấy phép độc quyền hoặc nguồn mở - Cung cấp hồ sơ toàn diện và tính pháp lý của mã nguồn mở. Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				

STT	Yêu cầu chi tiết	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
30	Cung cấp thông tin có giá trị về cảnh báo được tạo cho các thư viện cụ thể, trong đó bao gồm: - Mô tả lỗ hổng. - Mức độ nghiêm trọng. - Lỗi CVE hoặc CWE có liên quan. - Hậu quả nếu bị khai thác - Thông tin về bản quyền thư viện. - Thông tin về tuân thủ. - Thông tin về hành động nên được thực hiện (hướng dẫn khắc phục) - Các phiên bản cũ mới. - Chất lượng được tính theo mức độ tin cậy của từng phiên bản cập nhật. Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
31	Cung cấp biểu đồ về tình trạng bảo mật theo thời gian trong đó: - Kèm theo kết quả của mã nguồn nhiều lỗ hổng nhiều hơn hay ít hơn. - Liên quan đến xử lý các lỗ hổng bảo mật đã thực hiện trong tổ chức. Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
IV.3	**Tích hợp với ứng dụng khác thông qua API**				
32	Cung cấp API RESTful để cho phép tích hợp các ứng dụng do doanh nghiệp tự viết với ứng dụng này. Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
33	Khả năng tạo báo cáo thông qua API dựa trên rủi ro bảo mật, các loại giấy phép, điểm chất lượng. Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
34	Cung cấp API để các phần mềm khác lấy dữ liệu CVE, Điểm CVSS, Biện pháp khắc phục. Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				

STT	Yêu cầu chi tiết	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
35	Công cụ này phải hỗ trợ các API cho phép các ứng dụng khác cấu hình hệ thống. - Các chính sách, nhóm, người dùng, tạo và xóa dự án, v.v.				
IV.4	**Quản lý truy cập**				
36	Khả năng tương tác và tích hợp với hệ thống SSO dành cho xác thực và ủy quyền				
37	Phần mềm hỗ trợ ghi nhận được các thông tin như quản lý mật khẩu, Kiểm tra hành động của người dùng trong hệ thống theo ID người dùng, IP, và định danh.				
38	Yêu cầu bắt buộc kiểm soát truy cập dựa trên vai trò theo mô hình từ nhỏ dần như sau - cấp tổ chức - cấp dự án - cấp sản phẩm - xác định phạm vi chức năng và quyền quản lý mà có thể được cấp cho người dùng Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
39	Giới hạn khả năng hiển thị kết quả quét ở mức các chủ dự án để phân chia theo chức năng nhiệm vụ của từng dự án				
40	Có chức năng cho phép kỹ sư của nhà sản xuất - Được truy cập vào ứng dụng quét mã nguồn để sửa lỗi theo cách thức on/off ngay trên ứng				
V	**Yêu cầu chung với ứng dụng quét mã nguồn mở SCA (Software Composition Analysis)**				
V.1	**Khả năng phát hiện.**				
41	Yêu cầu bắt buộc có khả năng quét ngoại tuyến - Trường hợp quét tại môi trường do PGBank quản lý. - Trong quá trình quét mất kết nối internet không làm dán đoạn hoặc mất thông tin trong khi thực hiện Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				

STT	Yêu cầu chi tiết	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
42	Có khả năng quét theo chỉ định và khả năng loại trừ - Thư mục lưu trữ - Tệp tin lưu trữ Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
43	Cho phép quét bằng phương pháp sử dụng dòng lệnh dạng windows mode nhưng không được phép upload mã nguồn trong khi sử dụng từ: - Máy tính cá nhân nhà phát triển (Developers) - Máy chủ lưu trữ mã nguồn (Repository) Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
V.2	**Khả năng phân tích gói tin độc hại**				
44	Yêu cầu có chức năng giám sát liên tục và không cần quét lại thủ công mỗi khi phát sinh lỗ hổng mới Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
45	Bắt buộc cung cấp cơ chế và thông tin chính xác để giảm thiểu dương tính/âm tính giả. Tăng khả năng nhận diện và đánh giá mức độ lỗ hổng là chính xác, không chính xác. - ưu tiên những lỗ hổng có thể được khai thác - cung cấp các phương án phân tích sâu mã nguồn để tìm ra cách chúng có thể bị khai thác. Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
46	Cung cấp hướng dẫn khắc phục và phương pháp vá lỗi các thư viện, cập nhật kiến thức cơ bản về lỗ hổng.				

STT	Yêu cầu chi tiết	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
47	Bắt buộc ứng dụng cho phép truy cập và cập nhật danh mục các lỗ hổng. Tăng tài nguyên tham chiếu không chỉ ở thư viện mở mà còn thư viện của nhà sản xuất. - Truy cập cơ sở dữ liệu công cộng. - Truy cập cơ sở dữ liệu của hãng công nghệ.				
48	Khả năng bỏ qua và kích hoạt lại cảnh báo các lỗ hổng an ninh thông tin.				
V.3	**Khả năng phân tích/kiểm tra bản quyền giấy phép đối với source code**				
49	Khả năng hiển thị thông tin chi tiết về giấy phép của phần mềm nguồn mở OSS (Open source software) các thành phần.				
50	Khả năng quản lý giấy phép thư viện, bao gồm cả việc gán hoặc xóa giấy phép.				
51	Khả năng đưa ra các khuyến nghị để giảm thiểu các thành phần không tuân thủ (ví dụ: thư viện không có giấy phép được chỉ định hoặc bản quyền): - Tên thư viện - Tình trạng được giải quyết - Thời gian yêu cầu được giải quyết Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
52	Khả năng bỏ qua và kích hoạt lại cảnh báo vi phạm giấy phép. Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
VI	**Yêu cầu cho sản phẩm quét mã nguồn tĩnh SAST (Static Application Security Testing)**				
VI.1	**Về luồng dữ liệu và điểm yếu bảo mật**				
53	Phải có chức năng cho phép quét trên đa nền tảng. - Quét từ linux, macOS - Quét thông qua public API với ứng dụng khác.				

