|  |
| --- |
| **ĐỀ CƯƠNG NHIỆM VỤ**  **HỆ THỐNG SĂN TÌM MỐI NGUY CƠ TRÊN MẠNG MTQS**  **TRÊN ĐỊA BÀN MIỀN TRUNG – TÂY NGUYÊN**  **Đà Nẵng, tháng 03 năm 2025** |

|  |
| --- |
| **Tên nhiệm vụ:** Hệ thống săn tìm mối nguy cơ trên mạng MTQS trên địa bàn miền Trung – Tây Nguyên.  **Đà Nẵng, tháng 03 năm 2025** |

**MỤC LỤC**

[I. THÔNG TIN CHUNG 1](#_Toc193884435)

[1. Căn cứ pháp lý 1](#_Toc193884436)

[2. Mục đích, yêu cầu, nhu cầu đầu tư 1](#_Toc193884437)

[3. Tên nhiệm vụ 1](#_Toc193884438)

[4. Đơn vị sử dụng ngân sách 1](#_Toc193884439)

[5. Địa điểm thực hiện nhiệm vụ 2](#_Toc193884440)

[6. Tổ chức thực hiện 2](#_Toc193884441)

[7. Loại nguồn vốn 2](#_Toc193884442)

[8. Dự kiến hiệu quả đạt được 2](#_Toc193884443)

[9. Đề xuất kiến nghị 2](#_Toc193884444)

[II. SỰ CẦN THIẾT PHẢI ĐẦU TƯ 2](#_Toc193884445)

[1. Thực trạng nhiệm vụ săn tìm mối nguy cơ 2](#_Toc193884446)

[2. Tính cấp thiết cần triển khai nhiệm vụ 5](#_Toc193884447)

[3. Tính khoa học của nhiệm vụ 5](#_Toc193884448)

[III. GIẢI PHÁP KỸ THUẬT CÔNG NGHỆ 6](#_Toc193884449)

[1. Phương pháp kỹ thuật và giải pháp thực hiện 6](#_Toc193884450)

[2. Danh sách chức năng của phần mềm 6](#_Toc193884451)

[1. Tổng hợp dự toán 18](#_Toc193884452)

[V. DỰ KIẾN TIẾN ĐỘ THỰC HIỆN 19](#_Toc193884453)

[VI. PHƯƠNG ÁN TỔ CHỨC THỰC HIỆN 19](#_Toc193884454)

[1. Tiến độ dự kiến thực hiện 19](#_Toc193884455)

[2. Phương án tổ chức thực hiện vận hành, khai thác 20](#_Toc193884456)

[2.1. Phương án cài đặt, triển khai, vận hành 20](#_Toc193884457)

[2.2. Phương án kiểm thử các yêu cầu chức năng và phi chức năng của hệ thống 20](#_Toc193884458)

[2.3. Cam kết của đơn vị phát triển về quá trình bảo hành và hỗ trợ kỹ thuật sau khi hệ thống đưa vào vận hành, khai thác 20](#_Toc193884459)

**ĐỀ CƯƠNG NHIỆM VỤ**

Hệ thống săn tìm mối nguy cơ trên mạng máy tính quân sự

trên địa bàn miền Trung – Tây Nguyên

# I. THÔNG TIN CHUNG

## 1. Căn cứ pháp lý

- Thông tư số 03/2020/TT-BTTTT ngày 24/02/2020 của Bộ Thông tin và Truyền thông Quy định về lập đề cương và dự toán chi tiết đối với hoạt động ứng dụng công nghệ thông tin sử dụng kinh phí chi thường xuyên thuộc nguồn vốn ngân sách nhà nước;

- Hướng dẫn được ban hành kèm theo Quyết định số 671/BTTTT ngày 26/4/2024 của Bộ Thông tin và Truyền thông hướng dẫn xác định chi phí phát triển, nâng cấp phần mềm nội bộ;

- Hướng dẫn kèm Quyết định số 129/QĐ-BTTTT ngày 03/02/2021 của Bộ Thông tin và Truyền thông về xác định đơn giá nhân công trong quản lý chi phí đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước.

- Kế hoạch số 2012/KH-BTL ngày 31/12/2023 của Bộ Tư lệnh 86 về triển khai xây dựng, thẩm định, xét duyệt các nhiệm vụ đề xuất triển khai theo Nghị quyết số 29/NQ-TW ngày 25/7/2018 của Bộ Chính trị về Chiến lược Bảo vệ Tổ quốc trên không gian mạng năm 2024.

## 2. Mục đích, yêu cầu, nhu cầu đầu tư

**a) Mục đích**

Phát triển hệ thống săn tìm mối nguy cơ trên mạng MTQS trên địa bàn miền Trung – Tây Nguyên.

**b) Yêu cầu**

- Thực hiện mua sắm hàng hóa đúng thủ tục, quy định, đúng tiến độ, tiết kiệm, chất lượng, hiệu quả;

- Tổ chức triển khai cài đặt, cấu hình hệ thống thiết bị theo đúng quy định, bảo đảm an toàn tuyệt đối về mọi mặt;

- Phối hợp tốt giữa các cơ quan, đơn vị để nghiệm thu đưa vào sử dụng hệ thống sau khi hoàn thiện.

## 3. Tên nhiệm vụ

Hệ thống săn tìm mối nguy cơ trên mạng MTQS trên địa bàn miền Trung – Tây Nguyên.

## 4. Đơn vị sử dụng ngân sách

Cụm 31/Trung tâm 386/BTL 86.

## 5. Địa điểm thực hiện nhiệm vụ

Cụm 31/Trung tâm 386/BTL 86.

## 6. Tổ chức thực hiện

**- Chỉ đạo chung**

Đồng chí Thiếu tá Nguyễn Viết Học, Cụm trưởng Cụm 31.

**-** **Nhóm thực hiện nhiệm vụ**

+ Đại úy Nguyễn Đức Anh - Đội trưởng Đội 1, Cụm 31: Chủ nhiệm nhiệm vụ.

+ Trung úy Lê Thế Nhật - SQTCM Đội 1/Cụm 31: Thành viên.

+ Trung úy Mạnh Tuấn Đạt - SQTCM Đội 1/Cụm 31: Thành viên.

+ Thượng úy Ngô Thị Hòa - Trợ lý KHTH/Cụm 31: Thành viên.

## 7. Loại nguồn vốn

|  |  |
| --- | --- |
| ***Nguồn*** | ***Tổng vốn*** *(đồng)* |
| Từ kinh phí nghiệp vụ thường xuyên | 800.000.000 |
| Từ nguồn vốn tự có của cơ quan |  |
| Từ nguồn khác |  |

## 8. Dự kiến hiệu quả đạt được

- Hệ thống hỗ trợ cho nhiệm vụ Săn tìm mối nguy cơ được triển khai trên mạng Máy tính quân sự (MTQS). Hệ thống có chức năng thu thập, phân tích, đánh giá, cảnh báo các dấu hiệu mất an toàn thông tin trong hệ thống mạng MTQS. Hệ thống cũng tích hợp cơ sở dữ liệu địa chỉ máy chủ độc hại để kịp thời phát hiện các máy tính có truy vấn bất thường.

- Phạm vi ứng dụng: Sản phẩm sẽ được sử dụng tại Trung tâm 386. Bên cạnh đó, kết quả của nhiệm vụ có thể ứng dụng tại các đơn vị khác có liên quan đến nhiệm vụ săn tìm mối nguy cơ trong BTL86.

