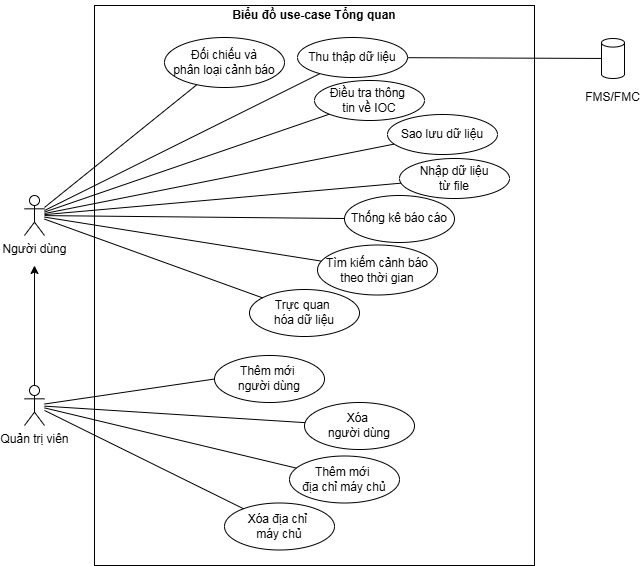
**4. Phân tích hệ thống**

**4.1. Biểu đồ use-case tổng quan hệ thống**

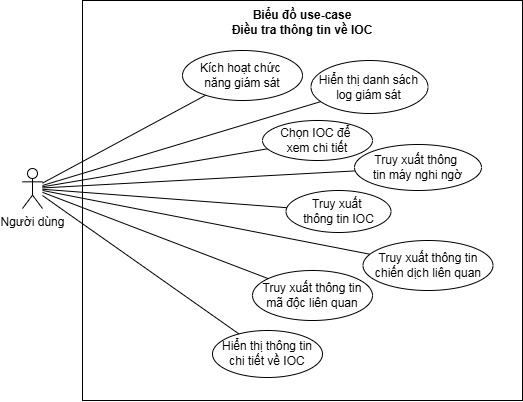
Từ sự phân tích các chức năng đặt ra cho hệ thống săn tìm mối nguy cơ trên mạng MTQS, xác định biểu đồ thể hiện tổng quan tương tác giữa người dùng là cán bộ thực hiện nhiệm vụ và các chức năng của hệ thống:



*Biểu đồ use-case tổng quan hệ thống*

**4.2. Đặc tả use-case**

**a) Use-case Điều tra thông tin về IOC**

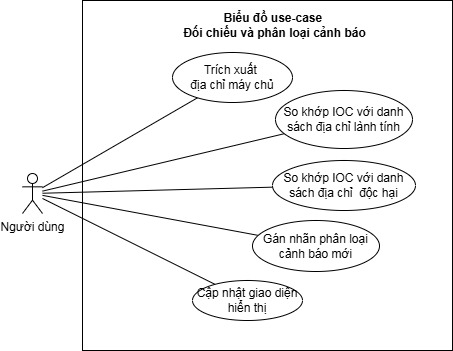
****

*Biểu đồ use-case Điều tra thông tin về IOC*

*Bảng 1. Đặc tả use-case Điều tra thông tin về IOC*

|  |  |
| --- | --- |
| Use-case: Điều tra thông tin về IOC | Mức độ quan trọng: Cao |
| Mô tả: Người dùng truy xuất các thông tin chi tiết, cụ thể về địa chỉ IOC | |
| Điều kiện bắt đầu: Đã đăng nhập tài khoản người dùng hệ thống, hiển thị danh mục các chức năng hệ thống | |
| Kịch bản:  1. Người dùng kích hoạt chức năng “Giám sát”  2. Hệ thống hiển thị danh sách log giám sát  3. Người dùng click chọn trường IOC để xem thông tin chi tiết  4. Hệ thống truy xuất thông tin máy nghi ngờ  5. Hệ thống truy xuất thông tin IOC  6. Hệ thống truy xuất thông tin chiến dịch liên quan  7. Hệ thống truy xuất thông tin mã độc liên quan  8. Hệ thống hiển thị thông tin chi tiết về IOC | |

