Bkav®

Cyber Range
Your digital battlefield

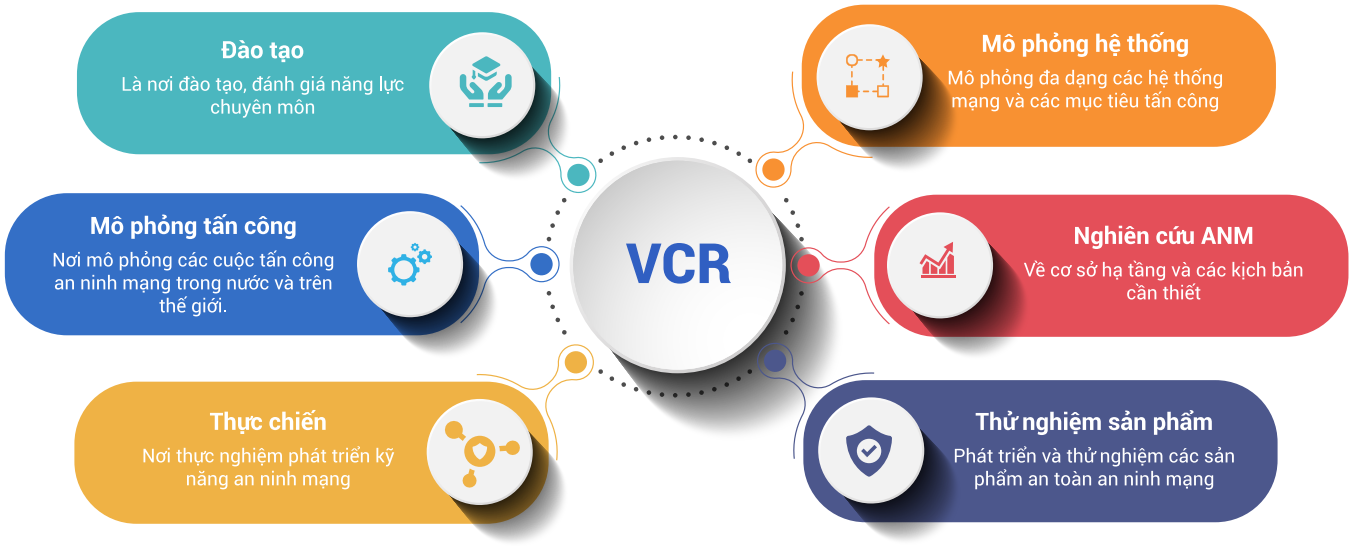
THAO TRƯỜNG AN NINH MẠNG VIET NAM CYBER RANGE

Giới thiệu tổng quan

Thao trường an ninh mạng - Viet Nam Cyber Range (VCR) là một hệ thống mô phỏng gần như đầy đủ các hệ thống mạng, thiết bị mạng, thiết bị điều khiển công nghiệp ICS/SCADA, các loại máy chủ, các phần mềm, ứng dụng của các tổ chức.

Hệ thống bao gồm cả phần mềm và phần cứng kết hợp với nhau để tạo ra các mạng mô phỏng, cung cấp một môi trường an toàn, đảm bảo về mặt pháp lý để đối tượng tham gia có thể đạt được các kỹ năng thực hành, từ đó giúp quá trình phát triển các sản phẩm, kiểm thử bảo mật có thể nhanh và đơn giản hơn.

Mục tiêu của VCR



Đối tượng sử dụng

• **Chuyên gia - Các chuyên gia từ các nhóm khác nhau**: IT, an ninh mạng, thực thi pháp luật, người xử lý sự cố và những nhóm người khác sử dụng Viet Nam Cyber Range để cải thiện kiến thức và năng lực cá nhân, nhóm.

• **Sinh viên**: Sử dụng Viet Nam Cyber Range để áp dụng kiến thức trong môi trường mạng mô phỏng, phát triển các kỹ năng về mạng, lập trình, an ninh mạng, ... làm việc theo nhóm để giải quyết các vấn đề và chuẩn bị cho các kỳ thi lấy chứng chỉ.

• **Giảng viên**: Sử dụng Viet Nam Cyber Range như một trợ lý trong khi đào tạo hoặc hướng dẫn, đánh giá học sinh trên thực tế.

