Bkav Pro Cyber Range
Your digital battlefield

THAO TRƯỜNG AN NINH MẠNG VIET NAM CYBER RANGE

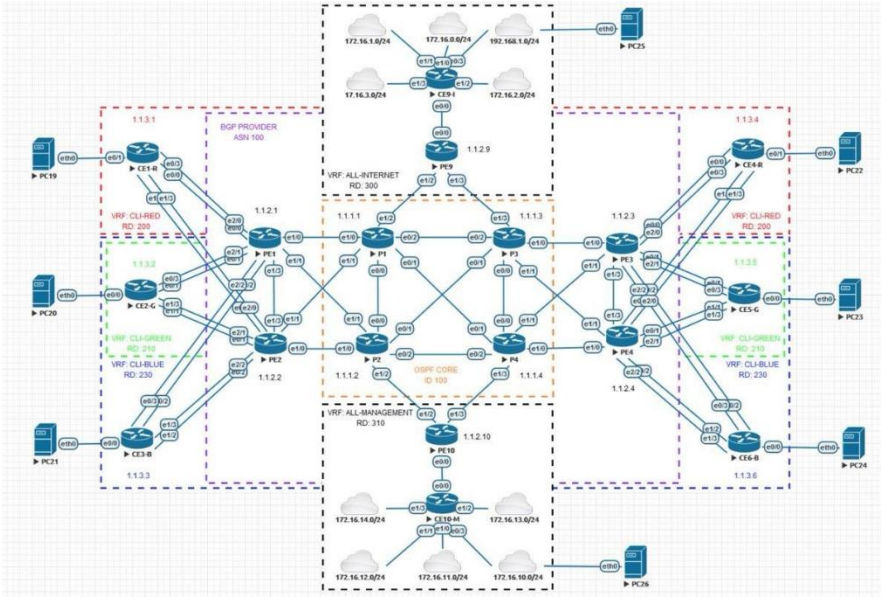
Phiên bản Standard

1. Giới thiệu tổng quan

Phần mềm thao trường mạng phục vụ huấn luyện, diễn tập, sát hạch an toàn thông tin phục vụ chính phủ điện tử - Vietnam Cyber Range (VCR) là hệ thống thao trường mạng cho đào tạo, huấn luyện, diễn tập đảm bảo an ninh, an toàn thông tin có các chức năng cơ bản của Cyberbit, Cisco Cyber Range. Việc tham gia thao trường thực hiện qua môi trường điện toán đám mây và môi trường diễn tập được khoanh vùng tập trung nên đảm bảo dễ triển khai và độ an toàn cao cho hệ thống cũng như người tham gia thao diễn.

Phần mềm thao trường mạng phục vụ huấn luyện, diễn tập, sát hạch an toàn thông tin phục vụ chính phủ điện tử - Vietnam Cyber Range (VCR) được xây dựng để huấn luyện, diễn tập, sát hạch an toàn thông tin phục vụ Chính phủ điện tử, đáp ứng được các mục tiêu cơ bản gồm:

- Hình thành một phần mềm giả lập, mô tả hệ thống CNTT cơ bản của cơ quan, tổ chức và một số hệ thống phục vụ chính phủ điện tử nhằm huấn luyện, diễn tập kỹ năng thực chiến trên không gian mạng cho đội ngũ nhân lực an toàn thông tin và ứng cứu sự cố ATTT mạng.



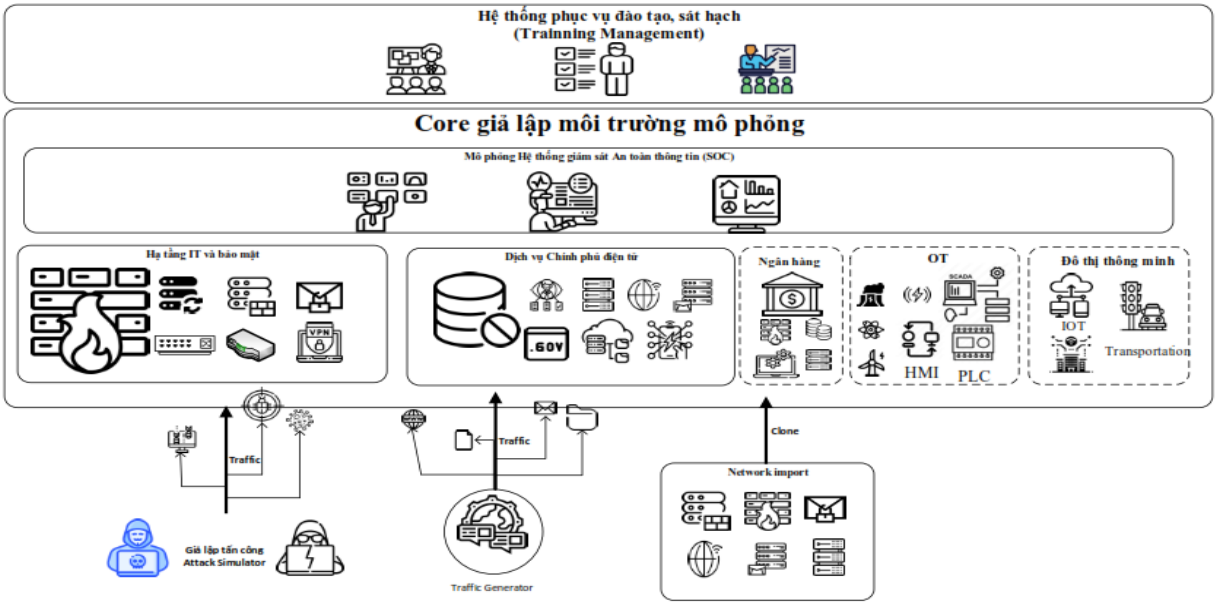
Hình 1.1: Ví dụ về giả lập hệ thống mạng của VCR

- Hình thành một phần mềm giả lập, mô tả hệ thống CNTT cơ bản của cơ quan, tổ chức và một số hệ thống phục vụ chính phủ điện tử nhằm huấn luyện, diễn tập kỹ năng thực chiến trên không gian mạng cho đội ngũ nhân lực an toàn thông tin và ứng cứu sự cố ATTT mạng.

- Phục vụ công tác kiểm tra, đánh giá năng lực, kỹ năng nhân lực an toàn thông tin và ứng cứu sự cố.
- Nâng cao năng lực kỹ thuật, trình độ chuyên môn, kỹ năng an toàn thông tin cho Cục An toàn thông tin và đội ngũ nhân lực của các cơ quan nhà nước.
- Tạo lập môi trường nghiên cứu, thử nghiệm các mô hình tấn công, mối đe dọa đối với một số hệ thống, dịch vụ CNTT phục vụ chính phủ điện tử và trên không gian mạng.
  - ✓ Tổ chức diễn tập từ xa, phục vụ 24/7.
  - ✓ 100% các đơn vị chuyên trách CNTT, An toàn thông tin của Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ; và UBND các tỉnh, thành phố trực thuộc Trung ương tham gia diễn tập.
  - ✓ Tối thiểu 300 người tham gia diễn tập theo kịch bản đơn giản.
  - ✓ Tối thiểu 30 người tham gia huấn luyện trực tiếp.
  - ✓ Mô phỏng được tối thiểu 3 lĩnh vực: Chính phủ điện tử, Đô thị thông minh và hệ thống hạ tầng quan trọng.

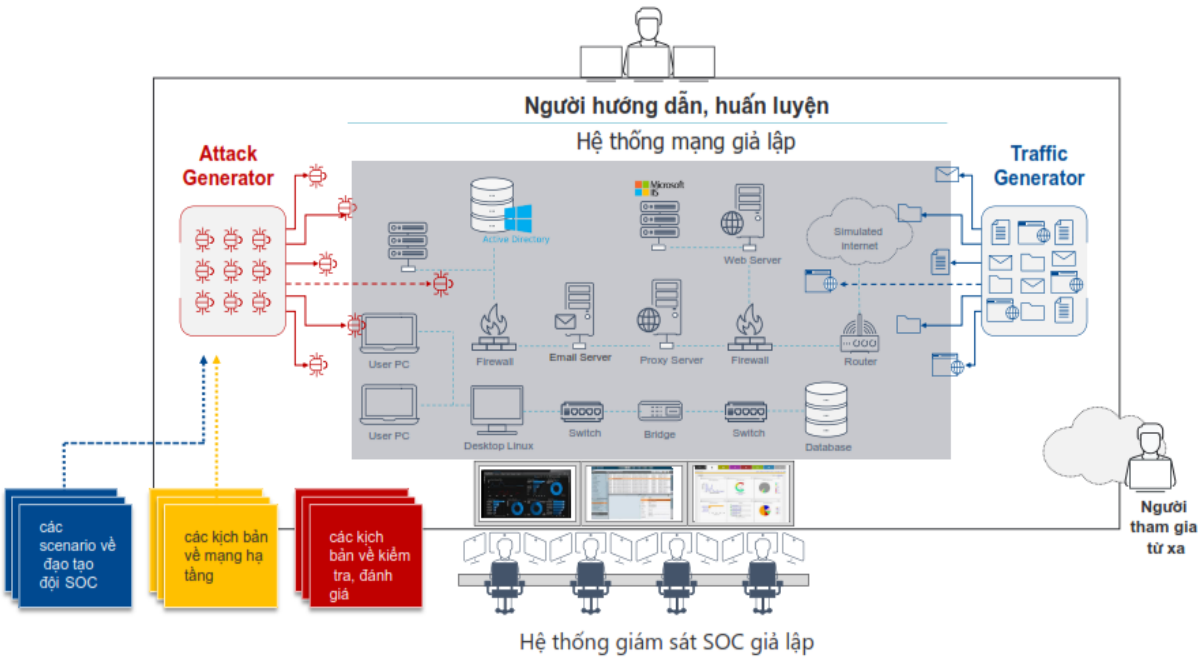
2. Mô hình và Kiến trúc tích hợp của hệ thống

Mô hình hệ thống thao trường ATTTM dựa trên các môi trường không gian mạng giả lập được mô tả tóm tắt trong sơ đồ sau đây (Hình 2).



Hình 2. Mô hình kiến trúc hệ thống thao trường ATTTM

Khác với các môi trường mô phỏng truyền thống, môi trường giả lập (emulation) là mô hình của một hệ thống thực có khả năng thực hiện các kết nối chức năng giữa các dữ liệu và thông tin đầu vào và đầu ra của hệ thống thực dựa trên các quy trình giống hệt như hoặc tương tự như các quy trình thực của hệ thống đó và được xây dựng bằng các nguyên liệu giống như của hệ thống thực. Hệ thống giả lập hoạt động chính xác giống như hệ thống thực và tuân theo tất cả các quy tắc của hệ thống thực được giả lập. Trong khi môi trường mô phỏng (simulation) chỉ là mô hình của một hệ thống thực, tuy cũng có khả năng thực hiện các kết nối chức năng giữa các dữ liệu và thông tin đầu vào và đầu ra của hệ thống thực nhưng không nhất thiết phải dựa trên các quy trình giống như hoặc tương tự như của hệ thống thực. Mô hình mô phỏng chỉ cung cấp cho người dùng ý tưởng về cách thức hoạt động của một hệ thống thực được mô phỏng.



Hình 3. Mô hình hệ thống thao trường ATTTM
dựa trên các môi trường giả lập hệ thống Chính phủ điện tử, Trung tâm SOC.

Hệ thống thao trường ATTTM dựa trên các môi trường giả lập sẽ là nơi mà người tham gia huấn luyện, diễn tập có thể trải nghiệm các cuộc tấn công mạng thực, theo thời gian thực, và trong các điều kiện thực giống như khi họ phải đối mặt với chúng trong phạm vi không gian mạng thực của tổ chức nơi mà họ đang làm việc. Hệ thống cho phép người tham gia trải nghiệm "Một trận chiến trên không gian mạng" bằng cách sử dụng cơ sở hạ tầng phục vụ huấn luyện, diễn tập được trang bị trong hệ thống thao trường ATTTM và các kiến thức chuyên gia của đội ngũ hướng dẫn, giám sát và vận hành hệ thống thao trường.

