Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

1. Giới thiệu chung về gói thầu

- Tên gói thầu: Bảo đảm an toàn thông tin mạng trên địa bàn TP Hồ Chí Minh.
- Nguồn vốn: UBND Thành phố hỗ trợ năm 2025.
- Hình thức lựa chọn nhà thầu: đấu thầu rộng rãi.
- Phương thức lựa chọn nhà thầu: một giai đoạn một túi hồ sơ.
- Thời gian bắt đầu tổ chức lựa chọn nhà thầu: Quý IV/2025.
- Loại hợp đồng: Trọn gói.
- Thời gian thực hiện gói thầu: 15 ngày.
- Địa điểm thực hiện: Thành phố Hồ Chí Minh
- Quy mô:

Hoạt động: "Bảo đảm an toàn thông tin mạng trong các cơ quan nhà nước trên địa bàn Thành phố Hồ Chí Minh năm 2025", Bao gồm các hạng mục sau:

Tổ chức kiểm tra, đánh giá an toàn thông tin và tổ chức diễn tập thực chiến bảo đảm an toàn thông tin mạng năm 2025;

Ứng phó sự cố, đảm bảo an toàn thông tin trên địa bàn Thành phố;

Mua sắm, bổ sung dịch vụ đảm bảo an toàn thông tin cho thiết bị đầu cuối;

Kiểm tra, phân tích, đánh giá an toàn thông tin cho hạ tầng mạng, máy chủ, máy trạm và thiết bị số tại các cơ quan, đơn vị trên địa bàn Thành phố;

Rà quét, bóc tách mã độc tại các cơ quan đơn vị trên địa bàn Thành phố.

2. Mục tiêu công việc

Các thành viên đội ứng cứu sự cố có cơ hội tham gia, rèn luyện kỹ năng, quy trình ứng phó sự cố thực tế thông qua hoạt động diễn tập thực chiến trên hệ thống thực đang vận hành.

Trang bị những kiến thức, kỹ năng cần thiết cho cán bộ chuyên trách CNTT các cơ quan, đơn vị kịp thời ứng phó, giải quyết các vấn đề mất an toàn thông tin thông qua kịch bản giả định tấn công vào mạng máy tính nội bộ (mạng LAN) của các cơ quan, đơn vị mà không sử dụng virus; chiếm tài khoản người dùng và lây lan ngang hàng (lateral movement) đánh cắp dữ liệu; phòng ngừa tấn công giả mạo (phishing) chiếm quyền kiểm soát máy người dùng, leo thang đặc quyền chiếm điều khiển máy chủ.

Nâng cao kiến thức và kỹ năng thực hành về an toàn thông tin mạng cho Đội Ứng cứu sự cố an toàn thông tin mạng và các đơn vị trên địa bàn Thành phố Hồ Chí Minh.

Tăng cường chia sẻ, học tập kinh nghiệm, kiến thức đảm bảo an toàn thông tin mạng giữa các đơn vị của Thành phố Hồ Chí Minh, qua đó góp phần đảm bảo an toàn thông tin mạng trên địa bàn, phục vụ công tác chỉ đạo điều hành của Thành phố.

Rà soát và đảm bảo An toàn hệ thống sau diễn tập: Kiểm tra, rà soát đánh giá và phục hồi toàn diện hệ thống sau khi kết thúc đợt diễn tập khai thác lỗ hổng bảo mật, đảm bảo rằng hệ thống đã hoàn toàn thoát khỏi trạng thái bị tác động từ các hoạt động diễn tập và trở về trạng thái hoạt động ổn định và an toàn an ninh thông tin theo tiêu chuẩn kỹ thuật đã thiết lập. Nội dung chi tiết sẽ thực hiện trong hạng mục "Kiểm tra, phân tích, đánh giá an toàn thông tin cho hạ tầng mạng, máy chủ, máy trạm và thiết bị số tại các cơ quan, đơn vị trên địa bàn Thành phố".

3. Yêu cầu kỹ thuật của gói thầu

3.1. Quy mô, nội dung công việc

3.1.1. Tổ chức kiểm tra, đánh giá an toàn thông tin và tổ chức diễn tập thực chiến bảo đảm an toàn thông tin mạng năm 2025

STT	Nội dung công việc	Đơn vị tính	Khối lượng
I	Dịch vụ diễn tập thực chiến và tổ chức đào tạo		
1	Thuê hội trường – Khai mạc, đào tạo, bế mạc (3 ngày): Hội trường sức chứa tối thiểu 200 học viên, khai mạc, bế mạc, đào tạo diễn tập; Màn hình led trong hội trường kích thước tối thiểu 6,4m x 2,88m, màn hình thông báo nội dung sự kiện rộng 32 inch gắn bên ngoài mỗi phòng họp; - Đã bao gồm sân khấu và bục phát biểu - Đã bao gồm ghế cho 200 khách - Đã bao gồm hệ thống âm thanh, ánh sáng và 2 mic - Đã bao gồm 2 màn hình thông báo nội dung sự kiện rộng 32 inch gắn bên ngoài mỗi phòng họp	Gói	1
2	Màn hình LED quảng cáo bên ngoài sự kiện diễn ra chương trình - 2 Màn hình LED lớn tại 2 cổng chào - 10 Màn hình LED nhỏ bên trong khu tổ chức sự kiện	Gói	1
3	Trang trí hội trường, cổng chào: - Hội trường: 3 vị trí trong khu vực (2 dãy bàn đại biểu + bục phát biểu); - Cổng chào: ≥ 28 m2;	Gói	1
4	Trang trí khu vực chụp hình, phỏng vấn báo chí đài truyền hình: Khu vực chụp hình, phỏng vấn báo chí đài truyền hình: ≥ 15 m2	Gói	1

STT	Nội dung công việc	Đơn vị tính	Khối lượng
5	Standee (Poster được gắn trên giá đỡ); Kích thước: 0,8m x 1,8 m; Kèm khung đỡ.	Bộ	4
6	Standee điện tử	Cái	2
7	Hoa tươi bục phát biểu (khai mạc và bế mạc)	Lẵng	2
8	Gói hoa trang trí, hoa để bàn (khai mạc và bế mạc)	Lẵng	8
9	Hoa tặng khách mời (bế mạc)	Bó	10
10	MC dẫn chương trình - Khai mạc, đào tạo, bế mạc	Người	1
11	Quay phim và chụp hình - Khai mạc, đào tạo, bế mạc	Gói	1
12	Xây dựng kịch bản, dựng clip phóng sự về tình hình, thực trạng an ninh thông tin và tổng kết giai đoạn của chuỗi sự kiện	Clip	1
13	Vệ sinh hội trường - Xuyên suốt chương trình	Gói	1
14	Teabreak (Khai mạc)	Người	200
15	Teabreak (Đào tạo)	Người	100
16	Teabreak (Bế mạc)	Người	140
17	Nước uống	Thùng	30
18	Bảng tên đại biểu	Cái	10
19	Thiết kế phông nền, backdrop, chỉnh sửa theo yêu cầu không quá 5 lần	Cái	1
20	In ấn bảng tên và dây đeo thẻ	Gói	1
21	Dịch vụ viết thông cáo báo chí	Gói	1
22	Dịch vụ phòng VIP phục vụ tiếp khách, hội nghị quy mô không quá 20 người	Gói	1
23	Trang trí khu vực tác chiến: đội tấn công, đội phòng thủ, bàn ghế, giá treo màn hình quan sát	Gói	1
24	Triển khai lắp đặt và tháo dỡ	Gói	1

STT	Nội dung công việc	Đơn vị tính	Khối lượng
25	Vận chuyển các thiết bị	Gói	1
26	In tài liệu học và thực hành	Bộ	80
27	In giấy chứng nhận học viên	Gói	1
28	Văn phòng phẩm: bút, viết, giấy photo...	Gói	1
29	Áo đồng phục (đã bao gồm thiết kế)	Cái	250
30	In giấy chứng nhận các đội tham gia	Tờ	10
II	Chuyên gia xây dựng và tư vấn đào tạo nhận thức an toàn thông tin mạng		
1	Hoạt động 1: Chia sẻ kiến thức, đào tạo an toàn thông tin		
1.1	Chuyên gia trình bày điều phối, thuyết minh	Người	2
1.2	Chuyên gia Hỗ trợ học viên trong quá trình diễn tập	Người	4
2	Hoạt động 2: diễn tập thực chiến bảo đảm an toàn thông tin mạng		
2.1	Chuyên gia tư vấn, thiết kế thao trường	Người	4
2.2	Chuyên gia xây dựng, duy trì thao trường	Người	8
2.3	Chuyên gia điều phối diễn tập	Người	2
2.4	Các chuyên gia lập quy chế, thể lệ thi dấu, chấm điểm và chuyên gia lập báo cáo tổng kết	Người	4
III	Hệ thống xây dựng thao trường kịch bản đào tạo		
1	Thuê thiết kế kịch bản cho thao trường	Kịch bản	3
2	Thuê đường truyền internet	Line	2
3	Hệ thống UPS dự phòng	Gói	1
4	Ổ điện kết nối theo mô hình diễn tập	Cái	26
5	Thuê dịch vụ hệ thống máy chủ (3 máy chủ vật lý)	Hệ thống	1
6	Thuê dịch vụ bản quyền phần mềm ảo hóa	Gói	1

STT	Nội dung công việc	Đơn vị tính	Khối lượng
7	Thuê dịch vụ phần mềm tường lửa ứng dụng cho các mục tiêu của Thao trường	Gói	1
8	Thuê dịch vụ phòng chống mã độc cho các mục tiêu của Thao trường	Gói	1
9	Thuê dịch vụ lưu trữ	TB	10
10	Thuê dịch vụ tường lửa tích hợp IPS	Hệ thống	1
11	Thuê dịch vụ giám sát an toàn mạng	Hệ thống	1
12	Thuê dịch vụ Web proxy security (F5)	Hệ thống	1
13	Thuê dịch vụ hỗ trợ chấm điểm dành cho Ban giám khảo và học viên	Gói	1
14	Thuê thiết bị hỗ trợ mạng nội bộ cho phòng đào tạo và diễn tập (Switch + Modem tốc độ cao)	Bộ	1
15	Thuê Laptop cấu hình mạnh cho hoạt động thực hành kịch bản đào tạo an ninh thông tin: CPU i5 Ram: 16GB SSD 256GB Màn hình: 14 inch	Cái	24
16	Thuê Màn hình giám sát 60 inch + chân đứng	Cái	2
17	Dây cáp HDMI 30m	sợi	2

3.1.2. Ứng phó sự cố, đảm bảo an toàn thông tin trên địa bàn Thành phố

STT	Dịch vụ cung cấp	Đơn vị tính	Số lượng
I	**Dịch vụ tổ chức đào tạo, tập huấn ứng phó sự cố ATTT**		
1	Thuê hội trường – Khai mạc, đào tạo, bế mạc (3 ngày): Hội trường sức chứa tối thiểu 200 học viên, khai mạc, bế mạc, đào tạo diễn tập; Màn hình led trong hội trường kích thước tối thiểu 6,4m x 2,88m, màn hình thông báo nội dung sự kiện rộng 32 inch gắn bên ngoài mỗi phòng họp;	Mặt bằng	1

STT	Dịch vụ cung cấp	Đơn vị tính	Số lượng
	- Đã bao gồm sân khấu và bục phát biểu - Đã bao gồm ghế cho 200 khách - Đã bao gồm hệ thống âm thanh, ánh sáng và 2 mic - Đã bao gồm 2 màn hình thông báo nội dung sự kiện rộng 32 inch gắn bên ngoài mỗi phòng họp		
2	Thuê hội trường – Khai mạc, đào tạo, bế mạc (3 ngày): Hội trường sức chứa tối thiểu 100 học viên, khai mạc, bế mạc, đào tạo diễn tập; Màn hình led trong hội trường kích thước tối thiểu 6,4m x 2,88m, màn hình thông báo nội dung sự kiện rộng 32 inch gắn bên ngoài mỗi phòng họp; - Đã bao gồm sân khấu và bục phát biểu - Đã bao gồm ghế cho 100 khách - Đã bao gồm hệ thống âm thanh, ánh sáng và 2 mic - Đã bao gồm 2 màn hình thông báo nội dung sự kiện rộng 32 inch gắn bên ngoài mỗi phòng họp	Mặt bằng	2
3	Màn hình LED quảng cáo bên ngoài sự kiện diễn ra chương trình - 2 Màn hình LED lớn tại 2 cổng chào - 10 Màn hình LED nhỏ bên trong khu tổ chức sự kiện	Gói	1
4	Trang trí hội trường, cổng chào: - Hội trường: 3 vị trí trong khu vực (2 vị trí bàn khách dại biểu/ 1 vị trí bục phát biểu); - Cổng chào: ≥ 28 m2	Gói	1
5	Trang trí khu vực chụp hình, phỏng vấn báo chí đài truyền hình: Khu vực chụp hình, phỏng vấn báo chí đài truyền hình: ≥ 15 m2	Gói	1
6	Standee (Poster được gắn trên giá đỡ); Kích thước: 0,8m x 1,8 m; Kèm khung đỡ.	Bộ	4
7	Hoa tươi bục phát biểu (khai mạc và bế mạc)	Lẵng	2
8	Gói hoa trang trí, hoa để bàn (khai mạc và bế mạc)	Lẵng	8

STT	Dịch vụ cung cấp	Đơn vị tính	Số lượng
9	Hoa tặng khách mời (bế mạc)	Bó	5
10	MC dẫn chương trình - Khai mạc, đào tạo, bế mạc	Nhân sự	1
11	Quay phim và Chụp hình phục vụ Truyền thông	Gói	3
12	Vệ sinh hội trường - Xuyên suốt chương trình	Gói	3
13	Tea-break ngày 1	Người	320
14	Tea-break ngày 2	Người	320
15	Nước uống	Thùng	36
16	Bảng tên đại biểu	Cái	10
17	Thiết kế phông nền, backdrop, chỉnh sửa theo yêu cầu không quá 5 lần	Cái	1
18	In ấn bảng tên và dây đeo thẻ	Gói	1
19	In giấy chứng nhận học viên	Tờ	400
20	Khung giấy chứng nhận học viên	Cái	400
21	In tài liệu học và thực hành	Bộ	400
22	Văn phòng phẩm: bút, viết, giấy photo	Bộ	400
23	Quà tặng đội có thành tích tốt trong phiên tập huấn	Bộ	3
24	Áo đồng phục (đã bao gồm thiết kế)	Chiếc	30
25	Triển khai lắp đặt và tháo dỡ	Gói	3
26	Vận chuyển thiết bị (Tính trung bình cho 3 điểm)	Gói	3
27	Chi phí di chuyển Ban dự án	Gói	3
28	Chi phí nhân sự hỗ trợ On-site	Gói	1
II	**Chuyên gia xây dựng và tư vấn đào tạo tập huấn ứng phó sự cố ATTT**		
1	Giảng viên: - Chịu trách nhiệm đứng lớp, truyền đạt nội dung và trực tiếp điều hành buổi Đào tạo và Diễn tập.	Người	1

STT	Dịch vụ cung cấp	Đơn vị tính	Số lượng
2	Trợ giảng / Kỹ thuật viên Hỗ trợ: - Hỗ trợ Giảng viên trong việc quản lý lớp học, phân nhóm thảo luận và xử lý các vấn đề kỹ thuật cơ bản của học viên tại chỗ.	Người	8
3	Chuyên gia tư vấn, thiết kế Lab tập huấn	Người	3
4	Chuyên gia thiết kế kịch bản, viết tài liệu đào tạo	Người	3
III	**Hệ thống xây dựng kịch bản đào tạo, tập huấn**		
1	Thuê dịch vụ xây dựng Môi trường và Kịch bản Lab - Chuẩn bị và cấu hình sẵn kịch bản Lab - Cài đặt các công cụ phục vụ công tác tập huấn, diễn tập	Gói	1
2	Thuê Laptop cấu hình mạnh cho hoạt động thực hành kịch bản đào tạo an ninh thông tin - CPU: Core i7 - RAM: 32GB - SSD: 1TB	Cái	80
3	Gói công cụ giả lập sự cố: - Metasploit Framework: phát triển, kiểm tra và thực thi các mã khai thác để tấn công vào lỗ hổng bảo mật của mục tiêu. - Burpsuite Professional: chặn bắt/chỉnh sửa gói tin HTTP/S, quét lỗ hổng tự động và tấn công vét cạn/fuzzing. - Caldera: thực thi các kịch bản tấn công dựa trên ma trận MITRE ATT&CK để kiểm tra khả năng phát hiện và phản ứng của hệ thống phòng thủ. - Vmware: dựng môi trường Lab cô lập, an toàn, hỗ trợ chụp lại trạng thái hệ thống để phục vụ phân tích mã độc hoặc thử nghiệm tấn công mà không ảnh hưởng máy thật.	Gói	1
4	Gói công cụ xử lý sự cố: - Network Packet Sniffer: bắt và giải mã chi tiết từng gói tin đi qua card mạng, phục vụ điều tra sự cố, phát hiện kết nối ngầm hoặc gỡ lỗi mạng. - SIEM: thu thập Log từ toàn bộ hệ thống, chuẩn hóa và phân tích tương quan theo thời gian thực - IDA: chuyển đổi file nhị phân thành hợp ngữ hoặc giả mã, giúp chuyên gia phân tích loại mã độc hoặc tìm lỗ hổng phần mềm.	Gói	1

STT	Dịch vụ cung cấp	Đơn vị tính	Số lượng
	- Endpoint security: giám sát hành vi bất thường, cách ly máy nhiễm và điều tra nguyên nhân gốc rễ		
IV	**Chi phí khác**		
1	Thuê đường truyền Internet	Đường	6
2	Ổ điện kết nối	Cái	40
3	Dây cáp HDMI 30m kết nối máy tính giảng viên đến màn hình LED	Sợi	2

3.1.3. Mua sắm, bổ sung dịch vụ đảm bảo an toàn thông tin cho thiết bị đầu cuối

STT	Danh mục	Đơn vị tính	Số lượng
1	**Giải pháp phòng chống mã độc. đảm bảo an toàn thông tin cho thiết bị đầu cuối - Endpoint**		
1.1	Mô tả chung - Có chức năng cho phép cập nhật tự động phiên bản mới của các phần mềm phòng, chống mã độc được cài đặt trên các máy trạm và máy chủ (agent). - Có chức năng cho phép cập nhật tự động dấu hiệu phát hiện mã độc mới trên các agent. - Có cơ chế cập nhật online và offline Chức năng quản trị tập trung Chức năng quản lý chính sách tập trung: - Cho phép tạo nhóm và phân loại thiết bị đầu cuối theo các nhóm định nghĩa. Chức năng thống kê các thông tin sau: - Tình hình lây nhiễm mã độc trên các máy trạm và máy chủ: IP máy bị nhiễm, tên máy bị nhiễm, thông tin về mã độc. - Các kết nối nguy hiểm trên các máy trạm và máy chủ: IP máy có kết nối nghi ngờ, Tên máy có kết nối nghi ngờ, Thông tin kết nối nghi ngờ: Tên phần mềm thực hiện kết nối nghi ngờ; Mã MD5 của phần mềm có kết nối nghi ngờ; IP đích của kết nối nghi ngờ.	Phần mềm	5564

STT	Danh mục	Đơn vị tính	Số lượng
	- Các hệ điều hành đang sử dụng trên các máy trạm và máy chủ: IP của máy trạm và máy chủ báo cáo thông tin hệ điều hành; Hệ điều hành đang sử dụng trên máy trạm và máy chủ; Thời gian cập nhật gần nhất của hệ điều hành trên máy trạm và máy chủ. - Trạng thái cập nhật giải pháp phòng, chống mã độc trên các máy trạm và máy chủ. Các thông tin thống kê bao gồm: số máy trạm và máy chủ không cập nhật trong vòng 15 ngày. - Tình hình virus trong hệ thống, đưa ra chi tiết các máy bị nhiễm, các dòng virus lây nhiễm và tình trạng virus đã được xử lý. - Thống kê theo cảnh báo, xuất cảnh báo. Khả năng điều khiển các agent: - Cho phép ra lệnh quét cho các agent trên từng máy trạm và máy chủ, nhóm máy trạm và máy chủ hoặc toàn bộ máy trạm và máy chủ trong hệ thống. - Cho phép điều khiển thay đổi các chính sách phát hiện, ngăn chặn mã độc trên các agent. - Cho phép điều khiển cập nhật phiên bản phần mềm và dấu hiệu phát hiện mã độc trên mỗi agent. - Ra lệnh cập nhật/quét virus trên máy trạm và máy chủ từ xa, đặt lịch quét/update định kỳ. Hỗ trợ cập nhật offline trong hệ thống nội bộ, không cần máy trạm và máy chủ kết nối internet. - Tìm kiếm log event trên toàn bộ máy trạm và máy chủ. - Hỗ trợ cô lập (network, process) tạm thời các máy phục vụ điều tra. Chức năng phòng chống mã độc: * Kiểm soát ứng dụng - Tính năng Blocklist chặn thực thi file theo giá trị hàng băm của chúng, hỗ trợ MD5 và SHA256, hỗ trợ đồng thời theo đường dẫn & liên kết của ứng dụng. * Kiểm soát thiết bị ngoại vi - Cho phép ngăn chặn rò rỉ dữ liệu nhạy cảm và nhiễm phần mềm độc hại thông qua ngăn chặn các thiết bị ngoại vi.		

STT	Danh mục	Đơn vị tính	Số lượng
	- Giám sát việc kết nối, sử dụng các thiết bị lưu trữ ngoài, USB, thẻ nhớ trên các thiết bị đầu cuối (read-only). * Kiểm soát truy cập web/mail - Bảo vệ máy trạm và máy chủ khi truy cập web.		
	* Công nghệ chống mã độc - Ngăn chặn mã độc, bảo vệ máy trạm và máy chủ theo thời gian thực. - Công nghệ quét thông minh. - Công nghệ kiểm soát mối đe dọa nâng cao, phân tích hành động đáng ngờ như: ngụy trang loại quy trình, thực hiện thực thi mã trong không gian bộ nhớ của một quy trình khác (thu giữ bộ nhớ quy trình để leo thang đặc quyền), tái tạo, gửi tệp, tránh bị phát hiện từ các ứng dụng liệt kê quy trình. - Tính năng phòng chống virus mã hóa dữ liệu. - Phát hiện và giảm thiểu rủi ro mất dữ liệu trong các cuộc tấn công ransomware nâng cao, tạo ra một bản sao dự phòng thời gian thực của các tệp trước khi chúng bị sửa đổi bởi các quy trình đáng ngờ. - Tự động phát hiện và chặn các cuộc tấn công không sử dụng tệp (fileless) - Tính năng tự động bảo vệ phần mềm bảo mật khỏi bị vô hiệu hóa hoặc thay đổi bởi những kẻ tấn công trên điểm cuối. - Tự động phát hiện và chặn các cuộc tấn công thông qua dòng lệnh mà không sử dụng tệp. - Chống lại tấn công mạng thế hệ mới, bao gồm các mối đe dọa dai dẳng tiên tiến. Bảo vệ bằng các thuật toán mạnh mẽ dựa trên trí tuệ nhân tạo và máy học. * Bảo vệ mạng - Tường lửa kiểm soát quyền truy cập của ứng dụng vào ra mạng và Internet. - IDS (Intrusion Detection System) phát hiện các cuộc tấn công mạng như brute-force, khai thác mạng, đánh cắp mặt khẩu, chuyển hướng download, bots, và Trojans. * Bảo vệ lưu lượng mạng		

STT	Danh mục	Đơn vị tính	Số lượng
	- Phát hiện các cuộc tấn công mạng được thiết kế để có quyền truy cập vào các máy trạm và máy chủ thông qua các hình thức tấn công như: Tấn công brute-force, khai thác mạng, đánh cắp mặt khẩu, chuyển hướng download, bots, và Trojans. * Kiểm soát lổ hỏng bảo mật - Giám sát các hành vi người dùng, đưa ra các cảnh bảo về rủi ro hành vi người dùng, những nguy Cơ và mối đe dọa cho an ninh thông tin xuất phát từ hành vi của người dùng. - Giám sát Tình Trạng lỗ hỏng bảo mật, bản vá Hệ điều hành trên Hệ điều hành Windows và các phần mềm cài đặt trên máy người dùng. * Tương thích các hệ điều hành - Windows, Linux * Máy chủ quản trị - Giải pháp cho phép triển khai thành phần quản trị On-premise hoặc Cloud của hãng - Có thể triển khai linh hoạt trên hạ tầng vật lý hoặc ảo hóa dễ dàng nâng cấp và mở rộng quy mô khi cần thiết. - Cơ chế kiểm soát quyền quản trị viên, trong trường hợp hacker làm chủ được máy chủ quản lý trung tâm cũng không ra lệnh được xuống cho các máy trạm nếu không có USB token - Hỗ trợ triển khai máy chủ quản trị theo chế độ HA / Load Balancing, Replica Database đảm bảo tính sẵn sàng cao cho máy chủ quản trị và Cơ sở dữ liệu. Chức năng phát hiện và ứng phó - Khả năng tìm kiếm các chỉ số thỏa hiệp (IoC), đồ thị quá trình lấy nhiễm và tấn công, gán các giai đoạn tấn công tương ứng kỹ thuật trong MITRE ATT&CK framework. - Hành động phản hồi cách ly file, cô lập thiết bị, quét tự động, gửi file lên hộp cát phân tích. - Phân tích nguyên nhân gốc rễ. - Công cụ săn tìm mối de dọa Threat Hunting - Phát hiện, ngăn chặn tấn công APT nâng cao.		

