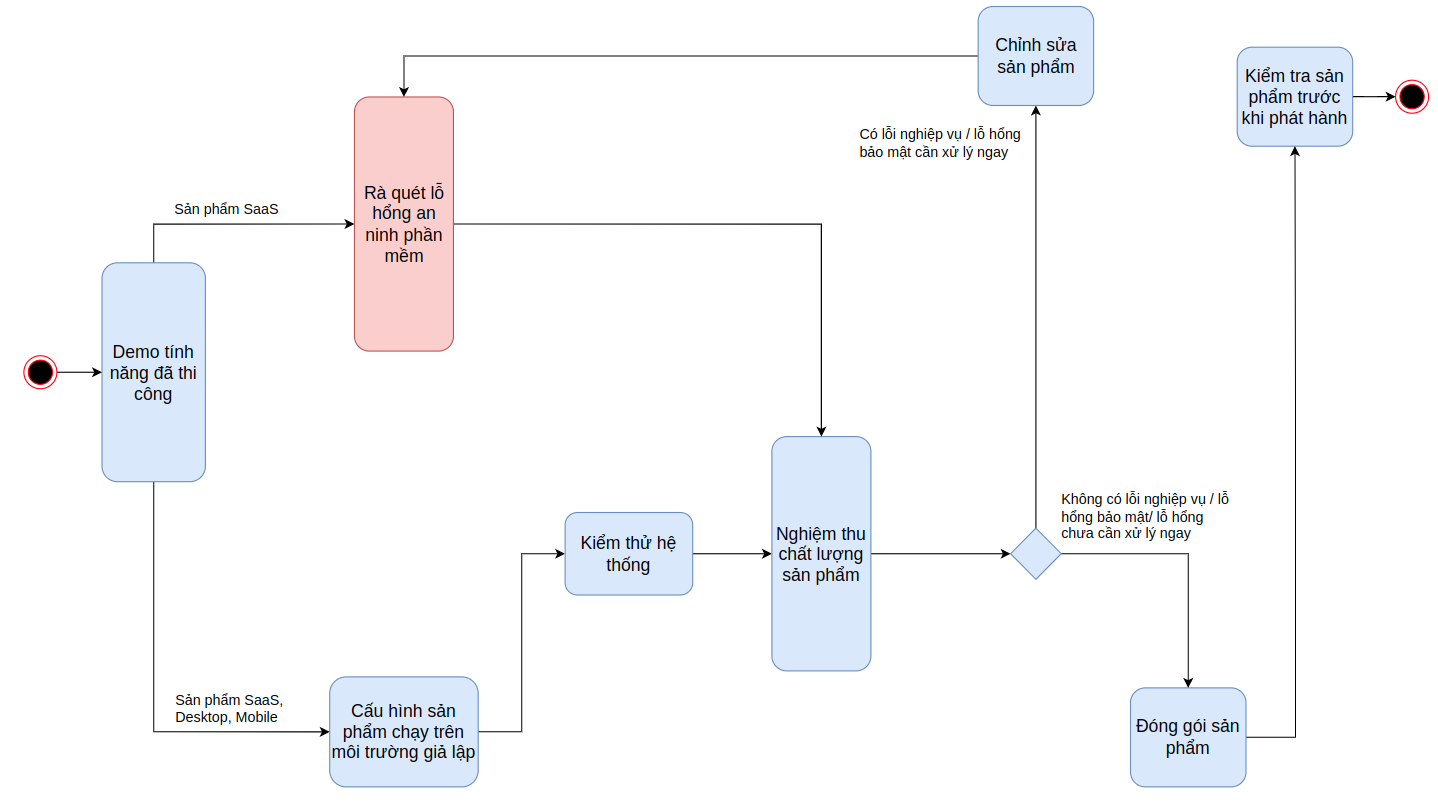
**QUY TRÌNH TÍCH HỢP CÔNG CỤ SAST VÀO QUÁ TRÌNH PHÁT TRIỂN PHẦN MỀM**

****

| **STT** | **Người thực hiện** | **Các bước thực hiện** | **Đầu ra** | **Yêu cầu/Thời gian** | **Ghi chú** |
| --- | --- | --- | --- | --- | --- |
| **Trước khi phát hành bản đầu tiên ra khách hàng** | | | | | |
| 1 | EM | * Gửi yêu cầu cho Ban ANTT để yêu cầu đánh giá an ninh ứng dụng trước khi phát hành chính thức. Lưu ý gửi kèm đường dẫn và tài khoản để phục vụ đánh giá | Email yêu cầu đánh giá | Trước khi phát hành chính thức sản phẩm ít nhất 3 ngày |  |
| 2 | Nhân viên ANTT | * Thực hiện đánh giá ANTT (pentest) theo yêu cầu * Xin ý kiến CSO về phương án, thời hạn cần xử lý lỗ hổng * Phản hồi kết quả đánh giá, phương án xử lý các lỗ hổng (nếu có) cho EM | Email thông báo kết quả đánh giá ANTT |  |  |
| 3 | EM | * Xem xet kết quả đánh giá, lập kế hoạch xử lý lỗ hổng * Xin ý kiến CSO về các lỗ hổng chưa xử lý được ngay   + Nếu CSO đồng ý, dự án tiếp tục các thủ tục phát hành sản phẩm | WI Bug ghi nhận lỗ hổng được cập nhật trạng thái sửa lỗi.  Email xác nhận của CSO về việc đồng ý/không đồng ý đề xuất của EM |  |  |
| **Đối với từng phiên bản phát hành** | | | | | |
| 1 | DevOps Engineer | * Thực hiện kéo source code về CI Server.   + Sử dụng công cụ SAST để thực hiện rà quét và tìm lỗ hổng trong bộ source code.   + Đẩy kết quả rà quét lên dashboard quản lý lỗ hổng tập trung theo mã dự án và phiên bản phát hành.   + Thông báo tới nhân viên ANTT về kết quả lỗ hổng trên trình quản lý lỗ hổng. | - File kết quả rà quét lỗ hổng  - Danh sách lỗ hổng trên dashboard |  |  |
