TÀI LIỆU ĐỀ XUẤT GIẢI PHÁP PHẦN MỀM ANALYTIC PORTAL

# 1. Giới thiệu

## 1.1. Mục đích

Tài liệu này là để mô tả các yêu cầu Giải pháp Phần mềm "Web Portal" (sau đây gọi là Phần mềm) hỗ trợ cho khách hàng gửi các tệp tin, các mẫu thử cần phân tích về an toàn thông tin lên hệ thống CORE phân tích của Melltrix, và hiển thị lại các kết quả dưới dạng biểu đồ

## 1.2. Phạm vi dự án

Phần mềm được xây dựng dựa trên cơ sở yêu cầu xây dựng phần mềm của Công Ty Asic, Giúp cho khách hàng gửi mẫu phân tích và nhận về kết quả phân tích một cách trực quan và tiện dụng nhất

Phần mềm cũng là công cụ để khách hàng theo lưu trữ và theo dõi các mẫu cũng như kết quả phân tích một cách dễ dàng

# 2. Tóm tắt giải pháp

## 2.1. Vấn đề hiện tại

- Cần 1 hệ thống web cho phép khách hàng và hệ thống CORE tương tác được với nhau, để khách hàng có thể gửi mẫu và nhận được kết quả

- Nếu như hệ thống CORE chưa thể phân tích tự động thì sẽ chuyển qua người phụ trách trực tiếp phân tích và trả về kết quả

## 2.2. Giải pháp đề xuất

Hệ thống bao gồm các các chức năng chính

* **1. Gửi Mẫu Tài Liệu và Phân Tích Mã Độc**
  + 1.1. Upload Tài Liệu
    - Chức năng: Cho phép người dùng tải lên các mẫu tài liệu cần phân tích.
    - Hỗ trợ nhiều định dạng file (PDF, DOCX, XLSX...).
    - Kiểm tra kích thước và định dạng file trước khi upload.
    - Giao diện thân thiện để kéo và thả file hoặc chọn từ máy tính.
  + 1.2. Gửi Yêu Cầu Phân Tích
    - Chức năng: Gửi tài liệu đã upload lên hệ thống phân tích mã độc.
    - Tự động chuyển file lên hệ thống phân tích.
    - Đảm bảo dữ liệu được truyền tải an toàn (sử dụng mã hóa SSL/TLS).
    - Ghi nhận thông tin yêu cầu gửi đi (người gửi, thời gian, trạng thái).
  + 1.3. Theo Dõi Trạng Thái Xử Lý
    - Chức năng: Cung cấp khả năng theo dõi tiến độ phân tích của tài liệu.
    - Hiển thị trạng thái hiện tại (Đang xử lý, Hoàn thành, Lỗi).
    - Cập nhật thời gian dự kiến hoàn thành.
    - Thông báo khi có kết quả mới.
* **2. Nhận và Hiển Thị Kết Quả Phân Tích**
  + 2.1. Nhận Kết Quả Từ Hệ Thống Phân Tích
    - Chức năng: Nhận kết quả phân tích mã độc từ hệ thống phân tích.
    - Tự động nhận dữ liệu kết quả sau khi phân tích hoàn tất.
    - Lưu trữ kết quả vào cơ sở dữ liệu nội bộ.
    - Đảm bảo tính toàn vẹn và bảo mật của dữ liệu nhận được.
  + 2.2. Hiển Thị Kết Quả Dưới Dạng Báo Cáo
    - Chức năng: Tạo và hiển thị báo cáo chi tiết về kết quả phân tích.
    - Bao gồm các thông tin như loại mã độc, mức độ nguy hiểm, khuyến nghị xử lý.
    - Cho phép tải xuống báo cáo dưới các định dạng khác nhau (PDF, DOCX).
  + 2.3. Hiển Thị Kết Quả Dưới Dạng Biểu Đồ
    - Chức năng: Trực quan hóa kết quả phân tích thông qua các biểu đồ.
    - Sử dụng các loại biểu đồ như biểu đồ cột, biểu đồ tròn, biểu đồ đường để thể hiện dữ liệu.
    - Cho phép người dùng tùy chỉnh các tham số hiển thị.
    - Cập nhật dữ liệu biểu đồ tự động khi có kết quả mới.
* **3. Quản lý lịch sử và báo cáo phân tích**
  + 3.1 Lịch sử phân tích:
    - Người dùng có thể xem lại các tệp đã gửi phân tích cùng với kết quả và trạng thái của chúng.
  + 3.2 Xuất báo cáo:
    - Cho phép xuất báo cáo phân tích dưới dạng PDF hoặc Excel.
    - Báo cáo tổng hợp theo phòng ban, đại lý hoặc thời gian để dễ dàng đánh giá hiệu quả.
* **4. Quản lý tài khoản người dùng**
  + 4.1 Đăng ký/Đăng nhập:
    - Cho phép người dùng tạo tài khoản và đăng nhập vào hệ thống.
    - Tích hợp xác thực 2 yếu tố (2FA) để tăng cường bảo mật.
  + 4.2 Quản lý thông tin cá nhân:
    - Người dùng có thể cập nhật thông tin cá nhân (tên, email, mật khẩu...).
    - Cài đặt quyền hạn cho từng loại người dùng (admin, nhân viên phân tích, đại lý).
  + 4.3 Quản lý quyền và phân quyền:
    - Hệ thống phân quyền, có các vai trò như: Quản trị viên (Admin), Người dùng thường, Người phân tích.
* **5. Quản lý phòng ban và đơn vị**
  + 5.1 Tạo và quản lý phòng ban:
    - Admin có thể tạo mới, sửa đổi, xóa các phòng ban.
    - Gán người dùng vào các phòng ban.
  + **5.**2 Quản lý đơn vị:
    - Hệ thống cho phép admin tạo mới các đại lý, quản lý thông tin liên quan (địa chỉ, thông tin liên hệ...).
    - Gán người dùng của đại lý và phân quyền tương ứng.
* **6.** **Thông báo và cảnh báo**