**b) Use-case Đối chiếu và phân loại cảnh báo**

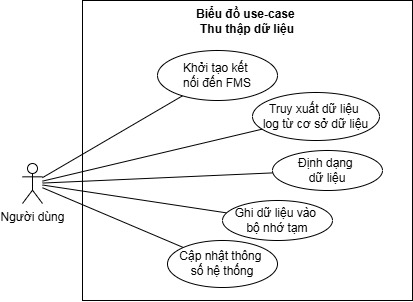
****

*Biểu đồ use-case Đối chiếu và phân loại cảnh báo*

*Bảng 2. Đặc tả use-case Đối chiếu và phân loại cảnh báo*

|  |  |
| --- | --- |
| Use-case: Đối chiếu và phân loại cảnh báo | Mức độ quan trọng: Cao |
| Mô tả: Tiến hành đối chiếu và phân loại cảnh báo | |
| Điều kiện bắt đầu: Đã đăng nhập tài khoản người dùng hệ thống, hiển thị danh mục các chức năng hệ thống | |
| Kịch bản:  1. Người dùng kích hoạt chức năng “Giám sát”  2. Hệ thống trích xuất địa chỉ máy chủ  3. Hệ thống so khớp IOC với danh sách địa chỉ lành tính  4. So khớp IOC với danh sách địa chỉ độc hại  5. Tiến hành gán nhãn phân loại cảnh báo mới  6. Hệ thống cập nhật giao diện hiển thị | |

**b) Use-case Thu thập dữ liệu**

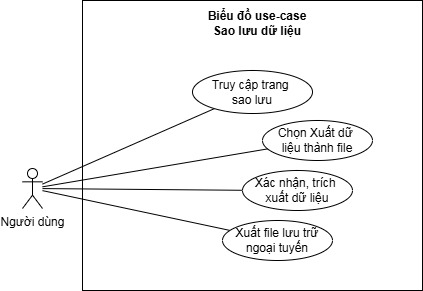
****

*Biểu đồ use-case Thu thập dữ liệu*

*Bảng 2. Đặc tả use-case Thu thập dữ liệu*

|  |  |
| --- | --- |
| Use-case: Thu thập dữ liệu | Mức độ quan trọng: Cao |
| Mô tả: Thu thập dữ liệu từ CSDL FMS | |
| Điều kiện bắt đầu: Đã đăng nhập tài khoản người dùng hệ thống, hiển thị danh mục các chức năng hệ thống | |
| Kịch bản:  1. Người dùng kích hoạt chức năng “Giám sát”  2. Hệ thống khởi tạo kết nối đến Cơ sở dữ liệu của FMS  3. Truy xuất dữ liệu log từ cơ sở dữ liệu  4. Định dạng lại dữ liệu  5. Ghi dữ liệu vào bộ nhớ tạm  6. Cập nhật thông số hệ thống | |

**b) Use-case Sao lưu dữ liệu**

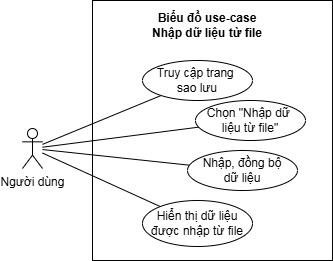
****

*Biểu đồ use-case Sao lưu dữ liệu*

*Bảng 2. Đặc tả use-case Sao lưu dữ liệu*

|  |  |
| --- | --- |
| Use-case: Sao lưu dữ liệu | Mức độ quan trọng: Cao |
| Mô tả: Sao lưu dữ liệu ra dạng file để lưu trữ ngoại tuyến | |
| Điều kiện bắt đầu: Đã đăng nhập tài khoản người dùng hệ thống, hiển thị danh mục các chức năng hệ thống | |
| Kịch bản:  1. Truy cập trang sao lưu  2. Chọn Xuất dữ liệu thành file  3. Xác nhận, trích xuất dữ liệu  4. Xuất file lưu trữ ngoại tuyến | |