Kiến trúc tích hợp của hệ thống thao trường bao gồm ba lớp chính để cùng nhau cung cấp một khái niệm huấn luyện, diễn tập, thực hành và cách thức tiếp cận toàn diện trong việc ứng phó với các sự cố an toàn, an ninh mạng. Hệ thống thao trường tích hợp này sẽ cung cấp cho người tham gia (cả đội ngũ cán bộ kỹ thuật và phi kỹ thuật) các kỹ năng cần thiết để sẵn sàng ứng phó một cách hiệu quả với các mối đe dọa không gian mạng có thể xảy ra trong thực tế đối với cơ quan, tổ chức của mình. Các lớp kiến trúc tích hợp của hệ thống thao trường bao gồm: (1) Lớp Cơ sở hạ tầng của hệ thống (Lớp tích hợp 1); (2) Lớp Tuỳ biến & Tích hợp (Lớp tích hợp 2); và (3) Lớp Quản trị & Vận hành hệ thống (Lớp tích hợp 3) (Hình 4).

Hình 4. Sơ đồ kiến trúc tích hợp của hệ thống thao trường ATTTM dựa trên các môi trường giả lập.

Hệ thống thao trường ATTTM dựa trên các môi trường giả lập sẽ là nơi mà người tham gia huấn luyện, diễn tập có thể trải nghiệm các cuộc tấn công mạng thực, theo thời gian thực, và trong các điều kiện thực giống như khi họ phải đối mặt với chúng trong phạm vi không gian mạng thực của tổ chức nơi mà họ đang làm việc. Hệ thống cho phép người tham gia trải nghiệm "Một trận chiến trên không gian mạng" bằng cách sử dụng cơ sở hạ tầng phục vụ huấn luyện, diễn tập được trang bị trong hệ thống thao trường ATTTM và các kiến thức chuyên gia của đội ngũ hướng dẫn, giám sát và vận hành hệ thống thao trường.

Kiến trúc tích hợp của hệ thống thao trường bao gồm ba lớp chính để cùng nhau cung cấp một khái niệm huấn luyện, diễn tập, thực hành và cách thức tiếp cận toàn diện trong việc ứng phó với các sự cố an toàn, an ninh mạng. Hệ thống thao trường tích hợp này sẽ cung cấp cho người tham gia (cả đội ngũ cán bộ kỹ thuật và phi kỹ thuật) các kỹ năng cần thiết để sẵn sàng ứng phó một cách hiệu quả với các mối đe dọa không gian mạng có thể xảy ra trong thực tế đối với cơ quan, tổ chức của mình. Các lớp kiến trúc tích hợp của hệ thống thao trường bao gồm: (1) Lớp Cơ sở hạ tầng của hệ thống (Lớp tích hợp 1); (2) Lớp Tuỳ biến & Tích hợp (Lớp tích hợp 2); và (3) Lớp Quản trị & Vận hành hệ thống (Lớp tích hợp 3) (Hình 4).

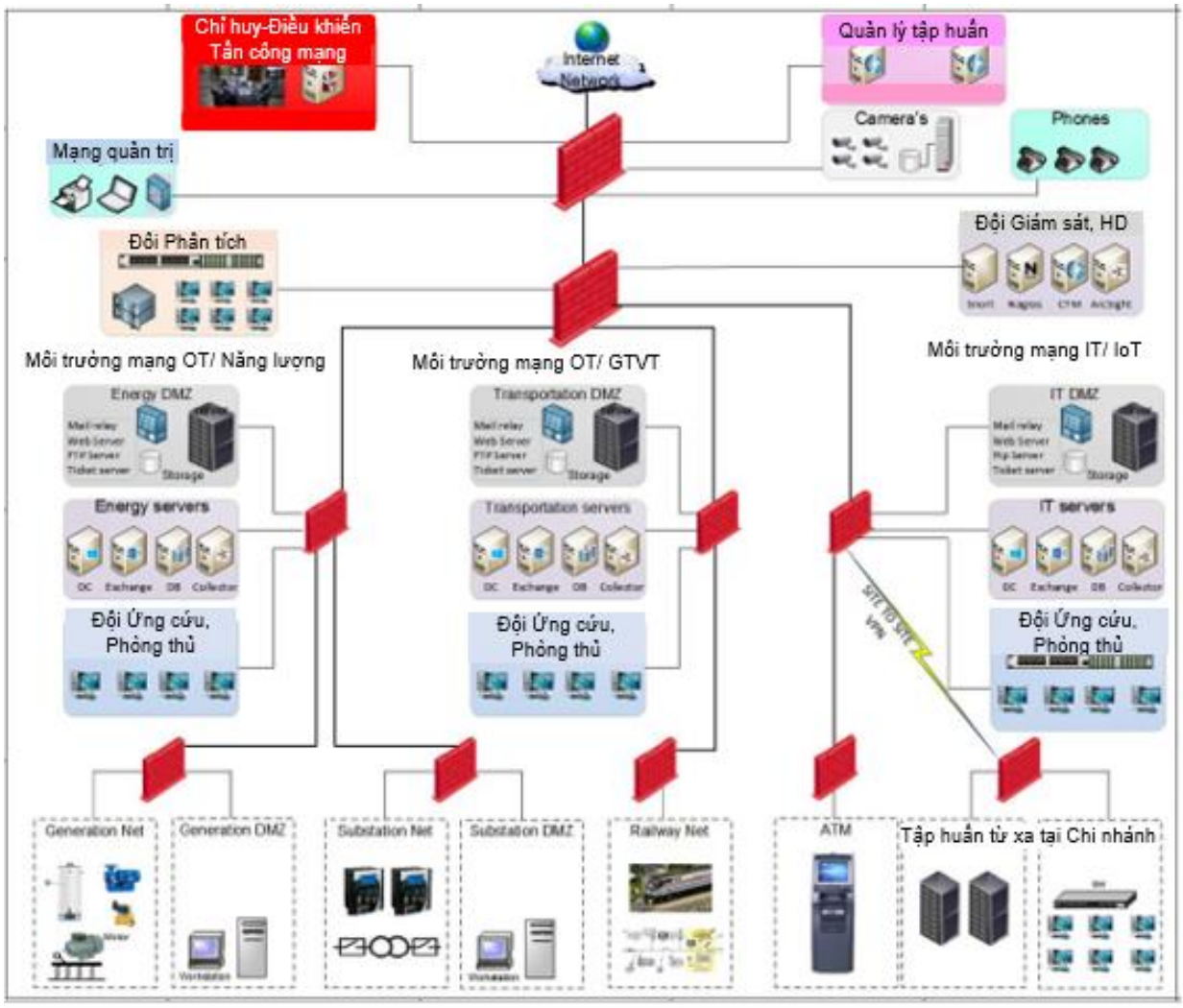
a) Lớp Cơ sở hạ tầng của hệ thống (Lớp tích hợp 1)

Các trang thiết bị của hệ thống thao trường ATTTM sẽ cung cấp một môi trường không gian mạng thực để người tham gia huấn luyện quản lý và truy cập, kiểm soát trong quá trình tham gia huấn luyện, diễn tập. Các trang thiết bị được thiết kế để cho phép người tham gia được trải nghiệm, kiểm soát, ngăn chặn và giảm nhẹ nguy cơ, sự cố ATTT mạng theo các kịch bản tấn công mạng trong một môi trường mạng thực.

Các trang thiết bị của lớp Cơ sở hạ tầng của hệ thống được phân chia thành nhiều mô đun và bao gồm các tổ hợp chính, ví dụ như:

- *Mô đun hỗ trợ huấn luyện:* Mô đun này được thiết kế để cung cấp các hỗ trợ cho cơ sở hạ tầng của hệ thống thao trường ATTTM. Mô đun bao gồm mạng của các hệ thống hỗ trợ việc huấn luyện và quản lý, vận hành trên hệ thống thao trường ATTTM.

- Mô đun chuyên ngành Công nghệ thông tin, Chính phủ điện tử: mô đun này được thiết kế để cung cấp cơ sở hạ tầng cho các khóa huấn luyện có liên quan đến các hệ thống, dịch vụ CNTT phục vụ chính phủ điện tử, tài chính – Ngân hàng (ví dụ như mạng ATM). Mô đun giả lập hệ thống mạng thông tin của một tổ chức bao gồm cả các chi nhánh ở xa.



Hình 5. Sơ đồ kiến trúc kết nối mạng lớp Cơ sở hạ tầng của hệ thống thao trường ATTTM dựa trên các môi trường giả lập.

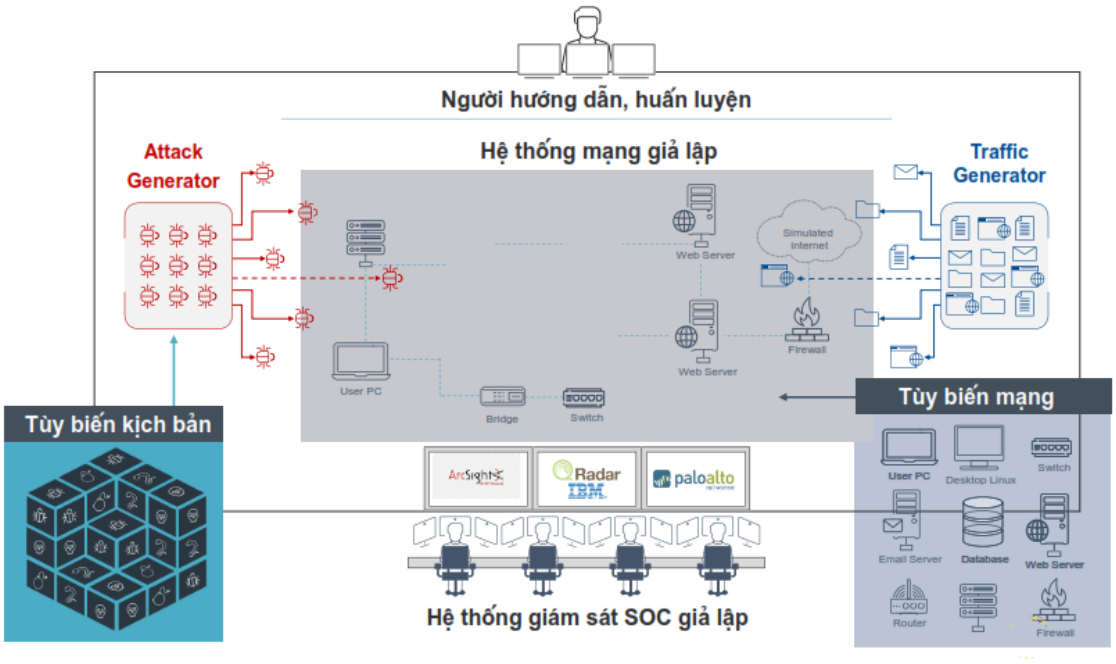
- Mô đun chuyên ngành Công nghệ thông tin, Chính phủ điện tử: Mô đun này được thiết kế để cung cấp cơ sở hạ tầng cho các khóa huấn luyện có liên quan đến các hệ thống, dịch vụ CNTT phục vụ chính phủ điện tử, tài chính – Ngân hàng (ví dụ như mạng ATM). Mô đun giả lập hệ thống mạng thông tin của một tổ chức bao gồm cả các chi nhánh ở xa.

- Mô đun chuyên ngành năng lượng: Mô đun này được thiết kế để cung cấp cơ sở hạ tầng cho các khóa huấn luyện liên quan đến các hệ thống thông tin và điều khiển của ngành năng lượng, ví dụ như các quy trình sản xuất và truyền tải phân phối điện, vận chuyển và phân phối dầu khí… Mô đun giúp giả lập các hệ thống điều khiển công nghiệp của một tổ chức, bao gồm việc giả lập các quy trình sản xuất, truyền tải và phân phối để bắt chước giống hệt các quy trình thực tế.

- Mô đun chuyên ngành đô thị thông minh, giao thông vận tải: Mô đun này được thiết kế để cung cấp cơ sở hạ tầng cho các khóa huấn luyện liên quan đến điều hành đô thi thông minh, các hệ thống điều khiển công nghiệp ứng dụng trong ngành giao thôngvận tải, ví dụ như các hệ thống quản lý giao thông đường sắt, cảng hàng không dân dụng...

b) Lớp Tùy biến và Tích hợp (Lớp tích hợp 2)

Hệ thống thao trường ATTTM được thiết kế và tích hợp với các phần mềm nền tảng cung cấp các khả năng tùy biến theo yêu cầu của người sử dụng nhằm đảm bảo các lĩnh vực và môi trường không gian mạng liên quan được giả lập và triển khai. Tùy theo yêu cầu của người sử dụng, hệ thống thao trường sẽ được thiết kế và tạo lập cơ sở hạ tầng liên quan để cung cấp cho người sử dụng các môi trường không gian mạng giả lập tùy biến và được tích hợp sao cho phù hợp với nhu cầu huấn luyện của người tham gia. Đây cũng là một phần của quy trình chuẩn bị cho các khóa huấn luyện trên hệ thống.