| 2 | Nhân viên ANTT, EM/SWE Lead | * Nhân viên ANTT đánh giá lại kết quả lỗ hổng tìm ra được:   + Dựa vào kết quả rà quét, nhân viên ANTT review code, kiểm tra lại lỗi đó là đúng hay sai, đánh giá mức độ nghiêm trọng cũng như những tác động gây hại mà nó có thể gây ra.   + Nhân viên ANTT có thể trao đổi với EM/SWE Lead dự án để hỗ trợ đánh giá một cách chính xác nhất.   + Sau khi đánh giá lỗi, nhân viên ANTT cập nhật lại kết quả trên trình quản lý tập trung và gửi mail thông báo tới EM dự án kết quả đánh giá cuối cùng. * EM/SWE Lead:   + Hỗ trợ nhân viên ANTT đánh giá lỗ hổng khi có yêu cầu. | Danh sách lỗ hổng mới sau khi được đánh giá lại | 3 tiếng kể từ khi nhận được thông báo |  |
| 3 | Nhân viên ANTT, CSO, GĐK dự án | * Thống nhất phương án xử lý lỗ hổng:   + Nhân viên ANTT đề xuất phương án và thời điểm xử lý lỗ hổng: xác định lỗ hổng nào cần phải được sửa trước khi triển khai; lỗ hổng nào được phép sửa sau khi triển khai.   + Nhân viên ANTT cùng với CSO thống nhất phương án xử lý và thời hạn xử lý lỗ hổng.   + Nhân viên ANTT thông báo EM xử lý lỗ hổng. Lưu ý: không nêu lỗ hổng là gì? Chỉ nêu cần phải làm gì? và làm như thế nào?   + Nhân viên ANTT cập nhật kết quả rà quét lỗ hổng và biện pháp xử lý vào Báo cáo an ninh thông tin | * Email về việc xử lý lỗ hổng gửi cho EM dự án. | Theo kế hoạch xử lý lỗi và được thống nhất giữa Ban AN và EM dự án |  |

**Phụ lục:**

* Công cụ SAST phục vụ rà quét lỗ hổng: CodeQL
* Trình quản lý lỗ hổng tập trung: Defect Dojo