**b) Use-case Nhập dữ liệu từ file**

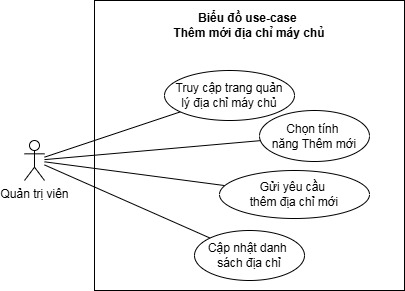
****

*Biểu đồ use-case Nhập dữ liệu từ file*

*Bảng 2. Đặc tả use-case Nhập dữ liệu từ file*

|  |  |
| --- | --- |
| Use-case: Nhập dữ liệu từ file | Mức độ quan trọng: Cao |
| Mô tả: Người dùng import dữ liệu từ file để truy xuất | |
| Điều kiện bắt đầu: Đã đăng nhập tài khoản người dùng hệ thống, hiển thị danh mục các chức năng hệ thống | |
| Kịch bản:  1. Truy cập trang sao lưu  2. Chọn Nhập dữ liệu từ file  3. Nhập, đồng bộ dữ liệu  4. Hiển thị dữ liệu được nhập từ file | |

**b) Use-case Thêm mới địa chỉ máy chủ**

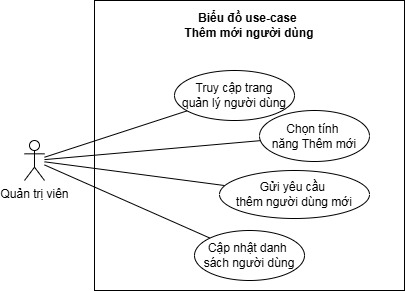
****

*Biểu đồ use-case Thêm mới địa chỉ máy chủ*

*Bảng 2. Đặc tả use-case Thêm mới địa chỉ máy chủ*

|  |  |
| --- | --- |
| Use-case: Thêm mới địa chỉ máy chủ | Mức độ quan trọng: Cao |
| Mô tả: Quản trị viên thực hiện thêm mới địa chỉ máy chủ | |
| Điều kiện bắt đầu: Đã đăng nhập tài khoản quản trị viên hệ thống, hiển thị danh mục các chức năng hệ thống | |
| Kịch bản:  1. Truy cập trang quản lý địa chỉ máy chủ  2. Chọn tính năng Thêm mới địa chỉ máy chủ  3. Gửi yêu cầu thêm địa chỉ mới  4. Cập nhật danh sách máy chủ | |

**b) Use-case Thêm mới người dùng**

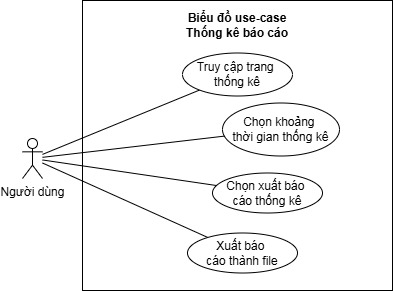
****

*Biểu đồ use-case Thêm mới người dùng*

*Bảng 2. Đặc tả use-case Thêm mới người dùng*

|  |  |
| --- | --- |
| Use-case: Thêm mới người dùng | Mức độ quan trọng: Cao |
| Mô tả: Quản trị viên thực hiện thêm mới người dùng | |
| Điều kiện bắt đầu: Đã đăng nhập tài khoản quản trị viên hệ thống, hiển thị danh mục các chức năng hệ thống | |
| Kịch bản:  1. Truy cập trang quản lý người dùng  2. Chọn tính năng Thêm mới  3. Gửi yêu cầu thêm người dùng mới  4. Cập nhật danh sách người dùng | |