Hình 6. Tính năng tuy biến

Khả năng tuỳ biến của các phần mềm nền tảng của hệ thống cho phép thực hiện sự phân loại, tùy biến kịch bản, chương trình, nội dung thực hành theo các chuyên ngành, lĩnh vực khác nhau sao cho phù hợp với nhu cầu của từng khóa huấn luyện, diễn tập, đào tạo. Sự phân loại này có thể được sửa đổi để áp dụng cho các loại hình dịch vụ khác nhau, ví dụ như:

- Ngành Công nghệ thông tin và Tài chính: các hệ thống, dịch vụ CNTT ứng dụng trong Chính phủ điện tử, các hệ thống thanh toán bằng thẻ tín dụng...
- Ngành năng lượng: có thể phân loại theo các chuyên ngành sản xuất và phân phối Điện, truyền tải Dầu mỏ và Khí đốt...
- Ngành giao thông vận tải: có thể phân loại theo các chuyên ngành Đường sắt, Cảng hàng không dân dụng, Tàu điện ngầm...

Khả năng tích hợp của hệ thống cho phép tích hợp các điều kiện huấn luyện cụ thể đối với các nhóm tham gia huấn luyện, học viên khác nhau. Ví dụ như:

- Thiết lập cấu hình của hệ thống giám sát an toàn mạng (SIEM) và các hệ thống đảm bảo ATTT mạng.
- Tối ưu hóa cơ sở hạ tầng của hệ thống để phục vụ cho khóa huấn luyện, bao gồm việc thiết lập cấu hình các quy tắc và các dịch vụ liên quan.
- Tích hợp các mô hình vật lý, bao gồm việc thiết lập các cuộc tấn công mạng và các nhiệm vụ tác nghiệp ứng phó sự cố.
- Các điều chỉnh liên quan đến cơ sở hạ tầng thông tin để huấn luyện.
- Các kịch bản, tình huống tấn công mạng.

c) Lớp quản lý và vận hành hệ thống (Lớp tích hợp 3)

Lớp này bao gồm các phần mềm ứng dụng nền tảng có bản quyền được thiết kế và phát triển chuyên dụng cho việc quản lý và vận hành hệ thống thao trường ATTTM dựa trên các môi trường giả lập.

Hình 7. Hệ thống quản lý huấn luyện, đánh giá, sát hạch

c.1) Phần mềm mô phỏng và thực hiện các cuộc tấn công mạng

Phần mềm cung cấp một nền tảng dựa và khuôn khổ để khởi động các cuộc tấn công mạng theo giáo trình huấn luyện và thời hạn kịch bản tấn công đã được thiết kế chuyên biệt cho mỗi khóa huấn luyện. Với phần mềm này, đội tham gia huấn luyện đảm nhận nhiệm vụ tấn công mạng (Đội Tấn công) cũng có thể khởi động các cuộc tấn công "thủ công" theo yêu cầu để tấn công các mô hình giả lập cơ sở hạ tầng được bảo vệ tốt. Phần mềm cho phép Đội Tấn công dễ dàng triển khai các cuộc tấn công vào Đội Phòng thủ.

Phần mềm bao gồm các thành phần chủ yếu như Kho chứa dữ liệu các cuộc tấn công mạng, Cơ chế chỉ huy, điều khiển các cuộc tấn công và các bộ thu thập bằng chứng số… Nó cung cấp cho Đội Tấn công các khả năng chỉ huy và điều khiển các cuộc tấn công mạng được thiết kế để lây nhiễm và tấn công các hệ thống mạng mục tiêu một cách hiệu quả trong quá trình huấn luyện. Phần mềm cho phép thực hiện một loạt các cuộc tấn công không gian mạng được thiết lập cấu hình sẵn và được tùy biến cho phù hợp với từng khóa huấn luyện. Điều này cho phép Đội Tấn công thực hiện các tác nghiệp của mình một cách hiệu quả hơn, đồng thời cũng giúp tăng cường năng lực phòng thủ trên mạng của Đội Phòng thủ.

c.2) Phần mềm xây dựng các chương trình huấn luyện an toàn an ninh mạng

Phần mềm cung cấp một nền tảng để thiết kế, quản lý các yêu cầu huấn luyện và thiết lập các khóa huấn luyện cho các học viên. Phần mềm bao gồm các mô đun chủ yếu như:

- Mô đun Quản lý các yêu cầu huấn luyện: Lập kế hoạch huấn luyện và quản lý các yêu cầu huấn luyện của các tổ chức sử dụng hệ thống thao trường ATTTM dựa trên môi trường giả lập.
- Mô đun quản lý và tạo lập các giai đoạn huấn luyện và lịch trình huấn luyện.
- Mô đun Xây dựng các khóa huấn luyện: Xác định chuyên ngành để huấn luyện, các kịch bản huấn luyện, các cuộc tấn công và các hoạt động dự kiến.
- Mô đun Kiến thức cơ sở: Lưu trữ tất cả các tài liệu huấn luyện, diễn tập và đào tạo liên quan được thực hiện trên hệ thống thao trường ATTTM.
- Mô đun trợ giúp việc thảo luận và phân tích dữ liệu: giúp theo dõi và đánh giá các hoạt động của học viên trong quá trình huấn luyện.

Phần mềm xây dựng các chương trình huấn luyện ATTTM là một phần mềm quản lý cung cấp một nền tảng để tạo lập và quản lý các chương trình huấn luyện về an ninh mạng hoàn chỉnh, nhắm tới các đối tượng khác nhau với mức độ kinh nghiệm và kiến thức khác nhau. Phần mềm có chức năng chấm điểm cụ thể của người tham gia, các học viên, qua đó sẽ cho phép thực hiện việc đánh giá, đào tạo, sát hạch cấp chứng chỉ các kỹ năng về ATTT cho người tham gia huấn luyện, các học viên theo các chương trình huấn luyện, đào tạo tiêu chuẩn, đồng thời theo dõi quá trình phát triển kỹ năng và các điểm mạnh, điểm yếu của người tham gia, các học viên.

c.3) Phần mềm quản lý khóa huấn luyện

Phần mềm cung cấp một nền tảng cho việc giao tiếp, theo dõi và quản lý quá trình diễn ra một khóa huấn luyện. Các chức năng chính của phần mềm:

- Giám sát các hoạt động của khóa huấn luyện.
- Thẩm tra và xác minh tiến trình của khóa huấn luyện diễn ra theo kế hoạch đã định trước.
- Cung cấp phương thức truyền thông giữa các nhóm và cá nhân khác nhau tham gia trong khóa huấn luyện.
- Quản lý nguồn tài nguyên của khóa huấn luyện.
- Đánh giá và đo lường các hoạt động của người tham gia trong khóa huấn luyện.

Phần mềm quản lý khóa huấn luyện cung cấp một nền tảng để quản lý và đánh giá các hoạt động trong một khóa huấn luyện, cung cấp cho các chuyên gia huấn luyện và các thành viên giám sát (Đội Giám sát) các công cụ để giao tiếp, quản lý và đánh giá tình hình huấn luyện và hiệu suất của các học viên. Các tính năng của phần mềm cũng được thiết kế để cung cấp cho đội học viên đảm nhận nhiệm vụ phòng thủ mạng (Đội Phòng thủ) những hiểu biết về tác động của các cuộc tấn công mạng và của những hành động ứng phó sự cố lên tổ chức của họ trong một không gian mạng thực.

3. Kỹ thuật công nghệ sử dụng

3.1 Công nghệ Frontend

a) Angular JS: Là một framework có cấu trúc cho các ứng dụng web động. Nó cho phép bạn sử dụng HTML cho phép bạn mở rộng cú pháp của HTML để diễn đạt các thành phần ứng dụng của bạn một cách rõ ràng và súc tích. Hai tính năng cốt lõi: Data binding và Dependency injection của AngularJS loại bỏ phần lớn code mà bạn thường phải viết. Bản chất của AngularJS là hoạt động dạng Single Page, sử dụng API để lấy data, cho nên bạn cần biết các kĩ thuật DHTML, AJAX.

Đặc trưng của AngularJS:

- Phát triển dự trên Javascript.
- Tạo các ứng dụng client-side theo mô hình MVC.
- Khả năng tương thích cao, tự động xử lý mã javascript để phù hợp vúi mỗi trình duyệt.
- Mã nguồn mở, miễn phí hoàn toàn và được sủ dụng rộng rãi.

Các tính năng cơ bản:

- Scope: Là đối tượng có nhiệm vụ giao tiếp giữa controller và view của ứng dụng.
- Controller: Xử lí dữ liệu cho đối tượng $scope, từ đây bên views sẽ sử dụng các dữ liệu trong scope để hiển thị ra tương ứng.
- Data-binding: Tự động đồng bộ dữ liệu giữa model và view
- Service: Là singleton object được khởi tạo 1 lần duy nhất cho mỗi ứng dụng, cung cấp các phương thức lưu trữ dữ liệu có sãn. ($http, $httpBackend, $sce, $controller, $document, $compile, $parse, $rootElement, $rootScope...).
- Filter: Lọc các tập con từ tập item trong các mảng và trả về các mảng mới.
- Directive: Dùng để tạo các thẻ HTML riêng phục vụ những mục đích riêng. AngularJS có những directive có sẵn như ngBind, ngModel…

- Temple: Một thành phần của view, hiển thị thông tin từ controller
- Routing: Chuyển đổi giữa các action trong controller, qua lại giữa các view.
- MVC & MVVM: Mô hình thiết kế để phân chia các ứng dụng thành nhiều phần khác nhau (gọi là Model, View và Controller) mỗi phần có một nhiệm vụ nhất định. AngularJS không triển khai MVC theo cách truyền thống, mà gắn liền hơn với Model-View-ViewModel.
- Deep link: Liên kết sâu, cho phép bạn mã hóa trạng thái của ứng dụng trong các URL để nó có thể bookmark với công cụ tìm kiếm. Các ứng dụng có thể được phục hồi lại từ các địa chỉ URL với cùng một trạng thái.
- Dependency Injection: AngularJS có sẵn một hệ thống con dependency injection để giúp các lập trình viên tạo ra các ứng dụng dễ phát triển, dễ hiểu và kiểm tra.

b) NGINX: Là một web server mạnh mẽ mã nguồn mở. Nginx sử dụng kiến trúc đơn luồng, hướng sự kiện vì thế nó hiệu quả hơn Apache server. Nó cũng có thể làm những thứ quan trọng khác, chẳng hạn như load balancing, HTTP caching, hay sử dụng như một reverse proxy. Nginx là kiến thức không thể thiếu đối với một web developer, system administrator hay devops.

Những tính năng của máy chủ HTTP Nginx:

- Có khả năng xử lý hơn 10.000 kết nối cùng lúc với bộ nhớ thấp.
- Phục vụ tập tin tĩnh (static files) và lập chỉ mục tập tin.
- Tăng tốc reverse proxy bằng bộ nhớ đệm (cache), cân bằng tải đơn giản và khả năng chịu lỗi.
- Hỗ trợ tăng tốc với bộ nhớ đệm của FastCGI, uwsgi, SCGI, và các máy chủ memcached.
- Kiến trúc modular, tăng tốc độ nạp trang bằng nén gzip tự động.
- Hỗ trợ mã hoá SSL và TLS.
- Cấu hình linh hoạt; lưu lại nhật ký truy vấn.
- Chuyển hướng lỗi 3XX-5XX…
- Rewrite URL (URL rewriting) dùng regular expressions.
- Khả năng nhúng mã PERL.
- Hỗ trợ và tương thích với IPv6.
- Hỗ trợ WebSockets.
- Hỗ trợ truyền tải file FLV và MP4.
- Những tính năng máy chủ mail proxy của Nginx…

Các phương pháp xác thực:

- POP3: USER/PASS, APOP, AUTH LOGIN/PLAIN/CRAM-MD5.
- IMAP: LOGIN, AUTH LOGIN/PLAIN/CRAM-MD5.
- SMTP: AUTH LOGIN/PLAIN/CRAM-MD5.
- Hỗ trợ SSL, STARTTLS và STLS.