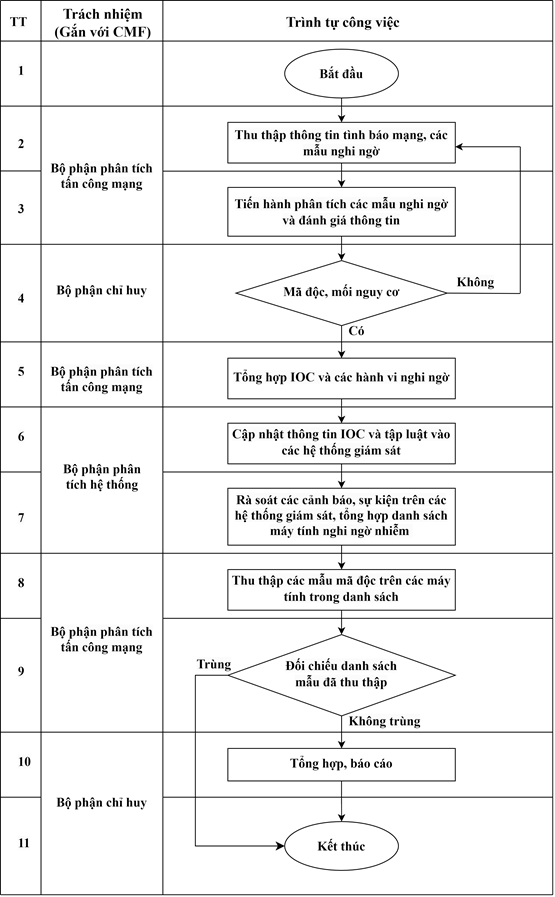
## 9. Đề xuất kiến nghị

Trong quá trình thực hiện nhiệm vụ, kính đề nghị chỉ huy, lãnh đạo các cơ quan thường xuyên quan tâm, chỉ đạo cũng như tạo điều kiện thuận lợi về thời gian, thủ tục để bảo đảm triển khai tốt nhiệm vụ, đúng tiến độ và mục tiêu đã đề ra.

# II. SỰ CẦN THIẾT PHẢI ĐẦU TƯ

## 1. Thực trạng nhiệm vụ săn tìm mối nguy cơ

Hiện nay, lực lượng tác chiến mạng đang tiến hành các hoạt động săn tìm mối nguy cơ trên các hệ thống giám sát tập trung, nổi bật là FMS. Đây là hệ thống hỗ trợ mạnh mẽ cho nhiệm vụ săn tìm mối nguy cơ với tính năng thống kê, giám sát chặt chẽ các hoạt động, truy vấn bất thường từ máy tính, máy chủ trong mạng. Mặc dù rất hữu ích trong nhiệm vụ săn tìm mối nguy cơ, tuy nhiên các tính năng lại hỗ trợ gián tiếp và chưa thực sự rõ nét. Hệ thống chỉ mang tính cảnh báo, thông báo các hành vi, hoạt động đáng ngờ, các truy vấn của máy tính đến các địa chỉ, IP độc hại. Chưa hỗ trợ nhiều trong phân tích, xác định chiến dịch tấn công, thống kê và trực quan hóa các hành vi đáng ngờ của máy tính trong mạng. Các nhiệm vụ săn tìm, phát hiện mối nguy cơ vẫn đang tiêu tốn rất nhiều sức lực, nhân lực, chưa thể có một cái nhìn nhanh chóng và tổng quan đối với các hạ tầng mạng mà đơn vị giám sát, quản lý.

****

*Quy trình săn tìm mối nguy cơ*

Từ quy trình săn tìm mối nguy cơ của lực lượng tác chiến mạng, ứng dụng CNTT vào quá trình thực hiện nhiệm vụ:

| **TT** | **Hoạt động** | **Trách nhiệm** | **Mô tả** | **Ứng dụng CNTT** |
| --- | --- | --- | --- | --- |
|  |  |  | Bắt đầu công tác săn tìm các mối nguy cơ trong mạng MTQS thường xuyên. |  |
| B1 | Thu thập thông tin các mẫu nghi ngờ | Bộ phận giám sát, phòng thủ | - Giám sát hoạt động của các máy tính trong mạng MTQS.  - Phát hiện và điều ra các hoạt động bất thường của các máy tính trong mạng MTQS.  - Liên hệ thu thập các thông tin liên quan đến mẫu nghi ngờ kết hợp với công tác kiểm tra ATTT tại các cơ quan, đơn vị. | Tự động rà soát, thu thập hành vi bất thường của các máy tính trong mạng MTQS |
| B2 | Phân tích các mẫu nghi ngờ và đánh giá thông tin | - Phân tích các mẫu nghi ngờ sử dụng công cụ kiểm tra ATTT và phân tích mã độc.  - Phân tích, so sánh (địa chỉ máy chủ độc hại, hành vi) với các mẫu mã độc có trong CSDL.  - Kiểm tra các truy vấn lạ trên hệ thống Virustotal. | Tự động đối chiếu, so sánh các truy vấn nghi ngờ với CSDL |
| B3 | Xác định mối nguy cơ | Bộ phận  chỉ huy | Đánh giá kết quả, xác định mối nguy cơ:  - Có: Chuyển sang bước 4.  - Không: Quay lại bước 1. | Gán nhãn các truy vấn là lành tính, nguy cơ |
| B4 | Tổng hợp  kết quả phân tích | Bộ phận giám sát, phòng thủ | - Tổng hợp địa chỉ máy chủ độc hại và các hành vi nghi ngờ.  - Xây dựng các tập luật dựa trên địa chỉ máy chủ độc hại và các hành vi nghi ngờ. |  |
| B5 | Cập nhật địa chỉ máy chủ động hại và tập luật | Bộ phận giám sát, phòng thủ | Cập nhật địa chỉ máy chủ độc hại và tập luật vào các hệ thống giám sát. | Tự động cập nhật tập luật, địa chỉ máy chủ độc hại vào CSDL |
| B6 | Rà soát, tổng hợp danh sách máy tính nghi nhiễm | - Tiến hành rà soát các cảnh báo và sự kiện dựa trên các thông tin đã cập nhật.  - Tổng hợp danh sách các máy tính có hành vi nghi ngờ nhiễm mã độc. | Tổng hợp các danh sách máy tính xuất hiện các cảnh báo |
| B7 | Tổng hợp báo cáo | Bộ phận  chỉ huy | Tổng hợp báo cáo phát hiện mẫu biến thể mã độc mới trong hệ thống. | Tổng hợp báo cáo theo mẫu |
| B8 | Kết thúc,  Phê duyệt báo cáo | Phê duyệt báo cáo, phát hành báo cáo khi đạt yêu cầu. |  |

## 2. Tính cấp thiết cần triển khai nhiệm vụ

Mặc dù trên thế giới đã có nhiều hệ thống, phần mềm quản lý, trực quan hóa, so sánh dữ liệu, tuy nhiên đều rất khó để cấu hình và sử dụng cho mục đích đặc thù của nhiệm vụ Săn tìm mối nguy cơ trong Quân đội.

Ở trong nước, đặc biệt là Quân đội, hiện chưa có nhiều nghiên cứu, hệ thống cung cấp các chức năng hỗ trợ tốt cho nhiệm vụ săn tìm mối nguy cơ, ứng dụng vào các hoạt động tác chiến mạng.

Bài toán đặt ra cho nhiệm vụ tác chiến mạng là xây dựng một hệ thống có thể quản lý, trực quan hóa dữ liệu giám sát, bên cạnh đó cung cấp các tính năng hữu ích, tự động hóa một số công đoạn trong nhiệm vụ săn tìm mối nguy cơ trên mạng máy tính quân sự.

Vì vậy, nhiệm vụ xây dựng hệ thống hỗ trợ săn tìm mối nguy cơ, để phục vụ trong các nhiệm vụ tác chiến của đơn vị nói riêng và của Bộ Tư lệnh nói chung là vô cùng cần thiết.