STT	Danh mục	Đơn vị tính	Số lượng
2	**Máy chủ trung tâm**		
2.1	- Bộ vi xử lý: ≥ 2 x Intel® Xeon® Gold 5418Y 2G, 24C/48T, 16GT/s, 45M Cache, Turbo, HT (185W) - Bộ nhớ tạm: ≥ 8 x 32GB RDIMM, 5600MT/s, Dual Rank - Ổ cứng: ≥ 4 x 3.84TB SSD SATA Read Intensive 6Gbps - Broadcom 57414 Dual Port 10/25GbE SFP28, OCP NIC 3.0 - Motherboard with Broadcom 5720 Dual Port 1Gb On-Board LOM CPU: 2 x Intel® Xeon® Gold 5418Y (2GHz, 24 nhân, 48 luồng, 45MB Cache, Turbo, HT, 185W) - Hỗ trợ các tiêu chuẩn bảo mật cơ bản và nâng cao: + Cryptographically signed firmware + Secure Boot + Secure Erase + Silicon Root of Trust + System Lockdown <yêu cầu license tương ứng> + TPM 1.2/2.0 FIPS, CC-TCG certified, TPM 2.0; - Yêu cầu về ATTTT: + Chi phí thuê chỗ đặt và các dich vụ ANTT kèm theo(không bao gồm dịch vụ sao lưu phục hồi dữ liệu); + Dich vụ. ANTT gồmn (dịch vụ VPN, dịch vụ tường lửa đa lớp, dịch vụ IPS, dịch vụ giám sát và cảnh báo sớm)	Thiết bị	01

3.1.4. Kiểm tra, phân tích, đánh giá an toàn thông tin cho hạ tầng mạng, máy chủ, máy trạm và thiết bị số tại các cơ quan, đơn vị trên địa bàn Thành phố

STT	Dịch vụ cung cấp	Đơn vị tính	Số lượng
1	**Kiểm tra. đánh giá hiện trạng theo hồ sơ đề xuất cấp độ hệ thống thông tin**	**Hệ thống**	**5**
1.1	- Khảo sát. thiết kế hệ thống thông tin theo cấp độ		
1.2	- Kiểm tra. đánh giá tuân thủ đối với đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin		

STT	Dịch vụ cung cấp	Đơn vị tính	Số lượng
1.3	- Kiểm tra. đánh giá tuân thủ đối với đơn vị vận hành.		
1.4	- Kiểm tra. đánh giá việc tổ chức thực thi các biện pháp bảo đảm an toàn thông tin		
1.5	- Kiểm tra tính đầy đủ và phù hợp của Quy chế bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin về quản lý được phê duyệt.		
1.6	- Đánh giá việc tuân thủ các quy định. quy trình trong Quy chế bảo đảm an toàn thông tin trong quá trình vận hành. khai thác. kết thúc hoặc hủy bỏ hệ thống thông tin.		
1.7	- Đánh giá việc thiết kế hệ thống theo phương án bảo đảm an toàn thông tin được phê duyệt.		
1.8	- Đánh giá việc thiết lập. cấu hình hệ thống theo phương án bảo đảm an toàn thông tin được phê duyệt.		
2	**Kiểm tra đánh giá an toàn thông tin cho các ứng dụng**	**Hệ thống**	**5**
2.1	+ Kiểm tra. đánh giá Quản lý cấu hình & triển khai		
2.2	+ Kiểm tra. đánh giá Quản lý định danh		
2.3	+ Kiểm tra. đánh giá Xác thực		
2.4	+ Kiểm tra. đánh giá Phân quyền		
2.5	+ Kiểm tra. đánh giá Quản lý phiên		
2.6	+ Kiểm tra. đánh giá Quản lý phiên		
2.7	+ Kiểm tra. đánh giá Sàng lọc dữ liệu đầu vào		
2.8	+ Kiểm tra. đánh giá Cơ chế xử lý lỗi		
2.9	+ Kiểm tra. đánh giá Thuật toán mã hóa		
2.10	+ Kiểm tra. đánh giá Logic nghiệp vụ		
2.11	+ Kiểm tra Xử lý phía người dùng		

STT	Dịch vụ cung cấp	Đơn vị tính	Số lượng
2.12	Lập báo cáo kết quả đánh giá và khuyến nghị khắc phục		
3	**Kiểm tra đánh giá an toàn thông tin cho các máy chủ**	**Hệ thống**	**5**
3.1	+ Dò quét các dịch vụ. phần mềm. cổng mạng… đang chạy trên máy chủ để phát hiện các lỗ hổng. bản vá còn thiếu		
3.2	+ Kiểm tra cấu hình hệ điều hành.		
3.3	+ Kiểm tra cấu hình chứng thực.		
3.4	+ Kiểm tra cấu hình log. giám sát.		
3.5	+ Kiểm tra các cấu hình chính sách nội bộ.		
3.6	+ Kiểm tra. đánh giá cấu hình chính sách tài khoản.		
3.7	+ Kiểm tra chính sách kết nối quản trị.		
3.8	+ Kiểm tra các giải pháp về phòng. chống mã độc		
3.9	Lập báo cáo kết quả đánh giá và khuyến nghị khắc phục		
4	**Kiểm tra đánh giá an toàn thông tin cho các thiết bị mạng**	**Hệ thống**	**5**
4.1	+ Dò quét các dịch vụ. cổng mạng… đang chạy trên thiết bị để phát hiện các lỗ hổng. bản vá còn thiếu		
4.2	+ Kiểm tra. đánh giá cấu hình lớp an ninh.		
4.3	+ Kiểm tra. đánh giá cấu hình quản trị.		
4.4	+ Kiểm tra. đánh giá cấu hình chính sách tài khoản.		
4.5	+ Kiểm tra chính sách kết nối quản trị.		
4.6	+ Kiểm tra cấu hình log. giám sát.		
4.7	Lập báo cáo kết quả đánh giá và khuyến nghị khắc phục		

3.1.5. Rà quét, bóc tách mã độc tại các cơ quan đơn vị trên địa bàn Thành phố

STT	Nội dung	Đơn vị	Số lượng
I	**Thuê thiết bị và phần mềm**		
1	**Hạ tầng thiết bị**		
1,1	Máy chủ tại TTDL có cấu hình tối thiểu:	Máy chủ	1
	+ CPU 96 cores		
	+ RAM 512GB		
	+ Storage 4TB SSD. 8TB HDD		
	Vai trò quản lý và hỗ trợ: Dashboard tổng hợp. quản lý cấu hình tập trung. Báo cáo và thống kê toàn hệ thống.		
	- Dịch vụ thuê vị trí đặt thiết bị và ATTTT: + Chi phí thuê chỗ đặt và các dich vụ ANTT kèm theo(không bao gồm dịch vụ sao lưu phục hồi dữ liệu); + Dich vụ. ANTT gồmn (dịch vụ VPN, dịch vụ tường lửa đa lớp, dịch vụ IPS, dịch vụ giám sát và cảnh báo sớm)		
1,2	Thiết bị phân tích thông minh tại đơn vị. phân cứng tối thiểu:	Thiết bị	15
	+ CPU 24 cores		
	+ RAM 96 GB		
	+ Storage 2TB SSD. 8TB HDD		
	+ 02 NIC 1Gbps		
	+ Năng lực xử lý chính: Deep Packet Inspection (DPI), ML/AI Engine tích hợp. Phát hiện C&C Communication. Network Behavior Analysis. Lateral Movement Detection. Network scanning		
2	**Phần mềm**		
2,1	Phần mềm quản trị tập trung	Bản quyền	1
	+ Quản trị tập trung các thiết bị tại đơn vị		
	+ Quản lý kết quả rà soát mã độc. tổng hợp thông tin. hỗ trợ báo cáo		

STT	Nội dung	Đơn vị	Số lượng
2,2	Phần mềm phân tích thông minh tại đơn vị. thực hiện phân tích. rà quét. nhận diện mã độc tại đơn vị.	Bản quyền	15
II	**Dịch vụ chuyên gia rà quét. bóc tách mã độc**		
	- Thực hiện theo dõi và rà quét. thực hiện đánh giá xâm nhập. săn tìm mã độc và các mối đe dọa tiềm ẩn trên luồng mạng: + Phát hiện C&C. botnet + Phát hiện truy vấn tên miền độc hại + Phát hiện hacking tool + Phát hiện hành vi khai thác lỗ hổng + Phát hiện tấn công APT. malware APT - Phân tích và điều tra chi tiết mã độc - Loại bỏ mã độc và làm sạch. hỗ trợ phục hồi hệ thống - Lập báo cáo kết quả rà quét. bóc tách mã độc và khuyến nghị nâng cao an toàn thông tin	Gói	1

3.2. Yêu cầu kỹ thuật về nội dung hạng mục công việc

3.2.1. Hạng mục: Tổ chức kiểm tra, đánh giá an toàn thông tin và tổ chức diễn tập thực chiến bảo đảm an toàn thông tin mạng năm 2025

3.2.1.1. Yêu cầu năng lực, kinh nghiệm

a) Yêu cầu về kinh nghiệm, năng lực tổ chức

Nhà cung cấp dịch vụ cần chứng minh đã từng thực hiện tối thiểu 01 dự án tương tự trong vòng 03 năm gần nhất.

Nhà cung cấp dịch vụ phải có chứng chỉ ISO 27001 về tiêu chuẩn quản lý an toàn thông tin còn hiệu lực.

Nhà cung cấp dịch vụ phải có giấy phép kinh doanh dịch vụ an ninh thông tin còn hiệu lực.

b) Yêu cầu về nhân sự

STT	Nội dung	Số lượng (người)	Số năm kinh nghiệm	Bằng cấp liên quan
1.	Nhóm Chuyên gia trình bày điều phối, thuyết minh	2	≥ 15 năm bậc đại học	Tốt nghiệp các chuyên ngành Toán tin, Công nghệ thông tin, Điện tử , Viễn thông, Khoa hoc máy tính, An ninh mang, An toàn thông tin, Kỹ thuật phần mềm, Hệ thống thông tin

STT	Nội dung	Số lượng (người)	Số năm kinh nghiệm	Bằng cấp liên quan
2.	Nhóm chuyên gia Hỗ trợ học viên trong quá trình diễn tập	4	≥ 5 năm bậc đại học	Tốt nghiệp các chuyên ngành Toán tin, Công nghệ thông tin, Điện tử , Viễn thông, Khoa hoc máy tính, An ninh mang, An toàn thông tin, Kỹ thuật phần mềm, Hệ thống thông tin
3.	Nhóm Chuyên gia tư vấn, thiết kế thao trường	4	≥ 9 năm bậc đại học	Tốt nghiệp các chuyên ngành Toán tin, Công nghệ thông tin, Điện tử , Viễn thông, Khoa hoc máy tính, An ninh mang, An toàn thông tin, Kỹ thuật phần mềm, Hệ thống thông tin
4.	Nhóm Chuyên gia xây dựng, duy trì thao trường	8	≥ 9 năm bậc đại học	Tốt nghiệp các chuyên ngành Toán tin, Công nghệ thông tin, Điện tử , Viễn thông, Khoa hoc máy tính, An ninh mang, An toàn thông tin, Kỹ thuật phần mềm, Hệ thống thông tin
5	Nhóm Chuyên gia điều phối diễn tập	2	≥ 9 năm bậc đại học	Tốt nghiệp các chuyên ngành Toán tin, Công nghệ thông tin, Điện tử , Viễn thông, Khoa hoc máy tính, An ninh mang, An toàn thông tin, Kỹ thuật phần mềm, Hệ thống thông tin
6	Nhóm chuyên gia lập quy chế, thể lệ thi dấu, chấm điểm và chuyên gia lập báo cáo tổng kết	4	≥ 9 năm bậc đại học	Tốt nghiệp các chuyên ngành Toán tin, Công nghệ thông tin, Điện tử , Viễn thông, Khoa hoc máy tính, An ninh mang, An toàn thông tin, Kỹ thuật phần mềm, Hệ thống thông tin
	Tổng cộng	**24**		

3.2.1.2. Hoạt động 1

Tổ chức diễn tập thực chiến cho Đội ứng cứu sự cố an toàn mạng thành phố, bộ phận kỹ thuật đang vận hành tại Trung tâm dữ liệu Thành phố Hồ Chí Minh; diễn tập thực chiến là diễn tập không có kịch bản, các bên tham gia tấn công/phòng thủ trên hệ thống ứng dụng/cổng thông tin đang vận hành chính thức đã được phê duyệt cấp độ 3.

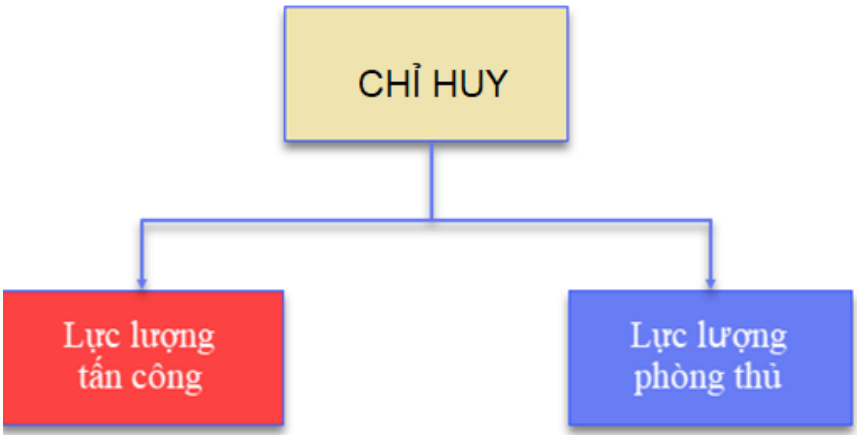
3.2.1.3. Hoạt động 2

Công tác đào tạo các kỹ năng, kiến thức về an toàn thông tin cho cho cán bộ phụ trách công nghệ thông tin, an toàn thông tin cho các Sở, ban, ngành và UBND các phường, xã, đặc khu mới sau sáp nhập. Công tác đào tạo được xây dựng gồm 02 phần (lý thuyết và thực hành); phần lý thuyết đào tạo cho học viên nắm rõ các cấp độ ATTT: phân biệt cấp độ, các phương án đảm bảo ATTT đối với cấp độ 2 và 3; phần thực hành được xây dựng các kịch bản tác chiến an toàn thông tin trên thao trường diễn tập giúp cho học viên nắm rõ quy trình, các bước tấn công, hình thức khai thác lỗ hổng bảo mật, các dấu hiệu nhận biết khi bị tấn. Các kịch bản tác chiến an toàn thông tin trong quá trình đào tạo bao gồm:

- Kịch bản 1: Tác chiến phòng chống tấn công APT sử dụng kỹ thuật Living-off-the-Land.
- Kịch bản 2: Tác chiến phòng chống tấn công phương thức cập nhật UltraVNC.
- Kịch bản 3: Tác chiến phòng chống tấn công qua kết nối api giữa logistics và cổng thanh toán.

3.2.1.4. Nội dung hoạt động 1–Công tác diễn tập thực chiến an toàn thông tin mạng

Lực lượng thực hiện được tổ chức thành 3 lực lượng chính sau:



Hình 1: Các lực lượng chính tham gia diễn tập

a. Chỉ huy (PA05):

- Quản lý chung, điều phối nhân lực thực hiện công tác đảm bảo ATTT cho Thành phố.
- Phê duyệt kế hoạch diễn tập, thành lập Ban tổ chức, Ban giám khảo, thể lệ cuộc thi, ứng dụng/cổng thông tin được phép khai thác.

b. Lực lượng tấn công (RedTeam):

- Mời các cơ quan, doanh nghiệp có kinh nghiệm hoạt động trong lĩnh vực an toàn thông tin để thực hiện các công việc sau:
- Trinh sát dò tìm lỗ hổng của ứng dụng.
- Tấn công xâm nhập hệ thống.

- Cung cấp thông tin, bằng chứng tấn công thành công về Ban tổ chức.

c. Lực lượng phòng thủ (BlueTeam) gồm các thành phần sau:

- Bộ phận kỹ thuật quản lý vận hành Trung tâm dữ liệu.
- Đơn vị vận hành phần mềm ứng dụng.
  - Thực hiện quản trị giám sát ATTT hệ thống tham gia vào diễn tập.
  - Hoạt động theo cơ chế trực ca 24/7.
  - Báo cáo các nội dung phát hiện, ngăn chặn cho Ban tổ chức.

Mô hình ứng dụng (3 lớp: web-app-db) tiêu biểu như sau:

- Tầng giao diện người dùng (web layer): là tầng mà người dùng tương tác trực tiếp với ứng dụng web thông qua trình duyệt. Nó chứa các thành phần như HTML, CSS và JavaScript để hiển thị giao diện cho người dùng.
- Tầng ứng dụng (application layer): tầng này chứa các logic xử lý nghiệp vụ của ứng dụng web, xử lý các yêu cầu từ tầng giao diện người dùng và truy xuất các dữ liệu từ tầng cơ sở dữ liệu để thực hiện các tác vụ cụ thể.
- Tầng cơ sở dữ liệu (database layer): tầng này chứa các cơ sở dữ liệu được sử dụng để lưu trữ và quản lý dữ liệu của ứng dụng web. Các thông tin như thông tin người dùng, thông tin sản phẩm và các dữ liệu khác được lưu trữ và truy xuất thông qua các câu truy vấn đến cơ sở dữ liệu.
- Thời gian diễn tập: Quý IV năm 2025.
- Hình thức diễn tập: tổ chức diễn tập trong 5 ngày với hình thức khai thác lỗ hổng từ xa.
- Số lượng tham gia:
  - Số lượng Blue team: dự kiến 30 người
  - Số lượng Red team: 8 đội (dự kiến 80 người).
- Tổng số lượng người tham dự và khách mời dự kiến: 168 người (chi tiết theo danh sách sau):

STT	Thành phần tham dự	Số lượng
1	Red team	80
2	Blue team	30
3	Ban giám khảo	5
4	Ban tổ chức (BTC)	10
5	Khách mời	20
6	Phóng viên các Báo, Đài truyền hình	15

STT	Thành phần tham dự	Số lượng
7	VNCERT (trực thuộc Trung tâm An ninh mạng quốc gia của cục A05 – Cục An ninh mạng và Phòng, chống tội phạm công nghệ cao Bộ Công an)	8
	Tổng cộng	**168**

3.2.1.5. Nội dung hoạt động 2 – Công tác đào tạo kỹ năng, kiến thức về an toàn thông tin

- Thời gian: 02 ngày
- Hình thức tổ chức đào tạo tập trung vào các vấn đề:
  - Công tác đào tạo được xây dựng gồm 02 phần (lý thuyết và thực hành); phần lý thuyết đào tạo cho học viên nắm rõ các cấp độ ATTT: phân biệt cấp độ, các phương án đảm bảo ATTT đối với cấp độ 2 và 3. Hướng dẫn, làm quen các tình huống của kịch bản diễn tập. Hoạt động này diễn ra trong 1 ngày.
  - Thực hành diễn tập an toàn thông tin mạng trên thao trường diễn tập, mô tả các kịch bản và báo cáo tổng kết Diễn tập, diễn ra trong 1 ngày.

3.2.2. Hạng mục: Ứng phó sự cố, đảm bảo an toàn thông tin trên địa bàn Thành phố

3.2.2.1. Yêu cầu năng lực, kinh nghiệm

a) Yêu cầu về kinh nghiệm, năng lực tổ chức:

Nhà cung cấp dịch vụ cần chứng minh đã từng thực hiện tối thiểu 01 dự án đào tạo/tập huấn tương tự trong vòng 03 năm gần nhất.

b) Yêu cầu về Đội ngũ Chuyên gia, Giảng viên và Công cụ:

Yêu cầu này đảm bảo rằng Nhà cung cấp Dịch vụ triển khai dự án phải có nguồn nhân lực chất lượng cao, có kinh nghiệm thực tế và khả năng truyền đạt phù hợp với đối tượng đào tạo.

STT	Nội dung	Số lượng (người)	Số năm kinh nghiệm	Bằng cấp liên quan
1.	Giảng viên	01	≥ 05 năm bậc đại học	Tốt nghiệp các chuyên ngành Toán tin, Công nghệ thông tin, Điện tử, Viễn thông, Khoa học máy tính, An ninh mạng, An toàn thông tin, Kỹ thuật phần mềm, Hệ thống thông tin - Có đồng thời các chứng chỉ Offensive Security Certified Professional (OSCP), Offensive Security Defense Analyst (OSDA) hoặc tương đương.

STT	Nội dung	Số lượng (người)	Số năm kinh nghiệm	Bằng cấp liên quan
2.	Trợ giảng / Kỹ thuật viên hỗ trợ	8	≥ 05 năm bậc đại học	Tốt nghiệp các chuyên ngành Toán tin, Công nghệ thông tin, Điện tử, Viễn thông, Khoa học máy tính, An ninh mạng, An toàn thông tin, Kỹ thuật phần mềm, Hệ thống thông tin
3.	Chuyên gia tư vấn, thiết kế lab tập huấn	3	≥ 10 năm bậc đại học	Tốt nghiệp các chuyên ngành Toán tin, Công nghệ thông tin, Điện tử, Viễn thông, Khoa học máy tính, An ninh mạng, An toàn thông tin, Kỹ thuật phần mềm, Hệ thống thông tin
4.	Chuyên gia thiết kế kịch bản, viết tài liệu đào tạo	3	≥ 05 năm bậc đại học	Tốt nghiệp các chuyên ngành Toán tin, Công nghệ thông tin, Điện tử, Viễn thông, Khoa học máy tính, An ninh mạng, An toàn thông tin, Kỹ thuật phần mềm, Hệ thống thông tin
	Tổng cộng	**15**		

Nhà cung cấp dịch vụ chịu trách nhiệm chuẩn bị các thiết bị phục vụ cho tập huấn và diễn tập hệ thống Lab với cấu hình tối thiểu như sau:

Cấu hình phần cứng:

- CPU: Core i7
- RAM: 32GB
- SSD: 1TB

Phần mềm được cài đặt sẵn: Các phần mềm phục vụ cho công tác tập huấn (công cụ giả lập sự cố, công cụ xử lý sự cố)

3.2.2.2. Yêu cầu về Nội dung Đào tạo và Giảng viên

a) Yêu cầu về Chất lượng Nội dung

Nội dung phải đảm bảo tính phổ cập, dễ tiếp thu và tập trung vào hành vi ứng phó hơn là các kỹ thuật chuyên sâu:

Sử dụng ngôn ngữ dễ tiếp cận và minh họa trực quan (hình ảnh, video, kịch bản) để giải thích các mối đe dọa.

Nội dung cần bao quát các rủi ro thường gặp nhất cuộc sống và quy trình ứng phó sự cố.

Cung cấp các Hướng dẫn Thực hành Sơ bộ để cán bộ biết chính xác phải làm gì khi màn hình bị khóa, máy tính bị chậm bất thường, hoặc nhận được email đáng ngờ.

Thời lượng phù hợp: Ưu tiên 60% Lý thuyết (Kỹ năng nhận thức) và 40% Diễn tập tình huống.

b) Yêu cầu về Giảng viên

Giảng viên không chỉ cần kiến thức bảo mật mà còn cần có kỹ năng sư phạm và truyền đạt đại chúng:

Kinh nghiệm tư vấn chính sách: Giảng viên có kinh nghiệm tư vấn về quy định và nâng cao nhận thức cho khối cơ quan hành chính nhà nước.

Dùng ngôn ngữ phổ thông: Giảng viên cần hạn chế tối đa các thuật ngữ kỹ thuật chuyên môn sâu và luôn giải thích cặn kẽ nếu phải sử dụng.

3.2.2.3. Yêu cầu về Đảm bảo Chất lượng và Sản phẩm bàn giao

Cam kết SLA về Tỷ lệ Hấp thụ: Nhà cung cấp dịch vụ cần cam kết đạt được Tỷ lệ giảm nhấp chuột vào link độc hại trong các chiến dịch Phishing giả lập giảm tối thiểu 50% so với trước khi đào tạo (đây là chỉ số đo lường hiệu quả nhận thức cốt lõi).

Hỗ trợ Hậu cần: Có đội ngũ chuyên trách về hậu cần, đảm bảo việc sắp xếp phòng học, điểm danh, cung cấp tài liệu cho số lượng lớn học viên diễn ra trôi chảy, không ảnh hưởng đến thời gian làm việc hành chính.

3.2.2.4. Yêu cầu về giám sát chất lượng dịch vụ

Phòng PA05 – Công an Thành Phố Hồ Chí Minh:

Thực hiện đánh giá trước đối với toàn bộ giáo trình, tài liệu giảng dạy, và kịch bản diễn tập để xác nhận tính phù hợp với đối tượng tham gia và tính tuân thủ các quy định của Thành phố.

Giám sát việc chuẩn bị cơ sở vật chất, hệ thống âm thanh, ánh sáng và các điều kiện hậu cần khác tại địa điểm tổ chức đào tạo.

Giám sát và xác nhận tính chính xác của danh sách học viên tham gia, hồ sơ điểm danh, và quy trình cấp phát tài liệu, chứng nhận.

Giám sát việc tuân thủ các quy định về bảo mật thông tin và phòng chống rủi ro trong quá trình tổ chức tập huấn.

3.2.3. Hạng mục: Mua sắm, bổ sung dịch vụ đảm bảo an toàn thông tin cho thiết bị đầu cuối

3.2.3.1. Yêu cầu chất lượng dịch vụ

- Đảm bảo bàn giao đầy đủ bản quyền và tài liệu hướng dẫn sử dụng.
- Đảm bảo giải pháp phòng chống mã độc đáp ứng đầy đủ các yêu cầu về kỹ thuật.
- Thực hiện công tác bảo đảm an toàn cho dữ liệu liên quan đến hệ thống được cài đặt.
- Việc cài đặt Endpoint phòng chống mã độc phải bảo đảm không ảnh hưởng đến hoạt động bình thường của hệ thống.

3.2.3.2. Yêu cầu chung

- Cài đặt, triển khai phần mềm có bản quyền cho trên các thiết bị đầu cuối (máy chủ và máy trạm) phải có chứng nhận bản quyền của nhà cung cấp dịch vụ tương ứng với dịch vụ cung cấp;

- Khả năng giải quyết sự cố tối đa sau 02 tiếng kể từ khi nhận được thông báo, có cử chuyên gia đến hiện trường để xử lý (hoặc từ xa);
- Cho phép cập nhật tự động phiên bản phần mềm và dấu hiệu nhận diện mã độc mới, hỗ trợ cả chế độ online và offline
- Có hệ thống quản lý, giám sát và cấu hình tập trung, tích hợp với môi trường ảo hóa và phân nhóm thiết bị theo nhiều tiêu chí
- Áp dụng và quản lý chính sách bảo vệ khác nhau cho từng nhóm thiết bị, hỗ trợ cách ly, giám sát và điều khiển từ xa
- Tích hợp công nghệ chống virus, ransomware, tấn công zero-day, tấn công không dùng file (fileless) và chống khai thác lỗ hổng
- Có khả năng phát hiện IoC, phân tích nguyên nhân, cách ly thiết bị/tệp tin, săn tìm mối đe dọa (Threat Hunting) và chống tấn công APT.

3.2.3.3. Mô hình triển khai

Mô hình triển khai hệ thống bảo mật thiết bị đầu cuối được thiết kế theo kiến trúc tập trung, trong đó một máy chủ trung tâm đặt tại Trung tâm Dữ liệu của Thành phố hoặc Công an Thành phố đóng vai trò quản lý, giám sát, thu thập sự kiện và điều phối hoạt động bảo mật trên toàn hệ thống. Máy chủ trung tâm có cấu hình với 24 core CPU, RAM 256GB, Storage 16TB SSD, đảm bảo hiệu năng cao, khả năng xử lý đồng thời hàng nghìn tác vụ và đáp ứng nhu cầu mở rộng trong tương lai.

Trên máy chủ trung tâm, hệ thống cài đặt phần mềm quản trị Endpoint, cho phép quản lý tập trung toàn bộ các máy trạm, máy chủ bổ sung tại các Sở, UBND phường xã. Các thiết bị đầu cuối tại các đơn vị được cài đặt agent bảo mật kết nối trực tiếp về máy chủ trung tâm thông qua kênh truyền được mã hóa. Agent chịu trách nhiệm giám sát hành vi, phát hiện mã độc, ngăn chặn tấn công, thu thập sự kiện và gửi dữ liệu về hệ thống phân tích trung tâm.

Máy chủ trung tâm đảm nhiệm vai trò triển khai và phân phối chính sách bảo mật, cập nhật cơ sở dữ liệu nhận diện mã độc, điều phối quét tự động, và xử lý cảnh báo theo thời gian thực. Hệ thống cho phép quản lý phân tầng theo nhóm đơn vị, hỗ trợ áp dụng các chính sách phù hợp cho từng khu vực hoặc loại hình thiết bị. Khi phát hiện bất thường, EDR thực hiện cách ly endpoint, thu thập dấu vết số, và gửi dữ liệu phân tích lên máy chủ để đánh giá và phản ứng nhanh.

3.2.3.4. Yêu cầu về an toàn bảo mật thông tin, dữ liệu

Nội dung cung cấp phải được kiểm soát chặt chẽ và đặc biệt là phải có sự ràng buộc đối với các cán bộ của nhà cung cấp giải pháp cũng như nhà cung cấp giải pháp trong việc triển khai các giải pháp kỹ thuật công nghệ, giải pháp an toàn, an ninh, bảo mật và các vấn đề khác có liên quan.