3.2 Công nghệ Backend

a) Ansible: Là một công cụ dùng để tự động hóa việc cấu hình trên nhiều server. So với các công cụ khác với tính năng tương đương thì Ansible dễ học và dễ tiếp cận hơn rất nhiều. Cộng đồng người dùng cũng nhiều hơn so với các công cụ khác.

Ansible sử dụng kiến trúc agentless để giao tiếp với các máy khác mà không cần agent. Cơ bản nhất là giao tiếp thông qua giao thức SSH trên Linux, WinRM trên Windows hoặc giao tiếp qua chính API của thiết bị đó cung cấp.

Ansible có thể giao tiếp với rất nhiều platform, OS và loại thiết bị khác nhau. Từ Ubuntu, CentOS, VMware, Windows cho tới AWS, Azure, các thiết bị mạng Cisco và Juniper... (hoàn toàn không cần agent khi giao tiếp).

Chính cách thiết kế này làm tăng tính tiện dụng của Ansible do không cần phải setup bảo trì agent trên nhiều host. Có thể coi đây là một thế mạnh của Ansible so với các công cụ có cùng chức năng như Chef, Puppet, SaltStack (Salt thì hỗ trợ cả 2 mode là agent và agentless, có thời gian thì mình sẽ viết 1 bài về Salt).

Ansible có rất nhiều ứng dụng trong triển khai phần mềm và quản trị hệ thống:

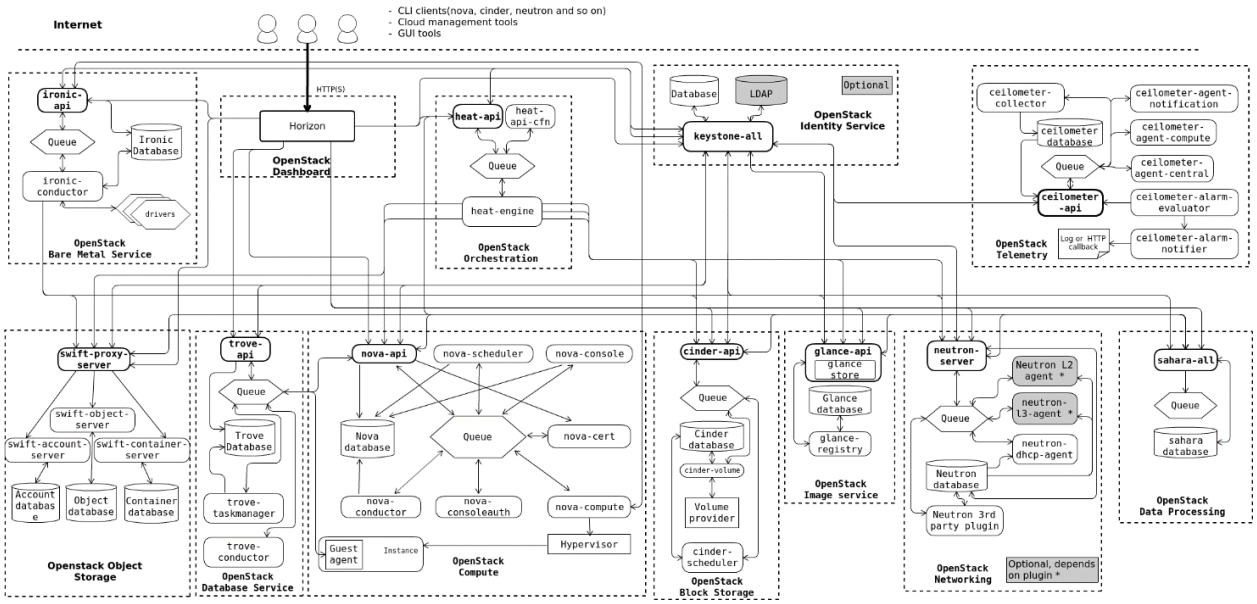
- Provisioning: Khởi tạo VM, container hàng loạt trong môi trường cloud dựa trên API (OpenStack, AWS, Google Cloud, Azure…).
- Configuration Management: Quản lý cấu hình tập trung các dịch vụ tập trung, không cần phải tốn công chỉnh sửa cấu hình trên từng server.
- Application Deployment: Deploy ứng dụng hàng loạt, quản lý hiệu quả vòng đời của ứng dụng từ giai đoạn dev cho tới production.
- Security & Compliance: Quản lý các chính sách về an toàn thông tinmột cách đồng bộ trên nhiều môi trường và sản phẩm khác nhau (deploy policy, cấu hình firewall hàng loạt trên nhiều server…).

c) Django rest Framework

REST là viết tắt của REpresentational State Transfer (dịch là chuyển trạng thái đại diện) là một kiểu kiến trúc lập trình, nó định nghĩa các quy tắc để thiết kết các web service chú trọng vào tài nguyên hệ thống. Trong kiến trúc REST mọi thứ đều được coi là tài nguyên, chúng có thể là: tệp văn bản, ảnh, trang html, video, hoặc dữ liệu động… REST server cung cấp quyền truy cập vào các tài nguyên, REST client truy cập và thay đổi các tài nguyên đó. Ở đây các tài nguyên được định danh dựa vào URI, REST sử dụng một vài đại diện để biểu diễn các tài nguyên như văn bản, JSON, XML.

3.3 Công nghệ hạ tầng ảo hóa

Openstack: Là một nền tảng cloud computing mã nguồn mở được xây dựng từ nhiều thành phần phần mềm khác nhau để cung cấp các dịch vụ như Infrastructure as a Service (IaaS), Platform as a Service (PaaS) và Software as a Service (SaaS).



Hình 3.3.1: Mô hình kiến trúc của hệ thống openstack

Các thành phần bên trong Openstack:

- **Keystone**: Keystone là thành phần quản lý xác thực và phân quyền trong OpenStack. Nó quản lý các thông tin đăng nhập của người dùng, vai trò của họ và quyền truy cập đến các tài nguyên trong hệ thống.
- **Nova**: Nova là thành phần chịu trách nhiệm quản lý máy ảo (VM) trong OpenStack. Nó quản lý các chu kỳ vòng đời của VM, bao gồm khởi tạo, khởi động, dừng và xóa các VM.
- **Glance**: Glance là thành phần quản lý các hình ảnh (image) của VM. Nó cung cấp các công cụ để tạo, lưu trữ và chia sẻ các hình ảnh của VM giữa các người dùng trong hệ thống.
- **Neutron**: Neutron là thành phần quản lý mạng trong OpenStack. Nó cung cấp các dịch vụ để tạo, quản lý và kết nối các mạng ảo (Virtual Network) để cho phép các VM có thể liên lạc với nhau và với bên ngoài.
- **Cinder**: Cinder là thành phần quản lý lưu trữ (storage) trong OpenStack. Nó cung cấp các dịch vụ để tạo, quản lý và cung cấp dữ liệu cho các VM.
- **Swift**: Swift là thành phần quản lý đối tượng (object storage) trong OpenStack. Nó cung cấp các dịch vụ để lưu trữ và truy xuất các đối tượng (object) lớn như tài liệu, video, hình ảnh,...
- **Horizon**: Horizon là giao diện người dùng web (Web UI) cho OpenStack. Nó cho phép người dùng quản lý các tài nguyên trong hệ thống OpenStack bằng cách sử dụng giao diện web thân thiện.

4. Đặc tính và thông số kỹ thuật

- ✓ Hệ thống có các đặc tính và thông số kỹ thuật chính như sau:
- ✓ Hỗ trợ tổ chức huấn luyện, diễn tập, sát hạch an toàn thông tin trên môi trường giả lập.
- ✓ Hỗ trợ tổ chức diễn tập từ xa, phục vụ vận hành 24/7.
- ✓ Hỗ trợ tới 300 người tham gia diễn tập theo kịch bản đơn giản.
- ✓ Hỗ trợ tối thiểu 30 người tham gia huấn luyện trực tiếp.
- ✓ Hỗ trợ mô phỏng tối thiểu 03 lĩnh vực: Chính phủ điện tử, Đô thị thông minh và hệ thống hạ tầng quan trọng.
- ✓ Hỗ trợ tạo lập, quản lý, cấp phát và thu hồi môi trường huấn luyện trên nền tảng ảo hóa/điện toán đám mây.
- ✓ Hỗ trợ theo dõi, đánh giá kết quả huấn luyện, diễn tập và sát hạch.

Hệ thống có các phiên bản thương mại sau:

STT	Đặc tính & Thông số	Standard	Advance	Premium
1	Quy mô người dùng đồng thời	**30 – 50**	**150 - 200**	**300+**
2	Quy mô tính năng	Pilot Lab Phòng thực nghiệm	Specialization Đào tạo khoa chuyên môn	University of IT Đào tạo toàn trường về CNTT

5. Yêu cầu hạ tầng triển khai

TT	Hạng mục	Thành phần	Số lượng	Cấu hình phần cứng	Khả năng phục vụ	Lý do/Giải thích	Ghi chú
1	**Phiên bản Standard (1–2 lớp, 30–50 SV)**	Controller Node	3	CPU: Xeon 8 core RAM: 64 GB Storage: 2×500 GB SSD (RAID1) Network: 2×10 GbE	Quản lý OpenStack ổn định	Tối thiểu 3 node để HA, 8 core + 64 GB RAM đủ cho dịch vụ quản trị.	24 core; 192 GB RAM
		Compute Node	2	CPU: 32 core RAM: 256 GB Storage: 2×500 GB SSD (RAID1) Network: 2×25 GbE	~60 tài khoản đồng thời	Đủ cho 1–2 lớp 30 SV. Có thể mở rộng bằng cách bổ sung Compute node.	64 core; 512 GB RAM
		Storage Node (Ceph)	3	CPU: 8 core RAM: 64 GB OS: 2×500 GB SSD (RAID1) Journal: 1×500 GB NVMe Data: 4×8 TB HDD Network: 2×25 GbE	~28 TB usable	Ceph cluster tối thiểu (3 node) để replication 3×, đủ dung lượng cho lab và snapshot nhỏ.	24 core; 192 GB RAM
2	**Phiên bản Advance (4–6 lớp, 150–200 SV)**	Controller Node	3	CPU: Xeon 16 core RAM: 128 GB Storage: 2×1 TB SSD (RAID1) Network: 2×25 GbE	Quản lý 200+ account	CPU/RAM cao hơn để xử lý nhiều API call và orchestration.	
		Compute Node	5	CPU: 48 core RAM: 512 GB Storage: 2×1 TB SSD (RAID1) Network: 2×25 GbE	~200 tài khoản đồng thời	Phù hợp 4–6 lớp chạy song song, mỗi SV 1 account.	
		Storage Node (Ceph)	5	CPU: 16 core RAM: 128 GB OS: 2×1 TB SSD (RAID1) Journal: 2×1 TB NVMe Data: 8×12 TB HDD Network: 2×25 GbE	~144 TB usable	Đủ lưu trữ nhiều lớp học, có snapshot và backup.	
3	**Phiên bản Premium: (10+ lớp, 300+ SV)**	Controller Node	3	CPU: Xeon 32 core RAM: 256 GB Storage: 2×2 TB NVMe (RAID1) Network: 2×100 GbE	Quản lý 300+ account	Controller mạnh hơn để phục vụ quy mô toàn trường.	
		Compute Node	10	CPU: 64 core RAM: 1 TB Storage: 2×2 TB NVMe (RAID1) Network: 2×100 GbE	~400 tài khoản đồng thời	Đáp ứng 10 lớp song song (300 SV). Có thể mở rộng thêm node để phục vụ nhiều hơn.	
		Storage Node (Ceph)	7	CPU: 32 core RAM: 256 GB OS: 2×2 TB NVMe (RAID1) Journal: 4×2 TB NVMe Data: 12×18 TB HDD Network: 2×100 GbE	~450 TB usable	Ceph dung lượng lớn, IOPS cao, đủ cho toàn trường và nhiều năm sử dụng.	