Chức năng này cho phép gửi thông báo tới người dùng về kết quả phân tích và cảnh báo nếu có mã độc nguy hiểm.

* + 6.1 Thông báo kết quả
    - Gửi thông báo khi quá trình phân tích hoàn thành.
    - Gửi email/SMS thông báo kết quả hoặc trạng thái phân tích.
  + 6.2 Cảnh báo khẩn cấp
    - Khi phát hiện mã độc nguy hiểm, hệ thống gửi cảnh báo đến quản trị viên hoặc người dùng liên quan để xử lý.
* **7.** **Chuyển phân tích tới người thực hiện khi hệ thống không tự động phân tích được mẫu thử**
  + Chuyển tới mẫu thử tới người thực hiện khi hệ thống không tự phân tích được
  + Chức năng gửi kết quả phân tích tới khách hàng
* **8. Lập lịch và tự động hóa phân tích**
  + Người dùng có thể lên lịch tự động phân tích mã độc theo thời gian định trước (ví dụ: hàng ngày, hàng tuần).
  + Tự động gửi email hoặc thông báo khi kết quả phân tích hoàn tất.
* **9. Chức năng chia sẻ kết quả**
  + Người dùng có thể chia sẻ kết quả phân tích cho các phòng ban hoặc đại lý khác thông qua email hoặc đường dẫn trực tiếp (với quyền truy cập bảo mật).
* **10. Quản lý nhật ký và giám sát hệ thống**
  + Quản lý nhật ký hoạt động (Audit Log):
    - Hệ thống cần ghi lại toàn bộ các hoạt động của người dùng như tải lên tệp, xem kết quả, xuất báo cáo... để phục vụ cho việc kiểm tra bảo mật và giám sát.
* **11. Tích hợp với các hệ thống khác**
  + - Tích hợp với các hệ thống quản lý thông tin: Cho phép tự động lấy thông tin về người dùng, phòng ban từ các hệ thống khác để giảm thiểu việc nhập liệu thủ công
    - Hỗ trợ cung cấp và sử dụng API để tự động gửi tài liệu cần phân tích từ các ứng dụng khác.
* **12. Quản lý phiên bản tài liệu**
  + **Chức năng quản lý phiên bản**
    - Mỗi tài liệu có thể có nhiều phiên bản khi được tải lên nhiều lần để phân tích lại. Hệ thống lưu trữ các phiên bản cũ của tài liệu, cho phép người dùng xem và so sánh kết quả phân tích qua từng phiên bản.
    - Cho phép khôi phục phiên bản trước đó nếu cần.