Trong quá trình cung cấp giải pháp, Nhà thầu phải tuân thủ nghiêm ngặt các quy trình vận hành, cài đặt phần mềm; quy chế khai thác, sử dụng hệ thống của Thành phố. Đảm bảo bảo mật thông tin, dữ liệu chặt chẽ dựa trên các tiêu chí sau đây:

- Mỗi người sử dụng hợp pháp chỉ được truy cập vào hệ thống theo thẩm quyền thông qua quyền được cấp và mã nhận dạng trên mạng cục bộ cũng như đối với truy cập từ xa.

- Không được mang các vật mang tin (như đĩa mềm, USB, …) vào/ra nơi đặt máy chủ, thiết bị CNTT.
- Thực hiện đúng các cam kết về bảo đảm an toàn, an ninh thông tin.
- Xây dựng một số biện pháp rõ ràng để phản ứng trước các tình huống có thể xảy ra đối với hệ thống.

3.2.3.5. Yêu cầu đối với nhà cung cấp phần mềm

Có Trung tâm SOC tại TPHCM và cam kết cử nhân sự onsite phối hợp ứng phó sự cố ATTT trong vòng 02 giờ.

3.2.3.6. Yêu cầu đối với phần cứng phần mềm

STT	Nội dung	Mô tả yêu cầu	Số lượng	Ghi chú
1	Máy chủ trung tâm quản lý tập trung	Thông số kỹ thuật: - Bộ vi xử lý: ≥ 2 x Intel® Xeon® Gold 5418Y 2G, 24C/48T, 16GT/s, 45M Cache, Turbo, HT (185W) - Bộ nhớ tạm: ≥ 8 x 32GB RDIMM, 5600MT/s, Dual Rank - Ổ cứng: ≥ 4 x 3.84TB SSD SATA Read Intensive 6Gbps - Broadcom 57414 Dual Port 10/25GbE SFP28, OCP NIC 3.0 - Motherboard with Broadcom 5720 Dual Port 1Gb On-Board LOM CPU: 2 x Intel® Xeon® Gold 5418Y (2GHz, 24 nhân, 48 luồng, 45MB Cache, Turbo, HT, 185W) - Hỗ trợ các tiêu chuẩn bảo mật cơ bản và nâng cao: + Cryptographically signed firmware + Secure Boot + Secure Erase + Silicon Root of Trust + System Lockdown <yêu cầu license tương ứng> + TPM 1.2/2.0 FIPS, CC-TCG certified, TPM 2.0	1	Thời hạn sử dụng 6 tháng
2	Phần mềm	Bản quyền phần mềm đảm bảo an toàn thông tin thiết bị đầu cuối - Endpoint	5.564	

3.2.4. Hạng mục: Kiểm tra, phân tích, đánh giá an toàn thông tin cho hạ tầng mạng, máy chủ, máy trạm và thiết bị số tại các cơ quan, đơn vị trên địa bàn Thành phố

3.2.4.1. Yêu cầu chung

a) Yêu cầu về kinh nghiệm, năng lực tổ chức

Nhà cung cấp dịch vụ cần chứng minh đã từng thực hiện tối thiểu 01 dự án kiểm tra, đánh giá tương tự trong vòng 03 năm gần nhất.

Nhà cung cấp dịch vụ phải có chứng chỉ ISO 27001 về tiêu chuẩn quản lý an toàn thông tin còn hiệu lực.

Nhà cung cấp dịch vụ phải có giấy phép kinh doanh dịch vụ an ninh thông tin còn hiệu lực.

b) Yêu cầu đối với nhân sự chuyên gia

STT	Nội dung	Số lượng (người)	Số năm kinh nghiệm	Bằng cấp liên quan
1	Trưởng nhóm đánh giá	01	≥ 10 năm bậc đại học	- Tốt nghiệp các chuyên ngành Toán tin, Công nghệ thông tin, Điện tử, Viễn thông, Khoa học máy tính, An ninh mạng, An toàn thông tin, Kỹ thuật phần mềm, Hệ thống thông tin. - Có đồng thời các chứng chỉ Certified Information Systems Security Professional (CISSP), GIAC Web Application Penetration Tester (GWAPT), GIAC Certified Incident Handler Certification (GCIH), Certified Ethical Hacker (CEH) hoặc tương đương. - Có công bố phát hiện tối thiểu 01 lỗ hổng bảo mật CVE cho các sản phẩm uy tín trên thế giới.
2	Chuyên gia cao cấp đánh giá an toàn thông tin	06	≥ 10 năm bậc đại học	- Tốt nghiệp các chuyên ngành Toán tin, Công nghệ thông tin, Điện tử, Viễn thông, Khoa học máy tính, An ninh mạng, An toàn thông tin, Kỹ thuật phần mềm, Hệ thống thông tin.
3	Chuyên gia đánh	11	≥ 05 năm bậc đại	- Tốt nghiệp các chuyên ngành Toán tin, Công nghệ thông tin,

STT	Nội dung	Số lượng (người)	Số năm kinh nghiệm	Bằng cấp liên quan
	giá an toàn thông tin		học	Điện tử, Viễn thông, Khoa học máy tính, An ninh mạng, An toàn thông tin, Kỹ thuật phần mềm, Hệ thống thông tin.
4	Chuyên viên đánh giá an toàn thông tin	22	≥ 03 năm bậc đại học	- Tốt nghiệp các chuyên ngành Toán tin, Công nghệ thông tin, Điện tử, Viễn thông, Khoa học máy tính, An ninh mạng, An toàn thông tin, Kỹ thuật phần mềm, Hệ thống thông tin.
	Tổng cộng	**40**		

3.2.4.2. Yêu cầu về chất lượng Dịch vụ kiểm tra, đánh giá an toàn thông tin

- Sau khi kết thúc quá trình đánh giá nhà cung cấp có trách nhiệm thông báo cho đơn vị vận hành hệ thống thông tin biết và bàn giao tài liệu, trang thiết bị sử dụng (nếu có) trong quá trình kiểm tra.
- Báo cáo tổng hợp tất cả các lỗ hổng đã phát hiện được, phân loại theo mức độ nghiêm trọng, mô tả chi tiết về lỗ hổng, cách thức đã dùng để khai thác, phân tích nguyên nhân.
- Các khuyến nghị, giải pháp, hướng dẫn khắc phục ghi rõ hoặc tham chiếu tới tài liệu của các nhà sản xuất, công ty bảo mật.
- Đơn vị chủ trì đánh giá có trách nhiệm dự thảo Báo cáo đánh giá, gửi cho đơn vị vận hành hệ thống thông tin để lấy ý kiến. Trong thời hạn 05 ngày kể từ ngày nhận được dự thảo Báo cáo đánh giá, đơn vị vận hành hệ thống thông tin có trách nhiệm có ý kiến đối với các nội dung dự thảo.
- Trên cơ sở dự thảo Báo cáo đánh giá, ý kiến của đơn vị vận hành hệ thống thông tin, đơn vị chủ trì đánh giá hoàn thiện Báo cáo đánh giá, gửi đơn vị vận hành và chủ quản hệ thống thông tin.
- Thực hiện công tác bảo đảm an toàn cho dữ liệu liên quan đến hệ thống được đánh giá, không công bố dữ liệu liên quan khi chưa được sự đồng ý của chủ quản hệ thống thông tin.

3.2.4.3. Yêu cầu về kỹ thuật, công nghệ, phạm vi công việc để đáp ứng yêu cầu chất lượng dịch vụ kiểm tra, đánh giá an toàn thông tin

a) Kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ

Kiểm tra, đánh giá an toàn thông tin theo các nội dung được quy định tại Điều 11, 12 Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-

CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ:

Kiểm tra, đánh giá tuân thủ đối với đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin.

Kiểm tra, đánh giá tuân thủ đối với đơn vị vận hành.

Kiểm tra, đánh giá việc tổ chức thực thi các biện pháp bảo đảm an toàn thông tin.

b) Kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin được phê duyệt

Kiểm tra tính đầy đủ và phù hợp của Quy chế bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin về quản lý được phê duyệt.

Đánh giá việc tuân thủ các quy định, quy trình trong Quy chế bảo đảm an toàn thông tin trong quá trình vận hành, khai thác, kết thúc hoặc hủy bỏ hệ thống thông tin.

Đánh giá việc thiết kế hệ thống theo phương án bảo đảm an toàn thông tin được phê duyệt.

Đánh giá việc thiết lập, cấu hình hệ thống theo phương án bảo đảm an toàn thông tin được phê duyệt.

Kiểm tra việc cấu hình, tăng cường bảo mật cho thiết bị hệ thống, hệ điều hành, ứng dụng, cơ sở dữ liệu và các thành phần khác liên quan trong hệ thống theo hướng dẫn.

c) Kiểm tra đánh giá an toàn thông tin cho các ứng dụng

Bằng các kỹ thuật nghiệp vụ và hỗ trợ bởi các công cụ, việc đánh giá sẽ phát hiện:

Các lỗ hổng bảo mật xuất hiện trong ứng dụng do việc lập trình không tốt hoặc luồng hoạt động không đảm bảo tính an toàn.

Các lỗ hổng bảo mật đã/chưa được công bố trên toàn cầu liên quan đến thư viện hoặc các chức năng có thể ảnh hưởng đến ứng dụng.

Các nhóm đánh giá cho ứng web bao gồm:

- Thăm dò, thu thập thông tin
- Kiểm tra quản lý cấu hình & triển khai
- Kiểm tra quản lý định danh
- Kiểm tra xác thực
- Kiểm tra phân quyền
- Kiểm tra quản lý phiên
- Kiểm tra sàng lọc dữ liệu đầu vào
- Kiểm tra cơ chế xử lý lỗi
- Kiểm tra thuật toán mã hóa
- Kiểm tra logic nghiệp vụ
- Kiểm tra xử lý phía người dùng

d) Kiểm tra đánh giá an toàn thông tin cho máy chủ

Thu thập thông tin máy chủ: Địa chỉ IP và địa chỉ MAC của máy chủ; Thông tin về hệ điều hành, phiên bản và cấu hình hệ thống;

Thực hiện kiểm tra, rà soát lỗ hổng, điểm yếu, cấu hình của máy chủ

Xác định các bản vá bảo mật chưa được áp dụng và kiểm tra khả năng cập nhật của hệ thống

Kiểm tra thông tin về các tiến trình đang thực thi

Kiểm tra các cổng kết nối, các dịch vụ, các chính sách thiết lập trên máy chủ.

e) Kiểm tra đánh giá an toàn thông tin cho các thiết bị mạng

Thu thập thông tin thiết bị: địa chỉ IP, địa chỉ MAC, nhận dạng thiết bị mạng: Router, Firewall, Switch

Thực hiện rà soát, kiểm tra hệ thống mạng, phát hiện các dịch vụ đang mở của các thiết bị, giao thức mạng truyền tải trên hệ thống được coi là các điểm yếu.

Kiểm tra, rà soát lỗ hổng của dịch vụ kết hợp với kiểm tra, đánh giá thủ công đảm bảo phát hiện tốt đa các lỗ hổng, vấn đề về an toàn thông tin tồn tại trên thiết bị

Kiểm tra tập các cấu hình, các luật cấu hình, kiểm tra các chức năng liên quan tới xác thực và phân quyền.

3.2.4.4. Yêu cầu về an toàn bảo mật thông tin, dữ liệu và các yêu cầu khác của TP.HCM

Các yêu cầu về an ninh bảo mật, an toàn mạng lưới, thông tin, dữ liệu liên quan tới hạng mục thuê dịch vụ được thực hiện tuân thủ theo quy định về an toàn, an ninh, bảo mật trong các văn bản pháp luật liên quan bao gồm: Luật Công nghệ thông tin số 67/2006/QH11 ngày 29/6/2006 của Quốc hội khóa XI; Luật Giao dịch điện tử số 51/2005/QH11 ngày 29/11/2005 của Quốc hội khóa XI; Luật Viễn thông số 41/2009/QH12 ngày 23/11/2009 của Quốc hội khoá XII.

Bởi vì đây là hạng mục thuê dịch vụ thuộc lĩnh vực công nghệ thông tin nhằm phục vụ cho hoạt động của các cơ quan quản lý nhà nước, cho nên cần phải được kiểm soát chặt chẽ và đặc biệt là phải có sự ràng buộc đối với các cán bộ của nhà cung cấp dịch vụ cũng như nhà cung cấp dịch vụ trong việc cấu trúc mạng lưới, các giải pháp kỹ thuật công nghệ, giải pháp an toàn, an ninh, bảo mật và các vấn đề khác có liên quan.

Trong quá trình cung cấp dịch vụ, Nhà cung cấp dịch vụ phải tuân thủ nghiêm ngặt các quy trình vận hành, cài đặt ứng dụng; quy chế khai thác, sử dụng hệ thống của TP.HCM. Xây dựng nội quy bảo mật thông tin, dữ liệu chặt chẽ dựa trên các tiêu chí sau đây:

- Mỗi người sử dụng hợp pháp chỉ được truy cập vào hệ thống theo thẩm quyền thông qua quyền được cấp và mã nhận dạng trên mạng cục bộ cũng như đối với truy cập từ xa.
- Mỗi người dùng phải chịu trách nhiệm về nội dung dữ liệu do mình cập nhật, xử lý, bộ phận dữ liệu nào thì chỉ được phép sửa đổi, chỉnh lý phần dữ liệu đó.
- Không được mang các vật mang tin (như đĩa mềm, USB, …) vào/ra nơi đặt máy chủ, thiết bị CNTT.

- Thực hiện đúng các cam kết với Chủ trì thuê dịch vụ về bảo đảm an toàn, an ninh thông tin.
- Xây dựng một số biện pháp rõ ràng để phản ứng trước các tình huống có thể xảy ra đối với hệ thống.
- Cam kết tuân thủ, bảo mật thông tin và quyền sở hữu trí tuệ hệ thống CNTT đảm bảo an toàn thông tin cho hệ thống CNTT của TP.HCM.

3.2.4.5. Yêu cầu về giám sát chất lượng dịch vụ

Phòng PA05 – Công an Thành Phố Hồ Chí Minh:

- Thực hiện giám sát các nhà cung cấp dịch vụ theo đúng các quy định của hợp đồng thuê dịch vụ.
- Thực hiện đánh giá các báo cáo định kỳ và đột xuất, phối hợp với nhà cung cấp dịch vụ trong việc xử lý các sự cố.
- Chịu trách nhiệm giám sát nhằm đảm bảo không lộ lọt, thất thoát thông tin về phạm vi thực hiện và quy mô của dự án.
- Chịu trách nhiệm về chất lượng dịch vụ của nhà cung cấp dịch vụ
- Nhà cung cấp dịch vụ kiểm tra, đánh giá an toàn thông tin:
- Báo cáo kết quả đánh giá chi tiết các phương pháp và kỹ thuật được sử dụng trong quá trình thực hiện dịch vụ.
- Báo cáo kết quả đánh giá hồ sơ cấp độ đối với các hệ thống mục tiêu

3.2.5. Hạng mục: Rà quét, bóc tách mã độc tại các cơ quan đơn vị trên địa bàn Thành phố

3.2.5.1. Yêu cầu năng lực, kinh nghiệm

a) Yêu cầu về kinh nghiệm, năng lực tổ chức:

Có Trung tâm SOC tại TPHCM và cam kết cử nhân sự onsite phối hợp ứng phó sự cố ATTT trong vòng 02 giờ.

Nhà cung cấp dịch vụ phải có chứng chỉ ISO 27001 về tiêu chuẩn quản lý an toàn thông tin còn hiệu lực.

Nhà cung cấp dịch vụ phải có giấy phép kinh doanh dịch vụ an ninh thông tin còn hiệu lực

b) Yêu cầu đối với đội ngũ chuyên gia:

STT	Nội dung	Số lượng (người)	Số năm kinh nghiệm	Bằng cấp liên quan
1	Chuyên gia phân tích chuyên sâu mã độc	01	≥ 10 năm bậc đại học	- Tốt nghiệp các chuyên ngành Toán tin, Công nghệ thông tin, Điện tử, Viễn thông, Khoa học máy tính, An ninh mạng, An toàn thông tin, Kỹ thuật phần mềm, Hệ thống thông tin.

STT	Nội dung	Số lượng (người)	Số năm kinh nghiệm	Bằng cấp liên quan
2	Chuyên gia phân tích các dấu hiệu, hành vi mã độc	01	≥ 05 năm bậc đại học	- Tốt nghiệp các chuyên ngành Toán tin, Công nghệ thông tin, Điện tử, Viễn thông, Khoa học máy tính, An ninh mạng, An toàn thông tin, Kỹ thuật phần mềm, Hệ thống thông tin. - Có đồng thời các chứng chỉ eLearnSecurity Certified Threat Hunting Professional (eCTHP), Certified Ethical Hacker (CEH), Certified SOC Analyst (CSA) hoặc tương đương. - Có công bố phát hiện tối thiểu 01 lỗ hổng bảo mật CVE cho các sản phẩm uy tín trên thế giới.
3	Chuyên gia triển khai rà quét	03	≥ 03 năm bậc đại học	- Tốt nghiệp các chuyên ngành Toán tin, Công nghệ thông tin, Điện tử, Viễn thông, Khoa học máy tính, An ninh mạng, An toàn thông tin, Kỹ thuật phần mềm, Hệ thống thông tin.
	Tổng cộng	**05**		

3.2.5.2. Xác định yêu cầu về chất lượng dịch vụ

- Báo cáo tổng hợp tất cả các mã độc đã phát hiện được, phân loại theo mức độ nghiêm trọng, mô tả chi tiết về lỗ hổng, cách thức đã dùng để khai thác, phân tích nguyên nhân.
- Các khuyến nghị, giải pháp, hướng dẫn khắc phục, bóc tách mã độc ghi rõ hoặc tham chiếu.
- Thực hiện công tác bảo đảm an toàn cho dữ liệu liên quan đến hệ thống được rà quét.
- Việc rà quét phát hiện mã độc phải bảo đảm không ảnh hưởng đến hoạt động bình thường của hệ thống.
- Báo cáo rà quét mã độc phải bao gồm các chi tiết về mã độc và hướng dẫn khắc phục, biện pháp khắc phục thay thế, cũng như minh chứng về việc khai thác thành công.

3.2.5.3. Yêu cầu về kỹ thuật, công nghệ để đáp ứng yêu cầu chất lượng dịch vụ

a) Yêu cầu chung

Giải pháp rà quét và bóc tách mã độc được thiết kế với hiệu năng cao, khả năng xử lý linh hoạt và đáp ứng tiêu chuẩn cao, cụ thể như sau:

- Hiệu năng xử lý mạnh mẽ, có khả năng phân tích và giám sát lưu lượng mạng từ 500 Mbps đến 10 Gbps, phù hợp với hạ tầng mạng quy mô lớn của các cơ quan nhà nước.
- Tích hợp công nghệ Trí tuệ nhân tạo (AI) và Machine Learning, cho phép phát hiện và nhận diện chính xác các hành vi mã độc ẩn sâu trong lưu lượng mạng, bao gồm cả các máy chủ điều khiển C&C được sinh ra theo thuật toán (algorithm-based C2) – giúp nâng cao đáng kể hiệu quả phát hiện so với các phương pháp truyền thống.
- Triển khai hoàn toàn trong môi trường mạng nội bộ (Metronet), hoạt động offline, tách biệt hoàn toàn với Internet bên ngoài, đảm bảo tính bảo mật tuyệt đối cho dữ liệu giám sát và phân tích.
- Hỗ trợ nhận diện và kiểm tra hơn 1.200 giao thức mạng, bao quát hầu hết các dịch vụ và ứng dụng phổ biến, từ đó tăng độ chính xác trong việc phân tích hành vi và bóc tách mã độc.
- Ứng dụng khung tiêu chuẩn MITRE ATT&CK trong việc xác định và phân loại các hành vi tấn công, giúp nhận diện chính xác các kỹ thuật mà mã độc đang sử dụng để lây lan hoặc duy trì hiện diện trong hệ thống.
- Áp dụng phương pháp giám sát "non-invasive", triển khai ở chế độ TAP/SPAN, không cài agent, không thay đổi cấu hình mạng hiện hữu và không gây gián đoạn hoạt động của hệ thống trong quá trình rà quét.
- Tuân thủ các tiêu chuẩn và khung hướng dẫn quốc tế, bao gồm TCVN 14423:2025 về hệ thống thông tin quan trọng, NIST Cybersecurity Framework, và MITRE ATT&CK Framework, đảm bảo tính tương thích, minh bạch và hiệu quả trong triển khai

b) Mô hình triển khai

Quản lý Trung tâm – Core Server tại Trung tâm Dữ liệu (TTDL):

- Được triển khai tại hạ tầng Trung tâm Dữ liệu Thành phố, đóng vai trò bộ điều hành và phân tích tập trung của toàn hệ thống. Cấu hình phần cứng: CPU 96 cores, RAM 512 GB, Storage gồm 2 TB SSD tốc độ cao và 8 TB HDD dung lượng lớn.

Chức năng, nhiệm vụ:

- Tổng hợp dữ liệu và hiển thị Dashboard tập trung từ 15 đơn vị giám sát.
- Quản lý cấu hình hệ thống, đồng bộ chính sách và cập nhật cơ sở dữ liệu nhận diện mã độc.
- Thực hiện tổng hợp báo cáo, thống kê và phân tích xu hướng toàn hệ thống, hỗ trợ công tác điều hành và ra quyết định của đơn vị quản lý an toàn thông tin cấp Thành phố.

Đơn vị – Thiết bị phân tích Sensor:

- Được triển khai trực tiếp tại 15 cơ quan, đơn vị, đóng vai trò nút phân tích độc lập nhằm giám sát, nhận diện và bóc tách mã độc tại chỗ. Cấu hình phần cứng:

CPU 24 cores, RAM 96 GB, Storage 1 TB SSD và 8 TB HDD, trang bị hai cổng mạng (NIC) 1 Gbps đảm bảo hiệu năng xử lý lưu lượng lớn và ổn định.

Năng lực xử lý chính:

- Phân tích gói tin chuyên sâu (Deep Packet Inspection – DPI) tại điểm đầu mạng (edge).
- Tích hợp bộ máy học và trí tuệ nhân tạo (ML/AI Engine) để tự động nhận diện hành vi bất thường.
- Phát hiện các hành vi tấn công mạng tiên tiến, bao gồm C&C Communication, Network Behavior Analysis, Lateral Movement Detection và Network Scanning.

3.2.5.4. Yêu cầu về phạm vi công việc

STT	Công việc	Nội dung cần thực hiện
1	Thực hiện rà soát mã độc qua luồng mạng ở các Sở trên địa bàn	Hệ thống được triển khai tại 15 đơn vị, với kế hoạch mỗi đơn vị thực hiện rà soát trong vòng 10 ngày, bao gồm thu thập dữ liệu, phân tích, và hoàn thành báo cáo đánh giá chi tiết về tình trạng an toàn thông tin Trong thời gian triển khai, hệ thống sẽ theo dõi, phát hiện và phân tích các dấu hiệu lây nhiễm mã độc, đồng thời lập báo cáo kết quả và đề xuất biện pháp bóc gỡ, xử lý triệt để Quá trình thực hiện không gây ảnh hưởng đến hoạt động của hệ thống CNTT hiện hữu, không thay đổi kiến trúc mạng, không cài đặt phần mềm hoặc agent trên máy tính của đơn vị.
2	Phương án xử lý mã độc	Thực hiện ngắt kết nối và cô lập tạm thời các thiết bị đầu cuối được xác định có dấu hiệu nhiễm mã độc theo kết quả phân tích và báo cáo kỹ thuật Kiểm tra tình trạng hoạt động, phiên bản và mức độ cập nhật của các phần mềm phòng chống mã độc đang được cài đặt trên thiết bị Sao lưu dữ liệu quan trọng, tiến hành cài đặt lại hệ điều hành và cấu hình phần mềm phòng chống mã độc mới Căn cứ kết quả phân tích, xây dựng và triển khai biện pháp bóc tách, làm sạch mã độc triệt để Thu thập, lưu trữ và chuẩn hóa toàn bộ dữ liệu, nhật ký xử lý và báo cáo chi tiết để phục vụ đánh giá, tổng kết
3	Báo cáo	Tóm tắt thông tin đơn vị đang rà soát; Thống kê và mô tả chi tiết các mã độc được phát hiện (nếu có) theo từng thiết bị đầu cuối

STT	Công việc	Nội dung cần thực hiện
		Phương án và kết quả xử lý (nếu có). Khuyến nghị phương án tăng cường Thống kê các rủi ro bảo mật theo mức độ nghiêm trọng/cao/trung bình/thấp Khuyến nghị cách thức khắc phục trong hệ thống.

3.2.5.5. Yêu cầu về an toàn bảo mật thông tin, dữ liệu

Bởi vì đây là hạng mục thuê dịch vụ thuộc lĩnh vực công nghệ thông tin nhằm phục vụ cho hoạt động của các cơ quan quản lý nhà nước, cho nên cần phải được kiểm soát chặt chẽ và đặc biệt là phải có sự ràng buộc đối với các cán bộ của nhà cung cấp dịch vụ cũng như nhà cung cấp dịch vụ trong việc cấu trúc mạng lưới, các giải pháp kỹ thuật công nghệ, giải pháp an toàn, an ninh, bảo mật và các vấn đề khác có liên quan.

Trong quá trình cung cấp dịch vụ, Nhà thầu phải tuân thủ nghiêm ngặt các quy trình vận hành, cài đặt ứng dụng; quy chế khai thác, sử dụng hệ thống của Thành phố. Đảm bảo bảo mật thông tin, dữ liệu chặt chẽ dựa trên các tiêu chí sau đây:

- Mỗi người sử dụng hợp pháp chỉ được truy cập vào hệ thống theo thẩm quyền thông qua quyền được cấp và mã nhận dạng trên mạng cục bộ cũng như đối với truy cập từ xa.
- Mỗi người dùng phải chịu trách nhiệm về nội dung dữ liệu do mình cập nhật, xử lý, bộ phận dữ liệu nào thì chỉ được phép sửa đổi, chỉnh lý phần dữ liệu đó.
- Dữ liệu cần phải được sao lưu và cất giữ theo quy chế bảo mật. Nên sử dụng các thiết bị công nghệ thông tin có độ tin cậy, chất lượng cao.
- Không được mang các vật mang tin (như đĩa mềm, USB, …) vào/ra nơi đặt máy chủ, thiết bị CNTT.
- Thực hiện đúng các cam kết về bảo đảm an toàn, an ninh thông tin.
- Xây dựng một số biện pháp rõ ràng để phản ứng trước các tình huống có thể xảy ra đối với hệ thống.