## 3. Tính khoa học của nhiệm vụ

Nhiệm vụ có ý nghĩa khoa học quan trọng trong việc nghiên cứu, xây dựng được một hệ thống hỗ trợ đặc thù cho nhiệm vụ săn tìm mối nguy cơ, phục vụ trong các nhiệm vụ tác chiến mạng. Bằng cách phân tích, đánh giá, đối chiếu hành vi bất thường của máy tính trong mạng với dấu hiệu của các cuộc tấn công, đồng thời thu thập và lưu trữ, quản lý dữ liệu của các máy chủ C&C mã độc. Qua đó, hỗ trợ tích cực cho nhiệm vụ săn tìm mối nguy cơ trên địa bàn.

# III. GIẢI PHÁP KỸ THUẬT CÔNG NGHỆ

## 1. Phương pháp kỹ thuật và giải pháp thực hiện

Với ý tưởng xây dựng một hệ thống hỗ trợ nhiệm vụ săn tìm mối nguy cơ trên mạng MTQS. Hệ thống có chức năng thu thập và quản lý các địa chỉ IP độc hại trên mạng Internet, lưu trữ và quản lý các thông tin liên quan như các nhóm hacker, mẫu mã độc liên quan và hành vi nổi bật.

Hệ thống này sẽ kết nối với cơ sở dữ liệu của hệ thống FMS để lấy dữ liệu, từ đó xử lý và xác định các cảnh báo về các hành vi truy vấn đến các địa chỉ máy chủ độc hại. Quá trình này sẽ phân tích dữ liệu thu được, so sánh và đối chiếu với cơ sở dữ liệu các địa chỉ máy chủ độc hại đã được thu thập, lưu trữ và quản lý. Dữ liệu sau khi xử lý sẽ được phân loại, đánh giá và đưa ra các cảnh báo tương ứng.

Quá trình thu thập dữ liệu từ FMS và phân tích sẽ được thực hiện tự động hóa, kết hợp với hệ thống giám sát thông minh. Các cảnh báo sẽ được tạo ra khi phát hiện truy vấn đến các địa chỉ máy chủ độc hại, giúp các máy tính trong mạng có thể kịp thời nhận biết và ứng phó.

Ngoài ra, hệ thống sẽ cung cấp các chức năng thống kê và trực quan hóa dữ liệu, cho phép người dùng theo dõi tổng quan các hành vi truy vấn của máy tính trong mạng, từ đó phân loại và xác định các nguy cơ bảo mật, nguy cơ nhiễm mã độc, trong một số trường hợp, có thể xác định các cuộc tấn công APT vào hệ thống mạng MTQS.

## 2. Danh sách chức năng của phần mềm

Hệ thống được triển khai dưới dạng ứng dụng web, gồm các chức năng chính sau:

**a) Đối chiếu và phân loại cảnh báo**

Dữ liệu thu thập được từ cơ sở dữ liệu của hệ thống FMS sẽ được xử lí, trích xuất các thông tin quan trọng (các hành vi kết nối, truy vấn đáng ngờ, …). Sau đó tiến hành đối chiếu với cơ sở dữ liệu máy chủ độc hại của hệ thống để nhận định, đánh giá. Nếu trùng khớp với cơ sở dữ liệu các máy tính độc hại, các kết nối này được gán nhãn là độc hại, ngược lại, được gán nhãn là lành tính. Các kết nối, truy vấn không được gán nhãn, sẽ được tổng hợp để tiếp tục phân tích, đánh giá.

**b) Sao lưu dữ liệu**

Dữ liệu xử lý trong hệ thống được sao lưu định kỳ hoặc đột xuất, xuất ra dưới dạng file json để nhằm tối ưu bộ nhớ và linh hoạt trong quá trình quản lý, lưu trữ dữ liệu. Khi cần thiết, có thể import file dữ liệu vào hệ thống để tiến hành tra cứu, trích xuất thông tin.

**c) Quản lý đăng nhập**

Hệ thống cung cấp tính năng phân quyền để phân loại quyền hạn của người dùng thông thường và người quản trị đối với hệ thống. Sử dụng mật khẩu để xác thực người dùng. Hệ thống cũng sử dụng mã băm để quản lý cơ sở dữ liệu người dùng, giúp giảm thiểu rủi ro lộ lọt tài khoản và mất an toàn thông tin.

**d) Thu thập dữ liệu**

Hệ thống tự động hóa việc thu thập dữ liệu bằng cách thiết lập kết nối trực tiếp đến máy chủ cơ sở dữ liệu của hệ thống FMS, thu thập dữ liệu theo thời gian cảnh báo, mức độ cảnh báo, phân loại hành vi, mô tả hành vi. Dữ liệu sau khi thu thập được xử lý trực tiếp và loại bỏ ngay sau đó để tối ưu dung lượng bộ nhớ.

**e) Quản lý địa chỉ máy chủ**

Các địa chỉ máy chủ được xác định là độc hại sẽ được lưu trữ trong cơ sở dữ liệu. Hệ thống cho phép người dùng có quyền hạn nhất định được thêm mới, sửa đổi và xóa các địa chỉ máy chủ trong cơ sở dữ liệu.

**f) Trực quan hóa dữ liệu**

Hệ thống hỗ trợ hiển thị dữ liệu dưới dạng bảng và biểu đồ, cung cấp cho người sử dụng cái nhìn tổng quan và cụ thể về tình trạng an toàn thông tin của các đơn vị trên địa bàn.

**g) Thống kê báo cáo**

Từ kết quả xử lý dữ liệu, hệ thống tiến hành thống kê số lượng truy vấn đến các địa chỉ máy chủ độc hại theo địa chỉ nguồn, địa chỉ đích … Đồng thời cùng cấp tính năng xuất báo cáo thống kê theo mẫu được xây dựng từ trước. Qua các con số thống kê, hệ thống cũng hỗ trợ đánh giá, nhận định về mức độ mất an toàn thông tin của từng đơn vị trên địa bàn.

**3. Thành phần hệ thống**

- Back-end: Ngôn ngữ lập trình Python, framework Flask.

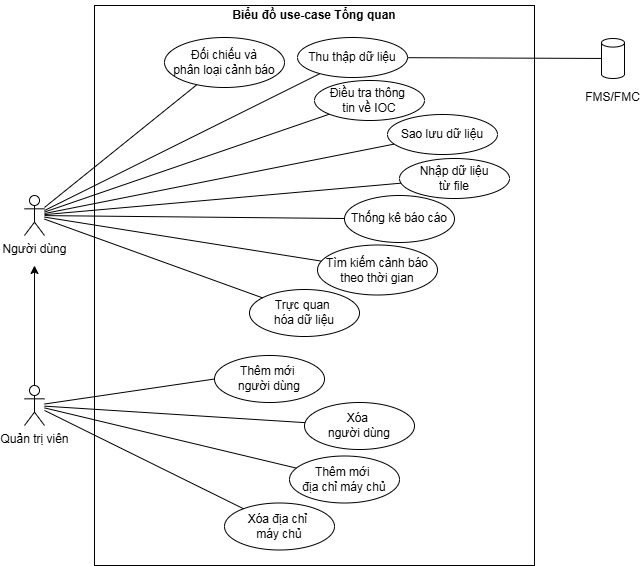
- Front-end: Framework Bootstrap.

- Cơ sở dữ liệu: mongodb.