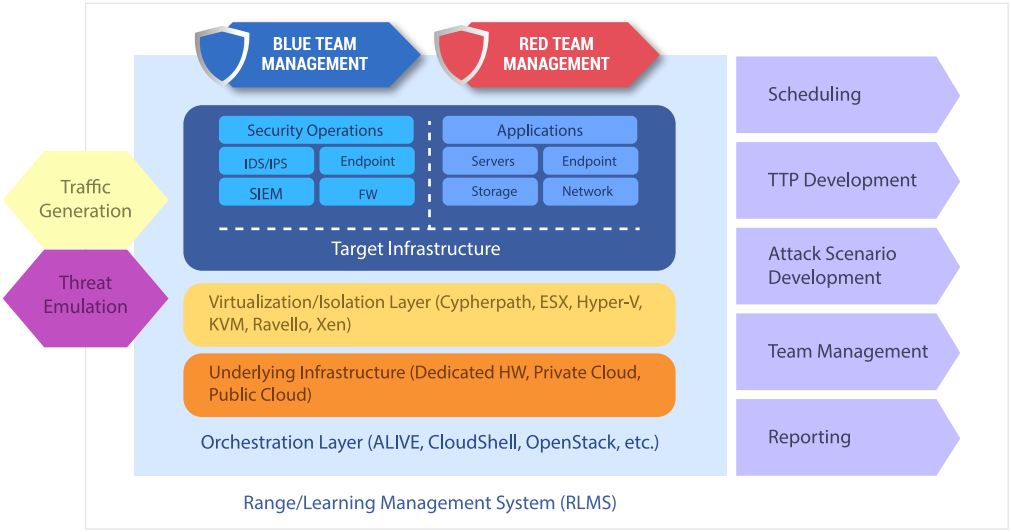
• **Tổ chức**: Sử dụng Viet Nam Cyber Range để đánh giá hệ thống mạng của họ (đánh giá performance, đánh giá an ninh, ...), để thử nghiệm các quy trình mới, đào tạo nhóm của họ về các giao thức và môi trường tổ chức và kỹ thuật mới trước khi chúng được đưa vào môi trường của tổ chức và mở rộng khả năng nhân sự.

Mô hình kiến trúc hệ thống

Range Learning Management System (RLMS)

Đây là một hệ thống trung tâm của Cyber Range. Hệ thống RLMS chứa các tính năng tiêu chuẩn của một LMS (Quản lý, tạo ra các kịch bản đào tạo diễn tập; quản lý, giám người tham gia; báo cáo, lập lịch, ...) và các tính năng đặc trưng của hệ thống VCR (quản lý, tạo lưu lượng mạng, ...)

Sơ đồ dưới đây minh họa các thành phần kỹ thuật của hệ thống:



Lớp điều phối - Orchestration Layer

Lấy đầu vào từ RLMS, lớp điều phối kéo tất cả các thành phần công nghệ hoặc dịch vụ của hệ thống cyber range lại với nhau. Lớp điều phối cung cấp các dịch vụ để tạo điều kiện thuận lợi cho việc chia lưới các lớp khác: Lớp cơ sở hạ tầng (underlying infrastructure), lớp ảo hóa (virtualization layer), lớp mô phỏng (target infrastructure). Lớp này có thể sử dụng các phần mềm thương mại hoặc mã nguồn mở ví dụ như: Openstack, CloudShell, ...

Cơ sở hạ tầng - Underlying Infrastructure

Cyber Range được triển khai trên cơ sở hạ tầng gồm network, servers và storage. Một số Hệ thống có thể được triển khai trên cơ sở hạ tầng vật lý (switches, routers, firewalls, endpoints, ...) mặc dù điều này thường đắt và việc mở rộng cũng khó hơn. Vì lý do khả năng mở rộng, chi phí nên một số hệ thống CR đã chuyển sang hạ tầng cloud.

Lớp ảo hóa - Virtualization Layer

Lớp này cung cấp các công nghệ ảo hóa để có thể mô phỏng được các loại thiết bị vật lý. Ở đây có thể sử dụng các công nghệ: ESX, Hyper-V, KVM, ...

Lớp mô phỏng cơ sở hạ tầng mục tiêu - Target Infrastructure

Đây là lớp mô phỏng các cơ sở hạ tầng mục tiêu như hệ thống mạng, thiết bị mạng, thiết bị điều khiển công nghiệp ICS/SCADA, các loại máy chủ, các phần mềm, ứng dụng, ... Dựa trên sự tương tác của sinh viên, RLMS sẽ tạo ra các tập lệnh để điều khiển lớp điều phối (Orchestration Layer) tạo các cơ sở hạ tầng mục tiêu. Các tập lệnh này bao gồm các thông tin cấu hình thiết bị như địa chỉ IP, thông tin định tuyến, dịch vụ cài đặt ,...