3.2.5.6. Yêu cầu đối với phần cứng, trang thiết bị

STT	Nội dung	Mô tả yêu cầu	Số lượng	Ghi chú
I	Tại Trung tâm dữ liệu thành phố			
1	Máy chủ	Máy chủ để cài đặt hệ thống rà quét, bóc tách mã độc tại nhà cung cấp có cấu hình tối thiểu: 96 core CPU, 512 GB RAM, 2 TB SSD 8TB HDD.	1	
2	Phần mềm	Bản quyền phần mềm phân tích mạng, rà quét mã độc, bóc tách mã độc	1	
II	Tại cơ quan, đơn vị			

STT	Nội dung	Mô tả yêu cầu	Số lượng	Ghi chú
1	Thiết bị	Thiết bị để cài đặt hệ thống thu thập thông tin rà quét, bóc tách mã độc tại Đơn vị có cấu hình tối thiểu: 24 core CPU, 96 GB RAM, 1 TB SSD 8TB HDD, 02 NIC (card mạng)	15	
2	Phần mềm	Bản quyền phần mềm phân tích mạng, rà quét mã độc, bóc tách mã độc	15	

3.3. Yêu cầu về phương án, cách thức, điều kiện triển khai

3.3.1. Phương án triển khai tổ chức kiểm tra, đánh giá an toàn thông tin và tổ chức diễn tập thực chiến bảo đảm an toàn thông tin mạng năm 2025

3.3.1.1. Yêu cầu về công tác tổ chức diễn tập thực chiến

3.3.1.1.1. Công tác tổ chức

STT	Nội dung	Mô tả yêu cầu
1	Địa điểm tổ chức	Tại Thành phố Hồ Chí Minh
2	Hội trường	- Hội trường diện tích tối thiểu 28m x 14,8m sức chứa 200 - 300 khách tổ chức. - Bố trí bàn ghế, bục phát biểu, sân khấu. - Bố trí âm thanh, ánh sáng. - Phục vụ cho ngày khai mạc, bế mạc và các ngày tổ chức đào tạo, tập huấn.
3	Màn hình LED/màn hình trình chiếu	- Màn hình LED trong hội trường dùng để trình chiếu nội dung của diễn tập và nội dung trình bày của các chuyên gia. Quy chuẩn màn hình có kích thước tối thiểu 3m x 6,4 m; độ nét tối phiểu P2.5. - 02 Màn hình LED cổng chào ngoài trời xuyên suốt 1 tuần diễn ra chương trình: + Kích thước mỗi màn hình Led: 3840 x 5760mm hoặc 960 x 1440 pix (tương đương 3,840m x 5,760m = 22m2). + Khung giờ phát từ 7h30 – 17h30 - 10 màn hình LED đặt khu vực diễn ra sự kiện xuyên suốt 1 tuần: + Kích thước: 2560 x 1600mm hoặc 640 x 400 pix + Khung giờ phát từ 7h30 – 17h30

STT	Nội dung	Mô tả yêu cầu
4	Trang trí Hội trường, sảnh đón khách	Thiết kế và in ấn: - 01 Cổng chào - 01 Băng rôn - 01 Backdrop - 04 Standee (bao gồm khung đứng) - 02 Standee điện tử Hoa trang trí: - Giỏ hoa: dùng để bàn tiếp tân, bục phát biểu, hoa bàn đại biểu/ khách VIP. - Hoa tặng cho đơn vị tham dự. - Loại hoa: Hoa hồng, hoa hướng dương, Hoa loa kèn, Hoa đồng tiền, hoa cẩm chướng, hoa ly. Phòng VIP phục vụ tiếp khách, hội nghị quy mô không quá 20 người
5	Trang trí khu vực chụp hình, phỏng vấn báo chí đài truyền hình	In hiflex, căng khung sắt kích thước tối thiểu cao 2.7m x ngang 5.7m
6	Xây dựng kịch bản, dựng clip phóng sự về tình hình, thực trạng an ninh thông tin và tổng kết giai đoạn của chuỗi sự kiện	- Nội dung Clip là phóng sự toàn bộ quá trình từ khai mạc đến kết thúc Diễn tập với thời lượng biên tập từ 10 đến 15 phút. - Thời gian bàn giao sản phẩm sau 07 ngày làm việc kể từ ngày kết thúc Diễn tập.
7	Truyền thông sự kiện	Thông cáo báo chí. Mời cơ quan báo chí, thông tấn đến đưa tin sự kiện.
8	Người dẫn chương trình	- Giọng nói: từ tốn, rõ chữ. - Ngoại hình: duyên dáng, thanh lịch. - Có kiến thức về công nghệ thông tin; có khả năng khai thác đề tài và sử dụng ngôn từ khi dẫn chương trình. - Có khả năng diễn đạt cảm xúc theo vấn đề, tạo được cảm xúc cho khách mời tham dự.
9	Tea break	Phục vụ nước uống và giải khát giữa giờ cho các Học viên, khách mời, các chuyên gia và

STT	Nội dung	Mô tả yêu cầu
		Ban tổ chức trong suốt thời gian của sự kiện diễn tập.
10	Tài liệu, văn phòng phẩm	In tài liệu đào tạo, tập huấn. In giấy chứng nhận học viên. Văn phòng phẩm: bút, viết, giấy photo... In ấn bảng tên và dây đeo thẻ. Áo đồng phục. In giấy chứng nhận các đội tham gia.

3.3.1.1.1.1. Công tác chuẩn bị

STT	Phân công nhiệm vụ	Phụ trách chính	Phối hợp	Tiến độ hoàn thành	Ghi chú
I	**GIAI ĐOẠN CHUẨN BỊ**				
1	**Hồ sơ, thủ tục**				
1.1	Xác định mục tiêu, kịch bản diễn tập	CATP			
1.2	Lập dự toán	CATP			
1.3	Trình phê duyệt dự toán	CATP			
1.4	Lập hồ sơ mời thầu, tổ chức đấu thầu	CATP			
1.5	Phê duyệt kết quả lựa chọn nhà thầu, tiến hành ký kết Hợp đồng	CATP			
2	**Nội dung diễn tập**				
2.1	Lập quyết định thành lập BTC, Ban Giám khảo	CATP			Chọn hệ thống thực chiến, thống nhất kịch bản
2.2	Lập thể lệ, nội dung, kịch bản diễn tập	CATP			

STT	Phân công nhiệm vụ	Phụ trách chính	Phối hợp	Tiến độ hoàn thành	Ghi chú
2.3	Chọn đội tấn công (redteam), đội phòng thủ (blueteam)	CATP			
3	**Ban giám khảo, blueteam, redteam**				
3.1	Mời Ban giám khảo và trao đổi nội dung công việc cụ thể	CATP			
3.2	Mời đội tấn công và trao đổi nội dung công việc cụ thể	CATP			
3.3	Thông báo đội phòng thủ và trao đổi nội dung công việc cụ thể	CATP			
II	**GIAI ĐOẠN TRIỂN KHAI**				
1	**Lập Danh sách và mời tham dự**				
1.1	Mời Lãnh đạo, BGK, chuyên gia tham dự khai mạc và bế mạc	CATP			
1.2	Gửi công văn mời học viên là cán bộ phụ trách CNTT Sở Ban ngành, phường xã tham dự	CATP			
2	**Công tác chuẩn bị hậu cần**				
2.1	Thiết kế và gửi CĐT phê duyệt cổng chào, backdrop, standee, thẻ đeo	NCC dịch vụ	CATP		
2.2	Soạn thảo và gửi CĐT phê duyệt TCBC, MC Script, agenda chương trình, thông cáo báo chí	NCC dịch vụ	CATP		
2.3	Tiến hành triển khai, thi công các hạng mục trong Hợp đồng	NCC dịch vụ			
3	**Công tác chuẩn bị cho chương trình khai mạc và bế mạc**				
3.1	Gửi DS khách mời, DS học viên để checkin	CATP			

STT	Phân công nhiệm vụ	Phụ trách chính	Phối hợp	Tiến độ hoàn thành	Ghi chú
3.2	Gửi DS khách VIP để NCC chuẩn bị bảng tên	CATP			
3.3	Tổng kết và chuẩn bị kết quả diễn tập	CATP			
3.4	Báo cáo kết quả diễn tập vào ngày bế mạc	CATP			
3.5	Tổng kết, tặng hoa cho BGK, chuyên gia, và trao giải cho các đội tham dự	CATP			
3.6	Soạn thảo và gửi CĐT phê duyệt TCBC ngày bế mạc	NCC dịch vụ	CATP		
III	**GIAI ĐOẠN NGHIỆM THU**				
1	Nghiệm thu kết quả thực hiện gói thầu	NCC dịch vụ	CATP		
2	Hoàn tất các hồ sơ nghiệm thu, thanh toán	NCC dịch vụ	CATP		
3	Nghiệm thu - Thanh toán	CATP	NCC dịch vụ		

3.3.1.1.1.2. Công tác đào tạo, tập huấn

3.3.1.1.1.2.1. Nội dung yêu cầu

STT	Nội dung	Thời gian
I	**Chủ đề trình bày**	
1	- Tình hình ATTT: Bức tranh ATTT thế giới, Việt Nam trong năm 2025; - Xu hướng tấn công mạng cho năm 2025, các case study tấn công và phòng thủ.	01 ngày

STT	Nội dung	Thời gian
2	- Đào tạo cấp độ ATTT: phân biệt cấp độ, các phương án đảm bảo ATTT đối với cấp độ 2 và 3.	
II	**Thực hành**	
	Kịch bản 1: Tác chiến phòng chống tấn công APT sử dụng kỹ thuật Living-off-the-Land Mục tiêu: Hướng dẫn học viên cách nhận biết và ứng phó với kiểu tấn công mà hacker không dùng virus, chỉ dùng các công cụ có sẵn trên Windows như PowerShell, WMI, các lệnh tương tác network. Đây là kiểu tấn công ẩn mình rất tốt, khó bị phần mềm diệt virus phát hiện. Môi trường diễn tập: Tạo ra mạng lưới ảo gồm (sử dụng cho các kịch bản khác): Mạng DMZ (chứa web/email server) Mạng nội bộ (máy tính người dùng, file server) Mạng quản lý (hệ thống giám sát như SIEM) Có các máy ảo đóng vai nhiều vai trò: Domain Controller, File Server, Workstation, Mail Server, máy tấn công (C2), máy giám sát (SIEM). Các bước tấn công của chuyên gia thao trường: Bước 1: Thu thập thông tin về tổ chức, nhân viên (Reconnaissance). Bước 2: Tạo file Excel có mã độc, gửi email giả mạo IT tới người dùng, dụ họ mở file và bật macro. Bước 3: Khi người dùng mở file, mã độc sẽ chạy qua PowerShell, kết nối về máy chủ C2 của hacker. Bước 4: Hacker chiếm quyền, cài đặt các tác vụ tự động (Scheduled Task) để duy trì sự kiểm soát. Bước 5: Tìm kiếm mật khẩu, thông tin nhạy cảm trên máy bị chiếm quyền, leo thang đặc quyền nếu có thể. Bước 6: Di chuyển sang các máy khác trong mạng (lateral movement) bằng kỹ thuật WMI hoặc các lệnh mạng. Bước 7: Thu thập, nén, mã hóa dữ liệu rồi gửi ra ngoài bằng cách upload lên dịch vụ cloud hợp pháp (trong môi trường diễn tập).	01 ngày

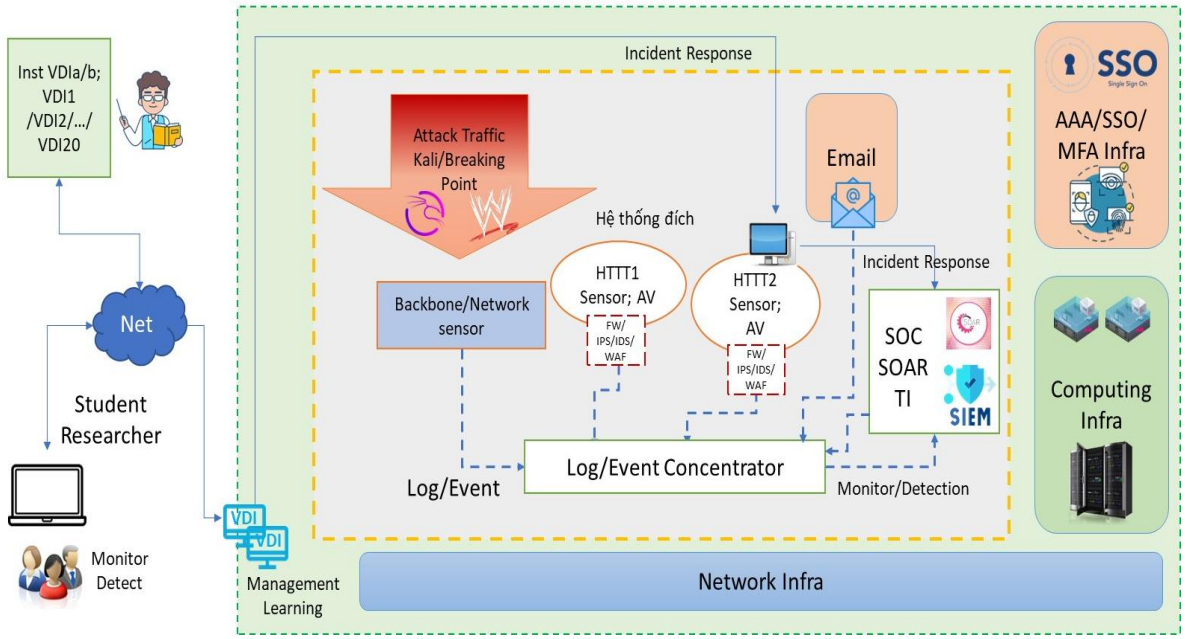
STT	Nội dung	Thời gian
	Cách phát hiện và phòng thủ của học viên: Cấu hình Sysmon/SIEM để ghi log và cảnh báo khi có dấu hiệu PowerShell đáng ngờ hoặc kết nối mạng lạ. Playbook ứng phó sự cố: Kiểm tra các process PowerShell đang chạy, xem lệnh nào bất thường. Kiểm tra các kết nối mạng của process PowerShell. Chặn địa chỉ IP của máy tấn công (C2). Vô hiệu hóa Scheduled Task lạ, dừng process PowerShell độc hại. Thu thập log để điều tra, kiểm tra dấu hiệu di chuyển ngang trong mạng.	
	Kịch bản 2: Tác chiến phòng chống tấn công phương thức cập nhật UltraVNC. Mục tiêu: Học viên sẽ được huấn luyện nhận biết, phát hiện và xử lý khi hacker giả mạo cập nhật phần mềm UltraVNC (phần mềm điều khiển máy tính từ xa), một phần mềm vốn rất quen thuộc trong doanh nghiệp. Mục tiêu là giúp học viên nhận ra các dấu hiệu bất thường khi update phần mềm, xây dựng quy trình kiểm tra cập nhật phần mềm an toàn. Môi trường diễn tập: Thiết lập mạng nội bộ mô phỏng công ty, có các máy tính của người dùng, máy chủ chạy UltraVNC, máy siêu giám sát (SIEM), máy giả lập hacker (Fake Update Server). Có router/firewall kiểm soát giao thông giữa các mạng. Máy của hacker sẽ đóng vai trò server cung cấp bản cập nhật UltraVNC giả mạo. Các bước tấn công của chuyên gia thao trường: Bước 1: Tìm hiểu cách UltraVNC kiểm tra và cập nhật phần mềm. Tạo ra một server giả mạo phiên bản cập nhật mới. Bước 2: Tiến hành tấn công DNS hoặc ARP để các máy nội bộ khi kiểm tra cập nhật sẽ trỏ tới server giả mạo thay vì trang chính hãng. Bước 3: Khi người dùng hoặc server UltraVNC kiểm tra cập nhật, sẽ tải về file cài đặt đã bị cài backdoor từ máy của hacker.	

STT	Nội dung	Thời gian
	Bước 4: Sau khi cài đặt, backdoor được kích hoạt, giúp hacker kiểm soát máy, thu thập mật khẩu, chụp màn hình, di chuyển sang các máy khác trong mạng. Bước 5: Hacker duy trì kết nối, tạo các tác vụ tự động để backdoor tự khởi động khi máy bật lên, tiếp tục kiểm soát và thu thập dữ liệu. Cách phát hiện và phòng thủ của học viên: Theo dõi DNS: Cảnh báo khi truy vấn tới uvnc.com trả về IP không thuộc về hãng UltraVNC. Giám sát file: Theo dõi sự thay đổi trong thư mục cài UltraVNC, kiểm tra hash của file mới để phát hiện thay đổi bất thường. Kiểm tra certificate: Đảm bảo kết nối tới server cập nhật dùng đúng chứng chỉ SSL của hãng. Xử lý sự cố: Chặn domain và IP đáng ngờ. Tìm và cô lập các máy bị nhiễm. Dừng và xóa dịch vụ lạ, file lạ. Cài lại phần mềm UltraVNC từ nguồn sạch, kiểm tra hash xác thực.	
	Kịch bản 3: Tác chiến phòng chống tấn công qua kết nối api giữa logistics và cổng thanh toán. Mục tiêu: Huấn luyện học viên phát hiện, xử lý các cuộc tấn công vào hệ thống kết nối giữa công ty vận chuyển (logistics) và cổng thanh toán (payment gateway). Giúp nhận biết các dấu hiệu bất thường liên quan đến xác thực, phân quyền, kiểm tra logic nghiệp vụ khi các hệ thống gọi API lẫn nhau. Môi trường diễn tập: Mô phỏng một hệ thống gồm nhiều máy chủ: API Gateway, Payment Gateway, Database, Portal cho đối tác, máy giám sát, máy của hacker... Các máy này chia thành các mạng riêng biệt: DMZ (public API), nội bộ (backend), partner (cổng thanh toán), quản lý (giám sát). Các bước tấn công của chuyên gia thao trường:	

STT	Nội dung	Thời gian
	Bước 1: Tìm hiểu các API công khai (API Discovery), dò quét các endpoint, tìm các file tài liệu API bị lộ (Swagger/OpenAPI). Bước 2: Khai thác xác thực yếu qua JWT (JSON Web Token) - thử các secret phổ biến, giả mạo token admin để truy cập chức năng nội bộ. Bước 3: Khai thác logic nghiệp vụ - ví dụ như thao túng loại tiền tệ, số lượng, trạng thái đơn hàng, qua đó chiếm đoạt hoặc gây thiệt hại tài chính. Bước 4: Tạo API key backdoor hoặc tiêm webhook độc (injection malicious webhook, có thể thực hiện được) để duy trì quyền kiểm soát hoặc liên tục thu thập dữ liệu. Bước 5: Truy cập dữ liệu của các đối tác khác, thu thập thông tin giá, đơn hàng, và dữ liệu nhạy cảm (vẫn qua API). Bước 6: Thao túng tài chính như tạo các giao dịch hoàn tiền hàng loạt, trì hoãn thanh toán cho nhà cung cấp... Bước 7: Thu thập và gửi dữ liệu ra ngoài qua webhook hoặc kênh ngầm (tunnel). Cách phát hiện và phòng thủ của học viên: Giới hạn tốc độ API (Rate Limiting): Ngăn chặn spam hoặc truy cập bất thường. Kiểm tra xác thực JWT: Dùng secret mạnh, thường xuyên xoay vòng (rotation), kiểm tra kỹ vai trò (role) trong token. Kiểm tra logic nghiệp vụ: Xác thực dữ liệu đầu vào, kiểm tra giá trị tiền tệ, số lượng, trạng thái... đảm bảo không bị thao túng. Giám sát và cảnh báo: Thiết lập các rule trong hệ thống giám sát để phát hiện hành vi bất thường, như role admin từ IP ngoài, nhiều giao dịch lạ... Phản ứng sự cố: Chặn IP nghi ngờ, thu hồi token, khoá tài khoản đối tác bị lộ, xoay vòng API key (rotation), thông báo cho các đối tác, lưu lại log phục vụ điều tra.	
	Thảo luận về các tình huống và bài học kinh nghiệm.	

3.3.1.1.1.2.2. Yêu cầu về thao trường thực hành

3.3.1.1.1.2.2.1. Thiết kế tổng quan



Hình 2: Kiến trúc Logic Lab & Cyber Range

Hạ tầng dịch vụ mạng:

Kết nối được vào Virtual Desktop Infrastructure (VDI), không cho phép kết nối trực tiếp từ endpoint tới các thành phần của Thao trường diễn tập.

Thao trường có ít nhất 2 đường kết nối internet. Đường thứ nhất để phục vụ cho giảng viên và học viên thực hiện kết nối vào thao trường và tra cứu thông tin trên môi trường internet trong quá trình diễn tập. Đường thứ hai là kết nối trực tiếp vào hệ thống thao trường để phục vụ cho các kịch bản diễn tập thông tin.

Hệ thống đích có giả lập với IP Public của Việt Nam, cụ thể là IP của Trung tâm dữ liệu Thành phố.

Mỗi máy chủ, hệ thống SOC có 2 cổng (interface) tách biệt, dành cho mục đích quản trị, thu thập logs và cho người dùng.

Hệ thống router ảo dành cho thao trường thực hành. Tất cả các tấn công/phòng thủ đều diễn ra ở đây. Xác thực (AAA), DNS, email,… đều kết nối thông qua hệ thống router ảo này.

Vai trò người dùng trong hệ thống:

Quản trị (Cyber Range Admin): là người phụ trách cấu hình và vận hành thao trường thực hành. Cyber Range Admin có toàn quyền trên hệ thống, từ các máy chủ phần cứng, hạ tầng ảo hóa mạng, máy chủ, máy trạm, Cyber SOC vùng cho thao trường thực hành.

Giảng viên (Instructor): là người đứng lớp huấn luyện, trợ giảng cũng là Instructor. Instructor có thông tin đăng nhập đến các hệ thống của Cyber Range, trừ phần cứng và vùng vCenter. Instructor là người giả lập tin tặc (hacker) và người dùng (victim).

Học viên (Student): là người tham gia đào tạo, tập huấn. Đối tượng này có thể giả lập thành người quản trị ATTT (Security Admin) trong thực tế; có các thông tin đăng nhập trên Cyber SOC, Collector, máy trạm của nạn nhân (giả định là nạn nhân để cung cấp thông tin đăng nhập trên máy chủ, máy trạm của nạn nhân nhằm được hỗ trợ).

Nạn nhân (Victim): là người dùng cuối. Instructor giả lập người dùng cuối để thực thi các click (nếu cần thiết) và gửi thông tin tới học viên để yêu cầu qua các kênh hỗ trợ: chat, phone, email,…

Hạ tầng VDI: Là hệ thống máy tính mà các đối tượng người sử dụng thao trường thực hành ở trên kết nối vào để từ đó kết nối quan các hệ thống khác. Người dùng thao trường thực hành sẽ kết nối đến máy chủ Vmware Horizon để sau đó nối tới các VDI tùy theo vai trò tham gia diễn tập.

Hệ thống VDI có liên kết và đồng bộ với hệ thống AD với domain (ví dụ hcr.vn)

Hệ thống sẽ chỉ cho học viên (trừ CR Admin) kết nối vào thao trường thực hành thông qua VDI.

Từ kiến trúc Cyber Range và nhu cầu huấn luyện thực tế, hệ thống thiết lập vùng mạng cho VDI tương ứng với 10 nhóm

Hạ tầng phát động tấn công: là tập hợp các máy tính (Kali Linux) để thực hiện tấn công. Thao trường tập huấn cho phép giảng viên bổ sung các thiết bị chuyên dụng để phát sinh các tấn công và lưu lượng nền trong các giai đoạn để có thể thực thi được nhiều loại hình tấn công khác nhau.

Các máy chủ C&C, website giả cũng nằm trong vùng hệ thống tấn công.

Sẽ có 10 máy Kali tương ứng với 10 Group độc lập với vùng IP giả lập trên môi trường Internet. Trong trường hợp này cả 10 Group đều sử dụng với 1 IP cho máy Kali Linux

Bên cạnh có hệ thống phát nhiễu (noise) dữ liệu để tăng độ khó trong phân tích, điều tra.

Hạ tầng mạng đích (target): là các hệ thống bị tấn công. Các hệ thống đích có thể có cấu hình khác nhau, từ đơn giản là một vài máy tính tới một mạng phức hợp như mạng máy tính của đơn vị.

Với hệ thống đích được xây dựng từ thực tế, có thể xem thao trường tập huấn tương tự như diễn tập thực chiến bằng cách sao chép nguyên trạng một hệ thống đích hoặc một mạng có chứa máy chủ đích.

Cyber Range đảm nhận huấn luyện xử lý sự cố nên có nhiều hệ thống đích khác nhau. Mỗi nhóm (Group) học viên sẽ có một hệ thống đích độc lập.

Hệ thống đích tấn công được phân hoạch vùng IP giả lập (vùng mạng HCM City và không tương tác trực tiếp với môi trường Internet).

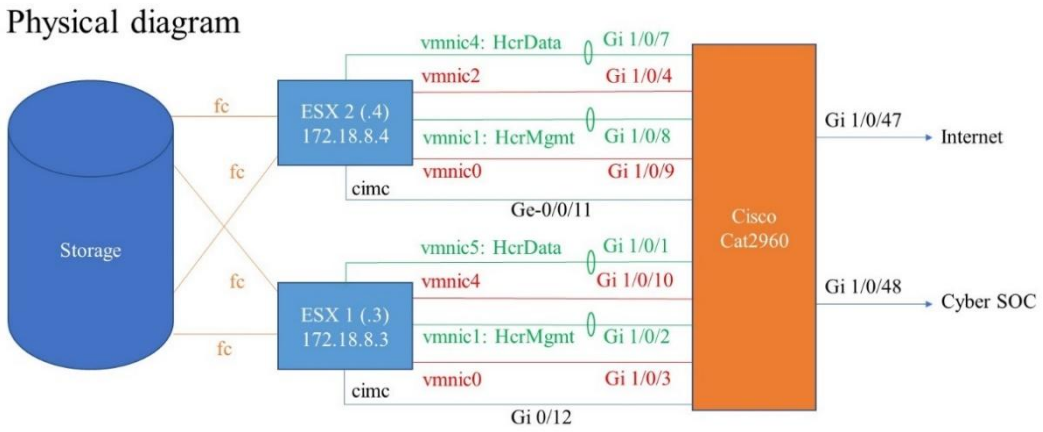
Hạ tầng Cyber SOC: Có 2 thành phần chính của hệ thống Cyber SOC:

Log Collector: là một máy tính trong Cyber Range chuyên nhận các log event từ tất cả các hệ thống thành phần của Cyber Range qua đường quản trị (mgmt)

Người dùng kết nối đến Cyber SOC để Detection/ Investigation/ Incident Response từ thiết bị máy tính của học viên/giảng viên qua hạ tầng mạng Internet

Kết nối giữa Log Collector và Cyber SOC được thực hiện qua mạng Mgmt của Cyber Range.

3.3.1.1.1.2.2.2. Thiết kế hạ tầng mạng



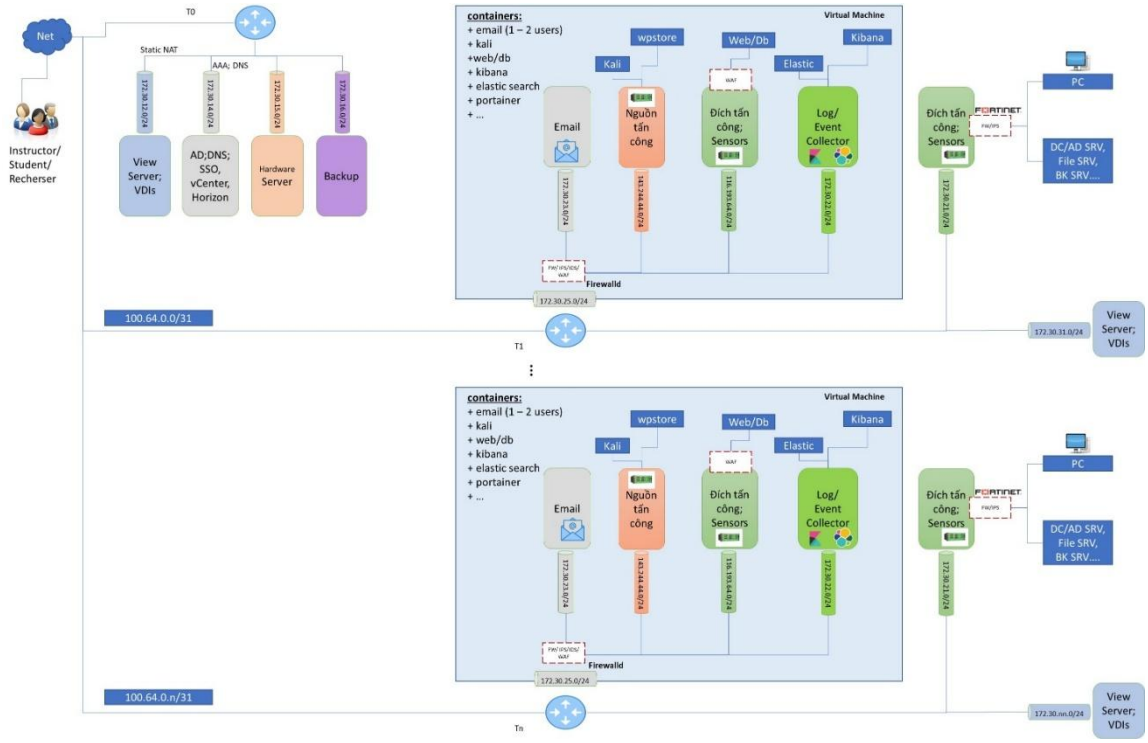
Hình 3: Mô hình hạ tầng mạng

Thiết kế đảm bảo dự phòng tối thiểu: có 2 host triển khai nền tảng ảo hóa

Có hệ thống lưu trữ tập trung để chứa các image: kịch bản, VDI, Kali….