**4. Phân tích hệ thống**

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

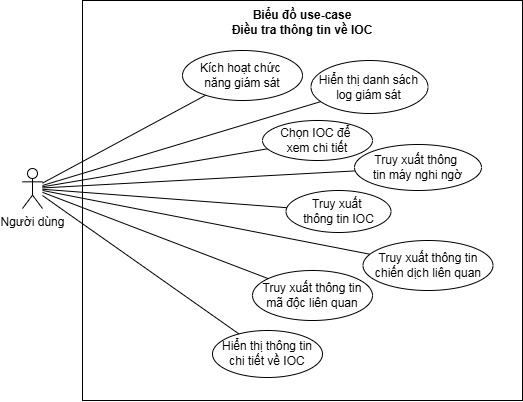
Từ sự phân tích các chức năng đặt ra cho hệ thống săn tìm mối nguy cơ trên mạng MTQS, xác định biểu đồ thể hiện tổng quan tương tác giữa người dùng là cán bộ thực hiện nhiệm vụ và các chức năng của hệ thống:



*Biểu đồ use-case tổng quan hệ thống*

**4.2. Đặc tả use-case**

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

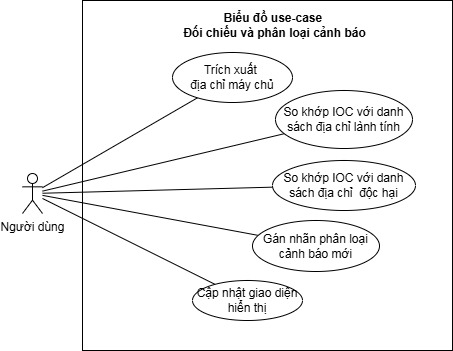
****

*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**

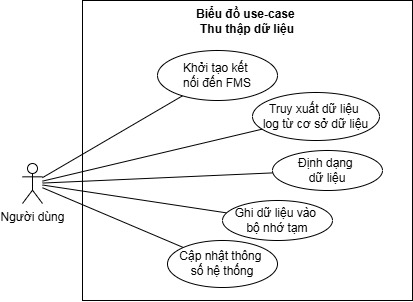
****

*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 | |

**c) Use-case Thu thập dữ liệu**

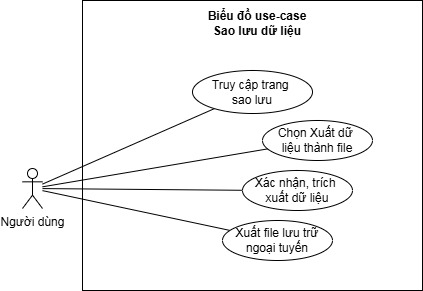
****

*Biểu đồ use-case Thu thập dữ liệu*

*Bảng 3. 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 | |

**d) Use-case Sao lưu dữ liệu**

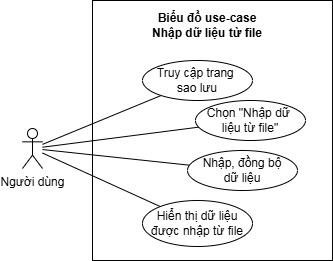
****

*Biểu đồ use-case Sao lưu dữ liệu*

*Bảng 4. 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 | |

**e) Use-case Nhập dữ liệu từ file**

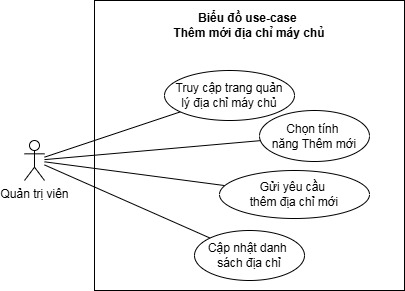
****

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

*Bảng 5. 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 | |

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

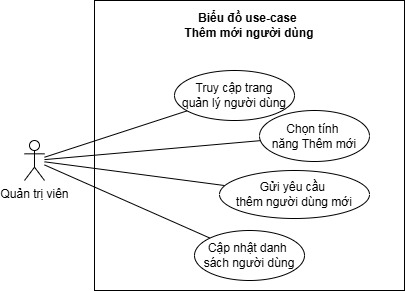
****

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

*Bảng 6. 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 | |

**g) Use-case Thêm mới người dùng**

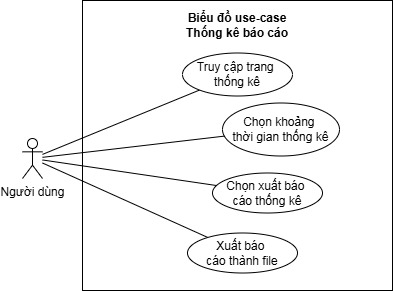
****

*Biểu đồ use-case Thêm mới người dùng*

*Bảng 7. 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 | |

**h) Use-case Thống kê báo cáo**

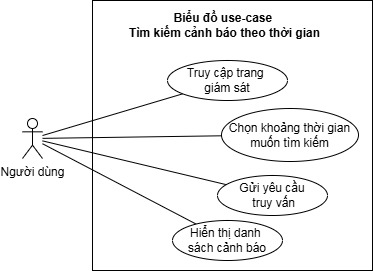
****

*Biểu đồ use-case Thống kê báo cáo*

*Bảng 8. 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 | |

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

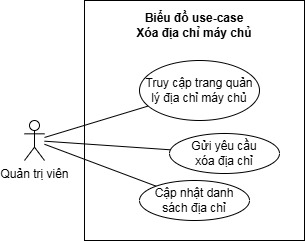
****

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

*Bảng 9. 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 | |

**k) Use-case Xóa địa chỉ máy chủ**

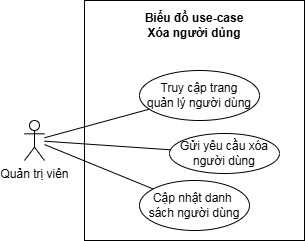
****

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

*Bảng 10. 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 | |

**l) Use-case Xóa người dùng**

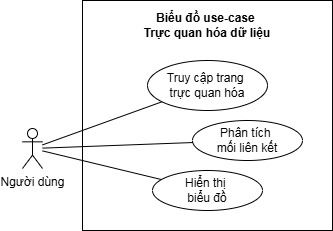
****

*Biểu đồ use-case Xóa người dùng*

*Bảng 11. 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 | |

**m) Use-case Trực quan hóa dữ liệu**

****

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

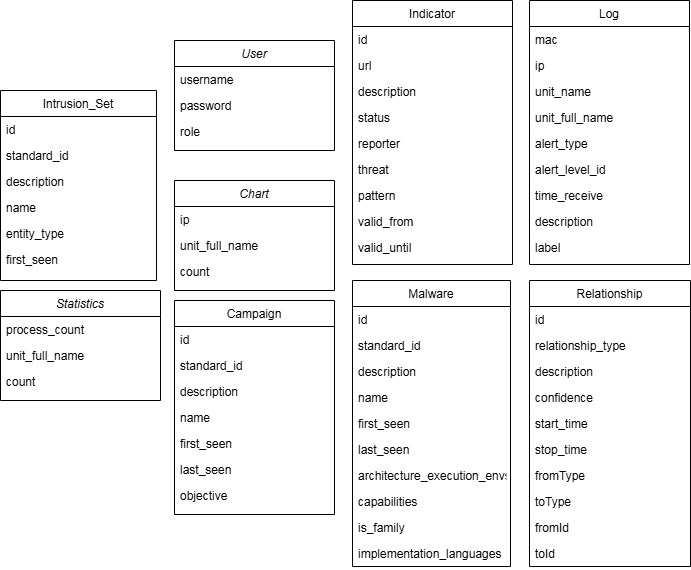
*Bảng 12. Đặc tả use-case Trực quan hóa dữ liệu*

|  |  |
| --- | --- |
| 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 | |

**4.3. Thiết kế cơ sở dữ liệu**

**a) Cơ sở dữ liệu**

Trong hợp lưu trữ, quản lý dữ liệu, hồ sơ đối với số lượng lớn mục tiêu thì đòi hỏi hệ thống phải sử dụng cơ sở dữ liệu. Việc quản lý dữ liệu bằng hệ thống cơ sở dữ liệu sẽ mang đến lợi ích tích cực, góp phần giúp cho việc lưu trữ, truy xuất, sử dụng và chỉnh sửa dữ liệu diễn ra nhanh chóng và mang đến hiệu suất công việc cao hơn. Hệ thống sử dụng Hệ quản trị cơ sở dữ liệu Mongodb để phù hợp với tính chất dữ liệu.