6. Tính năng an toàn thông tin

Hệ thống được thiết kế và triển khai với các cơ chế bảo đảm an toàn thông tin ở mức tổng thể, đáp ứng yêu cầu bảo mật trong quá trình vận hành, huấn luyện và diễn tập. Các tính năng chính bao gồm:

6.1 Xác thực và quản lý truy cập

Hệ thống áp dụng cơ chế xác thực người dùng thông qua các chuẩn phổ biến (OpenID Connect/LDAP), đảm bảo kiểm soát truy cập đối với tất cả người dùng và dịch vụ.

6.2 Phân quyền truy cập

Thực hiện phân quyền theo vai trò (RBAC), đảm bảo người dùng chỉ được cấp quyền phù hợp với chức năng, nhiệm vụ được giao.

6.3 Bảo mật truyền thông

Toàn bộ dữ liệu trao đổi giữa các thành phần hệ thống và người dùng được bảo vệ thông qua giao thức HTTPS/TLS, đảm bảo tính bảo mật và toàn vẹn dữ liệu trong quá trình truyền tải.

6.4 Ghi log và giám sát

Hệ thống ghi nhận và lưu trữ nhật ký hoạt động của người dùng và hệ thống, phục vụ công tác giám sát, kiểm tra và điều tra khi có sự cố an toàn thông tin xảy ra.

6.5 Cô lập môi trường huấn luyện

Các môi trường giả lập phục vụ huấn luyện, diễn tập được tách biệt với hệ thống thực, đảm bảo không ảnh hưởng đến hạ tầng vận hành và giảm thiểu rủi ro lan truyền sự cố.

6.6 Sao lưu và phục hồi dữ liệu

Hệ thống hỗ trợ cơ chế sao lưu định kỳ và phục hồi dữ liệu khi cần thiết, đảm bảo tính sẵn sàng và an toàn của thông tin trong quá trình vận hành.

7. Các tính năng chính

7. 1 Quản lý mô hình mạng

Tạo và quản lý các mô hình mạng, các thiết bị ảo hóa, thiết bị ngoại vi... Người dùng với vai trò người quản trị hoặc người hướng dẫn huấn luyện có thể truy cập phần này

- **Quản lý tài nguyên mô phỏng**
  - Hệ thống cung cấp chức năng hiển thị tổng quan tài nguyên, bao gồm các thông tin như số lượng máy ảo (instances), vCPU, RAM... và các tài nguyên mạng đang sử dụng.
  - Hệ thống cho phép hiển thị thông tin chi tiết của từng image OS sử dụng trong môi trường mô phỏng, phục vụ cấu hình và triển khai sandbox.
  - Hệ thống hỗ trợ chức năng lọc danh sách image OS, bao gồm tìm kiếm theo tên và lọc theo một số thuộc tính
  - Hệ thống hỗ trợ sắp xếp danh sách image OS theo các tiêu chí hiển thị trên giao diện, thông qua chức năng sắp xếp tại các cột dữ liệu.
- **Quản lý dịch vụ hệ thống**
  - Hệ thống cho phép người dùng truy cập vào trang đăng ký dịch vụ từ trang chủ.
  - Hệ thống cung cấp biểu mẫu đăng ký dịch vụ, cho phép người dùng nhập và gửi các thông tin cần thiết để đăng ký sử dụng một dịch vụ mới. Hệ thống thực hiện kiểm tra tính hợp lệ của dữ liệu trước khi tiếp nhận và xử lý đăng ký.
  - Hệ thống cho phép người dùng lọc danh sách các dịch vụ theo các tiêu chí tìm kiếm nhằm nhanh chóng tìm kiếm dịch vụ mong muốn.
  - Hệ thống cho phép người dùng sắp xếp danh sách dịch vụ theo các tiêu chí khác nhau theo thứ tự tăng dần hoặc giảm dần.
- **Quản lý mô hình mô phỏng:** Chức năng quản lý mô hình mô phỏng cho phép người dùng tạo lập, chỉnh sửa, tổ chức và quản lý các môi trường mô phỏng (sandbox/topology) phục vụ đào tạo và diễn tập.
  - Hệ thống cho phép tạo mới mô hình mô phỏng thông qua chức năng tạo sandbox definition. Người dùng khai báo Git URL và revision để thêm mới định nghĩa môi trường mô phỏng; định nghĩa này chứa thông tin cần thiết để tạo sandbox trong hạ tầng cloud.
  - Hệ thống cung cấp giao diện liệt kê toàn bộ sandbox definitions mà giảng viên có thể sử dụng. Mỗi dòng trong bảng tương ứng một mô hình mô phỏng; người dùng có thể bấm vào tiêu đề để xem thêm thông tin liên quan.
  - Hệ thống cung cấp chức năng sắp xếp danh sách thông qua giao diện bảng dữ liệu, thể hiện qua biểu tượng mũi tên tại tiêu đề cột (ví dụ cột Title), cho phép người dùng thực hiện sắp xếp tăng/giảm theo giá trị của cột.
  - Hệ thống cho phép xóa mô hình mô phỏng thông qua thao tác xóa trên từng sandbox definition.
  - Hệ thống cho phép người dùng xem chi tiết cấu trúc topology của mô hình mô phỏng (sandbox), bao gồm các thành phần như máy ảo (VM), các nút mạng và mối liên kết giữa các thành phần trong môi trường mô phỏng. Topology thể hiện cấu trúc mạng của mô hình, cho phép giảng viên theo dõi cách các thành phần được kết nối và tổ chức trong kịch bản mô phỏng.

7. Các tính năng chính

7.1 Quản lý mô hình mạng (tiếp)

- **Quản lý môi trường mô phỏng**: Chức năng quản lý môi trường mô phỏng là tập hợp các chức năng cho phép tạo lập, triển khai, vận hành và quản lý trạng thái các môi trường mô phỏng thực thi (sandbox instances) được sinh ra từ các mô hình mô phỏng nhằm phục vụ đào tạo, diễn tập và kiểm thử.
  - Hệ thống cho phép tạo môi trường mô phỏng (sandbox instance) từ các sandbox definition đã được cấu hình. Quá trình tạo môi trường bao gồm việc cấp phát tài nguyên từ pool và khởi tạo các máy ảo theo topology đã định nghĩa.
  - Hệ thống cung cấp giao diện hiển thị danh sách các môi trường mô phỏng đã được tạo, bao gồm các thông tin như tên, trạng thái, số lượng instances, tài nguyên sử dụng (CPU, RAM, network)... cho phép người dùng theo dõi và quản lý trạng thái vận hành của các môi trường.
  - Hệ thống hỗ trợ sắp xếp danh sách môi trường mô phỏng trong giao diện bảng thông qua các cột thông tin (ví dụ cột Title)…
  - Hệ thống cho phép xóa môi trường mô phỏng (sandbox instance/pool) thông qua các thao tác quản trị, giúp giải phóng tài nguyên và đảm bảo quản lý hiệu quả các môi trường không còn sử dụng.
  - Hệ thống cho phép tải xuống cấu hình SSH của từng môi trường mô phỏng (sandbox) dưới dạng tệp nén.
  - Hệ thống cho phép khóa và mở khóa môi trường mô phỏng ở mức sandbox instance.
  - Hệ thống cho phép người dùng xem chi tiết thông tin của từng môi trường mô phỏng (sandbox instance), bao gồm các thông tin như tên môi trường, trạng thái (locked/unlocked), số lượng instances, mức sử dụng tài nguyên (CPU, RAM, network) và các thông tin liên quan đến sandbox definition.
  - Chức năng này được thể hiện thông qua giao diện quản lý pool và danh sách sandbox instances, cho phép theo dõi trạng thái và cấu hình của từng môi trường cụ thể.
  - Hệ thống cho phép người dùng bố trí một tài nguyên hoặc nhiều tài nguyên cho môi trường mô phỏng.
  - Hệ thống cho phép người dùng xóa bỏ tài nguyên đã bố trí cho môi trường mô phỏng.
  - Hệ thống hỗ trợ hiển thị topology mạng của sandbox.
  - Hệ thống cho phép tải xuống cấu hình SSH của môi trường mô phỏng (sandbox instance).
  - Hệ thống có hỗ trợ chức năng khóa/mở khóa (Lock/Unlock) đối với môi trường mô phỏng (sandbox instance), cho phép kiểm soát trạng thái sử dụng của môi trường.
- **Quản lý các thiết bị ảo hóa:** Quản lý toàn bộ các imgae ảo hóa của hệ thống.
  - Thiết bị an ninh: Là các loại thiết bị đảm bảo an ninh an toàn không gian mạng.
  - Thiết bị ứng dụng: Là các loại thiết bị lớp ứng dụng và lớp mạng.
- **Quản lý các thiết bị ngoại vi.**

7.2 Quản lý bộ tạo tình huống

Bộ tạo kịch bản có khả năng tạo ra các cuộc tấn công tự động để đánh giá các mô hình thực tế hoặc tạo tình huống trong các kịch bản tấn công phòng thủ mạng. Các kịch bản tấn công được cập nhật thường xuyên với các hình thức và mã khai thác mới nhất với các thiết bị mạng thiết bị đầu cuối. Bộ tạo tấn công dựa trên AI cho phép tạo hình thức tấn công thông minh, sát với thực tế...

Bộ tạo tấn công cung cấp khả năng cấu hình đáp ứng toàn diện với hệ thống trong thao trường mạng như sau:

- Thay đổi địa chỉ IP.
- Thay đổi thời lượng, thời gian tấn công.
- Thay đổi cách thức tấn công.

7. Các tính năng chính

7.3 Quản lý bộ tạo lưu lượng/tấn công

Bộ tạo lưu lượng/tấn công mạng cho phép tạo ra các lưu lượng mạng giả lập, phục vụ tạo cuộc tấn công DDoS, đánh giá hoạt động của các thiết bị, mô hình, công cụ phân tích hay kiểm định mức chịu tải của thiết bị, hệ thống. Cho phép tạo các loại lưu lượng phong phú, mức độ tuỳ biến cao.

Bộ tạo lưu lượng mạng cung cấp khả năng cấu hình đáp ứng toàn diện với hệ thống trong thao trường mạng như sau:

- Nguồn và đích của lưu lượng được tạo.
- Loại lưu lượng và giao thức của lưu lượng được tạo.
- Thời lượng lưu lượng được tạo.

7.4 Quản lý các bài huấn luyện

Phân hệ này sẽ hỗ trợ người hướng dẫn xây dựng các nội dung bài huấn luyện, tạo, quản lý các phiên đào tạo và hỗ trợ người tham gia huấn luyện có thể tham gia thực hiện các bài huấn luyện.

- Quản lý các nhóm bài huấn luyện: Tạo các nhóm bài huấn luyện và nhóm các nội dung bài huấn luyện đơn lẻ.
- Quản lý nội dung bài huấn luyện: Hỗ trợ các giao diện để xây dựng nội dung bài huấn luyện và pha huấn luyện.
- Quản lý thông tin bài huấn luyện: Mô tả về bài huấn luyện.
- Quản lý các pha huấn luyện: Tạo ra các loại bài huấn luyện. Ở đây chia thành 3 loại: Training phase, Info phase, Assessment phase.
- Quản lý các bài thi huấn luyện.
- Tạo phiên đào tạo: Người hướng dẫn có thể tạo phiên đào tạo, đặt lịch trình cho bài huấn luyện, gán hệ thống phỏng và gán lưu lượng tấn công vào bài huấn luyện.
- Quản lý quá trình đào tạo: Người hướng dẫn có thể xem kết quả huấn luyện và theo dõi kết quả trong quá trình thực hành.
- Thực hiện bài huấn luyện: Người được huấn luyện có thể tham gia vào quá trình đào tạo theo nội dung kịch bản đã đề ra và có thể xem thông tin kết quả đã thực hiện, quay lại các bài đã từng tham gia.
- Đánh giá năng lực người tham gia huấn luyện: Đối với người mới tham gia vào Cyber Range, thì hệ thống cung cấp các câu hỏi nhanh để phân loại người chơi theo mức độ hoặc dạng bài.
- Chatbox: Module này hỗ trợ người hướng dẫn và người tham gia có thể tương tác với nhau trong quá trình thực hiện bài diễn tập.
- Quản lý tài liệu huấn luyện: Xem và lưu trữ thông tin về các tài liệu hướng dẫn cho người huấn luyện.

a) Quản lý kịch bản huấn luyện

- **Quản lý kịch bản huấn luyện tuần tự**
  - Hệ thống cho phép giảng viên xem danh sách các kịch bản huấn luyện tuần tự. Hệ thống iệt kê toàn bộ các kịch bản mà giảng viên được quyền truy cập và mỗi dòng trong bảng tương ứng một kịch bản huấn luyện; người dùng có thể bấm vào tên kịch bản để xem chi tiết.
  - Hệ thống cung cấp chức năng sắp xếp danh sách kịch bản huấn luyện tuần tự thông qua giao diện bảng dữ liệu, thể hiện bằng biểu tượng mũi tên tại tiêu đề cột
  - Hệ thống cung cấp chức năng lọc danh sách kịch bản huấn luyện tuần tự thông qua ô tìm kiếm trên giao diện quản lý. Chức năng này cho phép người dùng nhập tên kịch bản để rút gọn danh sách hiển thị theo tiêu chí tên, đáp ứng yêu cầu lọc danh sách theo tên kịch bản.
  - Hệ thống cho phép giảng viên tạo mới kịch bản huấn luyện tuần tự. Khi tạo mới, người dùng có thể khai báo các thông tin cơ bản như tên kịch bản, mô tả và cấu hình nội dung huấn luyện. Hệ thống hỗ trợ xây dựng kịch bản theo từng bước (levels), cho phép thêm, xóa, chỉnh sửa và sắp xếp thứ tự các giai đoạn, đảm bảo đúng mô hình huấn luyện tuần tự nhiều bước theo yêu cầu.