Có 2 kết nối truy nhập internet: 1 cho quản trị, thu thập logs và 1 cho người dùng.

3.3.1.1.1.2.2.3. Thiết kế hệ thống tấn công, giám sát và xử lý sự cố

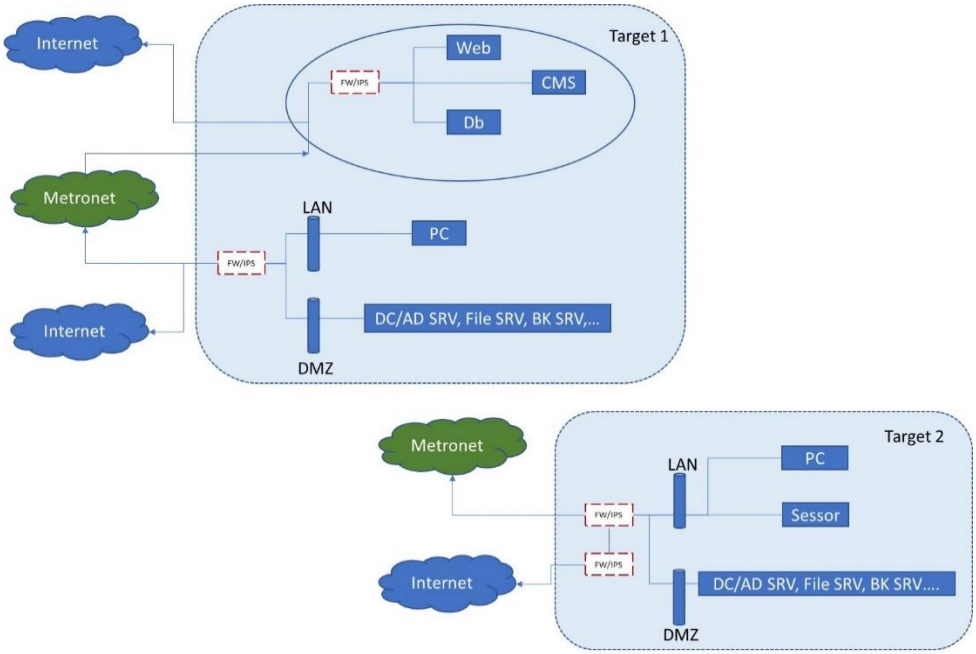


Hình 4: Mô hình cơ sở hệ thống tấn công, giám sát và xử lý sự cố

Các thành phần dùng chung như: quản lý hạ tầng ảo hóa, VDI, xác thực, sao lưu,… được triển khai tại tenant0.

Các nhóm huấn luyện cho học viên sẽ được thiết lập đồng bộ (thành phần tấn công, đích, SOC,….), đảm bảo thiết lập hoàn chỉnh cho 1 nhóm, sau đó thực hiện clone cho các nhóm còn lại, tương ứng với tenant1 đến tenant.

3.3.1.1.1.2.2.4. Thiết kế mạng đích



Hình 5: Mô hình mạng đích

Mạng đích mô phỏng hiện trạng thực tế hạ tầng ứng dụng của Thành phố được triển khai tại Trung tâm dữ liệu, cũng như hạ tầng mạng tại đơn vị.

Có thể mở rộng, bổ sung các thành phần thiết bị giả lập khác (none IT hoặc OT) có kết nối với hạ tầng mạng đơn vị. Ví dụ: camera, access control…

3.3.1.1.1.2.2.5. Kịch bản trong thao trường tập huấn

Kịch bản 1: Tác chiến phòng chống tấn công APT sử dụng kỹ thuật living-off-the-Land (hoặc tên gọi khác Malware-free)

Mục tiêu: Huấn luyện học viên đối phó với kiểu tấn công không dùng virus mà chỉ sử dụng các công cụ có sẵn của Windows như PowerShell, WMI.

Mô tả: Hacker gửi email giả mạo phòng IT với file Excel đính kèm có macro độc. Khi nhân viên mở file và bấm "Enable Content", macro chạy lệnh PowerShell ẩn để kết nối về máy chủ hacker. Điểm đặc biệt: không có virus nào được tải về máy, chỉ sử dụng những công cụ Windows hợp pháp. Hacker dùng lệnh hệ thống để ăn cắp mật khẩu, di chuyển sang máy khác trong mạng nội bộ qua Remote Desktop. Dữ liệu nhạy cảm được nén bằng công cụ có sẵn và gửi về thông qua các dịch vụ đám mây hợp pháp như OneDrive. Cả quá trình tấn công "vô hình" vì không có file virus nào để antivirus phát hiện.

Phương thức thực hiện: Xây dựng lab với các vm liên quan gồm máy chủ và máy nhân viên. Bật đầy đủ log để ghi lại mọi hoạt động PowerShell và dòng lệnh. Đội tấn công thực hiện từng bước: gửi email lừa đảo, chiếm máy đầu tiên, lan sang các máy khác, đánh cắp dữ liệu. Đội phòng thủ theo dõi các dấu hiệu bất thường: PowerShell chạy ẩn, kết nối mạng lạ từ các chương trình hệ thống, tài khoản đăng nhập bất thường.

Kịch bản 2: Tác chiến phòng chống tấn công qua phương thức cập nhật UltraVNC

Mục tiêu: Huấn luyện học viên phát hiện và xử lý tấn công giả mạo cập nhật từ phần mềm remote desktop tin cậy, giúp nhận biết các dấu hiệu bất thường trong quá trình update và xây dựng quy trình verify software updates an toàn.

Mô tả: Hacker thiết lập fake update server giả mạo uvnc.com/download. Khi UltraVNC client kiểm tra update định kỳ, thông qua DNS spoofing hoặc ARP poisoning trong mạng nội bộ, request được chuyển về server giả. Admin nhận thông báo có phiên bản mới 1.4.3.6 (fake version), click update và tải về UltraVNC_1.4.3.6_Setup.exe có chứa backdoor. Installer hợp lệ cài đặt UltraVNC bình thường nhưng thêm service ẩn chạy với quyền SYSTEM. Backdoor thu thập danh sách máy được remote, credentials được lưu, screenshot định kỳ. Sau 7 ngày im lặng, backdoor kích hoạt C2 channel qua HTTPS, cho phép attacker remote vào toàn bộ máy trong công ty thông qua chính UltraVNC.

Phương thức thực hiện: thiết lập lab với UltraVNC server/viewer trên các target. Tạo fake update server với SSL certificate hợp lệ. Red team thực hiện: DNS redirect, serve trojanized installer, maintain persistence qua scheduled task. Blue team deploy: DNS monitoring để phát hiện spoofing, verify digital signatures, so sánh hash với official site, monitor service creation và network connections bất thường từ UltraVNC process. Thực hành rollback và clean infected systems.

Kịch bản 3: Tác chiến phòng chống tấn công qua API integration của payment gateway logistics.

Mục tiêu: Huấn luyện học viên phát hiện và xử lý các cuộc tấn công nhắm vào hệ thống kết nối giữa công ty vận chuyển và cổng thanh toán, giúp nhận biết các dấu hiệu bất thường trong quá trình xác thực, phân quyền và logic nghiệp vụ của các lệnh gọi hệ thống, đồng thời xây dựng quy trình giám sát và bảo vệ an toàn cho hệ thống kết nối trong môi trường vận chuyển.

Mô tả: Hacker thực hiện do thám có chủ đích công ty logistics Example Corp, phát hiện API documentation bị expose và test endpoint payments. Khai thác lỗ hổng JWT token validation với weak secret key, hacker tạo malicious JWT để bypass authentication và truy cập unauthorized functions. Sử dụng compromised API access, hacker thực hiện thao túng đơn vị tiền tệ (ví dụ: giảm phí vận chuyển từ 50,000 xuống 5,000 VND), payment bypass cho COD orders giá trị cao, và truy cập dữ liệu đối tác. Attacker thiết lập persistence (duy trì trạng thái kết nối) thông qua API keys giả mạo, inject webhook endpoints độc hại để thu thập dữ liệu thanh toán khách hàng, thông tin giá cả đối thủ cạnh tranh. Giai đoạn cuối, hacker manipulate payment status của suppliers, delay xử lý thanh toán, tạo fake confirmations gây vận chuyển sai, trigger refunds tự động, tạo chaos tài chính ảnh hưởng cash flow và quan hệ đối tác.

Phương thức thực hiện: thiết lập lab với hệ thống logistics-api, payment-gateway và partner-portal có lỗ hổng. Red team thực hiện: API enumeration, JWT token exploitation, business logic bypass, rate manipulation, cross-partner data access, persistence establishment. Blue team triển khai: các biện pháp giám sát API bao gồm các quá trình xác thực và tương tác với giao diện API. Thực hành phát hiện: API authentication bypass, identify rate manipulation attempts, block malicious calls, forensic reconstruction và complete remediation cho affected transactions.

3.3.1.1.1.2.2.6. Yêu cầu về các thành phần của thao trường diễn tập

STT	Hệ thống	Đơn vị tính	Số lượng	Mô tả
1	Thiết kế kịch bản cho thao trường	Kịch bản	3	Thực hiện thiết kế, lên kịch bản phục vụ cho hoạt động diễn tập theo phương án phù hợp tại Mục 2.2.5
2	Đường truyền internet	Line	2	Băng thông tối thiểu 20Mbps đáp ứng phục vụ tối thiểu 80 học viên, 20 chuyên gia, kết nối đến thao trường diễn tập
3	Hệ thống UPS dự phòng	Gói	1	Hệ thống UPS dự phòng N+1 đáp ứng cung cấp điện liên tục 24/7 cho hệ thống thao trường diễn tập
4	Ổ điện kết nối theo mô hình diễn tập	Cái	26	Ổ điện dạng thanh có 6 lỗ cắm cung cấp nguồn điện cho thao trường diễn tập
5	Hệ thống máy chủ (3 máy chủ vật lý, thuê vị trí đặt máy chủ)	Hệ thống	1	Đáp ứng cung cấp cho 80 học viên (80 VM VDI để kết nối vào hệ thống diễn tập), 20 chuyên gia thực hiện trong lúc diễn tập (20 VM VDI để kết nối vào hệ thống diễn tập), hệ thống mô phỏng cho kịch bản gồm đáp ứng phục vụ cho 10 nhóm (mỗi nhóm có 8 máy chủ cho các thành phần: máy chủ cho kịch bản 1 (3 VM) máy chủ cho kịch bản 2 (3 VM) máy phát động tấn công (1 VM), máy thu thập phân tích (1 VM): tương đương 180 máy chủ ảo + 10 máy chủ ảo khác (active directory, DNS, VDI quản trị, quản trị hệ thống ảo hóa). Tài nguyên đủ dự phòng từ 15% đến 20% được sử dụng trong trường hợp cần thiết. - Yêu cầu về cấu hình kỹ thuật của máy chủ tối thiểu: + CPU: tối thiểu 2 CPU/2.40 GHz/ 12 Core/ 24 Threads + Ram: tối thiểu 1TB + Disk: tối thiểu 2 x 240 GB SSD + Cổng mạng vật lý: tối thiểu 1000Mbps
5	Bản quyền phần mềm ảo hóa	gói	1	- Phục vụ xây dựng cho các thành phần hạ tầng CNTT để thiết lập thao trường diễn tập

STT	Hệ thống	Đơn vị tính	Số lượng	Mô tả
				- Sử dụng đồng bộ một bộ giải pháp về ảo hóa - Phần mềm có khả năng ảo hóa máy chủ vật lý - Có khả năng quản lý tập trung và cluster các máy chủ vật lý. - Có khả năng kết nối đa dạng các chuẩn lưu trữ như: nfs, fc,... - Chức năng cấu hình mạng nâng cao có khả năng phân tách các segment mạng. - Có khả năng tạo nhiều router ảo.
6	Dịch vụ phần mềm tường lửa ứng dụng cho các mục tiêu của thao trường tập huấn	gói	1	- Thực hiện bảo vệ cho 10 hệ thống mục tiêu trong kịch bản diễn tập (tương ứng với 10 nhóm) - Có khả năng chống DOS layer 7 - Có khả năng chống tấn công top 10 OPSWAP như : SQL injection, XSS,... - Có khả năng tạo ra các chính sách chặn thủ công - Có khả năng tự học để phân tách traffic
7	Dịch vụ phòng chống mã độc cho các mục tiêu của thao trường tập huấn	gói	1	Bảo vệ cho các mục tiêu của thao trường tập huấn
8	Lưu trữ SAS	TB	10	Phục vụ lưu trữ tài nguyên diễn tập đáp ứng cho 182 máy chủ ảo (chụp snapshot sao lưu 1 bản), tài nguyên phục vụ cài đặt hệ thống (hệ điều hành, souce web, source tấn công, source phòng thủ, ảnh tường lửa, source cyber SOC)
9	Tường lửa tích hợp IPS	hệ thống	1	- Thực hiện bảo vệ mức ứng dụng cho 10 hệ thống mục tiêu trong kịch bản diễn tập (tương ứng với 10 nhóm) - Có khả năng ngăn chặn theo signature - Có khả năng lọc traffic bẩn theo: ip reputation, web reputation, C&C,...

STT	Hệ thống	Đơn vị tính	Số lượng	Mô tả
				- Có khả năng phát hiện tấn công qua yara rules
10	Hệ thống giám sát an toàn mạng	hệ thống	1	- Thực hiện thu thập toàn bộ các sự kiện bảo mật của 10 hệ thống mục tiêu trong kịch bản diễn tập (tương ứng với 10 nhóm) - Khả năng tạo ra các dashboard tùy biến - Correlation các sự kiện - Liên kết với các nguồn thông tin tình báo (TI) - Tích hợp sẵn endpoint security - Có khả năng tích hợp SOAR để thực hiện response.
11	Hệ thống Web proxy security	hệ thống	1	- Cung cấp các chức năng bảo mật và kiểm soát truy cập web cho 10 hệ thống mục tiêu trong kịch bản diễn tập (tương ứng với 10 nhóm) - Có khả năng cân bằng tải traffic cho các website - Có khả năng caching - Có khả năng mã hóa traffic bằng ssl
12	Thuê dịch vụ hỗ trợ chấm điểm dành cho Ban giám khảo và học viên	gói	1	Thuê dịch vụ hỗ trợ chấm điểm dành cho Ban giám khảo và học viên
13	Thiết bị hỗ trợ mạng nội bộ cho phòng học và diễn tập (Switch + Modem tốc độ cao)	bộ	1	Cung cấp kết nối đến thao trường đáp ứng tối thiểu 86 học viên, 16 chuyên gia tham gia diễn tập
14	Thuê Laptop cấu hình mạnh cho hoạt động thực hành kịch bản đào tạo an ninh thông tin	máy	24	Lapop với cấu hình tối thiểu CPU Core i5, Ram ≥ 8Gb, SSD ≥ 240 GB, màn hình ≥ 14 inch, pin lưu trữ 2 tiếng, kèm sạc adapter và chuột máy tính.

STT	Hệ thống	Đơn vị tính	Số lượng	Mô tả
15	Màn hình giám sát	bộ	2	Màn hình giám sát có kích thước tối thiểu 60 inch, hiển thị hoạt động diễn tập của thao trường và học viên.
16	Dây cáp HDMI 30m	sợi	2	Dây cáp HDMI 30m

3.3.1.1.2. Yêu cầu về đội ngũ chuyên gia

Stt	Chi phí	Số lượng	Nội dung công việc
1	Nhóm Chuyên gia trình bày điều phối, thuyết minh	2	Hoạt động 1: Chia sẻ kiến thức, đào tạo an toàn thông tin Kinh nghiệm trên 15 năm các chuyên ngành Toán tin; CNTT; Điện – Điện tử; Viễn thông
2	Nhóm chuyên gia Hỗ trợ học viên trong quá trình diễn tập	4	Hoạt động 1: Chia sẻ kiến thức, đào tạo an toàn thông tin Kinh nghiệm trên 5 năm các chuyên ngành Toán tin; CNTT; Điện – Điện tử; Viễn thông
3	Nhóm Chuyên gia tư vấn, thiết kế thao trường	4	Hoạt động 2: diễn tập thực chiến bảo đảm an toàn thông tin mạng Kinh nghiệm trên 9 năm các chuyên ngành Toán tin; CNTT; Điện – Điện tử; Viễn thông
4	Nhóm Chuyên gia xây dựng, duy trì thao trường	8	Hoạt động 2: diễn tập thực chiến bảo đảm an toàn thông tin mạng Kinh nghiệm trên 9 năm các chuyên ngành Toán tin; CNTT; Điện – Điện tử; Viễn thông
5	Nhóm Chuyên gia điều phối diễn tập	2	Hoạt động 2: diễn tập thực chiến bảo đảm an toàn thông tin mạng Kinh nghiệm trên 9 năm các chuyên ngành Toán tin; CNTT; Điện – Điện tử; Viễn thông
6	Nhóm chuyên gia lập quy chế, thể lệ thi đấu, chấm điểm và chuyên gia lập báo cáo tổng kết	4	Hoạt động 2: diễn tập thực chiến bảo đảm an toàn thông tin mạng Kinh nghiệm trên 9 năm các chuyên ngành Toán tin; CNTT; Điện – Điện tử; Viễn thông

Mô tả công việc của nhóm chuyên gia:

- Chuyên gia điều phối diễn tập: thực hiện thao tác đưa ra các tình huống tấn công để cho các Học viên thực hành phòng thủ; giám sát và điều phối các chuyên gia hỗ trợ đào tạo khi Học viên có nhu cầu.

- Chuyên gia thuộc Ban giám khảo: lập quy chế và thể lệ thi đấu cho các đội học viên thực hành, theo dõi quá trình thực hiện của Học viên và chấm điểm, phụ trách Báo cáo tổng kết sau khi hoạt động kết thúc.

- Chuyên gia xây dựng, duy trì thao trường diễn tập: phụ trách xây dựng thao trường theo kịch bản được chọn, viết tài liệu học tập: module tấn công, phòng thủ...

- Chuyên gia hỗ trợ đào tạo: hỗ trợ học viên trong quá trình thực hành, giải đáp thắc mắc về các thông tin hệ thống thao trường.

3.3.1.1.3. Yêu cầu về năng lực của nhà cung cấp dịch vụ

- Nhà cung cấp dịch vụ phải có chứng chỉ ISO 27001 về tiêu chuẩn quản lý an toàn thông tin còn hiệu lực.

- Nhà cung cấp dịch vụ phải có giấy phép kinh doanh dịch vụ an ninh thông tin còn hiệu lực

3.3.1.2. Thời gian thực hiện

Thời gian thực hiện: 15 ngày.

Danh sách các đơn vị tham gia diễn tập

STT	Tên đơn vị
Khối Sở, ngành; UBND phường, xã và đặc khu	
1	Văn phòng Thành ủy
2	Văn phòng Ủy ban nhân dân thành phố
3	Văn phòng Đoàn đại biểu Quốc hội và Hội đồng nhân dân thành phố
4	Ủy ban Mặt trận tổ quốc Việt Nam Thành phố Hồ Chí Minh
5	Sở Công Thương
6	Sở Khoa học và Công nghệ
7	Sở Nội vụ
8	Sở Tài chính
9	Sở Nông Nghiệp và Môi trường
10	Sở Tư pháp
11	Sở Văn hóa và Thể thao
12	Sở Du lịch

STT	Tên đơn vị
13	Sở Xây dựng
14	Sở Y tế
15	Sở Giáo dục và Đào tạo
16	Sở Dân tộc và Tôn giáo
17	Sở An toàn thực phẩm
18	Tòa án nhân dân khu vực 1-19 TPHCM
19	Viện Kiểm sát nhân dân khu vực 1-19 TPHCM
20	Thanh tra thành phố
21	Lực lượng Thanh niên xung phong
22	Ủy ban về người Việt Nam ở nước ngoài
23	Viện nghiên cứu phát triển
24	Học viện cán bộ thành phố
25	Liên hiệp hợp tác xã
26	BQL Công viên Lịch sử - Văn hóa dân tộc
27	BQL Đường sắt đô thị
28	BQL Dự án đầu tư xây dựng các công trình dân dụng và công nghiệp
29	BQL Phát triển đô thị
30	BQL Dự án đầu tư xây dựng các công trình giao thông
31	BQL Dự án đầu tư xây dựng hạ tầng đô thị
32	BQL dự án ngành NN-PTNT tỉnh Bình Dương
33	BQL dự án chuyên ngành nước thải tỉnh Bình Dương
34	BQL dự án đầu tư xây dựng công trình giao thông tỉnh Bình Dương
35	BQL dự án đầu tư xây dựng tỉnh Bình Dương
36	BQL Trung tâm Hành chính - Chính trị tỉnh Bà Rịa - Vũng Tàu
37	BQL Vườn Quốc gia Côn Đảo tỉnh Bà Rịa - Vũng Tàu

STT	Tên đơn vị
38	BQL dự án Giao thông khu vực và Chuyên ngành Nông nghiệp tỉnh Bà Rịa - Vũng Tàu
39	BQL dự án chuyên ngành Giao thông và Dân dụng tỉnh Bà Rịa - Vũng Tàu
40	Phường Tân Định
41	Phường Sài Gòn
42	Phường Bến Thành
43	Phường Cầu Ông Lãnh
44	Phường Bàn Cờ
45	Phường Xuân Hòa
46	Phường Nhiêu Lộc
47	Phường Xóm Chiếu
48	Phường Khánh Hội
49	Phường Vĩnh Hội
50	Phường Chợ Quán
51	Phường Chợ Lớn
52	Phường An Đông
53	Phường Bình Tiên
54	Phường Bình Tây
55	Phường Bình Phú
56	Phường Phú Lâm
57	Phường Tân Hưng
58	Phường Tân Mỹ
59	Phường Tân Thuận
60	Phường Phú Thuận
61	Phường Chánh Hưng

STT	Tên đơn vị
62	Phường Bình Đông
63	Phường Phú Định
64	Phường Diên Hồng
65	Phường Hòa Hưng
66	Phường Vườn Lài
67	Phường Phú Thọ
68	Phường Bình Thới
69	Phường Minh Phụng
70	Phường Hòa Bình
71	Phường Thới An
72	Phường Trung Mỹ Tây
73	Phường Tân Thới Hiệp
74	Phường Đông Hưng Thuận
75	Phường An Phú Đông
76	Phường Tân Sơn Hòa
77	Phường Tân Sơn Nhất
78	Phường Bảy Hiền
79	Phường Tân Hòa
80	Phường Tân Bình
81	Phường Tân Sơn
82	Phường Bình Thạnh
83	Phường Gia Định
84	Phường Bình Lợi Trung
85	Phường Thạnh Mỹ Tây
86	Phường Bình Quới

STT	Tên đơn vị
87	Phường Cầu Kiệu
88	Phường Đức Nhuận
89	Phường Phú Nhuận
90	Phường An Lạc
91	Phường Bình Trị Đông
92	Phường Bình Tân
93	Phường Bình Hưng Hòa
94	Phường Tân Tạo
95	Phường An Nhơn
96	Phường Hạnh Thông
97	Phường Gò Vấp
98	Phường Thông Tây Hội
99	Phường An Hội Đông
100	Phường An Hội Tây
101	Phường Tân Phú
102	Phường Tân Sơn Nhì
103	Phường Phú Thọ Hòa
104	Phường Phú Thạnh
105	Phường Tây Thạnh
106	Xã Hóc Môn
107	Xã Bà Điểm
108	Xã Xuân Thới Sơn
109	Xã Đông Thạnh
110	Xã Bình Mỹ
111	Xã Củ Chi

STT	Tên đơn vị
112	Xã An Nhơn Tây
113	Xã Thái Mỹ
114	Xã Phú Hoà Đông
115	Xã Nhuận Đức
116	Xã Tân An Hội
117	Xã Nhà Bè
118	Xã Hiệp Phước
119	Xã Cần Giờ
120	Xã Bình Khánh
121	Xã An Thới Đông
122	Xã Thạnh An
123	Xã Tân Vĩnh Lộc
124	Xã Vĩnh Lộc
125	Xã Bình Chánh
126	Xã Bình Hưng
127	Xã Tân Nhựt
128	Xã Bình Lợi
129	Xã Hưng Long
130	Phường An Khánh
131	Phường Bình Trưng
132	Phường Cát Lái
133	Phường Hiệp Bình
134	Phường Linh Xuân
135	Phường Long Bình
136	Phường Long Phước

STT	Tên đơn vị
137	Phường Long Trường
138	Phường Phước Long
139	Phường Tam Bình
140	Phường Tăng Nhơn Phú
141	Phường Thủ Đức
142	Xã Ngãi Giao
143	Xã Kim Long
144	Xã Bình Giã
145	Xã Nghĩa Thành
146	Xã Xuân Sơn
147	Xã Châu Đức
148	Đặc Khu Côn Đảo
149	Phường Bà Rịa
150	Phường Tam Long
151	Phường Long Hương
152	Phường Vũng Tàu
153	Phường Tam Thắng
154	Phường Rạch Dừa
155	Phường Phước Thắng
156	Xã Long Sơn
157	Phường Phú Mỹ
158	Phường Tân Phước
159	Phường Tân Hải
160	Phường Tân Thành
161	Xã Châu Pha

STT	Tên đơn vị
162	Xã Hồ Tràm
163	Xã Xuyên Mộc
164	Xã Bình Châu
165	Xã Hòa Hội
166	Xã Bàu Lâm
167	Xã Hòa Hiệp
168	Xã Đất Đỏ
169	Xã Long Điền
170	Xã Long Hải
171	Xã Phước Hải
172	Phường Bình Dương
173	Phường Thủ Dầu Một
174	Phường Phú Lợi
175	Phường Phú An
176	Phường Chánh Hiệp
177	Phường Dĩ An
178	Phường Đông Hòa
179	Phường Tân Đông Hiệp
180	Phường Thuận An
181	Phường Bình Hòa
182	Phường Thuận Giao
183	Phường Lái Thiêu
184	Phường An Phú
185	Phường Tân Uyên
186	Phường Tân Hiệp

STT	Tên đơn vị
187	Phường Tân Khánh
188	Phường Vĩnh Tân
189	Phường Bình Cơ
190	Xã Bắc Tân Uyên
191	Xã Thường Tân
192	Phường Bến Cát
193	Phường Thới Hòa
194	Phường Long Nguyên
195	Phường Tây Nam
196	Phường Chánh Phú Hòa
197	Phường Hòa Lợi
198	Xã Phú Giáo
199	Xã Phước Thành
200	Xã Phước Hòa
201	Xã An Long
202	Xã Dầu Tiếng
203	Xã Long Hòa
204	Xã Minh Thạnh
205	Xã Thanh An
206	Xã Bàu Bàng
207	Xã Trừ Văn Thố
Khối bệnh viện	
208	Bệnh viện Nguyễn Tri Phương
209	Bệnh viện Ung bướu
210	Bệnh viện Nhi đồng thành phố