**b) Use-case Thống kê báo cáo**

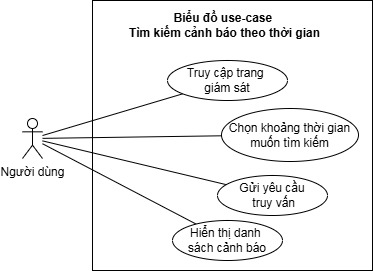
****

*Biểu đồ use-case Thống kê báo cáo*

*Bảng 2. Đặc tả use-case Thống kê báo cáo*

|  |  |
| --- | --- |
| Use-case: Thống kê báo cáo | Mức độ quan trọng: Cao |
| Mô tả: Người dùng tiến hành trích xuất thống kê báo cáo | |
| Điều kiện bắt đầu: Đã đăng nhập tài khoản người dùng hệ thống, hiển thị danh mục các chức năng hệ thống | |
| Kịch bản:  1. Truy cập trang thống kê  2. Chọn khoảng thời gian thống kê  3. Chọn xuất báo cáo thống kê  4. Xuất báo cáo thành file | |

**b) Use-case Tìm kiếm cảnh báo theo thời gian**

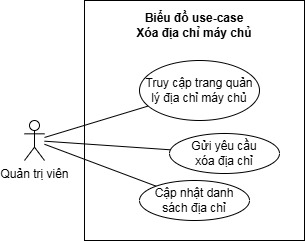
****

*Biểu đồ use-case Tìm kiếm cảnh báo theo thời gian*

*Bảng 2. Đặc tả use-case Tìm kiếm cảnh báo theo thời gian*

|  |  |
| --- | --- |
| Use-case: Tìm kiếm cảnh báo theo thời gian | Mức độ quan trọng: Cao |
| Mô tả: Người dùng tiến hành tìm kiếm cảnh báo theo thời gian | |
| Điều kiện bắt đầu: Đã đăng nhập tài khoản người dùng hệ thống, hiển thị danh mục các chức năng hệ thống | |
| Kịch bản:  1. Truy cập trang giám sát  2. Chọn khoảng thời gian muốn tìm kiếm  3. Gửi yêu cầu truy vấn  4. Hiển thị danh sách cảnh báo | |

**b) Use-case Xóa địa chỉ máy chủ**

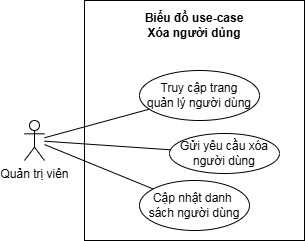
****

*Biểu đồ use-case Xóa địa chỉ máy chủ*

*Bảng 2. Đặc tả use-case Xóa địa chỉ máy chủ*

|  |  |
| --- | --- |
| Use-case: Xóa địa chỉ máy chủ | Mức độ quan trọng: Cao |
| Mô tả: Quản trị viên thực hiện xóa địa chỉ máy chủ | |
| Điều kiện bắt đầu: Đã đăng nhập tài khoản quản trị viên hệ thống, hiển thị danh mục các chức năng hệ thống | |
| Kịch bản:  1. Truy cập trang quản lý địa chỉ máy chủ  2. Gửi yêu cầu xóa địa chỉ máy chủ  3. Cập nhật danh sách máy chủ | |

**b) Use-case Xóa người dùng**

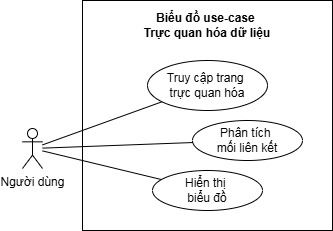
****

*Biểu đồ use-case Xóa người dùng*

*Bảng 2. Đặc tả use-case Xóa người dùng*

|  |  |
| --- | --- |
| Use-case: Xóa người dùng | Mức độ quan trọng: Cao |
| Mô tả: Quản trị viên thực hiện xóa người dùng | |
| Điều kiện bắt đầu: Đã đăng nhập tài khoản quản trị viên hệ thống, hiển thị danh mục các chức năng hệ thống | |
| Kịch bản:  1. Truy cập trang quản lý người dùng  2. Gửi yêu cầu xóa người dùng  3. Cập nhật danh sách người dùng | |