7. Các tính năng chính

7.4 Quản lý các bài huấn luyện (tiếp)

a) Quản lý kịch bản huấn luyện (tiếp)

- **Quản lý kịch bản huấn luyện tuần tự (tiếp)**
  - Hệ thống cho phép tạo kịch bản huấn luyện tuần tự thông qua việc tải lên (Upload) file JSON. Tệp JSON chứa cấu hình đầy đủ của kịch bản huấn luyện, bao gồm các bước (levels), nội dung và luồng thực hiện, và có thể được sử dụng để tái sử dụng kịch bản đã xây dựng trước đó.
  - Hệ thống cho phép giảng viên tạo và cấu hình các giai đoạn huấn luyện (level) trong kịch bản huấn luyện tuần tự. Mỗi giai đoạn có thể khai báo đầy đủ các thông tin như: tên giai đoạn, thời gian dự kiến hoàn thành, điểm số, giới hạn số lần trả lời sai, đáp án (secret answer), nội dung lời giải, gợi ý và danh sách lệnh yêu cầu. Hệ thống hỗ trợ tham chiếu tới ma trận MITRE ATT&CK thông qua việc gán các kỹ thuật tương ứng cho từng giai đoạn huấn luyện
  - Hệ thống cho phép giảng viên tạo mới giai đoạn huấn luyện với kiểu truy cập (Access Level). Giai đoạn này cung cấp thông tin truy cập môi trường và yêu cầu người học nhập passkey (mật mã) để chuyển sang bước tiếp theo.
  - Hệ thống cho phép tạo giai đoạn huấn luyện với kiểu đánh giá (Assessment Level), hỗ trợ xây dựng câu hỏi và đáp án để đánh giá người học. Mỗi loại câu hỏi có form cấu hình riêng, cho phép triển khai các bài kiểm tra trong kịch bản huấn luyện.
  - Hệ thống cho phép tạo giai đoạn huấn luyện với kiểu mức độ thông tin (Info Level), dùng để cung cấp nội dung thông tin, hướng dẫn hoặc mô tả cho người học.
  - Hệ thống cho phép giảng viên xóa giai đoạn huấn luyện (level) đã tạo trong kịch bản huấn luyện tuần tự. Người dùng có thể lựa chọn một hoặc nhiều level và thực hiện thao tác xóa khỏi kịch bản. Chức năng này đáp ứng yêu cầu quản lý và chỉnh sửa cấu trúc kịch bản huấn luyện.
  - Hệ thống cho phép giảng viên chỉnh sửa nội dung kịch bản huấn luyện tuần tự đã tạo. Người dùng có thể cập nhật các thông tin của kịch bản như tên, mô tả, cũng như chỉnh sửa nội dung chi tiết của từng giai đoạn (level), bao gồm nội dung bài học (Content), đáp án (Secret Answer), lời giải (Solution), gợi ý (Hints), và các cấu hình liên quan.Hệ thống hỗ trợ sắp xếp lại thứ tự các giai đoạn và cập nhật các thuộc tính như điểm số, thời gian dự kiến và kỹ thuật MITRE ATT&CK tương ứng, đảm bảo khả năng điều chỉnh toàn bộ nội dung kịch bản huấn luyện theo yêu cầu.
  - Hệ thống cho phép giảng viên tạo mới kịch bản huấn luyện tuần tự từ một kịch bản đã có. Người dùng có thể sao chép toàn bộ cấu hình của kịch bản, bao gồm các giai đoạn (levels), nội dung, cấu hình chấm điểm và các thiết lập liên quan, để tạo thành một kịch bản mới phục vụ mục đích chỉnh sửa hoặc tái sử dụng. Chức năng này đáp ứng yêu cầu tái sử dụng và mở rộng các kịch bản huấn luyện hiện có.
  - Hệ thống cho phép giảng viên xóa kịch bản huấn luyện tuần tự đã tạo. Người dùng có thể thực hiện thao tác xóa trực tiếp trên từng kịch bản trong danh sách, phục vụ việc quản lý và loại bỏ các kịch bản không còn sử dụng. Chức năng này đáp ứng yêu cầu quản lý vòng đời kịch bản huấn luyện.
  - Hệ thống cho phép giảng viên tải xuống kịch bản huấn luyện tuần tự. Kịch bản được xuất ra dưới dạng tệp JSON, bao gồm toàn bộ cấu hình của training definition như các giai đoạn (levels), nội dung, cấu hình chấm điểm và các thiết lập liên quan. Chức năng này hỗ trợ việc lưu trữ, sao lưu và tái sử dụng kịch bản huấn luyện.
  - Hệ thống cho phép giảng viên xem trước nội dung tổng thể của kịch bản huấn luyện tuần tự thông qua chức năng. Chức năng này cho phép hiển thị toàn bộ cấu trúc kịch bản, bao gồm danh sách các giai đoạn (levels) và nội dung chi tiết của từng bước, giúp giảng viên kiểm tra và đánh giá kịch bản trước khi đưa vào sử dụng. Chức năng này đáp ứng yêu cầu xem trước nội dung tổng thể của kịch bản huấn luyện.
  - Hệ thống cho phép giảng viên quản lý trạng thái kịch bản huấn luyện tuần tự thông qua các chức năng Release / Unrelease và Archive. Các chức năng này đáp ứng yêu cầu xuất bản và kiểm soát trạng thái sử dụng (khóa) của kịch bản huấn luyện.
    - ✓ **Release**: Xuất bản kịch bản để có thể sử dụng trong các phiên huấn luyện (training run).
    - ✓ **Unrelease**: Thu hồi trạng thái xuất bản khi cần chỉnh sửa hoặc tạm ngừng sử dụng.
    - ✓ **Archive**: Khóa/lưu trữ kịch bản, không cho phép sử dụng trong huấn luyện nhưng vẫn giữ lại để quản lý.
  - Hệ thống cung cấp giao diện danh sách kịch bản huấn luyện với đầy đủ các thông tin gồm tên kịch bản, trạng thái, thời lượng dự kiến, thời gian chỉnh sửa lần cuối và người chỉnh sửa cuối. Các thông tin được hiển thị trực quan trong bảng dữ liệu, đáp ứng yêu cầu xem thông tin kịch bản huấn luyện.
  - Hệ thống hỗ trợ Ma trận Kỹ thuật MITRE ATT&CK, cho phép giảng viên truy cập và tham chiếu các kỹ thuật MITRE ATT&CK gắn với từng giai đoạn huấn luyện.

7. Các tính năng chính

7.4 Quản lý các bài huấn luyện (tiếp)

a) Quản lý kịch bản huấn luyện (tiếp)

- **Quản lý kịch bản huấn luyện linh hoạt:** Chức năng quản lý kịch bản huấn luyện linh hoạt là tập hợp các chức năng cho phép giảng viên tạo, cấu hình, chỉnh sửa, theo dõi và tổ chức các kịch bản huấn luyện theo dạng linh hoạt (adaptive), trong đó nội dung và luồng huấn luyện có thể thay đổi tùy theo hành vi hoặc kết quả của người học.
  - Hệ thống cung cấp giao diện danh sách kịch bản huấn luyện linh hoạt (Adaptive Training Definition) với các thông tin như tên kịch bản, trạng thái, thời gian sửa đổi và người chỉnh sửa cuối, cho phép người dùng lựa chọn để truy cập chi tiết kịch bản.
  - Hệ thống hỗ trợ sắp xếp danh sách kịch bản huấn luyện linh hoạt thông qua giao diện bảng dữ liệu, thể hiện bằng biểu tượng mũi tên tại tiêu đề cột (ví dụ cột Title), cho phép người dùng sắp xếp theo giá trị của từng cột, đáp ứng yêu cầu sắp xếp dữ liệu.
  - Hệ thống cung cấp chức năng lọc/tìm kiếm danh sách kịch bản huấn luyện linh hoạt thông qua trường "Filter by title", cho phép người dùng lọc theo tên kịch bản, đáp ứng yêu cầu lọc dữ liệu.
  - Hệ thống cho phép giảng viên tạo mới kịch bản huấn luyện linh hoạt (Adaptive Training Definition), bao gồm khai báo các thông tin như tên kịch bản và mô tả, đồng thời cho phép xây dựng cấu trúc huấn luyện thông qua việc thêm các giai đoạn (phases) theo mô hình linh hoạt.
  - Hệ thống cho phép giảng viên tạo mới các giai đoạn huấn luyện (phase) trong kịch bản huấn luyện linh hoạt (Adaptive Training Definition), bao gồm các loại phase như Training, Questionnaire, Info và Access, phục vụ việc xây dựng luồng huấn luyện thích ứng theo hành vi và kết quả của người học. Hệ thống hỗ trợ tham chiếu tới ma trận MITRE ATT&CK thông qua việc gán các kỹ thuật tương ứng cho từng giai đoạn huấn luyện
  - Hệ thống cho phép giảng viên thêm câu hỏi cho các giai đoạn huấn luyện trong kịch bản huấn luyện linh hoạt thông qua Questionnaire Phase, hỗ trợ xây dựng nội dung đánh giá dưới dạng các câu hỏi nhằm phục vụ việc thu thập thông tin và đánh giá người học trong quá trình huấn luyện.
  - Hệ thống cho phép giảng viên tạo mới giai đoạn huấn luyện với kiểu Info Phase trong kịch bản huấn luyện linh hoạt (Adaptive Training Definition). Tại giai đoạn này, giảng viên có thể khai báo tên giai đoạn và nội dung thông tin để hiển thị cho người học trong quá trình huấn luyện.
  - Hệ thống cho phép giảng viên tạo mới giai đoạn huấn luyện với kiểu câu hỏi tổng quát (Questionnaire Phase) trong kịch bản huấn luyện linh hoạt (Adaptive Training Definition). Tại giai đoạn này, giảng viên có thể khai báo tên giai đoạn, thời gian dự kiến và thêm mới các câu hỏi với nhiều hình thức trả lời như câu hỏi tự do (free-form), câu hỏi trắc nghiệm (multiple choice) và câu hỏi đánh giá (rating), phục vụ việc thu thập thông tin và đánh giá người học trong quá trình huấn luyện.
  - Hệ thống cho phép giảng viên tạo mới giai đoạn huấn luyện với kiểu câu hỏi linh hoạt trong kịch bản huấn luyện linh hoạt (Adaptive Training Definition). Tại giai đoạn này, giảng viên có thể khai báo tên giai đoạn, thời gian dự kiến và thêm mới các câu hỏi với nhiều hình thức trả lời như câu hỏi tự do, nhiều đáp án, kết hợp.
  - Hệ thống cho phép giảng viên tạo mới giai đoạn huấn luyện với kiểu truy cập (Access Level). Giai đoạn này cung cấp thông tin truy cập môi trường và yêu cầu người học nhập passkey (mật mã) để chuyển sang bước tiếp theo.
  - Hệ thống cho phép giảng viên xóa giai đoạn huấn luyện (phase) đã tạo trong kịch bản huấn luyện linh hoạt.
  - Hệ thống cho phép giảng viên chỉnh sửa nội dung kịch bản huấn luyện linh hoạt đã tạo. Người dùng có thể cập nhật các thông tin của kịch bản như tên, mô tả, cũng như chỉnh sửa nội dung chi tiết của từng giai đoạn (phase).
  - Hệ thống cho phép tạo kịch bản huấn luyện linh hoạt thông qua việc tải lên (Upload) file JSON. Tệp JSON chứa cấu hình đầy đủ của kịch bản huấn luyện và có thể được sử dụng để tái sử dụng kịch bản đã xây dựng trước đó.
  - Hệ thống cho phép giảng viên tạo mới kịch bản huấn luyện linh hoạt từ một kịch bản đã có. Người dùng có thể sao chép toàn bộ cấu hình của kịch bản để tạo thành một kịch bản mới phục vụ mục đích chỉnh sửa hoặc tái sử dụng.
  - Hệ thống cho phép giảng viên xóa kịch bản huấn luyện linh hoạt đã tạo. Người dùng có thể thực hiện thao tác xóa trực tiếp trên từng kịch bản trong danh sách, phục vụ việc quản lý và loại bỏ các kịch bản không còn sử dụng.
  - Hệ thống cho phép giảng viên tải xuống kịch bản huấn luyện linh hoạt. Kịch bản được xuất ra dưới dạng tệp JSON, bao gồm toàn bộ cấu hình của kịch bản.