STT	Tên đơn vị
211	Bệnh viện Nhi đồng 1
212	Bệnh viện Nhi đồng 2
213	Bệnh viện Nhân dân 115
Khối công ty, doanh nghiệp	
214	Tổng Công ty Liksin - TNHH MTV
215	Tổng Công ty Bến Thành
216	Tổng Công ty Du lịch Sài Gòn - TNHH MTV
217	Tổng Công ty Thương mại Sài Gòn
218	Công ty cổ phần Văn hóa Sách Sài Gòn
219	Tổng Công ty Công nghiệp Sài Gòn - TNHH MTV
Khối cơ quan báo chí	
220	Đài Truyền hình Thành phố Hồ Chí Minh
221	Đài Tiếng nói Nhân dân Thành phố Hồ Chí Minh
222	Báo Pháp luật Thành phố Hồ Chí Minh
223	Tạp chí Du lịch Thành phố Hồ Chí Minh
224	Tạp chí Giáo dục Thành phố Hồ Chí Minh
225	Tạp chí Doanh nhân Sài Gòn
226	Tạp chí Kinh tế Sài Gòn

3.3.1.3. Hệ thống xây dựng thao trường kịch bản đào tạo

STT	Hệ thống	Đơn vị tính	Số lượng	Mô tả
1	Thiết kế kịch bản cho thao trường	Kịch bản	3	Kịch bản 1: Tác chiến phòng chống tấn công APT sử dụng kỹ thuật Living-off-the-Land Kịch bản 2: Tác chiến phòng chống tấn công phương thức cập nhật UltraVNC Kịch bản 3: Tác chiến phòng chống tấn công qua kết nối api giữa logistics và

STT	Hệ thống	Đơn vị tính	Số lượng	Mô tả
				cổng thanh toán.
2	Đường truyền internet	Line	2	Băng thông 20Mbps quốc tế, 1000Mbps trong nước đáp ứng phục vụ tối thiểu 80 học viên, 20 chuyên gia, kết nối đến thao trường đào tạo, tập huấn.
3	Hệ thống UPS dự phòng	Gói	1	Hệ thống UPS dự phòng N+1 đáp ứng cung cấp điện liên tục 24/7 cho hệ thống thao trường đào tạo, tập huấn.
4	Ổ điện kết nối theo mô hình đào tạo, tập huấn	Cái	26	Ổ điện dạng thanh có 6 lỗ cắm cung cấp nguồn điện cho thao trường đào tạo, tập huấn.
5	Hệ thống máy chủ (3 máy chủ vật lý, thuê vị trí đặt máy chủ)	Hệ thống	1	Đáp ứng cung cấp cho 80 học viên (80 VM VDI để kết nối vào hệ thống diễn tập), 20 chuyên gia thực hiện trong lúc diễn tập (20 VM VDI để kết nối vào hệ thống diễn tập), hệ thống mô phỏng cho kịch bản gồm đáp ứng phục vụ cho 10 nhóm (mỗi nhóm có 8 máy chủ cho các thành phần: máy chủ cho kịch bản 1 (3 VM) máy chủ cho kịch bản 2 (3 VM) máy phát động tấn công (1 VM), máy thu thập phân tích (1 VM): tương đương 180 máy chủ ảo + 10 máy chủ ảo khác (active directory, DNS, VDI quản trị, quản trị hệ thống ảo hóa). Tài nguyên đủ dự phòng từ 15% đến 20% được sử dụng trong trường hợp cần thiết. - Cấu hình kỹ thuật của máy chủ (tối thiểu như sau: +Máy 1: CPU: 2CPU/2.1GHz/64 Core/128 Threads, 1 TB RAM, Disk: 2 x 240 GB SSD, 6 NIC 1000Mbps; + Máy 2: CPU: 2CPU/2.1GHz/64 Core/128 Threads, 1 TB RAM, Disk: 2 x 240 GB SSD, 6 NIC 1000Mbps; + Máy 3: CPU: 2CPU/2.1GHz/64 Core/128 Threads, 1 TB RAM, Disk: 2 x 240 GB SSD, 6 NIC 1000Mbps.

STT	Hệ thống	Đơn vị tính	Số lượng	Mô tả
6	Bản quyền phần mềm ảo hóa	gói	1	- Phục vụ xây dựng cho các thành phần hạ tầng CNTT để thiết lập thao trường đào tạo, tập huấn; - Sử dụng đồng bộ một bộ giải pháp về ảo hóa; - Phần mềm có khả năng ảo hóa máy chủ vật lý; - Có khả năng quản lý tập trung và cluster các máy chủ vật lý; - Có khả năng kết nối đa dạng các chuẩn lưu trữ như: nfs, fc,... - Chức năng cấu hình mạng nâng cao có khả năng phân tách các segment mạng; - Có khả năng tạo nhiều router ảo.
7	Dịch vụ phần mềm tường lửa ứng dụng cho các mục tiêu của thao trường	gói	1	- Thực hiện bảo vệ cho 10 hệ thống mục tiêu trong kịch bản đào tạo, tập huấn (tương ứng với 10 nhóm); - Có khả năng chống DOS layer 7; - Có khả năng chống tấn công top 10 OPSWAP như : SQL injection, XSS,... - Có khả năng tạo ra các chính sách chặn thủ công; - Có khả năng tự học để phân tách traffic.
8	Dịch vụ phòng chống mã độc cho các mục tiêu của thao trường	gói	1	Bảo vệ cho các mục tiêu của thao trường.
9	Thuê dịch vụ lưu trữ	TB	10	Phục vụ lưu trữ SAS đáp ứng cho 180 máy chủ ảo (chụp snapshot sao lưu 1 bản), tài nguyên phục vụ cài đặt hệ thống (hệ điều hành, souce web, source tấn công, source phòng thủ, ảnh tường lửa, source cyber SOC).
10	Tường lửa tích hợp IPS	hệ thống	1	- Thực hiện bảo vệ mức ứng dụng cho 10 hệ thống mục tiêu trong kịch bản đào

STT	Hệ thống	Đơn vị tính	Số lượng	Mô tả
				tạo, tập huấn (tương ứng với 10 nhóm). - Có khả năng ngăn chặn theo signature; - Có khả năng lọc traffic bẩn theo: ip reputation, web reputation, C&C,... - Có khả năng phát hiện tấn công qua yara rules.
11	Hệ thống giám sát an toàn mạng	hệ thống	1	- Thực hiện thu thập toàn bộ các sự kiện bảo mật của 10 hệ thống mục tiêu trong kịch bản đào tạo, tập huấn (tương ứng với 10 nhóm); - Khả năng tạo ra các dashboard tùy biến; - Correlation các sự kiện; - Liên kết với các nguồn thông tin tình báo (TI); - Tích hợp sẵn endpoint security; - Có khả năng tích hợp SOAR để thực hiện response.
12	Thuê dịch vụ Web proxy security	hệ thống	1	- Cung cấp các chức năng bảo mật và kiểm soát truy cập web cho 10 hệ thống mục tiêu trong kịch bản đào tạo, tập huấn (tương ứng với 10 nhóm); - Có khả năng cân bằng tải traffic cho các website; - Có khả năng caching; - Có khả năng mã hóa traffic bằng ssl.
13	Thuê dịch vụ hỗ trợ chấm điểm dành cho Ban giám khảo và học viên	gói	1	Thuê dịch vụ hỗ trợ chấm điểm dành cho Ban giám khảo và học viên
14	Thuê thiết bị hỗ trợ mạng nội bộ cho phòng đào tạo và diễn tập (Switch + Modem tốc độ	bộ	1	Thiết bị Switch tốc độ kết nối tối thiểu 1Gb + wifi modem Aruba; Cung cấp kết nối đến thao trường đáp ứng tối thiểu 80 học viên, 20 chuyên gia tham gia đào tạo, tập huấn.

STT	Hệ thống	Đơn vị tính	Số lượng	Mô tả
	cao)			
15	Thuê Laptop cấu hình mạnh cho hoạt động thực hành kịch bản đào tạo an ninh thông tin	máy	24	Laptop cấu hình tối thiểu Core i5-6300U/ RAM 8GB/ SSD 256GB/ Màn hình 14 inch trở lên
16	Thuê Màn hình giám sát 60 inch + chân đứng	bộ	2	Màn hình giám sát có kích thước tối thiểu 60 inch, hiển thị hoạt động đào tạo, tập huấn của thao trường và học viên.
17	Dây cáp HDMI 30m	sợi	2	Dây cáp HDMI 30m.

3.3.2. Phương án triển khai ứng phó sự cố, đảm bảo an toàn thông tin trên địa bàn thành phố

3.3.2.1. Tiêu chuẩn thực hiện

Tiêu chuẩn thực hiện được thiết lập nhằm đo lường mức độ thành công của dự án, dựa trên kết quả đầu ra của học viên và chất lượng dịch vụ của Nhà cung cấp.

3.3.2.1.1. Tiêu chuẩn về Hiệu quả Đào tạo

Đây là các tiêu chí bắt buộc về việc thay đổi nhận thức và hành vi của cán bộ sau khi tham gia khóa tập huấn.

- Tỷ lệ Hoàn thành: 100% cán bộ thuộc danh sách mục tiêu phải hoàn thành tối thiểu 80% tổng thời lượng chương trình đào tạo và tham gia tập huấn.

- Cấp Chứng nhận: Tối thiểu 85% học viên phải đạt điểm tổng kết (kết hợp đào tạo và tập huấn) từ 75/100 điểm trở lên để được cấp Chứng nhận Hoàn thành khóa học.

3.3.2.1.2. Tiêu chuẩn về Chất lượng Vận hành Dịch vụ

Đây là các cam kết về mặt tổ chức, kỹ thuật và hậu cần của Nhà cung cấp dịch vụ.

- Mức độ Hài lòng: Mức độ hài lòng chung từ khảo sát học viên phải đạt điểm trung bình tối thiểu 4.2/5.0 đối với chất lượng giảng viên, nội dung và công tác tổ chức hậu cần.

- Tính kịp thời của Báo cáo: Nhà cung cấp dịch phải cung cấp Báo cáo Tiến độ (bao gồm danh sách điểm danh và kết quả đánh giá) trong vòng tối đa 02 ngày làm việc sau khi kết thúc đào tạo và tập huấn.

3.3.2.1.3. Tiêu chuẩn về Tính tuân thủ và Chuyển giao

- Bảo mật Dữ liệu: Tuân thủ 100% các yêu cầu bảo mật dữ liệu cán bộ và phải bàn giao/xóa dữ liệu theo quy trình đã ký kết trong Thỏa thuận Bảo mật Thông tin (NDA).

- Chất lượng Tài liệu Bàn giao: Toàn bộ học liệu điện tử (ví dụ: file, video, infographic) phải được bàn giao với chất lượng kỹ thuật cao, không lỗi và tuân thủ các chuẩn công nghệ đã quy định.

3.3.2.2. Yêu cầu kỹ thuật chi tiết

3.3.2.2.1. Yêu cầu về Hạ tầng, Tổ chức địa điểm và Hậu cần

Yêu cầu này nhằm đảm bảo môi trường vật chất và kỹ thuật tốt nhất để triển khai tập huấn, hỗ trợ quy mô lớn (từ 100 đến 300 học viên) và tính chất của dự án.

3.3.2.2.1.1. Yêu cầu về Quy mô và Bố trí địa điểm

Tiêu chuẩn	Yêu cầu Chi tiết	Mục đích
Sức chứa	Địa điểm phải có khả năng cung cấp các Hội trường / Phòng Hội thảo với sức chứa từ tối thiểu 100 học viên đến tối đa 300 học viên mỗi buổi.	Đáp ứng nhu cầu tổ chức tập trung theo cụm
Bố trí Linh hoạt	Cho phép sắp xếp bàn ghế theo kiểu Lớp học cho phần lý thuyết và có đủ không gian để chia nhỏ thành các Nhóm thảo luận cho phần Tập huấn ứng phó sự cố.	Tối ưu hóa không gian cho cả phần lý thuyết và thực hành quy trình.
Hệ thống An toàn	Đảm bảo tuân thủ nghiêm ngặt các quy tắc PCCC, có lối thoát hiểm rõ ràng và số lượng nhân viên hỗ trợ an ninh phù hợp với quy mô 300 người.	Đảm bảo an toàn tuyệt đối cho cán bộ Thành phố khi tham gia tập huấn.

3.3.2.2.1.2. Yêu cầu về Thiết bị và Công nghệ

Tiêu chuẩn	Yêu cầu Chi tiết	Mục đích
Kết nối Internet	Cung cấp đường truyền Internet cáp quang dự phòng. Băng thông tối thiểu phải là 100 Mbps và phải có mạng Wi-Fi đủ mạnh, hỗ trợ kết nối đồng thời 100% học viên.	Đảm bảo truy cập ổn định vào LMS/nền tảng đánh giá và tránh gián đoạn khi diễn tập.
Âm thanh và Trình chiếu	Âm thanh: Loa và Micro không dây chất lượng cao, đảm bảo âm thanh đồng đều tại mọi vị trí trong phòng. Trình chiếu: Máy chiếu hoặc màn hình LED/LCD có độ phân giải Full HD (1080p) và độ sáng cao (trên 5000 lumens) để hiển thị rõ các tài liệu trực quan	Đảm bảo chất lượng tiếp thu thông tin và hiển thị rõ ràng các biểu đồ, Infographic cho đối tượng tham gia.

Tiêu chuẩn	Yêu cầu Chi tiết	Mục đích
Nguồn Điện	Địa điểm phải được trang bị thiết bị UPS và Máy phát điện dự phòng có khả năng duy trì hoạt động của toàn bộ thiết bị trong ít nhất 04 giờ trong trường hợp mất điện lưới.	Đảm bảo tính liên tục của buổi đào tạo, đặc biệt là các buổi tập huấn quan trọng.

3.3.2.2.1.3. Yêu cầu về Hậu cần

Vị trí và Tiếp cận: Địa điểm tổ chức phải nằm ở vị trí thuận tiện di chuyển cho cán bộ từ các đơn vị mới sáp nhập, có khu vực đỗ xe rộng rãi và an toàn.

Tiện nghi: Hệ thống điều hòa không khí phải hoạt động tốt, đảm bảo nhiệt độ ổn định. Khu vực vệ sinh phải sạch sẽ và đủ tiêu chuẩn phục vụ quy mô lớn.

3.3.2.2.2. Yêu cầu về Đội ngũ Chuyên gia, Giảng viên và Công cụ

Yêu cầu này đảm bảo rằng Nhà cung cấp Dịch vụ triển khai dự án phải có nguồn nhân lực chất lượng cao, có kinh nghiệm thực tế và khả năng truyền đạt phù hợp với đối tượng đào tạo.

STT	Nội dung	Số lượng (người)	Số năm kinh nghiệm	Bằng cấp liên quan
1.	Giảng viên	01	≥ 05 năm bậc đại học	Tốt nghiệp các chuyên ngành Toán tin, Công nghệ thông tin, Điện tử, Viễn thông, Khoa học máy tính, An ninh mạng, An toàn thông tin, Kỹ thuật phần mềm, Hệ thống thông tin - Có đồng thời các chứng chỉ Offensive Security Certified Professional (OSCP), Offensive Security Defense Analyst (OSDA) hoặc tương đương.
2.	Trợ giảng / Kỹ thuật viên hỗ trợ	8	≥ 05 năm bậc đại học	Tốt nghiệp các chuyên ngành Toán tin, Công nghệ thông tin, Điện tử, Viễn thông, Khoa học máy tính, An ninh mạng, An toàn thông tin, Kỹ thuật phần mềm, Hệ thống thông tin
3.	Chuyên gia tư vấn, thiết kế lab tập huấn	3	≥ 10 năm bậc đại học	Tốt nghiệp các chuyên ngành Toán tin, Công nghệ thông tin, Điện tử, Viễn thông, Khoa học máy tính, An ninh mạng, An toàn thông tin, Kỹ thuật phần mềm, Hệ thống thông tin

STT	Nội dung	Số lượng (người)	Số năm kinh nghiệm	Bằng cấp liên quan
4.	Chuyên gia thiết kế kịch bản, viết tài liệu đào tạo	3	≥ 05 năm bậc đại học	Tốt nghiệp các chuyên ngành Toán tin, Công nghệ thông tin, Điện tử, Viễn thông, Khoa học máy tính, An ninh mạng, An toàn thông tin, Kỹ thuật phần mềm, Hệ thống thông tin
	Tổng cộng	**15**		

Nhà cung cấp dịch vụ chịu trách nhiệm chuẩn bị các thiết bị phục vụ cho tập huấn và diễn tập hệ thống Lab với cấu hình tối thiểu như sau:

Cấu hình phần cứng:

- CPU: Core i7
- RAM: 32GB
- SSD: 1TB

Phần mềm được cài đặt sẵn: Các phần mềm phục vụ cho công tác tập huấn (công cụ giả lập sự cố, công cụ xử lý sự cố)

3.3.2.2.3. Yêu cầu về năng lực Nhà cung cấp dịch vụ

Kinh nghiệm: Nhà cung cấp dịch vụ cần chứng minh đã từng thực hiện tối thiểu 01 dự án đào tạo/tập huấn tương tự trong vòng 03 năm gần nhất.

Nhà cung cấp dịch vụ phải có chứng chỉ ISO 27001 về tiêu chuẩn quản lý an toàn thông tin còn hiệu lực.

Nhà cung cấp dịch vụ phải có giấy phép kinh doanh dịch vụ an ninh thông tin còn hiệu lực.

3.3.2.2.4. Yêu cầu về Đối tượng tham gia dự án

Hạng mục được thiết kế để bao phủ toàn bộ các nhóm chức năng có vai trò trong việc bảo vệ và phản ứng đối với hệ thống thông tin của TP. HCM.

3.3.2.2.4.1. Nhóm Cán bộ Kỹ thuật Bán chuyên trách và Quản trị hệ thống

Nhóm này cần được đào tạo về kỹ năng ứng phó sơ bộ và phối hợp kỹ thuật với đội ngũ chuyên trách của Thành phố.

Thành phần: Cán bộ phụ trách CNTT/quản trị mạng/hệ thống bán chuyên trách tại các đơn vị hành chính và sự nghiệp.

Mục tiêu Tham gia:

- Nắm vững Quy trình Báo cáo và Liên lạc chính thức với đội ngũ ATTT của Thành phố (Trung tâm SOC).
- Thực hành các kỹ năng Khoanh vùng Sự cố Sơ bộ (ví dụ: cô lập máy tính bị nhiễm mã độc, kiểm tra nhật ký log đơn giản, sao lưu dữ liệu khẩn cấp).
- Hiểu rõ các công cụ / tài khoản cần thiết để phối hợp khắc phục sự cố.

Hình thức Tập huấn Ưu tiên: Kết hợp lý thuyết chuyên môn và Diễn tập Kỹ thuật Sơ cấp tập trung vào các tình huống xử lý tại chỗ.

3.3.2.2.4.2. Nhóm Cán bộ Văn phòng và Người dùng cuối

Đây là nhóm đối tượng lớn nhất và là trọng tâm của dự án đào tạo đại trà.

Thành phần: Toàn bộ công chức, viên chức, người lao động sử dụng máy tính, email, và các hệ thống thông tin trong công việc hàng ngày, không chuyên về CNTT/ATTT.

Mục tiêu Tham gia:

- Nâng cao Nhận thức Cá nhân để phòng ngừa các mối đe dọa phổ biến (Phishing, Social Engineering, Mật khẩu yếu).
- Nắm vững Quy tắc Hành động Sơ bộ (KHÔNG CLICK, TẮT MÁY/NGẮT MẠNG).
- Biết chính xác Đầu mối Báo cáo Sự cố và Quy trình Báo cáo 3 Bước khi phát hiện dấu hiệu bất thường.

Hình thức Tập huấn Ưu tiên: Các nội dung ngắn, trực quan, dễ hiểu (dùng Infographic, Video), và tập huấn mô phỏng tình huống lừa đảo.

3.3.2.3. Nội dung Đào tạo và Tập huấn Ứng phó sự cố ATTT

Kịch bản Đào tạo chính là trái tim của Dự án, được xây dựng một cách khoa học để chuyển hóa mục tiêu chiến lược thành năng lực thực tiễn. Dựa trên Bối cảnh sáp nhập và nhu cầu đào tạo có quy mô lớn, độ phủ cao, kịch bản được thiết kế tập trung vào các hành động ứng phó sơ bộ và quy trình báo cáo thống nhất. Cấu trúc 02 buổi cân bằng giữa việc nâng cao nhận thức cơ bản (Phishing, Mật khẩu) và việc thực hành quy trình qua tập huấn mô phỏng, đảm bảo đạt được các Tiêu chuẩn Thực hiện và mục tiêu giảm thiểu 30% thời gian xử lý sự cố.

3.3.2.3.1. Ngày 1: Nhận thức, Phòng ngừa và Khái quát quy trình Ứng phó sự cố An toàn thông tin (8 giờ):

Stt	Hạng mục	Nội dung	Thời lượng
1	Khai mạc Sự kiện	Giới thiệu thành phần tham gia Phát biểu về tầm quan trọng, chủ trương và tuyên bố khai mạc sự kiện	0,5 giờ
2	Bài 1. Tổng quan về ứng cứu sự cố	1. Tổng quan tình hình an toàn thông tin Tổng quan về tình hình an toàn thông tin ở Việt Nam và Quốc Tế Các sự cố gây mất an toàn thông tin điển hình: PVOIL, VNDIRECT 2. Vai trò và tầm quan trọng của công tác ứng cứu sự cố	1 giờ

Stt	Hạng mục	Nội dung	Thời lượng
		Công tác ứng cứu sự cố là thước đo năng lực an ninh mạng của một tổ chức. Nguyên nhân chủ quan và khách quan dẫn đến thất bại trong xử lý sự cố 3. Phân loại và định nghĩa sự cố Phân biệt "Sự kiện an ninh" và "Sự cố an ninh" Các yếu tố cốt lõi của một sự cố. 4. Các yếu tố tiên quyết để có thể thực hiện ứng cứu sự cố hiệu quả. Vai trò của công tác "Nhận diện", "Bảo vệ" và "Ứng cứu" 5. Mục tiêu và quy trình tổng thể Các mục tiêu cốt lõi Quy trình tổng thể 3 bước	
3	Bài 2. Xây dựng Lực lượng và Hệ thống Văn bản Chỉ đạo	1. Vai trò của lãnh đạo và xây dựng văn hóa an ninh thông tin Các phẩm chất người lãnh đào cần rèn luyện để phục vụ cho hoạt động ứng cứu sự cố. Các phương pháp luận để triển khai và thúc đẩy văn hóa an ninh trong toàn cơ quan, tổ chức. 2. Xây dựng lực lượng phục vụ ứng cứu sự cố Đội ứng cứu sự cố Các kỹ năng nghiệp vụ cần có Cân nhắc sử dụng đội ứng cứu sự cố bên ngoài 3. Công tác chuẩn bị về tổ chức và kỹ thuật Xác định các tài sản thông tin quan trọng Quản lý tài sản thông tin Phần vùng, chia nhỏ mạng, kiểm soát truy cập Ghi nhật ký Công cụ, thiết bị, phần mềm 4. Quy trình và cách thức phối hợp Các quy trình ứng cứu sự cố (SANS, NIST) Xây dựng quy trình ứng cứu sự cố	2 giờ

Stt	Hạng mục	Nội dung	Thời lượng
		Tổ chức nhân sự phối hợp Các chế tài và pháp lý	
4	Bài 3. Nhận diện sự cố và thực hiện điều tra	1. Xây dựng phương án xử lý trên cơ sở phương thức, thủ đoạn của kẻ tấn công Sử dụng vòng đời tấn công (Cyber Attack Life Cycle) 7 Giai đoạn của cuộc tấn công mạng 2. Giám sát và phát hiện chủ động Các công cụ giám sát hiện đại: SIEM, DLP, EDR … Phát hiện sớm các hành vi bất thường. 3. Khởi động quá trình điều tra ban đầu - Thu thập thông tin ban đầu - Các biểu mẫu chính cần có - Xây dựng bảng ghi nhận thời gian và diễn biến về sự cố (Timeline) 4. Điều tra tìm kiếm manh mối và dấu hiệu nhận diện Các đặc điểm của một manh mối phục vụ cho điều tra xử lý sự cố Sự liên quan của manh mối và dấu hiệu xâm nhập (IOC) Quy trình thực hiện có tính lặp lại	2 giờ
5	Bài 4. Điều tra, phân tích và khoanh vùng sự cố	1. Nguyên tắc khoanh vùng và ngăn chặn (Containment) Sử dụng dấu hiệu xâm nhập đã tìm thấy (IOC) Cách ly hệ thống Xây dựng các kịch bản xử lý 2. Kỹ thuật thu thập, bảo quản chứng cứ số (Digial Evidence) Thu thập dữ liệu nóng (Live Data) Các công cụ sử dụng trên Windows và Linux/Unix/Mac Tạo bản sao của chứng cứ số có tính pháp lý (Forensic Duplication)	2 giờ

Stt	Hạng mục	Nội dung	Thời lượng
		Phân loại các bản sao Sử dụng thiết bị chống ghi (Hardware Write Blocker) Xác minh tính toàn vẹn của bản sao 3. Phân tích, truy vết sự cố thông qua bằng chứng kỹ thuật số thu thập trên hệ thống Trên Windows: MFT, Perfetch, Windows Event Logs, Registry, Shellbags & UserAssist Trên Linux/Unix/Mac: Hệ thống tệp HFS+, EXT4, XFS, phân tích nhật ký hệ thống, các file tự khởi động, phân tích log kernel. 4. Phân tích ứng dụng và mã độc Điều tra ung dụng: Thu thập lịch sử (history), cache, và cookies từ các trình duyệt web (IE, Chrome, Firefox). Phân tích mã độc: Phân tích tĩnh (Static Analysis) Phân tích động (Dynamic Analysis)	
6	Bài 5. Khắc phục sự cố, phục hồi hệ thống và rút kinh nghiệm	1. Lập kế hoạch khắc phục và phục hồi (remediation) Lập đội khắc phục sự cố Lựa chọn thời điểm thực hiện 2. Quy trình khắc phục và gỡ bỏ mã độc khỏi hệ thống Chuẩn bị môi trường Ngăn chặn chủ động Triệt tiêu và loại bỏ Các nguyên tắc phải tuyệt đối tuân thủ. 3. Tổng kết và rút kinh nghiệm Tổ chức họp đánh giá sau sự cố Rút ra bài học kinh nghiệm và bổ sung tài liệu liên quan 4. Thực hiện lập báo cáo và hoàn thiện hồ sơ liên quan đến sự cố	0,5 giờ

Stt	Hạng mục	Nội dung	Thời lượng
		Nguyên tắc khi lập báo cáo Các yêu cầu của một báo cáo ứng cứu sự cố Cấu trúc một báo cáo và các báo cáo mẫu	