- Cơ sở dữ liệu gồm 09 bảng.

+ USER (username, password, information, role)

Bảng USER để lưu thông tin tài khoản gồm tên người dùng, mật khẩu (dưới dạng mã hash), thông tin người dùng và quyền người dùng

+ INDICATOR (id, url, description, status, reporter, threat, pattern, valid\_from, valid\_until)

Bảng INDICATOR để lưu thông tin về các mối đe dọa bao gồm mã định danh, Địa chỉ trang web hoặc máy chủ liên quan, mô tả sơ bộ, trạng thái hoạt động của mối đe dọa, người hoặc tổ chức báo cáo, loại mối đe dọa, mẫu pattern phát hiện, ngày bắt đầu hiệu lực, ngày kết thúc hiệu lực.

+ LOG (mac, ip, unit\_name, unit\_full\_name, alert\_type, alert\_level\_id, time\_receive, description, label)

Bảng LOG để lưu trữ thông tin về các sự kiện được xử lí gồm địa chỉ MAC, địa chỉ IP, tên đơn vị, loại cảnh báo, mức độ cảnh báo, thời gian xảy ra cảnh báo, mô tả sơ bộ, nhãn

+ STATISTICS (process\_count, detect\_count, database\_count)

Bảng STATISTICS lưu trữ thông tin về thống kê, gồm số lượng cảnh báo đã xử lý, số lượng cảnh báo được xác định là độc hại, số lượng mối đe dọa đang có trong cơ sở dữ liệu

+ CHART (ip, unit\_full\_name, count)

Bảng CHART thống kê các máy tính có lượng truy vấn độc hại lớn, gồm địa chỉ IP, tên đơn vị, số lượng truy vấn độc hại

+ CAMPAIGN (id, standard\_id, name, description, first\_seen, last\_seen, objective)

Bảng CAMPAIGN chứa thông tin về các chiến dịch tấn công mạng từng được ghi nhận gồm mã, tên chiến dịch, mô tả sơ bộ, thời gian bắt đầu và thời gian cuối cùng mà các hoạt động liên quan đến chiến dịch được ghi nhận.

+ INTRUSION\_SET (id, standard\_id, name, description, entity\_type, first\_seen)

Bảng INTRUSION\_SET chứa thông tin về các tổ chức lớn trong ngành an ninh mạng trên thế giới, gồm tên nhóm, mô tả sơ bộ, lần đầu tiên ghi nhận hoạt động.

+ MALWARE (id, standard\_id, name, description, malware\_types, first\_seen, last\_seen, architecture\_execution\_envs, implementation\_languages, capabilities, is\_family)

Bảng MALWARE chứa thông tin về các mẫu mã độc, gồm tên mã độc, mô tả, loại mã độc, lần đầu tiên được phát hiện, lần cuối ghi nhận hoạt động, …

+ RELATIONSHIP (id, relationship\_type, description, confidence, start\_time, stop\_time, fromType, toType, fromId, toId)

Bảng RELATIONSHIP chứa thông tin để kết nối giữa các bảng, phục vụ cho quá trình truy vết, liên kết thông tin.

**b) Đặc tả bảng dữ liệu**

*Bảng 8. Username*

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **TRƯỜNG DỮ LIỆU** | **KIỂU DỮ LIỆU** | **MÔ TẢ** |
| 1 | username | TEXT | Tên người dùng |
| 2 | password | TEXT | Mật khẩu |
| 3 | information | TEXT | Thông tin người dùng |
| 4 | role | TEXT | Quyền |

*Bảng 9. Indicator*

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **TRƯỜNG DỮ LIỆU** | **KIỂU DỮ LIỆU** | **MÔ TẢ** |
| 1 | id | TEXT | Mã định danh |
| 2 | url | TEXT | Địa chỉ web hoặc ip liên quan |
| 3 | description | TEXT | Mô tả |
| 4 | status | TEXT | Trạng thái |
| 5 | reporter | TEXT | Người báo cáo |
| 6 | threat | TEXT | Loại mối đe dọa |
| 7 | pattern | TEXT | Mẫu phát hiện |
| 8 | valid\_from | DATETIME | Ngày bắt đầu hiệu lực |
| 9 | valid\_until | DATETIME | Ngày kết thúc hiệu lực |

*Bảng 10. Log*

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **TRƯỜNG DỮ LIỆU** | **KIỂU DỮ LIỆU** | **MÔ TẢ** |
| 1 | mac | TEXT | Địa chỉ MAC |
| 2 | ip | TEXT | Địa chỉ IP |
| 3 | unit\_name | TEXT | Tên đơn vị |
| 4 | unit\_full\_name | TEXT | Tên đơn vị đầy đủ |
| 5 | alert\_type | TEXT | Loại cảnh báo |
| 6 | alert\_level\_id | INT | Mức độ cảnh báo |
| 7 | time\_receive | DATETIME | Thời gian nhận |
| 8 | description | TEXT | Mô tả |
| 9 | label | INT | Nhãn |

*Bảng 11. Statistic*

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **TRƯỜNG DỮ LIỆU** | **KIỂU DỮ LIỆU** | **MÔ TẢ** |
| 1 | process\_count | INT | Số cảnh báo đã xử lý |
| 2 | detect\_count | INT | Số cảnh báo được xác định là độc hại |
| 3 | database\_count | INT | Số lượng mối đe dọa trong cơ sở dữ liệu |

*Bảng 12. Chart*

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **TRƯỜNG DỮ LIỆU** | **KIỂU DỮ LIỆU** | **MÔ TẢ** |
| 1 | ip | TEXT | Địa chỉ IP |
| 2 | unit\_full\_name | TEXT | Tên đơn vị |
| 3 | count | INT | Số lượng truy vấn độc hại |

*Bảng 13. Malware*

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **TRƯỜNG DỮ LIỆU** | **KIỂU DỮ LIỆU** | **MÔ TẢ** |
| 1 | id | TEXT | Địa chỉ IP |
| 2 | standard\_id | TEXT | Tên đơn vị |
| 3 | name | TEXT | Số lượng truy vấn độc hại |
|  | description | TEXT | Mô tả |
|  | malware\_types | TEXT | Loại mã độc |
|  | first\_seen | DATETIME | Lần đầu tiên ghi nhận |
|  | last\_seen | DATETIME | Lần cuối cùng ghi nhận |
|  | architecture\_execution\_envs | TEXT | Thông tin về kiến trúc |
|  | implementation\_languages | TEXT | Ngôn ngữ |
|  | capabilities | TEXT | Khả năng của mã độc |
|  | is\_family | BOOLEAN | Là họ mã độc hay là biến thể |

*Bảng 14. Intrusion\_Set*

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **TRƯỜNG DỮ LIỆU** | **KIỂU DỮ LIỆU** | **MÔ TẢ** |
| 1 | id | TEXT | Mã định danh |
| 2 | standard\_id | TEXT | Mã định danh chuẩn |
| 3 | name | TEXT | Tên tác nhân |
| 4 | description | TEXT | Mô tả sơ bộ |
| 5 | entity\_type | TEXT | Loại tác nhân |
| 6 | first\_seen | DATETIME | Lần đầu tiên được ghi nhận |