Các phân hệ chính

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 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
- Định nghĩa hệ thống mô phỏng: Định nghĩa các cấu trúc mạng (topology) của một hệ thống mô phỏng:
  - Upload File YAML: định nghĩa mô hình mạng theo định dạng file YAM
  - Đồ họa kéo thả: định nghĩa mô hình mạng bằng cách kéo thả các thiết bị và liên kết mạng
- Quản lý các hệ thống mô phỏng: Là quá trình tạo ra và quản lý truy cập tới các hệ thống mô phỏng
  - Tạo các hệ thống mô phỏng
  - Quản lý cách thức truy cập tới hệ thống mô phỏng
  - Khóa hệ thống mô phỏng trong quá trình huấn luyện
  - Giải phóng các tài nguyên máy ảo
  - Quản lý giao tiếp với các thiết bị trong mạng mô phỏng.
- Quản lý các thiết bị ngoại vi.

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

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

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

Quản lý người tham gia huấn luyện

- 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
- Quản lý và phân quyền tài khoản: Tạo các tài khoản học viên và phần quyền các tài khoản
- Quản lý và phân quyền nhóm tài khoản: Tạo các nhóm tài khoản và phần quyền theo nhóm
- Quản lý và phân quyền nhóm tài khoản: Tạo các nhóm tài khoản và phần quyền theo nhóm

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.

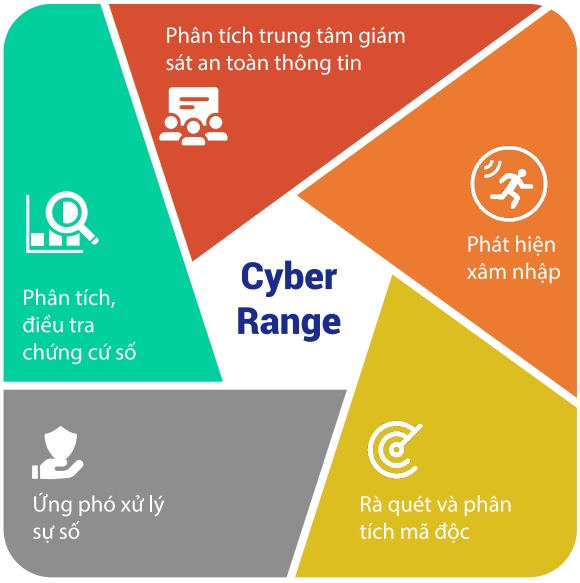
- Giám sát màn hình người tham gia huấn luyện, diễn tập: Người hướng dẫn huấn luyện có thể giám sát toàn bộ màn hình của các người tham gia huấn luyện.
- Giám sát trạng thái mục tiêu:
  - Giám sát tình huống: Người hướng dẫn, huấn luyện có thể theo dõi trạng thái hoàn thành/chưa hoàn thành bài huấn luyện 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.

Hình thức triển khai

Private Cloud **Public Cloud** **Hardware**

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)



Hệ thống thao trường mạng được xây dựng với **hơn 300 kịch bản** có sẵn giải quyết được việc tổ chức đào tạo, huấn luyện, diễn tập, nâng cao kỹ năng, năng lực, trình độ cho các lực lượng ứng cứu và sát hạch cấp chứng chỉ chuyên môn kỹ thuật cho đội ngũ nhân lực.

Các kịch bản hỗ trợ đầy đủ các nền tảng phần cứng, phần mềm phổ biến tại Việt Nam, hỗ trợ các mô hình hệ thống, các tính năng đánh giá, quản lý. Các tình huống tấn công mô phỏng thực tế được tạo ra từ bộ tạo tấn công, sẽ được lựa chọn và xây dựng tạo nên các kịch bản đáp ứng với học viên tham gia thao trường mạng.

Ngoài các kịch bản có sẵn hệ thống cho phép bổ sung và tuỳ biến thêm các kịch bản mới theo nhu cầu của đơn vị tổ chức.

Trụ sở chính: **Tòa nhà Bkav, Khu đô thị Yên Hòa, Cầu Giấy, Hà Nội**
Điện thoại: (024) 3763 2552 Số fax: (024) 3868 4755
Website: security.bkav.com Email: security@bkav.com
Bkav TP. HCM: Số 67, Đường số 3, Khu dân cư City Land, P. 7, Q. Gò Vấp, TP HCM
Điện thoại: (028) 6296 6626 Số fax: (028) 2253 6103

Bkav