**b) Use-case Trực quan hóa dữ liệu**

****

*Biểu đồ use-case Trực quan hóa dữ liệu*

*Bảng 2. Đặc tả use-case Trực quan hóa dữ liệu*

|  |  |
| --- | --- |
| Use-case: Trực quan hóa dữ liệu | Mức độ quan trọng: Cao |
| Mô tả: Người dùng chọn tính năng trực quan hóa, hệ thống hiện thị dữ liệu dưới dạng biểu đồ | |
| Điều kiện bắt đầu: Đã đăng nhập tài khoản người dùng hệ thống, hiển thị danh mục các chức năng hệ thống | |
| Kịch bản:  1. Truy cập trang trực quan hóa  2. Phân tích mối liên kết  3. Hiển thị biểu đồ | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Tên use-case** | **Tác nhân chính** | **Mô tả trường hợp sử dụng** | **Phân loại usecase** | **Mức độ cần thiết** |
| 1 | Thu thập dữ liệu |  | Khởi tạo kết nối đến FMS | Trung bình |  |
| Truy xuất dữ liệu log từ cơ sở dữ liệu |
| Định dạng dữ liệu |
| Ghi dữ liệu vào bộ nhớ tạm |
| Cập nhật thông số hệ thống |
| 2 | Điều tra thông tin về IOC | Người dùng | Kích hoạt chức năng giám sát | Phức tạp |  |
| Hiển thị danh sách log giám sát |
| Chọn IOC để xem chi tiết |
| Truy xuất thông tin máy nghi ngờ |
| Truy xuất thông tin IOC |
| Truy xuất thông tin chiến dịch liên quan |
| Truy xuất thông tin mã độc liên quan |
| Hiển thị thông tin chi tiết về IOC |
| 3 | Đối chiếu và phân loại cảnh báo | Người dùng | Trích xuất địa chỉ máy chủ | Trung bình |  |
| So khớp IOC với danh sách địa chỉ lành tính |
| So khớp IOC với danh sách địa chỉ độc hại |
| Gán nhãn phân loại cảnh báo mới |
| Cập nhật giao diện hiển thị |
| 4 | Sao lưu dữ liệu | Người dùng | Truy cập trang sao lưu | Trung bình |  |
| Chọn Xuất dữ liệu thành file |
| Xác nhận, trích xuất dữ liệu |
| Xuất file lưu trữ ngoại tuyến |
| 5 | Nhập dữ liệu từ file | Người dùng | Truy cập trang sao lưu | Trung bình |  |
| Chọn Nhập dữ liệu từ file |
| Nhập, đồng bộ dữ liệu |
| Hiển thị dữ liệu được nhập từ file |
| 6 | Quản lý người dùng | Quản trị viên | Truy cập trang quản lý người dùng | Trung bình |  |
| Chọn tính năng Thêm mới, Xóa người dùng |
| Gửi yêu cầu thêm, xóa người dùng |
| Cập nhật danh sách người dùng |
| 7 | Quản lý địa chỉ máy chủ | Quản trị viên | Truy cập trang quản lý địa chỉ máy chủ | Trung bình |  |
| Chọn tính năng Thêm mới, xóa địa chỉ máy chủ |
| Gửi yêu cầu thêm, xóa địa chỉ máy chủ |
| Cập nhật danh sách máy chủ |
| 8 | Thống kê báo cáo | Người dùng | Truy cập trang thống kê | Trung bình |  |
| Chọn khoảng thời gian thống kê |
| Chọn xuất báo cáo thống kê |
| Xuất báo cáo thành file |
| 9 | Tìm kiếm cảnh báo theo thời gian | Người dùng | Truy cập trang giám sát | Trung bình |  |
| Chọn khoảng thời gian muốn tìm kiếm |
| Gửi yêu cầu truy vấn |
| Hiển thị danh sách cảnh báo |
| 10 | Quản lý đăng nhập | Người dùng | Nhập thông tin đăng nhập | Trung bình |  |
| Gửi yêu cầu xác thực |
| Xác thực thông tin đăng nhập |
| Cấp quyền truy cập |
| Điều hướng sau đăng nhập |
| Thông báo lỗi đăng nhập (nếu có) |
| 11 | Trực quan hóa dữ liệu | Người dùng | Truy cập trang trực quan hóa | Đơn giản |  |
| Phân tích mối liên kết |
| Hiển thị biểu đồ |