7. Các tính năng chính

7.4 Quản lý các bài huấn luyện *(tiếp)*

a) Quản lý kịch bản huấn luyện (tiếp)

- **Quản lý kịch bản huấn luyện linh hoạt (tiếp):** Chức năng quản lý kịch bản huấn luyện linh hoạt là tập hợp các chức năng cho phép giảng viên tạo, cấu hình, chỉnh sửa, theo dõi và tổ chức các kịch bản huấn luyện theo dạng linh hoạt (adaptive), trong đó nội dung và luồng huấn luyện có thể thay đổi tùy theo hành vi hoặc kết quả của người học.
  - Hệ thống cho phép giảng viên xem trước nội dung tổng thể của kịch bản huấn luyện linh hoạt. Chức năng này cho phép hiển thị toàn bộ cấu trúc kịch bản, bao gồm danh sách các giai đoạn (phase) và nội dung chi tiết của từng bước, giúp giảng viên kiểm tra và đánh giá kịch bản trước khi đưa vào sử dụng.
  - Hệ thống cho phép giảng viên quản lý trạng thái kịch bản huấn luyện linh hoạt:
    - ✓ **Release**: Xuất bản kịch bản để có thể sử dụng trong các phiên huấn luyện (training run).
    - ✓ **Unrelease**: Thu hồi trạng thái xuất bản khi cần chỉnh sửa hoặc tạm ngừng sử dụng.
    - ✓ **Archive**: Khóa/lưu trữ kịch bản, không cho phép sử dụng trong huấn luyện nhưng vẫn giữ lại để quản lý.
  - Hệ thống cung cấp giao diện danh sách kịch bản huấn luyện linh hoạt với đầy đủ các thông tin gồm tên kịch bản, trạng thái, thời lượng dự kiến, thời gian chỉnh sửa lần cuối và người chỉnh sửa cuối. Các thông tin được hiển thị trực quan trong bảng dữ liệu, đáp ứng yêu cầu xem thông tin kịch bản huấn luyện.
  - Hệ thống hỗ trợ Ma trận Kỹ thuật MITRE ATT&CK, cho phép giảng viên truy cập và tham chiếu các kỹ thuật MITRE ATT&CK gắn với từng giai đoạn huấn luyện.

b) Quản lý chương trình đào tạo

- **Quản lý chương trình đào tạo tuần tự:** Chức năng quản lý chương trình đào tạo tuần tự là chức năng cho phép tạo, chỉnh sửa, cấu hình và quản lý các kịch bản huấn luyện tuần tự (Linear Training), bao gồm việc xây dựng các giai đoạn huấn luyện và luồng thực hiện theo trình tự xác định.
  - Hệ thống cho phép giảng viên xem danh sách các kịch bản huấn luyện tuần tự (Linear Training Definition) dưới dạng bảng dữ liệu.
  - Hệ thống hỗ trợ sắp xếp danh sách kịch bản huấn luyện tuần tự thông qua giao diện bảng dữ liệu, thể hiện bằng biểu tượng mũi tên tại tiêu đề các cột, cho phép người dùng sắp xếp tăng/giảm theo giá trị của từng cột hiển thị.
  - Hệ thống cung cấp chức năng lọc danh sách kịch bản huấn luyện tuần tự, cho phép người dùng tìm kiếm và rút gọn danh sách theo tên kịch bản, đáp ứng yêu cầu lọc dữ liệu cơ bản.
  - Hệ thống cho phép giảng viên tạo mới kịch bản huấn luyện tuần tự (Linear Training Definition), bao gồm khai báo tên kịch bản và cấu hình các giai đoạn huấn luyện (level) theo trình tự xác định, đáp ứng yêu cầu xây dựng nội dung đào tạo tuần tự.
  - Hệ thống cho phép giảng viên chỉnh sửa kịch bản huấn luyện tuần tự (Linear Training Definition), bao gồm cập nhật nội dung, cấu hình các giai đoạn (level) và thông tin liên quan trong kịch bản huấn luyện.
  - Hệ thống cho phép giảng viên copy token của chương trình đào tạo tuần tự
  - Hệ thống cho phép giảng viên xóa kịch bản huấn luyện tuần tự (Linear Training Definition) thông qua chức năng xóa trên giao diện quản lý danh sách kịch bản.
  - Hệ thống cho phép giảng viên tải xuống kịch bản huấn luyện tuần tự dưới dạng tệp cấu hình (JSON), phục vụ việc sao lưu và tái sử dụng kịch bản.
  - Hệ thống cho phép giảng viên tải xuống cấu hình SSH của chương trình đào tạo tuần tự
  - Hệ thống cho phép xem danh sách người tham gia huấn luyện thông qua giao diện Training Runs, hiển thị các thông tin như người tham gia (Player), thời gian bắt đầu, thời gian kết thúc, trạng thái thực hiện, thời lượng, email và thông tin ghi log.
  - Hệ thống cho phép xóa từng bản ghi huấn luyện của người tham gia thông qua biểu tượng xóa tại từng dòng trong danh sách Training Runs. Về bản chất, thao tác này tương ứng với việc xóa kết quả/phiên thực thi huấn luyện của một sinh viên cụ thể trong danh sách.

7. Các tính năng chính

7.4 Quản lý các bài huấn luyện *(tiếp)*

b) Quản lý chương trình đào tạo (tiếp)

- **Quản lý chương trình đào tạo tuần tự (tiếp):** Chức năng quản lý chương trình đào tạo tuần tự là chức năng cho phép tạo, chỉnh sửa, cấu hình và quản lý các kịch bản huấn luyện tuần tự (Linear Training), bao gồm việc xây dựng các giai đoạn huấn luyện và luồng thực hiện theo trình tự xác định.
    - Hệ thống cung cấp chức năng hiển thị Access Token của phiên huấn luyện (Training Instance) thông qua giao diện riêng ("Display Token"), cho phép người dùng dễ dàng sao chép và sử dụng để truy cập huấn luyện.
    - Hệ thống cho phép giảng viên xem thông tin chi tiết của phiên huấn luyện tuần tự thông qua các module Training Instance và Visualization, bao gồm trạng thái, thời gian bắt đầu/kết thúc, tiến độ thực hiện, kết quả huấn luyện và danh sách người tham gia. Ngoài ra, hệ thống hỗ trợ các chức năng liên quan như hiển thị access token, phát hiện gian lận và xuất dữ liệu kết quả.
- **Quản lý chương trình đào tạo linh hoạt:** Chức năng quản lý chương trình đào tạo linh hoạt là chức năng cho phép tạo, chỉnh sửa, cấu hình và quản lý các chương trình đào tạo linh hoạt (Adaptive Training), bao gồm việc thiết lập nội dung và điều kiện thực hiện trong quá trình đào tạo.
    - Hệ thống cung cấp giao diện danh sách các kịch bản huấn luyện linh hoạt (Adaptive Training Definitions) dưới dạng bảng dữ liệu, hiển thị các thông tin như tên kịch bản (Title), trạng thái (State), thời gian tạo (Created At), thời gian chỉnh sửa gần nhất (Last Edit) và người chỉnh sửa cuối (Last Edit By), đáp ứng yêu cầu xem danh sách chương trình đào tạo linh hoạt.
    - Hệ thống hỗ trợ sắp xếp danh sách kịch bản huấn luyện linh hoạt thông qua các cột hiển thị trong bảng, cho phép người dùng thay đổi thứ tự hiển thị theo tiêu chí mong muốn.
    - Hệ thống hỗ trợ chức năng lọc danh sách kịch bản huấn luyện linh hoạt thông qua trường tìm kiếm, cho phép người dùng nhanh chóng tra cứu và thu hẹp danh sách theo tên kịch bản.
    - Hệ thống cho phép giảng viên tạo mới kịch bản huấn luyện linh hoạt, bao gồm việc khai báo tên kịch bản và xây dựng nội dung huấn luyện theo các giai đoạn (phase) sau khi tạo.
    - Hệ thống cho phép giảng viên chỉnh sửa kịch bản huấn luyện linh hoạt, bao gồm cập nhật nội dung, cấu trúc các phase và thông tin liên quan của kịch bản đã tạo.
    - Hệ thống cho phép giảng viên copy token của chương trình đào tạo tuần tự
    - Hệ thống cho phép giảng viên xóa kịch bản huấn luyện linh hoạt thông qua chức năng xóa trong danh sách chương trình đào tạo linh hoạt.
    - Hệ thống hỗ trợ tải xuống (export) kịch bản huấn luyện linh hoạt dưới dạng tệp cấu hình (JSON), phục vụ mục đích lưu trữ hoặc tái sử dụng thông qua chức năng xuất dữ liệu trong Adaptive Training Definition.
    - Hệ thống cho phép giảng viên tải xuống cấu hình SSH của chương trình đào tạo linh hoạt
    - Hệ thống cho phép giảng viên xem danh sách người tham gia huấn luyện. Các thông tin hiển thị bao gồm người tham gia, trạng thái thực hiện, thời gian và thông tin liên quan đến phiên huấn luyện.
    - Hệ thống cho phép giảng viên xóa bản ghi huấn luyện (Training Run) của từng người tham gia trong Training Instance Detail thông qua thao tác xóa tương ứng với từng người dùng.
    - Hệ thống cung cấp chức năng hiển thị và sao chép access token của phiên huấn luyện, cho phép người dùng sử dụng token để truy cập phiên huấn luyện.
    - Hệ thống cho phép giảng viên xem thông tin chi tiết của phiên huấn luyện linh hoạt, bao gồm thông tin về trạng thái, thời gian thực hiện, danh sách người tham gia và các thông tin liên quan.

7. Các tính năng chính

7.4 Quản lý các bài huấn luyện *(tiếp)*

c) Hiển thị kết quả của chương trình đào tạo

- Hệ thống cho phép giảng viên theo dõi tiến độ tổng thể của chương trình đào tạo thông qua các giao diện và các biểu đồ trực quan hóa (Visualization). Các thông tin hiển thị bao gồm trạng thái thực hiện, thời gian, kết quả tổng thể và tình trạng của các phiên huấn luyện.
- Hệ thống cho phép giảng viên theo dõi tiến trình chi tiết của người tham gia thông qua giao diện Training Runs và các màn hình chi tiết của phiên huấn luyện, bao gồm trạng thái thực hiện, thời gian, kết quả và các thông tin liên quan đến quá trình huấn luyện của người dùng.
- Hệ thống cho phép phân tích câu lệnh, thể hiện trực quan, cung cấp các lệnh được sắp xếp theo thời gian của người dùng đã chọn, bao gồm chi tiết về cách sử dụng và thời điểm lệnh được thực thi.
- Hệ thống cho phép hiển thị tổng quan kết quả chương trình đào tạo của người dùng tham gia chương trình bằng các biểu đồ trực quan.
- Hệ thống hỗ trợ hiển thị số liệu thống kê các cấu trả lời ở mức độ đánh giá.
- Hệ thống hỗ trợ hiển thì các biểu đồ kết quả tổng hợp của toàn bộ người dùng tham gia các chương trình đào tạo có cùng mô hình huấn luyện.
- Hệ thống hỗ trợ hiển thị biểu đồ biểu thị kết quả diễn biến của một câu hỏi với hình ảnh trực quan cung cấp tổng quan nhanh về tỷ lệ thành công của mỗi người dùng trong từng câu hỏi. Mỗi biểu đồ tương ứng với một người dùng có ID được hiển thị ở phía bên trái.
- Hệ thống cho phép hiển thị danh sách các gian lận được phát hiện trong chương trình huấn luyện.
- Hệ thống cho phép tạo các tính năng phát hiện gian lận của người tham gia huấn luyện dựa trên câu trả lời tương tự, vị trí tương tự, thời gian tương tự, thời gian trả lời rất nhanh, không câu lệnh.