STT	Yêu cầu chi tiết	Đáp ứng toàn bộ	Đáp ứng 1 phần	Không đáp ứng	Thuyết minh
	Chú ý: PGBank chỉ chấp nhận đáp ứng toàn bộ.				
54	Yêu cầu bắt buộc cung cấp chức năng quét nhanh và ra báo cáo nhanh như - Chỉ định ngôn ngữ được quét - Chỉ định thư viện được nạp vào hệ thống - Sử dụng được trong Windows (vì có thể máy tính của nhà phát triển (Developers) dùng windows) - Định nghĩa được cách thực hiện thông qua pipeline				
55	Cung cấp cảnh báo bảo mật về các điểm yếu phần mềm theo danh sách CWE (Common Weakness Enumeration): Tập đoàn MITRE duy trì CWE, quản lý chương trình; và cung cấp hướng dẫn kỹ thuật khách quan cho Cộng đồng CWE trong suốt quá trình để đảm bảo CWE phục vụ lợi ích công cộng.				
56	Khả năng khuyến nghị dựa trên các ngưỡng lỗ hổng khác nhau theo tiêu chuẩn Common Vulnerability Scoring System - CVSS - Mức nghiêm trọng | cao | trung bình | thấp - số lượng lỗ hổng và tổng hợp số lượng từng mức có liên quan.				
57	Khả năng bỏ qua và kích hoạt lại cảnh báo các lỗ hổng an ninh thông tin.				
58	Phải cung cấp tài liệu giáo dục cho nhà phát triển (Developers) dựa trên phát hiện điểm yếu - Có sẵn trong nền tảng ứng dụng. - Có sẵn trong môi trường công khai				

Phần D. CÁC YÊU CẦU KHÁC

Yêu cầu về chuyển giao, đào tạo, bảo hành, bảo trì, hỗ trợ

STT	Cấu phần chuyên môn	Yêu cầu chi tiết	Bắt buộc/ Tùy chọn
1	**Yêu cầu đào tạo**	**Ngôn ngữ đào tạo:** Tiếng Việt. Nếu giáo viên là người nước ngoài thì phải có phiên dịch có chuyên môn.	**Bắt buộc**
		Tài liệu đào tạo: là bản sao điện tử (soft copy) bằng tiếng Việt hoặc tiếng Anh có bản dịch. Tài liệu đào tạo phải được cung cấp cho PGBank trước thời điểm đào tạo tối thiểu 05 ngày làm việc.	
		Môi trường đào tạo:	
		- *Nhà cung cấp phải cung cấp hoặc sử dụng các công cụ đào tạo thích hợp cho chương trình đào tạo được đề xuất, bao gồm lý thuyết, hướng dẫn thực hành và thao tác thực tế trên máy.*	
		- *Nhà cung cấp phải thiết lập môi trường đào tạo và thực hành cần thiết riêng biệt.*	
2	**Chuyển giao tài liệu đào tạo**	Các tài liệu chuyển giao cho PGBank phải là các tài liệu chuẩn, phù hợp với phiên bản ứng dụng triển khai tại PGBank.	**Bắt buộc**
		Nhà cung cấp phải thực hiện việc cập nhật tài liệu theo từng lần phát hành hoặc nâng cấp phần mềm tương ứng.	
		Tài liệu cần phải được chuyển giao theo hình thức là bản sao điện tử (soft copy).	
		Trong suốt quá trình triển khai dự án, Nhà cung cấp phải truyền đạt đầy đủ kiến thức và bàn giao công nghệ cho PGBank đảm bảo PGBank có thể tiếp nhận hệ thống.	
3	**Bàn giao**	- Thư xác nhận tài sản, hoặc dịch vụ từ hãng công nghệ. - Ứng dụng dạng tài sản, hoặc dịch vụ do PGBank được chứng nhận và quản lý - Tài liệu hướng dẫn cài đặt và triển khai - Xác nhận đào tạo chuyên môn từ nhà bán hàng.	**Bắt buộc**
4		Nhà cung cấp phải cung cấp **thư cam kết hỗ trợ, bảo hành, bảo trì** của nhà sản xuất đối với từng danh mục hàng hóa cung cấp	**Bắt buộc**
		Dưới đây là một số yêu cầu về dịch vụ Bảo hành, bảo trì và hỗ trợ kỹ thuật của PGBank, đề nghị Nhà cung cấp nêu rõ khả năng đáp ứng, mức độ đáp ứng, trường hợp không đáp ứng, đề nghị Nhà cung cấp nêu rõ lý do:	
		Hỗ trợ kỹ thuật chính hãng 24 giờ/ngày và 07 ngày/tuần.	
		Thời gian đáp ứng: 02 giờ kể từ thời điểm nhận được thông báo có sự cố (có phương án thực hiện hành động khắc phục).	
		Thời gian khắc phục sự cố tối đa: 04 giờ kể từ thời điểm nhận được thông báo có sự cố, Nhà cung cấp phải khắc	

STT	Cấu phần chuyên môn	Yêu cầu chi tiết	Bắt buộc/ Tùy chọn
		phục xong sự cố để PGBank có thể hoạt động nghiệp vụ bình thường.	
		Các hoạt động bảo hành, bảo trì và hỗ trợ kỹ thuật đều phải được ghi nhận nhật ký thực hiện.	