3.3.2.3.2. Ngày 2: Tập huấn, Thực hành Quy trình và Kỹ năng ứng phó (8 giờ)

STT	Phase	Đội ứng cứu sự cố	Ghi chú
1	Phase 01. Tiếp nhận và làm quen hệ thống	Đội ứng cứu sự cố tiền hành tiếp nhận và làm quen hệ thống diễn tập bao gồm: Hệ thống SIEM Máy tính của nạn nhân (Victim Workstation) Máy chủ tập tin (File Server) Và các tài liệu hỗ trợ quá trình diễn tập bao gồm: Tài liệu mô tả cấu trúc hệ thống Mẫu báo cáo phục vụ lập báo cáo phục vụ diễn tập Nhân sự đội ứng cứu sự cố tiền hành đăng nhập vào các hệ thống thông tin và máy chủ để sẵn sàng tham gia quá trình diễn tập.	
2	Phase 02. Xác định sự cố	Dựa trên các cảnh báo của hệ thống SIEM/EDR, nhân sự của Đội ứng cứu sự cố tiến hành xác định loại sự cố và tiến tiến hành thu thập các thông tin trên hệ thống giám sát và thực hiện tóm tắt sơ bộ sự cố. Trong giai đoạn này Đội ứng cứu sự cố phải xác định được các thông tin như sau: IP/hostname của các máy tính có liên quan đến sự cố Địa chỉ IP của kẻ tấn công có liên quan đến sự cố Chú ý: Các thông tin được chấp nhận trong phase này chỉ chấp nhận các thông tin được ghi nhận trên hệ thống giám sát.	
3	Phase 03. Thu thập bằng chứng số	Trong giai đoạn này của quá trình diễn tập, Đội ứng cứu sự cố tiến hành ghi nhận và bảo quản chứng cứ số liên quan đến sự cố, sử dụng	

STT	Phase	Đội ứng cứu sự cố	Ghi chú
		các công cụ hỗ trợ quá trình điều tra và thu thập chứng cứ số. Trong giai đoạn này đội ứng cứu sự cố phải ghi lại đầy đủ quá trình thu thập chứng cứ sồ, có thể ghi hình (video screen record hoặc chụp ảnh màn hình). Các bằng chứng số sau khi được bảo vệ với các cơ chế chống sửa đổi phù hợp với hoàn cảnh hiện tại. Các chứng cứ số sau khi được thu thập phải được liệt kê cụ thể tại báo cáo ứng cứu sự cố, và nguyên nhân thu thập các chứng cứ sồ này.	
4	Phase 04. Thực hiện điều tra	Tại giai đoạn này, Đội ứng cứu sự cố tiến hành sử dụng các công cụ và kỹ thuật điều tra chuyên sâu để có thể điều tra các hành vi mà kẻ tấn công thực hiện trên các máy tính và máy chủ đã được xác định là liên quan đến sự cố. Kết thúc quá trình này Đội ứng cứu sự cố phải xây dựng được bảng liệt kê bao gồm các nội dung: Thời gian thực hiện hành vi Hành vi đã thực hiện cụ thể (câu lệnh/tập tin liên quan/mô tả hành vi cụ thể), công cụ mà kẻ tấn công sử dụng để thực hiện hành vi trên các máy tính và máy chủ nêu trên Đối sánh hành vi với Tactics cụ thể được liệt kê tại Mittre Attack. Liệt kê được các IOC liên quan đến sự cố (IP, HASH, Port, Filename …) Trong giai đoạn này, ngoài việc liệt kê các thông tin dưới dạng bảng, việc vẽ được lưu đồ thời gian thực hiện các hành vi sẽ là một điểm cộng của đội nhóm tham gia diễn tập.	
5	Phase 5. Ngăn chặn, loại bỏ sự cố	Từ các thông tin đã thu thập từ quá trình điều tra tại Phase 04, Đội ứng cứu sự cố tiến hành thực hiện ngăn chặn sự cố. Có thể kể đến: Chặn địa chỉ IP Loại bỏ phần mềm độc hại (nếu có)	

STT	Phase	Đội ứng cứu sự cố	Ghi chú
		Thực hiện các hành động khác nhắn loại bỏ sự ản hưởng của sự cố đến hệ thống Tại giai đoạn này, các hành động nhằn thực hiện ngăn chặn hoặc loại bỏ sự ảnh hưởng của sự cố khỏi hệ thống thông tin sẽ phải được ghi lại dưới dạng hình ảnh và đưa vào báo cáo. Các bước thực hiện được ghi nhận càng chi tiết sẽ là một lợi thế của đội tham gia diễn tập trong quá trình đánh giá.	
6	Phase 6. Phục hồi	Tại giai đoạn này, Đội ứng cứu sự cố tiền hành thực hiện các hoạt động nhằm khôi phục hoạt động của hệ thống thông tin có thể bao gồm: Thay đổi mật khẩu tài khoản liên quan đến sự cố trên hệ thống Reset Kerberos trên hệ thống AD Thực hiện khôi phục các bản sao lưu sạch (nếu có) Ngoài các gợi ý nêu trên, Đợi ứng cứu sự cố có thể bổ sung các giải pháp của Đội mình tự nghĩ ra, với mục tiêu phục hồi và ổn định hoạt động của hệ thống sau sự cố. Đây sẽ là một lợi thế của Đội so với các đội khác trong quá trình thực hiện.	Phần này chuyên gia hỗ trợ.
7	Phase 7. Tổng kết, rút kinh nghiệm	Thực hiện họp tổng kết báo cáo kết quả diễn tập Lập báo cáo ứng cứu sự cố. Rút ra các kinh nghiệm trong quá trình ứng cứu sự cố và trao đổi cùng chuyên gia.	
8	Bế mạc	Trao giấy chứng nhận cho học viên tham gia Trao quà cho các đội có thành tích tốt nhất trong suốt thời gian đào tạo Tuyên bố bế mạc sự kiện	

3.3.2.4. Lập báo cáo kết quả đào tạo và tập huấn

Mục đích của Báo cáo Kết quả là tổng hợp toàn bộ dữ liệu dự án, chứng minh tính minh bạch, sự tuân thủ các Tiêu chuẩn Thực hiện (SLA) đã cam kết và đo lường sự cải thiện năng lực ứng phó của lực lượng cán bộ TP. HCM sau sáp nhập.

3.3.2.4.1. Cấu trúc và Yêu cầu báo cáo

Báo cáo phải được trình bày theo cấu trúc khoa học, dễ đọc, và phải được phê duyệt bởi Đơn vị Giám sát Chất lượng trước khi trình lên Chủ đầu tư.

Định dạng: Bản cứng và Bản điện tử (PDF/Word), kèm theo tệp dữ liệu gốc (CSV/Excel) của các bảng thống kê.

Thời điểm Bàn giao: Trong vòng tối đa 02 ngày kể từ ngày kết thúc buổi tập huấn cuối cùng.

3.3.2.4.2. Nội dung Báo cáo

3.3.2.4.2.1. Tóm tắt

Tổng kết nhanh về mục tiêu, phạm vi và kết quả chính (tỷ lệ tham gia, điểm cải thiện nhận thức, và mức độ đạt mục tiêu SLA).

Đánh giá mức độ thành công của dự án và các đề xuất chiến lược tiếp theo.

3.3.2.4.2.2. Thống kê và Phân tích

Yêu cầu Báo cáo	Mục tiêu Cần Chứng minh	Phương pháp Đo lường
Tỷ lệ Tham gia và Hoàn thành	Đảm bảo 100% đối tượng mục tiêu được tiếp cận và hoàn thành tối thiểu 80% khóa học.	Bảng tổng hợp điểm danh và dữ liệu.
Mức độ Hài lòng	Chứng minh điểm hài lòng chung đạt tối thiểu 4.2/5.0.	Báo cáo chi tiết kết quả khảo sát, bao gồm đánh giá chất lượng Giảng viên và Nội dung.

3.3.2.4.2.3. Phân tích theo Đơn vị Hành chính

Báo cáo phải có khả năng phân tích chi tiết kết quả đạt được theo từng đơn vị hành chính mới sáp nhập.

Biểu đồ Phân bổ: Sử dụng biểu đồ để trực quan hóa các đơn vị có hiệu suất cao nhất và điểm yếu cần khắc phục (cần đào tạo bổ sung).

3.3.2.4.2.4. Phân tích rủi ro thực tế và Bài học kinh nghiệm:

Tài liệu hóa các rủi ro thực tế đã xảy ra trong quá trình triển khai (ví dụ: khó khăn trong việc sắp xếp lịch, vấn đề kỹ thuật tại địa điểm) và các biện pháp khắc phục đã áp dụng.

Trình bày Bài học Kinh nghiệm để cải thiện quy trình tổ chức và nội dung cho các dự án đào tạo trong tương lai.

3.3.3. Phương án triển khai mua sắm, bổ sung dịch vụ đảm bảo an toàn thông tin cho thiết bị đầu cuối

3.3.3.1. Danh mục các quy chuẩn, tiêu chuẩn kỹ thuật được áp dụng

3.3.3.1.1. Tiêu chuẩn về công nghệ thông tin

Truyền thư điện tử (SMTP/MIME): sử dụng khi hệ thống trả lời tự động qua e-mail.

Dịch vụ đồng bộ thời gian (NTP v3): sử dụng trong việc đồng bộ dữ liệu giữa các DC.

Văn bản (.doc, .docx, .xls, .xlsx, .pdf): sử dụng cho các văn bản, tài liệu đính kèm.

Ảnh đồ họa (JPEG, TIFF, PNG): sử dụng cho các tệp tin ảnh của hệ thống. Bộ ký tự và mã hóa cho tiếng Việt (TCVN 6909:2001): sử dụng cho việc hiển thị thông tin tiếng Việt của hệ thống.

Các tiêu chuẩn kỹ thuật điện – điện tử IEEE;

Tiêu chuẩn kỹ thuật Internet IETF;

Chuẩn kết nối truyền thông hệ thống mở OSI;

Tiêu chuẩn mạng máy tính cục bộ Ethernet LAN;

Tiêu chuẩn mạng máy tính diện rộng IP WAN;

Tiêu chuẩn giao diện truyền thông mạng máy tính;

Tiêu chuẩn công nghệ lưu trữ trong máy tính;

Tiêu chuẩn hệ điều hành máy tính đa nhiệm/ Multi-task, đa người dùng/ multi-user.

3.3.3.1.2. Tiêu chuẩn về an toàn thông tin

- An toàn giao vận SSL v3.0;
- An toàn truyền tệp tin (HTTPS): sử dụng cho việc thiết lập SSL Certificate.
- An toàn giải thuật mã hóa (RSA, SHA-2): sử dụng giải thuật mã hóa công khai để thiết lập các giao dịch an toàn;
- An toàn trao đổi bản tin XML (XML Signature Syntax and Processing): sử dụng cho việc đồng bộ dữ liệu;
- Tiêu chuẩn về quản lý thông tin tài khoản người dùng;
- Tiêu chuẩn OpenID: là một chuẩn mở cho xác thực được quảng bá bởi tổ chức phi lợi OpenID Foundation (OpenID được sử dụng trên internet, và các công ty như Google, WordPress, Yahoo, Paypal... sử dụng OpenID để xác thực người dùng);
- Tiêu chuẩn Oauth 2.0 (OAuth2 là một chuẩn mở để ủy quyền/phân quyền (authorization), OAuth2 cũng là nền tảng của OpenID Connect, nó cung cấp OpenID (xác thực - authentication) ở phía trên của OAuth2 (ủy quyền - authorization) để có một giải pháp bảo mật hoàn chỉnh hơn;
- Tiêu chuẩn TCVN 11930:2017 về "Công nghệ thông tin – Các kỹ thuật an toàn – Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ";

- TCVN ISO/IEC 27001:2009 Công nghệ thông tin - Hệ thống quản lý an toàn thông tin – Các yêu cầu;
- - TCVN ISO/IEC 27002:2011 Công nghệ thông tin-Các kỹ thuật an toàn- Quy tắc thực hành Quản lý an toàn thông tin;
- TCVN 8709-1:2011 ISO/IEC 15408-1:2009 Công nghệ thông tin- Các kỹ thuật an toàn- Các tiêu chí đánh giá an toàn CNTT- Phần 1: Giới thiệu và mô hình tổng quát;
- TCVN 8709-2:2011 ISO/IEC 15408-2:2008 Công nghệ thông tin- Các kỹ thuật an toàn- Các tiêu chí đánh giá an toàn CNTT- Phần 2: Các thành phần chức năng an toàn;
- TCVN 8709-3:2011 ISO/IEC 15408-3:2008 Công nghệ thông tin- Các kỹ thuật an toàn- Các tiêu chí đánh giá an toàn CNTT- Phần 3: Các thành phần đảm bảo an toàn;
- TCVN 10295:2014 ISO/IEC 27005:2011 Công nghệ thông tin-Các kỹ thuật an toàn-Quản lý rủi ro an toàn thông tin;
- TCVN 10541:2014 ISO/IEC 27003:2010 Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn triển khai hệ thống quản lý an toàn thông tin;
- TCVN 10543:2014 ISO/IEC 27010:2012 Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý an toàn trao đổi thông tin liên tổ chức, liên ngành;
- TCVN 11239:2015 Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý sự cố an toàn thông tin;
- TCVN 11386:2016 Công nghệ thông tin - Các kỹ thuật an toàn - Phương pháp đánh giá an toàn công nghệ thông tin;
- Thông tư 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 Quy định chi tiết và hướng dẫn một số điều của nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

3.3.3.2. Tính năng kỹ thuật chi tiết

Stt	Tính năng kỹ thuật chi tiết
1	**Mô tả chung**
1.1	- Có chức năng cho phép cập nhật tự động phiên bản mới của các phần mềm phòng, chống mã độc được cài đặt trên các máy trạm và máy chủ (agent).
	- Có chức năng cho phép cập nhật tự động dấu hiệu phát hiện mã độc mới trên các agent.
1.2	- Có cơ chế cập nhật online và offline
2	**Chức năng quản trị tập trung**
2.1	Chức năng quản lý chính sách tập trung:
	- Cho phép tạo nhóm và phân loại thiết bị đầu cuối theo các nhóm định nghĩa.

Stt	Tính năng kỹ thuật chi tiết
2.2	Chức năng thống kê các thông tin sau:
	- Tình hình lây nhiễm mã độc trên các máy trạm và máy chủ: IP máy bị nhiễm, tên máy bị nhiễm, thông tin về mã độc.
	- Các kết nối nguy hiểm trên các máy trạm và máy chủ: IP máy có kết nối nghi ngờ, Tên máy có kết nối nghi ngờ, Thông tin kết nối nghi ngờ: Tên phần mềm thực hiện kết nối nghi ngờ; Mã MD5 của phần mềm có kết nối nghi ngờ; IP đích của kết nối nghi ngờ.
	- Các hệ điều hành đang sử dụng trên các máy trạm và máy chủ: IP của máy trạm và máy chủ báo cáo thông tin hệ điều hành; Hệ điều hành đang sử dụng trên máy trạm và máy chủ; Thời gian cập nhật gần nhất của hệ điều hành trên máy trạm và máy chủ.
	- Trạng thái cập nhật giải pháp phòng, chống mã độc trên các máy trạm và máy chủ. Các thông tin thống kê bao gồm: số máy trạm và máy chủ không cập nhật trong vòng 15 ngày.
	- Tình hình virus trong hệ thống, đưa ra chi tiết các máy bị nhiễm, các dòng virus lây nhiễm và tình trạng virus đã được xử lý.
	- Thống kê theo cảnh báo, xuất cảnh báo.
2.3	Khả năng điều khiển các agent:
	- Cho phép ra lệnh quét cho các agent trên từng máy trạm và máy chủ, nhóm máy trạm và máy chủ hoặc toàn bộ máy trạm và máy chủ trong hệ thống.
	- Cho phép điều khiển thay đổi các chính sách phát hiện, ngăn chặn mã độc trên các agent.
	- Cho phép điều khiển cập nhật phiên bản phần mềm và dấu hiệu phát hiện mã độc trên mỗi agent.
	- Ra lệnh cập nhật/quét virus trên máy trạm và máy chủ từ xa, đặt lịch quét/update định kỳ. Hỗ trợ cập nhật offline trong hệ thống nội bộ, không cần máy trạm và máy chủ kết nối internet.
	- Tìm kiếm log event trên toàn bộ máy trạm và máy chủ.
	- Hỗ trợ cô lập (network, process) tạm thời các máy phục vụ điều tra.
3	Chức năng phòng chống mã độc:
	* Kiểm soát ứng dụng

Stt	Tính năng kỹ thuật chi tiết
	- Tính năng Blocklist chặn thực thi file theo giá trị hàng băm của chúng, hỗ trợ MD5 và SHA256, hỗ trợ đồng thời theo đường dẫn & liên kết của ứng dụng.
	* Kiểm soát thiết bị ngoại vi
	- Cho phép ngăn chặn rò rỉ dữ liệu nhạy cảm và nhiễm phần mềm độc hại thông qua ngăn chặn các thiết bị ngoại vi.
	- Giám sát việc kết nối, sử dụng các thiết bị lưu trữ ngoài, USB, thẻ nhớ trên các thiết bị đầu cuối (read-only).
	* Kiểm soát truy cập web/mail
	- Bảo vệ máy trạm và máy chủ khi truy cập web.
	* Công nghệ chống mã độc
	- Ngăn chặn mã độc, bảo vệ máy trạm và máy chủ theo thời gian thực.
	- Công nghệ quét thông minh.
	- Công nghệ kiểm soát mối đe dọa nâng cao, phân tích hành động đáng ngờ như: ngụy trang loại quy trình, thực hiện thực thi mã trong không gian bộ nhớ của một quy trình khác (thu giữ bộ nhớ quy trình để leo thang đặc quyền), tái tạo, gửi tệp, tránh bị phát hiện từ các ứng dụng liệt kê quy trình.
	- Tính năng phòng chống virus mã hóa dữ liệu.
	- Phát hiện và giảm thiểu rủi ro mất dữ liệu trong các cuộc tấn công ransomware nâng cao, tạo ra một bản sao dự phòng thời gian thực của các tệp trước khi chúng bị sửa đổi bởi các quy trình đáng ngờ.
	- Tự động phát hiện và chặn các cuộc tấn công không sử dụng tệp (fileless)
	- Tính năng tự động bảo vệ phần mềm bảo mật khỏi bị vô hiệu hóa hoặc thay đổi bởi những kẻ tấn công trên điểm cuối.
	- Tự động phát hiện và chặn các cuộc tấn công thông qua dòng lệnh mà không sử dụng tệp.
	- Chống lại tấn công mạng thế hệ mới, bao gồm các mối đe dọa dai dẳng tiên tiến. Bảo vệ bằng các thuật toán mạnh mẽ dựa trên trí tuệ nhân tạo và máy học.
	* Bảo vệ mạng
	- Tường lửa kiểm soát quyền truy cập của ứng dụng vào ra mạng và Internet.

Stt	Tính năng kỹ thuật chi tiết
	- IDS (Intrusion Detection System) phát hiện các cuộc tấn công mạng như brute-force, khai thác mạng, đánh cắp mặt khẩu, chuyển hướng download, bots, và Trojans.
	* Bảo vệ lưu lượng mạng
	- Phát hiện các cuộc tấn công mạng được thiết kế để có quyền truy cập vào các máy trạm và máy chủ thông qua các hình thức tấn công như: Tấn công brute-force, khai thác mạng, đánh cắp mặt khẩu, chuyển hướng download, bots, và Trojans.
	* Kiểm soát lổ hỏng bảo mật
	- Giám sát các hành vi người dùng, đưa ra các cảnh bảo về rủi ro hành vi người dùng, những nguy Cơ và mối đe dọa cho an ninh thông tin xuất phát từ hành vi của người dùng.
	- Giám sát Tình Trạng lỗ hỏng bảo mật, bản vá Hệ điều hành trên Hệ điều hành Windows và các phần mềm cài đặt trên máy người dùng.
	* Tương thích các hệ điều hành
	- Windows, Linux
	* Máy chủ quản trị
	- Giải pháp cho phép triển khai thành phần quản trị On-premise hoặc Cloud của hãng
	- Có thể triển khai linh hoạt trên hạ tầng vật lý hoặc ảo hóa dễ dàng nâng cấp và mở rộng quy mô khi cần thiết.
	- Cơ chế kiểm soát quyền quản trị viên, trong trường hợp hacker làm chủ được máy chủ quản lý trung tâm cũng không ra lệnh được xuống cho các máy trạm nếu không có USB token
	- Hỗ trợ triển khai máy chủ quản trị theo chế độ HA / Load Balancing, Replica Database đảm bảo tính sẵn sàng cao cho máy chủ quản trị và Cơ sở dữ liệu.
4	Chức năng phát hiện và ứng phó
	- Khả năng tìm kiếm các chỉ số thỏa hiệp (IoC), đồ thị quá trình lấy nhiễm và tấn công, gán các giai đoạn tấn công tương ứng kỹ thuật trong MITRE ATT&CK framework.
	- Hành động phản hồi cách ly file, cô lập thiết bị, quét tự động, gửi file lên hộp cát phân tích.

Stt	Tính năng kỹ thuật chi tiết
	- Phân tích nguyên nhân gốc rễ.
	- Công cụ săn tìm mối de dọa Threat Hunting
	- Phát hiện, ngăn chặn tấn công APT nâng cao.

3.3.3.3. Tính năng chính của giải pháp phòng chống mã độc Endpoint

3.3.3.3.1. Quản lý chính sách tập trung

Giải pháp cho phép tạo nhóm và phân loại thiết bị đầu cuối (endpoint) dựa trên các tiêu chí định nghĩa sẵn như loại thiết bị (máy chủ, máy trạm), phòng ban, hoặc vị trí mạng, giúp tổ chức dễ dàng áp dụng chính sách phù hợp cho từng nhóm đối tượng.

3.3.3.3.2. Thống kê các thông tin

Giải pháp cho phép thống kê chi tiết tình hình lây nhiễm mã độc trên toàn bộ các máy trạm và máy chủ trong hệ thống. Thông qua cơ chế giám sát tập trung, hệ thống tự động thu thập và hiển thị các thông tin quan trọng như địa chỉ IP của máy bị nhiễm, tên thiết bị, thời điểm phát hiện, loại và họ mã độc, cùng với mức độ nguy hiểm và trạng thái xử lý (đã cách ly, đã xóa, chưa xử lý). Tính năng này giúp bộ phận quản trị an toàn thông tin nhận diện nhanh các điểm nhiễm, khoanh vùng khu vực bị ảnh hưởng và triển khai biện pháp khắc phục kịp thời, góp phần giảm thiểu rủi ro lây lan và đảm bảo tính ổn định, an toàn cho toàn bộ hệ thống mạng.

Giải pháp cung cấp tính năng giám sát toàn diện các kết nối mạng trên máy trạm và máy chủ, giúp phát hiện sớm những hoạt động truy cập tiềm ẩn rủi ro hoặc bất thường. Hệ thống tự động thu thập và phân tích các thông tin chi tiết bao gồm địa chỉ IP và tên máy có kết nối nghi ngờ, tên phần mềm hoặc tiến trình thực hiện kết nối, mã băm MD5 của phần mềm để phục vụ công tác truy vết nguồn gốc, cùng địa chỉ IP đích hoặc tên miền của kết nối nghi ngờ. Các thông tin này được sử dụng để nhận diện hành vi bất thường, phục vụ cho việc cảnh báo sớm và ngăn chặn các cuộc tấn công mạng.

Giải pháp được trang bị chức năng thống kê và giám sát thông tin hệ điều hành trên toàn bộ máy trạm và máy chủ trong hệ thống. Thông qua cơ chế thu thập dữ liệu tự động, hệ thống ghi nhận và hiển thị địa chỉ IP của từng thiết bị báo cáo, tên và phiên bản hệ điều hành đang sử dụng, cùng thời gian cập nhật bản vá bảo mật gần nhất. Việc quản lý tập trung này giúp kiểm soát mức độ an toàn của nền tảng hệ thống và phát hiện các thiết bị chưa cập nhật bản vá bảo mật.

Giải pháp cung cấp chức năng giám sát và thống kê chi tiết trạng thái cập nhật phần mềm mã độc của toàn bộ hệ thống máy trạm và máy chủ, bao gồm số lượng máy trạm và máy chủ chưa được cập nhật trong khoảng thời gian xác định (ví dụ 15 ngày), qua đó giúp quản trị viên nắm bắt mức độ tuân thủ chính sách an toàn thông tin của từng đơn vị.

Giải pháp cung cấp chức năng thống kê chi tiết tình hình virus trong toàn bộ hệ thống , giúp bộ phận an toàn thông tin nắm bắt và kiểm soát hiệu quả mức độ lây nhiễm mã độc trên các máy trạm và máy chủ. Hệ thống tự động tổng hợp và hiển thị danh sách các thiết bị bị nhiễm , bao gồm địa chỉ IP, tên máy, thời gian , cùng thông tin chi tiết về dòng virus (virus family), chủng loại và mức độ nguy hiểm. Ngoài ra, tính năng này còn

cho biết trạng thái xử lý của từng sự cố như đã xóa, đã cách ly, đang theo dõi hoặc chưa xử lý, giúp quản trị viên đánh giá nhanh hiệu quả phản ứng và khắc phục sự cố. Nhờ khả năng phân tích sâu và báo cáo trực quan, hệ thống hỗ trợ theo dõi xu hướng lây nhiễm theo thời gian, khu vực hoặc nhóm thiết bị, từ đó đưa ra biện pháp phòng ngừa chủ động, tối ưu chính sách bảo vệ và nâng cao khả năng phòng thủ trước các mối đe dọa mã độc phức tạp.

3.3.3.3.3. Quản lý và điều khiển các agent

Giải pháp phòng chống mã độc Endpoint được thiết kế với năng lực quản lý và điều khiển tập trung mạnh mẽ, cho phép thực hiện các thao tác điều khiển, quét và cập nhật trên các thiết bị đầu cuối (endpoint) một cách linh hoạt, đảm bảo việc vận hành, giám sát và ứng phó sự cố được thực hiện nhanh chóng, đồng bộ và an toàn, giúp đảm bảo phát hiện sớm và xử lý triệt để các mối đe dọa tiềm ẩn.

Giải pháp còn hỗ trợ điều chỉnh linh hoạt chính sách phát hiện, ngăn chặn mã độc theo từng khu vực hoặc nhóm người dùng, đồng thời điều khiển quá trình cập nhật phiên bản phần mềm và cơ sở dữ liệu nhận diện mã độc (signature, pattern) cho từng agent. Toàn bộ quá trình quét virus, cập nhật phần mềm hoặc mẫu nhận diện có thể được thực hiện từ xa hoặc đặt lịch tự động định kỳ , giúp tối ưu hiệu quả vận hành và giảm tải công việc thủ công cho đội ngũ quản trị.

Giải pháp hỗ trợ điều khiển cập nhật từ xa phiên bản phần mềm và cơ sở dữ liệu nhận diện mã độc (signature) cho từng agent, bảo đảm rằng mọi máy trạm và máy chủ luôn ở trạng thái được bảo vệ với khả năng nhận diện các mẫu tấn công mới nhất.

Đặc biệt giải pháp cho phép ra lệnh cập nhật hoặc quét virus từ xa đối với máy trạm và máy chủ, đồng thời hỗ trợ đặt lịch tự động quét và cập nhật theo chu kỳ định nghĩa (ngày/tuần/tháng). Bên cạnh đó giải pháp hỗ trợ hệ thống cập nhật trong môi trường nội bộ, đảm bảo máy trạm và máy chủ vẫn được cập nhật đầy đủ ngay cả khi không kết nối Internet, phù hợp với các khu vực mạng cách ly hoặc có yêu cầu bảo mật cao.

Giải pháp có khả năng tìm kiếm và truy vấn log sự kiện (event log) được ghi nhận từ tất cả các máy trạm và máy chủ, phục vụ cho công tác điều tra, phân tích sự cố và đánh giá tuân thủ chính sách bảo mật. Việc tra cứu có thể được thực hiện theo thời gian, tên thiết bị, người dùng hoặc loại sự kiện bảo mật.