*Bảng 15. Campaign*

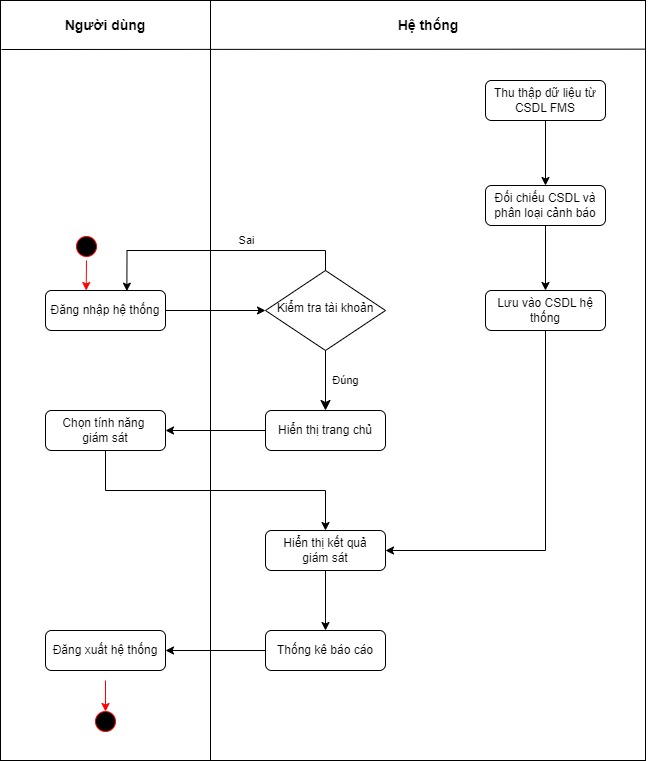
|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **TRƯỜNG DỮ LIỆU** | **KIỂU DỮ LIỆU** | **MÔ TẢ** |
| 1 | id | TEXT | Mã định danh |
| 2 | standard\_id | TEXT | Mã định danh chuẩn |
| 3 | name | TEXT | Tên chiến dịch |
| 4 | description | TEXT | Mô tả sở bộ |
| 5 | first\_seen | DATETIME | Lần đầu tiên được ghi nhận |
| 6 | last\_seen | DATETIME | Lần cuối cùng được ghi nhận |
| 7 | objective | TEXT | Loại chiến dịch |

*Bảng 16. Relationship*

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **TRƯỜNG DỮ LIỆU** | **KIỂU DỮ LIỆU** | **MÔ TẢ** |
| 1 | id | TEXT | Mã định danh |
| 2 | relationship\_type | TEXT | Loại quan hệ |
| 3 | description | TEXT | Mô tả |
| 4 | confidence | INT | Mức độ tin cậy của quan hệ |
| 5 | start\_time | DATETIME | Thời gian bắt đầu quan hệ |
| 6 | stop\_time | DATETIME | Thời gian kết thúc quan hệ |
| 7 | fromType | TEXT | Kiểu thực thể nguồn |
| 8 | toType | TEXT | ID thực thể đích |
| 9 | fromId | TEXT | ID thực thể nguồn |
| 10 | toId | TEXT | ID thực thể đích |

**5. Biểu đồ hoạt động**

Từ thực tiễn quy trình nghiệp vụ trinh sát, dò quét mục tiêu website, máy chủ của cán bộ, xác định biểu đồ hoạt động tập trung vào mô tả các hoạt động của cán bộ, luồng xử lý bên trong hệ thống.



*Biểu đồ hoạt động hệ thống*

**IV. DỰ TOÁN CHI TIẾT**

Nội dung dự toán chi tiết được lập như sau:

1. Tổng hợp dự toán

*Đơn vị tính: VNĐ.*

| **STT** | **Nội dung** | **Tổng dự toán** | **Ghi chú** |
| --- | --- | --- | --- |
| 1 | Chi phí xây dựng phần mềm nội bộ | 800.000.000 |  |
| **Tổng cộng:** | | **800.000.000** |  |

*(Bằng chữ: Tám trăm triệu đồng chẵn)*

**2. Chi tiết dự toán**

**Bảng tính giá trị phần mềm**

*Đơn vị tính: VNĐ.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TT** | **Hạng mục** | **Diễn giải** | **Giá trị** | **Ghi chú** |
| **I** | **Tính điểm trường hợp sử dụng (Use-Case)** |  |  |  |
| 1 | Điểm Actor (TAW) |  | 3 |  |
| 2 | Điểm Use case (TBF) |  | 108 |  |
| 3 | Tính điểm UUCP | UUCP = TAW +TBF | 112 |  |
| 4 | Điểm hệ số KT-CN (TCF) | TCF = 0,6 + (0,01 x TFW) | 0.96 |  |
| 5 | Điểm hệ số môi trường (EF) | EF = 1,4 + (-0,03 x EFW) | 0.965 |  |
| 6 | Tính điểm AUCP | AUCP = UUCP x TCF x EF | 103.7568 |  |
| **II** | **Nội suy thời gian lao động (P)** | P: người/giờ/AUCP | 29.5 |  |
| **III** | **Giá trị nỗ lực thực tế I** | E = 10/6 x AUCP | 172.9280 |  |
| **IV** | **Mức lương lao động bình quân (H)** | H: người/giờ | 64,101 |  |
| **V** | **Giá trị phần mềm nội bộ (G)** | G = 1,4 x E x P x H | **457,807,302.389** |  |
| **VI** | **Chi phí chung I** | C = G x 65% | 297,574,746.553 |  |
| **VII** | **Thu nhập chịu thuế tính trước (TL)** | TL = (G+C) x 6% | 45,322,922.936 |  |
| **VIII** | **Chi phí phần mềm (GPM)** | GPM = G + C + TL | 800,704,971.878 |  |
|  | **TỔNG CỘNG (làm tròn)** | **GPM** | 800,000,000 |  |

*(Bằng chữ: Tám trăm triệu đồng chẵn.)*

*(Chi tiết tại Phụ lục)*

# V. DỰ KIẾN TIẾN ĐỘ THỰC HIỆN

Hoàn thành mua sắm, lắp đặt, nghiệm thu và đưa vào sử dụng trước ngày 31/11/2025.

## VI. PHƯƠNG ÁN TỔ CHỨC THỰC HIỆN

## 1. Tiến độ dự kiến thực hiện

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Nội dung công việc** | **T6** | **T7** | **T8** | **T9** | **T10** | **T11** |
| Xây dựng thuyết minh nhiệm vụ |  |  |  |  |  |  |
| Tổ chức xây dựng phần mềm |  |  |  |  |  |  |
| Thử nghiệm và hiệu chỉnh hệ thống |  |  |  |  |  |  |
| Phối hợp với các cơ quan, đơn vị giám định chất lượng, kiểm tra an ninh, ATTT phần mềm và thiết bị |  |  |  |  |  |  |
| Viết báo cáo tổng hợp kết quả thực hiện nhiệm vụ |  |  |  |  |  |  |

## 2. Phương án tổ chức thực hiện vận hành, khai thác

2.1. Phương án cài đặt, triển khai, vận hành

Hệ thống sau khi được xây dựng sẽ triển khai áp dụng cho các nhiệm vụ tại Trung tâm 386/BTL86.

Trung tâm 386 chịu trách nhiệm vận hành, sử dụng hệ thống cho tới khi Quy chế vận hành hoặc Quy định khác về vận hành sử dụng hệ thống được ban hành.

Trong trường hợp chuyển giao cho đơn vị khác thực hiện quản trị, vận hành hệ thống, Trung tâm 386 có trách nhiệm đào tạo, chuyển giao công nghệ, tài khoản quản trị, … cho đơn vị nhận bàn giao.

Đơn vị vận hành, quản trị hệ thống có trách nhiệm hướng dẫn các cơ quan, đơn vị trong Bộ tư lệnh 86 làm nhiệm vụ săn tìm mối nguy cơ sử dụng công cụ trong thực hiện nhiệm vụ.

2.2. Phương án kiểm thử các yêu cầu chức năng và phi chức năng của hệ thống

Khi đơn vị triển khai thông báo là đã hoàn thành giai đoạn phát triển, các đơn vị cần tiến hành kiểm tra, chạy thử để hoàn thiện phần mềm trước khi tiến hành nghiệm thu sản phẩm.