7.5 Quản lý người tham gia huấn luyện

a) Quản lý VPN truy cập

- Tạo kênh truyền VPN để học viên truy cập hệ thống, mã hóa quá trình học tập.
- Phân quyền người tham gia vào các vùng mạng.
- Xác thực tài khoản truy cập hệ thống: Sử dụng openid connect để xác thực các tài khoản của các học viên.

b) Quản lý tài khoản

- Hệ thống hỗ trợ chức năng đăng nhập với nhiều phương thức xác thực (Local, Google, Microsoft, Facebook…) và điều hướng người dùng tới Dashboard sau khi xác thực thành công.
- Hệ thống cung cấp chức năng đăng xuất tại menu người dùng, có cơ chế xác nhận (confirm) trước khi thực hiện và điều hướng về trang đăng nhập sau khi đăng xuất.
- Hệ thống hỗ trợ chức năng import nhiều tài khoản người dùng từ file nhập bên ngoài với cấu trúc định sẵn thông qua chức năng “Import users”. Tài liệu chính thức mô tả việc lựa chọn file và cấu trúc dữ liệu chứa danh sách người dùng.
- Hệ thống cho phép xem chi tiết thông tin tài khoản người dùng bao gồm tên người dùng, email và số lượng role được gán. Đồng thời hiển thị danh sách các role và microservice tương ứng, cho phép mở rộng để xem mô tả của từng role. Hệ thống sử dụng cơ chế phân quyền theo role (vai trò - RBAC).
- Hệ thống hỗ trợ tải xuống tệp YAML chứa thông tin xác thực (login và password) của các người dùng được tạo trong local OIDC provider.
- Hệ thống hỗ trợ chức năng xóa một tài khoản người dùng trực tiếp tại giao diện quản lý Users thông qua thao tác xóa tương ứng với từng tài khoản.
- Hệ thống hỗ trợ chức năng xóa nhiều tài khoản người dùng đồng thời thông qua cơ chế chọn nhiều người dùng bằng checkbox và thực hiện thao tác xóa hàng loạt trên giao diện quản lý Users.
- Hệ thống hỗ trợ chức năng lọc và tìm kiếm tài khoản người dùng thông qua thanh tìm kiếm (search bar), cho phép quản trị viên tìm kiếm nhanh người dùng theo thông tin như tên đăng nhập hoặc email.
- Hệ thống hỗ trợ sắp xếp danh sách tài khoản theo các tiêu chí hiển thị trên giao diện, thông qua chức năng sắp xếp tại các cột dữ liệu.

7. Các tính năng chính

7.5 Quản lý người tham gia huấn luyện (tiếp)

c) Quản lý và phân quyền nhóm tài khoản

- Hệ thống hỗ trợ tạo nhóm người dùng mới trong module quản lý Groups, cho phép quản trị viên tổ chức người dùng theo từng nhóm phục vụ quản lý và phân quyền.
- Hệ thống cho phép thêm người dùng vào nhóm thông qua chức năng quản lý Groups, hỗ trợ gán thành viên vào từng nhóm để phục vụ quản lý và phân quyền.
- Hệ thống cho phép gán người dùng vào nhiều nhóm khác nhau, có thể thêm người dùng vào nhóm mới.
- Hệ thống hỗ trợ cơ chế phân quyền theo role (RBAC), cho phép gán vai trò nhằm kiểm soát quyền truy cập và chức năng của người dùng và nhóm trong hệ thống.
- Hệ thống cho phép xem thông tin chi tiết của nhóm bao gồm tên nhóm và danh sách thành viên. Đồng thời hiển thị các role được gán phục vụ phân quyền.
- Hệ thống hỗ trợ sắp xếp danh sách tài khoản trong nhóm.
- Hệ thống hỗ trợ sắp xếp danh sách quyền dưới dạng các role trong nhóm theo tên.
- Hệ thống cho phép lọc và tìm kiếm danh sách nhóm theo một hoặc nhiều tiêu chí nhằm xác định và tra cứu một nhóm cụ thể.
- Hệ thống hiển thị danh sách thành viên trong nhóm và cho phép quản trị viên theo dõi, tìm kiếm và quản lý.
- Hệ thống hỗ trợ chức năng lọc danh sách quyền (role) trong nhóm thông qua trường “Filter by role type", cho phép quản trị viên tìm kiếm và lọc các role được gán trong nhóm theo từng loại cụ thể.
- Hệ thống hỗ trợ sắp xếp danh sách nhóm.
- Hệ thống hỗ trợ chức năng cho phép quản trị viên thực hiện thao tác xóa đối với từng nhóm.
- Hệ thống hỗ trợ chức năng cho phép quản trị viên thực hiện thao tác xóa đối với nhiều nhóm cùng lúc.

d) Thống kê tài khoản

- Hệ thống hỗ trợ hiển thị thống kê nhóm theo thông tin cơ bản của nhóm như tên nhóm, mô tả nhóm, chức năng cho phép chỉnh sửa nhóm, xóa nhóm.
- Hệ thống hỗ trợ hiển thị thống kê tài khoản trong hệ thống theo các thông tin cơ bản của người dùng.

e) Tham gia chương trình đào tạo

- Hệ thống hỗ trợ quản lý phiên đào tạo của người tham gia huấn luyện. Người dùng có thể xem danh sách các phiên đào tạo đã tham gia, bao gồm các phiên chưa hoàn thành và kết quả các phiên đã hoàn thành.
- Người dùng có thể nhấn nút "Tiếp tục" để tham gia tiếp phiên đào tạo (chương trình đào tạo) chưa hoàn thành.
- Hệ thống cho phép người dùng nhập token để xác thực quyền được tham gia một chương trình đào tạo cụ thể.
- Hệ thống cho phép người dùng xem chương trình đào tạo mức độ thông tin.
- Hệ thống cho phép người dùng tham gia chương trình đào tạo các mức độ đánh giá, truy cập, đào tạo, câu hỏi tổng quát và câu hỏi linh hoạt. Hệ thống hiển thị các thông tin tên tài khoản, thời gian đã làm bài, mô hình mạng, ô submit đáp án và các gợi ý. Hệ thống cho phép người dùng kết nối đến máy ảo đào tạo qua console hoặc Giao diện đồ họa người dùng.
- Hệ thống cho phép người dùng xem gợi ý cho câu hỏi; xem kết quả của câu hỏi.
- Thao tác với máy ảo:
    - Hệ thống cho phép người dùng truy cập giao diện dòng lệnh thông qua các cơ chế truy cập trong sandbox, bao gồm kết nối SSH hoặc mở terminal trực tiếp từ các thiết bị trong mô hình (server, router, client), đáp ứng yêu cầu thao tác dòng lệnh.
    - Hệ thống hỗ trợ người dùng truy cập máy ảo thông qua các giao thức kết nối từ xa như SSH trong môi trường sandbox, cho phép thực hiện thao tác quản trị và khai thác trên các thiết bị ảo, đáp ứng yêu cầu truy cập từ xa.

7. Các tính năng chính

7.5 Quản lý người tham gia huấn luyện (tiếp)

e) Tham gia chương trình đào tạo (tiếp)

- Thao tác với máy ảo (tiếp):
  - Hệ thống cho phép người dùng mở giao diện đồ họa (GUI) của máy ảo thông qua chức năng "Open GUI" từ sơ đồ topology của môi trường mô phỏng, hỗ trợ thao tác trực quan trên các thiết bị như server, client, đáp ứng yêu cầu truy cập giao diện đồ họa.
  - Hệ thống cho phép sao chép thông tin máy ảo vào clipboard, bao gồm các thông tin tên host, địa chỉ IP, MAC Address.
- Quản lý kết quả đào tạo: Hệ thống cho phép người dùng xem thông tin kết quả đào tạo.

7.6 Giám sát người tham gia huấn luyện

- Người quản trị/Hướng dẫn có thể giám sát toàn bộ màn hình của các người được huấn luyện, giám sát các mục tiêu huấn luyện theo thời gian thực, cùng với đó là quản lý hệ thống cảnh báo báo cáo.
- Giám sát màn hình người tham gia huấn luyện, diễn tập: Người hướng dẫn huấn luyện có thể giám sát toàn bộ màn hình của các người tham gia huấn luyện.
- **Giám sát trạng thái mục tiêu:**
  - Giám sát tình huống: Người hướng dẫn, huấn luyện có thể theo dõi trạng thái hoàn thành/chưa hoàn thành bài huấn luyện của từng người tham gia huấn luyện
  - Giám sát trạng thái dịch vụ: Người hướng dẫn, huấn luyện có thể theo dõi trạng thái hoạt động/ không hoạt động người tham gia huấn luyện
- **Ghi nhật ký trong quá trình huấn luyện:**
  - Ghi nhật ký tình huống: Người hướng dẫn, huấn luyện có thể xem lại nhật ký trạng thái hoàn thành/chưa hoàn thành bài huấn luyện của từng người tham gia huấn luyện.
  - Ghi nhật ký trạng thái dịch vụ: Người hướng dẫn, huấn luyện có thể xem nhật ký trạng thái hoạt động/ không hoạt động người tham gia huấn luyện
- **Điều khiển bộ tạo tình huống:**
  - Cấu hình bộ tạo tình huống: Cho phép người hướng dẫn huấn luyện cấu hình các bộ tạo tình huống với mức độ tuỳ biến cao.
  - Điều khiển bộ tạo tình huống: Cho phép người hướng dẫn huấn luyện điều khiển bộ tạo tình huống trong thời gian diễn ra bài huấn luyện.
- **Điều khiển bộ tạo lưu lượng/tấn công:**
  - Cấu hình bộ tạo lưu lượng: Cho phép người hướng dẫn huấn luyện cấu hình các bộ tạo lưu lượng với mức độ tuỳ biến cao.
  - Cấu hình bộ tạo tấn công: Cho phép người hướng dẫn huấn luyện cấu hình các bộ tạo tấn công với mức độ tuỳ biến cao
- Điều khiển bộ tạo lưu lượng/tấn công: Cho phép người hướng dẫn huấn luyện điều khiển bộ tạo lưu lượng/tấn công trong thời gian diễn ra bài huấn luyện.

8. Tính năng khác

- Hệ thống hỗ trợ thông báo các hoạt động trên trang chủ quản trị, bao gồm các thông tin sự kiện diễn ra trên hệ thống, bao gồm thông tin sự kiên, tên sự kiện, thời gian xảy ra sự kiện.
- Hệ thống hỗ trợ hiển thị chi tiết nội dung thông báo, bao gồm tên sự kiện, loại sự kiện, thời gian sự kiện diễn ra.
- Hệ thống hỗ trợ hiển thị thông tin tài khoản, bao gồm tên tài khoản, nhóm của tài khoản, nút logout, và avatar của tài khoản.

9. Hình thức triển khai

10. Kịch bản đào tạo, diễn tập

Dựa trên khung NICE SP800-181 do Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) thuộc Bộ Thương mại Hoa Kỳ, kết hợp tham chiếu Phụ lục 02 – Quyết định số 05/2017/QĐ-TTg ngày ngày 16/3/2017 của Thủ tướng Chính phủ và Quyết định số 1233/QĐ-BTTTT ngày 27/07/2015 của Bộ Thông tin và Truyền thông, các kịch bản đào tạo, diễn tập chia thành 2 nhóm chính Cyber Lab (Các bài huấn luyện kỹ năng cơ bản) và Cyber Range (Các bài diễn tập).