2.3. Cam kết của đơn vị phát triển về quá trình bảo hành và hỗ trợ kỹ thuật sau khi hệ thống đưa vào vận hành, khai thác

- Thời gian bảo hành đối với phần mềm là 24 tháng kể từ ngày nghiệm thu bàn giao.

- Đơn vị triển khai nhiệm vụ phải có trách nhiệm bảo hành sản phẩm khi có bất kỳ một đơn vị thụ hưởng nào báo hệ thống có lỗi hoặc không đáp ứng yêu cầu và phải có trách nhiệm cập nhật bản vá lỗi cho tất cả các đơn vị thụ hưởng khác trong thời gian bảo hành. Một khi ứng dụng có sự điều chỉnh mã nguồn do khắc phục lỗi hoặc nâng cấp chức năng của phần mềm. Đơn vị triển khai phải bàn giao CD (2 bản có nội dung giống nhau) mã nguồn và các tài liệu có liên quan đến việc hiệu chỉnh phần mềm cho Chủ đầu tư.

- Thời gian xử lý lỗi tối đa không quá 03 ngày làm việc. Hình thức đơn vị vận hành thông báo phần mềm xuất hiện lỗi có thể bằng: văn bản, thư điện tử, điện thoại, …

|  |  |  |
| --- | --- | --- |
|  |  | *Đà Nẵng, ngày tháng 03 năm 2025* |
|  |  | **CHỦ NHIỆM NHIỆM VỤ**  **Đại úy Nguyễn Đức Anh** |

**Phụ lục  
DỰ TOÁN CHI TIẾT PHẦN MỀM NỘI BỘ**

**Bảng 1. Sắp xếp thứ tự ưu tiên các yêu cầu chức năng của phần mềm**

|  |  |  |
| --- | --- | --- |
| **STT** | **Chức năng** | **Mức độ** |
| 1 | Điều tra thông tin về IOC | Phức tạp |
| 2 | Đối chiếu và phân loại cảnh báo | Trung bình |
| 3 | Thu thập dữ liệu | Trung bình |
| 4 | Sao lưu dữ liệu | Trung bình |
| 5 | Nhập dữ liệu từ file | Trung bình |
| 6 | Thêm mới người dùng | Trung bình |
| 7 | Thêm mới địa chỉ máy chủ | Trung bình |
| 8 | Thống kê báo cáo | Trung bình |
| 9 | Tìm kiếm cảnh báo theo thời gian | Trung bình |
| 10 | Xóa địa chỉ máy chủ | Đơn giản |
| 11 | Xóa người dùng | Đơn giản |
| 12 | Trực quan hóa dữ liệu | Đơn giản |

**Bảng 2. Danh sách tác nhân**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên tác nhân** | **Ý nghĩa** | **Phân loại tác nhân** |
| 1 | Quản trị viên | Quản trị viên hệ thống | PT |
|  | Người dùng | Người dùng hệ thống | PT |
|  | FMS | Cơ sở dữ liệu FMS | ĐG |

**Bảng 3. Bảng chuyển đổi yêu cầu chức năng sang trường hợp sử dụng (use-case)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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 | Thêm mới người dùng | Quản trị viên | Truy cập trang quản lý người dùng | Trung bình |  |
| Chọn tính năng Thêm mới |
| Gửi yêu cầu thêm người dùng mới |
| Cập nhật danh sách người dùng |
| 7 | Thêm mới địa chỉ máy chủ | Quản trị viên | Truy cập trang quản lý địa chỉ máy chủ | Trung bình |  |
| Chọn tính năng Thêm mới địa chỉ máy chủ |
| Gửi yêu cầu thêm địa chỉ mới |
| 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 | Xóa địa chỉ máy chủ | Quản trị viên | Truy cập trang quản lý địa chỉ máy chủ | Đơn giản |  |
| Gửi yêu cầu xóa địa chỉ máy chủ |
| Cập nhật danh sách máy chủ |
| 11 | Xóa người dùng | Quản trị viên | Truy cập trang quản lý người dùng | Đơn giản |  |
| Gửi yêu cầu xóa người dùng |
| Cập nhật danh sách người dùng |
| 12 | Trực quan hóa dữ liệu | Người dùng | Truy cập trang trực quan hóa | Đơn giản |  |
| Phân tích mối liên kết |
| Hiển thị biểu đồ |

**Bảng 4. Tính toán điểm các tác nhân (Actors) tương tác trao đổi thông tin với phần mềm**

| **STT** | **Loại Actor** | **Mô tả** | **Trọng số** | **Số tác nhân** | **Điểm của từng loại tác nhân** |
| --- | --- | --- | --- | --- | --- |
| 1 | Đơn giản | Giao diện lập trình ứng dụng (API) | 1 | 1 | 1 |
| 2 | Trung bình | Giao diện dòng lệnh (CLI) hoặc giao diện thông qua một giao thức nào đó không phải là giao diện lập trình ứng dụng | 2 | 0 | 0 |
| 3 | Phức tạp | Giao diện đồ họa người dùng | 3 | 2 | 3 |
|  | **Cộng** |  |  |  | 7 |

**Bảng 5. Tính toán điểm các trường hợp sử dụng (Use-Case)**

| **TT** | **Loại** | **Trọng số** | **Hệ số BMT** | **Số trường hợp** | **Điểm TH sử dụng** | **Mô tả** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | **B** |  |  |  |  | Các yêu cầu phải thỏa mãn thì PM mới được chấp nhận |
|  | Đơn giản | 5 | 1 | 3 | 15 | Use case đơn giản có ≤ 3 transactions hoặc đường chỉ thị |
|  | Trung bình | 10 | 1 | 7 | 70 | Use case trung bình từ 4 đến 7 transactions |
|  | Phức tạp | 15 | 1 | 1 | 15 | Use case phức tạp > 7 transactions |
| 2 | **M** |  |  |  |  | Các chức năng không phải là cốt lõi hay các chức năng phụ trợ hoặc theo yêu cầu của bên đặt hàng |
|  | Đơn giản | 5 | 1.2 | 0 | 0 |
|  | Trung bình | 10 | 1.2 | 1 | 12 |
|  | Phức tạp | 15 | 1.2 | 0 | 0 |
| 3 | **T** |  |  |  |  | Các yêu cầu được bên PT PM tư vấn thêm hoặc đưa ra để bên đặt hàng lựa chọn thêm nếu muốn |
|  | Đơn giản | 5 | 1,5 | 0 | 0 |
|  | Trung bình | 10 | 1,5 | 0 | 0 |
|  | Phức tạp | 15 | 1,5 | 0 | 0 |
|  | **Cộng (B+M+T)** |  |  | 12 | **112** |  |

**Bảng 6. Tính toán hệ số phức tạp kỹ thuật - công nghệ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **TT** | **Các hệ số KT** | **Mức xếp hạng** | **Trọng số chuẩn** | **Giá trị xếp hạng** | **Kết quả** |
| **(Từ 0 đến 5)** |
| **I** | **Hệ số KT-CN (TFW)** |  |  |  |  |
| 1 | Xử lý phân tán | 0 = Không quan trọng | 1 | 1 | 1 |
| 5 = Có vai trò tác động căn bản |
| 2 | Mức độ quan trọng của hiệu năng | 0 = Không quan trọng | 1 | 2 | 2 |
| 5 = Có vai trò tác động căn bản |
| 3 | Hiệu quả sử dụng người dùng | 0 = Không quan trọng | 1 | 1 | 1 |
| 5 = Có vai trò tác động căn bản |
| 4 | Độ phức tạp của xử lý bên trong (complex internal processing) | 0 = Không quan trọng | 2 | 2 | 4 |
| 5 = Có vai trò tác động căn bản |
| 5 | Mã nguồn phải tái sử dụng được (Code must be reuseable) | 0 = Không quan trọng | 1 | 5 | 5 |
| 5 = Có vai trò tác động căn bản |
| 6 | Dễ cài đặt (Easy to install) | 0 = Không quan trọng | 0.5 | 3 | 1.5 |
| 5 = Có vai trò tác động căn bản |
| 7 | Dễ vận hành | 0 = Không quan trọng | 0.5 | 3 | 1.5 |
| 5 = Có vai trò tác động căn bản |
| 8 | Khả năng chuyển đổi (Portable) | 0 = Không quan trọng | 1 | 3 | 3 |
| 5 = Có vai trò tác động căn bản |
| 9 | Dễ dang bảo trì | 0 = Không quan trọng | 1 | 3 | 3 |
| 5 = Có vai trò tác động căn bản |
| 10 | Xử lý đồng thời (Concurrent) | 0 = Không quan trọng | 1 | 3 | 3 |
| 5 = Có vai trò tác động căn bản |
| 11 | Mức độ hỗ trợ bảo mật | 0 = Không quan trọng | 2 | 3 | 6 |
| 5 = Có vai trò tác động căn bản |
| 12 | Sự phụ thuộc vào mã lệnh của bên thứ 3 | 0 = Không quan trọng | 1 | 4 | 4 |
| 5 = Có vai trò tác động căn bản |
| 13 | Mức độ hỗ trợ đào tạo người sử dụng | 0 = Không quan trọng | 1 | 1 | 1 |
| 5 = Có vai trò tác động căn bản |
|  | Cộng I (TFW) |  |  |  | **36** |
| **II** | **Hệ số phức tạp về KT-CN (TCF)** | **TCF = 0,6 + (0,01 x TFW)** |  |  | **0.96** |

**Bảng 7. Tính toán hệ số tác động môi trường và nhóm làm việc, hệ số phức tạp về môi trường**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TT** | **Các hệ số tác động môi trường** | **Trọng số chuẩn** | **TB cộng giá trị xếp hạng** | **Kết quả (KQ)** | **Đánh giá độ ổn định KN** | **Diễn giải lý do** |
|
| I | ***Hệ số phức tạp về môi trường và nhóm làm việc (EFW)*** |  |  |  |  |  |
| 1 | Có áp dụng qui trình phát triển PM | 1.5 | 3 | 4.5 | 1 | Trung bình |
| 2 | Có kinh nghiệm về ứng dụng tương tự (application experiences) | 0.5 | 3 | 1.5 | 0.1 | Trung bình |
| 3 | Có kinh nghiệm về hướng đối tượng (Object Oriented) | 1 | 3 | 3 | 0.6 | Trung bình |
| 4 | Kinh nghiệm của trưởng nhóm lập trình | 0.5 | 3 | 1.5 | 0.1 | Trung bình |
| 5 | Tính chủ động | 1 | 3 | 3 | 0.6 | Trung bình |
| 6 | Độ ổn định của các yêu cầu | 2 | 1 | 2 | 0.1 | Trung bình |
| 7 | Có sử dụng các nhân viên làm Part-time | -1 | 0 | 0 | 0 | Không có |
| 8 | Kinh nghiệm sử dụng ngôn ngữ lập trình | -1 | 0 | 0 | 0 | Dễ |
|  | ***Cộng I*** |  |  | 15.5 |  |  |
| **II** | **Hệ số phức tạp về môi trường (EF)** |  |  | **0.935** |  |  |
| **III** | **Độ ổn định kinh nghiệm (ES)** |  |  |  | **2.5** |  |
| **IV** | **Nội suy thời gian lao động (P)** |  |  |  | **29,5** |  |

**Bảng 8. Mức lương lao động bình quân**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **TT** | **Tiêu chí xác định** | **Tỷ lệ/ hệ số xác định** | **Cấp bậc, hệ số, mức lương** | | | | | **Ghi chú** |
| 1 | Cấp bậc kỹ sư |  | Bậc 1 | Bậc 2 | Bậc 3 | Bậc 4 | Bậc 5 |  |
| 2 | Hệ số lương theo cấp bậc | HCB | 2,34 | 2,65 | 2,96 | 3,27 | 3,58 | *Quyết định số 129/QĐ-BTTTT ngày 03/02/2021 của Bộ TT&TT* |
| 3 | Hệ số phụ cấp lương | HPC | 0 | 0 | 0 | 0 | 0 |  |
| 4 | Mức lương cơ sở | MLCS | 2.340.000 | 2.340.000 | 2.340.000 | 2.340.000 | 2.340.000 | *Nghị định số 38/2019/NĐ-CP ngày 09/05/2019 của Chính phủ* |
| 5 | Lương cơ bản | LCB = (HCB + HPC)\*MLCS | 5.475.600 | 6.201.000 | 6.926.400 | 7.651.800 | 8.377.200 |  |
| 6 | Hệ số điều chỉnh tăng tiền lương | HĐC | 1,2 | 1,2 | 1,2 | 1,2 | 1,2 | *Vùng I Quyết định số 129/QĐ-BTTTT ngày 03/02/2021 của Bộ TT&TT* |
| 7 | Các khoản nộp theo lương (3% BHYT, 17.5% BHXH, 1% BHTN, 2% KPCĐ) | BHLĐ = 0,235\*LCB | 1.286.766 | 1.457.235 | 1.627.704 | 1.798.173 | 1.968.642 | *Nghị định số 58/2020/NĐ-CP, Quyết định số 595/QĐ-BHXH* |
| 8 | Đơn giá ngày công trực tiếp | GNC = (LCB \* (1+HĐC) + BHLĐ)/26 | 512.811 | 580.748 | 648.684 | 716.621 | 784.557 | *Thời gian lao động để tính mức lương lao động bình quân tháng là 26 ngày.* |
| 9 | Mức lương lao động/giờ | H = GNC/8 | 64.101 | 72.593 | 81.086 | 89.578 | 98.070 | *Thời gian lao động 08 giờ/ngày* |

**Bảng 9. Bảng tính giá trị phần mềm**

*ĐVT: Đồng.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TT** | **Hạng mục** | **Diễn giải** | **Giá trị** | **Ghi chú** |
| **I** | **Tính điểm trường hợp sử dụng (Use-Case)** |  |  |  |
| 1 | Điểm Actor (TAW) |  | 3 |  |
| 2 | Điểm Use case (TBF) |  | 108 |  |
| 3 | Tính điểm UUCP | UUCP = TAW +TBF | 112 |  |
| 4 | Điểm hệ số KT-CN (TCF) | TCF = 0,6 + (0,01 x TFW) | 0.96 |  |
| 5 | Điểm hệ số môi trường (EF) | EF = 1,4 + (-0,03 x EFW) | 0.965 |  |
| 6 | Tính điểm AUCP | AUCP = UUCP x TCF x EF | 103.7568 |  |
| **II** | **Nội suy thời gian lao động (P)** | P: người/giờ/AUCP | 29.5 |  |
| **III** | **Giá trị nỗ lực thực tế (E)** | E = 10/6 x AUCP | 172.9280 |  |
| **IV** | **Mức lương lao động bình quân (H)** | H: người/giờ | 64,101 |  |
| **V** | **Giá trị phần mềm nội bộ (G)** | G = 1,4 x E x P x H | **457,807,302.389** |  |
| **VI** | **Chi phí chung (C)** | C = G x 65% | 297,574,746.553 |  |
| **VII** | **Thu nhập chịu thuế tính trước (TL)** | TL = (G+C) x 6% | 45,322,922.936 |  |
| **VIII** | **Chi phí phần mềm (GPM)** | GPM = G + C + TL | 800,704,971.878 |  |
|  | **TỔNG CỘNG (làm tròn)** | **GPM** | 800,000,000 |  |

*Bằng chữ: Tám trăm triệu đồng chẵn.*