Trong trường hợp phát hiện thiết bị có dấu hiệu lây nhiễm hoặc hoạt động bất thường, giải pháp cho phép cô lập tạm thời máy trạm hoặc máy chủ ở cấp độ mạng (network isolation) hoặc tiến trình (process isolation), nhằm ngăn chặn lây lan và hỗ trợ công tác điều tra – xử lý sự cố. Tổ hợp các tính năng này giúp đơn vị vận hành chủ động, linh hoạt và an toàn hơn trong việc quản lý phòng chống mã độc trên quy mô lớn, đáp ứng đầy đủ yêu cầu vận hành an toàn thông tin theo các tiêu chuẩn quốc gia và quốc tế.

3.3.3.3.4. Kiểm soát ứng dụng

Giải pháp phòng chống mã độc được trang bị tính năng Blocklist tiên tiến, cho phép ngăn chặn việc thực thi các tệp tin đáng ngờ hoặc độc hại dựa trên giá trị băm (hash value) của chúng. Hệ thống hỗ trợ đồng thời hai chuẩn băm phổ biến là MD5 và SHA256, đảm bảo khả năng nhận diện chính xác và toàn diện các biến thể của mã độc hoặc tệp thực thi bị giả mạo. Thông qua cơ chế này, quản trị viên có thể thiết lập danh sách chặn (Blocklist) theo giá trị băm, đường dẫn hoặc liên kết ứng dụng, từ đó ngăn không cho các file có nguy cơ cao được khởi chạy hoặc truy cập trong môi trường hệ

thống. Tính năng này đặc biệt hữu ích trong việc ngăn chặn các mối đe dọa chưa có mẫu nhận diện (unknown threats) hoặc các biến thể mã độc tùy chỉnh (mutated malware) thường xuyên thay đổi cấu trúc. Khi một tệp tin trùng khớp với giá trị băm trong danh sách chặn, hệ thống sẽ tự động chặn thực thi, cô lập tiến trình và ghi nhận sự kiện cảnh báo, giúp giảm thiểu rủi ro lây nhiễm, bảo vệ tính toàn vẹn của hệ thống và tăng cường khả năng phòng thủ chủ động trước các hình thức tấn công hiện đại như ransomware, trojan, hay APT.

3.3.3.3.5. Kiểm soát thiết bị ngoại vi

Giải pháp cho phép kiểm soát toàn diện việc kết nối các thiết bị ngoại vi như USB, ổ cứng di động, thẻ nhớ, thiết bị di động hoặc ổ đĩa mạng. Khi người dùng cắm thiết bị ngoại vi, hệ thống sẽ tự động nhận diện, ghi lại thông tin và áp dụng chính sách phù hợp như cho phép, cảnh báo hoặc chặn truy cập.

Giải pháp cho phép quản trị viên cấu hình chính sách hạn chế hành động ghi dữ liệu ra thiết bị lưu trữ ngoài, chỉ cho phép truy cập đọc dữ liệu (read-only). Điều này đảm bảo rằng người dùng có thể truy xuất dữ liệu phục vụ công việc nhưng không thể sao chép hoặc di chuyển thông tin nhạy cảm ra khỏi tổ chức.

3.3.3.3.6. Kiểm soát truy cập web/mail

Giải pháp được trang bị tính năng bảo vệ toàn diện khi truy cập web , giúp ngăn chặn các mối đe dọa trực tuyến và đảm bảo an toàn cho người dùng cũng như hệ thống máy chủ trong quá trình truy cập Internet. Hệ thống tự động phân tích và kiểm soát các kết nối web , chặn truy cập đến các trang web độc hại, giả mạo, lừa đảo (phishing), hoặc chứa mã khai thác lỗ hổng (exploit code) có khả năng phát tán mã độc. Đồng thời, giải pháp giám sát và lọc nội dung truy cập, ngăn chặn tải xuống các tệp tin đáng ngờ hoặc thực thi không an toàn từ Internet.

3.3.3.3.7. Công nghệ chống mã độc

Giải pháp có khả năng ngăn chặn mã độc, bảo vệ máy trạm và máy chủ theo thời gian thực, đảm bảo phát hiện và xử lý sớm các mối đe dọa trước khi gây hại đến hệ thống.

Ứng dụng công nghệ quét thông minh giúp nhận diện nhanh các mẫu mã độc mới và hành vi bất thường, giảm thiểu cảnh báo giả và tăng hiệu quả xử lý sự cố.

Công nghệ kiểm soát mối đe dọa nâng cao cho phép phân tích hành vi đáng ngờ như ngụy trang quy trình, thực thi mã trong vùng nhớ của quy trình khác hoặc tái tạo và gửi tệp nhằm tránh bị phát hiện, từ đó giúp ngăn chặn sớm các hoạt động leo thang đặc quyền hoặc xâm nhập hệ thống.

Tính năng phòng chống virus mã hóa dữ liệu giúp ngăn chặn các cuộc tấn công ransomware, bảo vệ tính toàn vẹn của tệp và thông tin quan trọng trong hệ thống.

Cơ chế phát hiện và giảm thiểu rủi ro mất dữ liệu chủ động tạo bản sao lưu thời gian thực của các tệp quan trọng trước khi chúng bị sửa đổi hoặc mã hóa, đảm bảo khả năng khôi phục dữ liệu nhanh chóng.

Giải pháp có thể tự động phát hiện và chặn các cuộc tấn công không sử dụng tệp (fileless), vốn lợi dụng các tiến trình hợp pháp của hệ điều hành để thực thi mã độc mà không tạo ra tệp đáng ngờ.

Cơ chế tự bảo vệ giúp phần mềm bảo mật không bị vô hiệu hóa hoặc thay đổi bởi kẻ tấn công, đảm bảo khả năng hoạt động ổn định và liên tục của hệ thống phòng vệ.

Khả năng tự động phát hiện và chặn các cuộc tấn công thông qua dòng lệnh (command-line attacks) mà không cần sử dụng tệp, ngăn ngừa việc lạm dụng công cụ dòng lệnh của hệ điều hành để thực hiện hành vi xâm nhập.

Giải pháp có khả năng đối phó với các cuộc tấn công mạng thế hệ mới và mối đe dọa dai dẳng tiên tiến (APT), sử dụng các thuật toán học máy và trí tuệ nhân tạo để học và thích ứng với các hành vi tấn công mới.

3.3.3.3.8. Bảo vệ mạng

Tường lửa được cấu hình để kiểm soát quyền truy cập của các ứng dụng ra và vào mạng nội bộ cũng như Internet. Cơ chế này giúp ngăn chặn các ứng dụng trái phép hoặc không đáng tin cậy thực hiện kết nối ra ngoài, giảm thiểu nguy cơ rò rỉ dữ liệu và xâm nhập từ bên ngoài.

Hệ thống phát hiện xâm nhập (IDS – Intrusion Detection System) được triển khai để giám sát và phân tích lưu lượng mạng, có thể gắn cờ các hành vi bất thường như nỗ lực thay đổi giao diện hoặc nền màn hình, dấu hiệu cho thấy khả năng bị chiếm quyền điều khiển hoặc cài đặt mã độc. IDS cũng có khả năng phát hiện việc tiêm nhiễm các tệp DLL hoặc cài đặt trình điều khiển độc hại (malicious driver). Cơ chế giám sát cấp hệ thống cho phép nhận diện sớm các hành vi can thiệp sâu vào nhân hệ điều hành, ngăn chặn việc chiếm quyền hoặc kiểm soát trái phép. Bên cạnh đó, IDS được tích hợp để phát hiện và cảnh báo các loại tấn công mạng phổ biến như brute-force, khai thác lỗ hổng, đánh cắp mật khẩu, chuyển hướng tải xuống, botnet hoặc Trojan. Hệ thống này giúp đảm bảo khả năng phát hiện sớm và phản ứng kịp thời trước các mối đe dọa xâm nhập mạng

3.3.3.3.9. Bảo vệ lưu lượng mạng

Giải pháp bảo mật có khả năng phát hiện các cuộc tấn công mạng được thiết kế để xâm nhập và chiếm quyền điều khiển máy trạm hoặc máy chủ. Các hình thức tấn công được nhận diện bao gồm brute-force, khai thác lỗ hổng mạng, đánh cắp mật khẩu, chuyển hướng tải xuống độc hại, hoạt động của botnet và mã độc Trojan.

3.3.3.3.10. Kiểm soát lỗ hổng bảo mật

Giải pháp cung cấp tính năng giám sát hành vi người dùng trên máy trạm và máy chủ, nhằm phát hiện các hoạt động bất thường có thể gây rủi ro cho an ninh thông tin. Các hành vi như truy cập trái phép, thay đổi cấu hình hệ thống, sao chép hoặc truyền dữ liệu nhạy cảm ra ngoài đều được theo dõi và cảnh báo kịp thời.

Giải pháp đồng thời giám sát tình trạng lỗ hổng bảo mật và bản vá hệ điều hành, đặc biệt trên nền tảng Windows và các phần mềm cài đặt phổ biến. Hệ thống tự động thu thập, phân tích và đánh giá tình trạng cập nhật của từng thiết bị, giúp phát hiện những điểm yếu tiềm ẩn hoặc bản vá còn thiếu.

3.3.3.3.11. Tương thích các hệ điều hành

Giải pháp tương thích bảo vệ hệ điều hành Windows và Linux

3.3.3.3.12. Máy chủ quản trị tập trung

Giải pháp hỗ trợ triển khai linh hoạt thành phần quản trị dưới dạng On-premise hoặc Cloud do hãng cung cấp, giúp phù hợp với hạ tầng và chính sách vận hành của

từng tổ chức. Mô hình triển khai có thể tùy chọn theo nhu cầu bảo mật nội bộ hoặc tận dụng lợi thế mở rộng và quản lý tập trung từ nền tảng điện toán đám mây.

Giải pháp có khả năng triển khai trên cả hạ tầng vật lý và môi trường ảo hóa, hỗ trợ linh hoạt trong việc cấu hình, mở rộng quy mô hoặc nâng cấp khi cần thiết. Giải pháp được thiết kế theo kiến trúc module, giúp tối ưu tài nguyên và dễ dàng đáp ứng nhu cầu phát triển trong tương lai mà không ảnh hưởng đến hoạt động hiện tại.

Giải pháp cung cấp cơ chế kiểm soát quyền quản trị viên nâng cao, trong đó các lệnh điều khiển hoặc thay đổi cấu hình quan trọng chỉ được thực hiện khi có xác thực vật lý bằng USB Token. Điều này đảm bảo rằng ngay cả khi máy chủ quản lý trung tâm bị chiếm quyền, kẻ tấn công cũng không thể ra lệnh xuống các máy trạm, qua đó giảm thiểu nguy cơ tấn công lan rộng. Đây là tính năng cực kì quan trọng và mới trên thị trường, mang lại khả năng bảo vệ tầng cuối cùng trước nguy cơ kiểm soát hệ thống. Trong trường hợp hacker chiếm quyền kiểm soát máy chủ quản lý trung tâm, hacker không thể gửi lệnh xuống máy trạm nếu không có USB Token xác thực.

Hệ thống hỗ trợ triển khai máy chủ quản trị theo chế độ High Availability (HA), Load Balancing và Replica Database, nhằm đảm bảo khả năng chịu lỗi, tính sẵn sàng cao và hoạt động liên tục của hệ thống. Các cơ chế đồng bộ cơ sở dữ liệu và phân tải xử lý giúp duy trì hiệu năng ổn định, đáp ứng yêu cầu vận hành 24/7.

3.3.3.3.13. Phát hiện và ứng phó

Giải pháp có khả năng tìm kiếm và phân tích các chỉ số thỏa hiệp (Indicators of Compromise – IoC), cho phép xác định nhanh các dấu hiệu bất thường trong hệ thống như địa chỉ IP, tên miền, hash file, hoặc hành vi nghi ngờ. Hệ thống trực quan hóa toàn bộ đồ thị quá trình lây nhiễm và chuỗi tấn công, đồng thời liên kết từng giai đoạn với các kỹ thuật tương ứng trong khung MITRE ATT&CK, giúp nhà phân tích dễ dàng xác định chiến thuật và kỹ thuật được kẻ tấn công sử dụng.

Giải pháp hỗ trợ hành động phản hồi tự động hoặc bán tự động như cách ly file độc hại, cô lập thiết bị bị nhiễm khỏi mạng, thực hiện quét sâu toàn bộ hệ thống, hoặc gửi file đáng ngờ lên hộp cát (sandbox) để phân tích hành vi chi tiết. Những biện pháp phản ứng này giúp ngăn chặn sự lây lan của mã độc và giảm thiểu thiệt hại trong giai đoạn đầu của cuộc tấn công.

Giải pháp có chức năng phân tích nguyên nhân gốc rễ (Root Cause Analysis), cho phép truy vết toàn bộ tiến trình và sự kiện liên quan đến sự cố, xác định điểm khởi phát, cách thức lây nhiễm và phạm vi ảnh hưởng. Thông tin này hỗ trợ tối ưu cho công tác điều tra số (digital forensics) và nâng cao năng lực phòng thủ trong tương lai

Giải pháp được trang bị công cụ săn tìm mối đe dọa (Threat Hunting) giúp chuyên gia bảo mật chủ động rà soát hệ thống, tìm kiếm các hành vi ẩn giấu hoặc dấu vết tấn công mà các cơ chế phòng thủ tự động có thể bỏ sót. Tính năng này cho phép phát hiện sớm và xử lý kịp thời các mối đe dọa tiềm ẩn.

Ngoài ra, hệ thống còn có khả năng phát hiện và ngăn chặn các cuộc tấn công có chủ đích nâng cao (Advanced Persistent Threat – APT) bằng cách kết hợp công nghệ phân tích hành vi, trí tuệ nhân tạo và thông tin tình báo mối đe dọa (threat intelligence), giúp nhận diện các chiến dịch tấn công tinh vi và duy trì khả năng phòng thủ chủ động trên toàn hệ thống.

3.3.3.4. Yêu cầu kết quả đạt được

Việc bổ sung và mở rộng triển khai giải pháp bảo mật thiết bị đầu cuối là cần thiết nhằm tăng cường khả năng bảo vệ hạ tầng công nghệ thông tin của thành phố, bảo đảm an toàn mạng, dữ liệu và các hệ thống ứng dụng trọng yếu trong quá trình vận hành và chuyển đổi số.

Giải pháp mở rộng giúp nâng cao năng lực phòng, chống và giám sát phần mềm độc hại, đồng thời tăng cường mức độ tin cậy và tính sẵn sàng của hệ thống thông tin, góp phần bảo vệ hoạt động giao dịch điện tử và hạ tầng số của thành phố trước các mối đe dọa ngày càng tinh vi.

Hệ thống sau khi được bổ sung sẽ có khả năng phản ứng nhanh trước các sự cố an ninh mạng, hỗ trợ phát hiện, phân tích và xử lý mã độc theo thời gian thực, đồng thời chia sẻ dữ liệu và chỉ số lây nhiễm với các cơ quan chức năng theo đúng quy định.

Bên cạnh đó, việc mở rộng triển khai còn giúp đội ngũ quản trị hệ thống dễ dàng kiểm soát, theo dõi tình hình an ninh của các thiết bị đầu cuối, chủ động thiết lập các chính sách phòng thủ, ngăn chặn sự lan truyền của mã độc trong toàn bộ mạng nội bộ và hệ thống kết nối Metronet của thành phố.

3.3.4. Phương án triển khai kiểm tra, phân tích, đánh giá an toàn thông tin cho hạ tầng mạng, máy chủ, máy trạm và thiết bị số tại các cơ quan, đơn vị trên địa bàn thành phố

3.3.4.1. Tiêu chuẩn thực hiện

Đối với việc thực hiện kiểm tra, đánh giá an toàn thông tin cho hệ thống thông tin quan trong và ở cấp độ 3, vì vậy nhà cung cấp dịch vụ được yêu cầu phải đáp ứng các tiêu chuẩn thực hiện bên dưới.

3.3.4.1.1. Tiêu chuẩn Quốc gia TCVN 11930:2017 (TCVN 11930:2017)

Tiêu chuẩn Quốc gia TCVN 11930:2017 – Công nghệ thông tin – Các kỹ tuật an toàn – Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ. Tiêu chuẩn này quy định các yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ. Yêu cầu an toàn cơ bản quy định trong tiêu chuẩn này tập trung vào các yêu cầu đảm bản an toàn hệ thống thông tin. Các yêu cầu khác về an toàn thông tin, không liên quan trực tiếp đến bảo đảm an toàn hệ thống thông tin (ví dụ: bảo vệ thông tin cá nhân, bảo vệ trẻ em trên mạng…) không thuộc phạm vi của Tiêu chuẩn này.

Các yêu cầu của từng cấp độ được chia làm hai nhóm: yêu cầu quản lý và yêu cầu kỹ thuật.

- Yêu cầu quản lý: đưa ra các yêu cầu về mặt quản lý nhằm quản lý việc xây dựng, quản lý vận hành và gỡ bỏ hệ thống thông tin bảo đảm an toàn. Các yêu cầu quản lý được chia thành các nhóm yêu cầu: thiết lập chính sách an toàn thông tin; tổ chức đảm bảo an toàn thông tin; bảo đảm nguồn nhân lực; quản lý thiết kế, xây dựng hệ thống; quản lý vận hành hệ thống.

- Yêu cầu kỹ thuật: đưa ra các yêu cầu về mặt kỹ thuật để bảo đảm việc thiết kế, xây dựng và thiết lập hệ thống thông tin bảo đảm an toàn. Các yêu cầu kỹ thuật được chia thành các nhóm yêu cầu: bảo đảm an toàn mạng; bảo đảm an toàn máy chủ; bảo đảm an toàn ứng dụng; bảo đảm an toàn dữ liệu.

3.3.4.1.2. Thông tư số 12/2022/TT-BTTT

Thông tư 12/2022/TT-BTTTT ngày 12/8/2022 về Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ quy định chi tiết, hướng dẫn bảo đảm an toàn hệ thống thông tin theo cấp độ, bao gồm: xác định hệ thống thông tin và thuyết minh cấp độ an toàn hệ thống thông tin; yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ; kiểm tra, đánh giá an toàn thông tin; chế độ báo cáo. Đối với yêu cầu bảo đảm an toàn hệ thống thông tin thực hiện theo yêu cầu cơ bản quy định tại Thông tư này và Tiêu chuẩn quốc gia TCVN 11930:2017 về Công nghệ thông tin - các kỹ thuật an toàn - yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ. Yêu cầu cơ bản đối với từng cấp độ quy định tại Thông tư này là các yêu cầu tối thiểu để bảo đảm an toàn hệ thống thông tin, bao gồm yêu cầu cơ bản về quản lý, yêu cầu cơ bản về kỹ thuật và không bao gồm các yêu cầu bảo đảm an toàn vật lý.

3.3.4.1.3. Tiêu chuẩn Open Web Application Security Project (OWASP)

Tiêu chuẩn OWASP, là một nguồn tài liệu quan trọng về an ninh ứng dụng web và bảo mật thông tin. OWASP ra đời với mục tiêu bảo vệ ứng dụng web khỏi các mối đe dọa bảo mật thông qua việc cung cấp hướng dẫn, công cụ và kiến thức cho cộng đồng phát triển và quản lý ứng dụng web.

Tiêu chuẩn OWASP cung cấp nhiều dự án và tài liệu quan trọng, trong đó nổi bật nhất là "OWASP Top 10." Danh sách này liệt kê 10 lỗ hổng bảo mật phổ biến nhất trong ứng dụng web, giúp các nhà phát triển và chuyên gia bảo mật hiểu và ưu tiên những rủi ro quan trọng.

3.3.4.2. Yêu cầu kỹ thuật chi tiết

3.3.4.2.1. Kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ và Kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin được phê duyệt

Nội dung đánh giá cụ thể gồm các bước sau:

Bước 1: Khảo sát và thu thập thông tin:

- Khảo sát và thực hiện thu thập thông tin chủ quản hệ thống thông tin.
- Khảo sát và thực hiện thu thập thông tin đơn vị vận hành.
- Khảo sát phạm vi, quy mô của hệ thống.
- Khảo sát mô tả cấu trúc của hệ thống.
- Khảo sát hiện trạng và thành phần hệ thống đang có nhằm xác định cấp độ mà hệ thống thông tin đang đảm nhiệm.
- Khảo sát danh sách các cổng thông tin, hệ thống thông tin, phần mềm, ứng dụng đang có của đơn vị.
- Khảo sát các giải pháp bảo mật, giải pháp mạng và các thiết lập chung cho hệ thống.
- Khảo sát và phân loại thông tin đang được xử lý của hệ thống.

- Khảo sát thông tin người dùng và vai trò, trách nhiệm hệ thống thông tin đang cung cấp.

Bước 2: Đánh giá và lập hồ sơ cấp độ an toàn thông tin:

- Phân tích đánh giá hiện trạng.
- Đánh giá các biện pháp kiểm soát tương ứng với cấp độ đề xuất.
- Đánh giá việc thiết kế, thiết lập chính sách, cấu hình hệ thống theo phương án bảo đảm an toàn thông tin.

Stt	Nội dung công việc	Yêu cầu cơ bản
I	Yêu cầu quản lý	
1.1	Thiết lập chính sách an toàn thông tin	
1.1.1	Chính sách an toàn thông tin	Xây dựng chính sách an toàn thông tin, bao gồm:
1.1.1	Chính sách an toàn thông tin	Xây dựng chính sách an toàn thông tin, bao gồm:
		a) Xác định các mục tiêu, nguyên tắc bảo đảm an toàn thông tin;
		b) Xác định trách nhiệm của đơn vị chuyên trách về an toàn thông tin, các cán bộ làm về an toàn thông tin và các đối tượng thuộc phạm vi điều chỉnh của chính sách an toàn thông tin;
		c) Xác định phạm vi chính sách an toàn thông tin bao gồm:
		- Phạm vi quản lý về vật lý và logic của tổ chức;
		- Các ứng dụng, dịch vụ hệ thống cung cấp;
		- Nguồn nhân lực bảo đảm an toàn thông tin.
		d) Xây dựng chính sách an toàn thông tin bao gồm:
		- Quản lý an toàn mạng;
		- Quản lý an toàn máy chủ và ứng dụng;
		- Quản lý an toàn dữ liệu;
		- Quản lý an toàn thiết bị đầu cuối;
		- Quản lý phòng chống phần mềm độc hại;

Stt	Nội dung công việc	Yêu cầu cơ bản
		- Quản lý điểm yếu an toàn thông tin;
		- Quản lý giám sát an toàn hệ thống thông tin;
		- Quản lý an toàn người sử dụng đầu cuối.
1.1.2	Xây dựng và công bố	a) Chính sách được tổ chức/bộ phận được ủy quyền thông qua trước khi công bố áp dụng;
		b) Chính sách được công bố trước khi áp dụng.
1.1.3	Rà soát, sửa đổi	Định kỳ 02 năm hoặc khi có thay đổi chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.
1.2	Tổ chức bảo đảm an toàn thông tin	
1.2.1	Đơn vị chuyên trách về an toàn thông tin	a) Thành lập hoặc chỉ định đơn vị/bộ phận chuyên trách về an toàn thông tin trong tổ chức;
		b) Phân định vai trò, trách nhiệm, cơ chế phối hợp của các bộ phận, cán bộ trong đơn vị chuyên trách về an toàn thông tin.
1.2.2	Phối hợp với cơ quan/tổ chức có thẩm quyền	a) Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin;
		b) Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin;
		c) Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.
1.3	Bảo đảm nguồn nhân lực	
1.3.1	Tuyển dụng	a) Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng;
		b) Có quy định, quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ.

Stt	Nội dung công việc	Yêu cầu cơ bản
1.3.2	Trong quá trình làm việc	a) Có quy định về việc thực hiện nội quy, quy chế bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống;
		b) Có kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng;
		c) Định kỳ hàng năm, tổ chức đào tạo các kỹ năng cơ bản về an toàn thông tin cho người sử dụng.
1.3.3	Chấm dứt hoặc thay đổi công việc	a) Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức;
		b) Có quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc;
		c) Có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.
1.4	Quản lý thiết kế, xây dựng hệ thống	
1.4.1	Thiết kế an toàn hệ thống thông tin	a) Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin;
		b) Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin;
		c) Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ;
		d) Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin;
		đ) Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.
1.4.2	Phát triển phần mềm thuê khoán	a) Có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán;

Stt	Nội dung công việc	Yêu cầu cơ bản
		b) Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm;
		c) Kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng;
		d) Kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng.
1.4.3	Thử nghiệm và nghiệm thu hệ thống	a) Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng;
		b) Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống;
		c) Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống;
		d) Có đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống;
		đ) Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.
1.5	Quản lý vận hành hệ thống	
1.5.1	Quản lý an toàn mạng	Chính sách, quy trình quản lý an toàn mạng bao gồm:
		a) Quản lý, vận hành hoạt động bình thường của hệ thống;
		b) Cập nhật, sao lưu dự phòng và khôi phục hệ thống sau khi xảy ra sự cố;
		c) Truy cập và quản lý cấu hình hệ thống;
		d) Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác.
1.5.2	Quản lý an toàn máy chủ và ứng dụng	Chính sách, quy trình quản lý an toàn máy chủ và ứng dụng bao gồm:
		a) Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ;
		b) Truy cập mạng của máy chủ;

Stt	Nội dung công việc	Yêu cầu cơ bản
		c) Truy cập và quản trị máy chủ và ứng dụng;
		d) Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố;
		đ) Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng;
		e) Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống;
		g) Cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác.
1.5.3	Quản lý an toàn dữ liệu	Chính sách, quy trình quản lý an toàn dữ liệu bao gồm:
		a) Xây dựng và thực thi chính sách, quy trình dự phòng và khôi phục dữ liệu;
		b) Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.
1.5.4	Quản lý an toàn thiết bị đầu cuối	Chính sách, quy trình quản lý thiết bị đầu cuối bao gồm:
		a) Quản lý, vận hành hoạt động bình thường cho thiết bị đầu cuối;
		b) Kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa;
		c) Cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống.
1.5.5	Quản lý phòng chống phần mềm độc hại	Chính sách, quy trình quản lý phần mềm độc hại bao gồm:
		a) Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; dò quét, kiểm tra phần mềm độc hại trên máy tính, máy chủ và thiết bị di động;
		b) Cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng;
		c) Gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động;
		d) Định kỳ thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Thực hiện kiểm tra và xử lý phần

Stt	Nội dung công việc	Yêu cầu cơ bản
		mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.
1.5.6	Quản lý giám sát an toàn hệ thống thông tin	Chính sách, quy trình quản lý giám sát an toàn hệ thống thông tin bao gồm:
		a) Quản lý, vận hành hoạt động bình thường của hệ thống giám sát;
		b) Đối tượng giám sát bao gồm: thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống (nếu có);
		c) Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát;
		d) Truy cập và quản trị hệ thống giám sát;
		đ) Loại thông tin cần được giám sát;
		e) Lưu trữ và bảo vệ thông tin giám sát (nhật ký hệ thống);
		g) Đồng bộ thời gian giữa hệ thống giám sát và thiết bị được giám sát;
		h) Theo dõi, giám sát và cảnh báo sự cố phát hiện được trên hệ thống thông tin.
1.5.7	Quản lý điểm yếu an toàn thông tin	Chính sách, quy trình quản lý điểm yếu an toàn thông tin bao gồm:
		a) Quản lý thông tin các thành phần có trong hệ thống có khả năng tồn tại điểm yếu an toàn thông tin: thiết bị hệ thống, hệ điều hành, máy chủ, ứng dụng, dịch vụ và các thành phần khác (nếu có);
		b) Quản lý, cập nhật nguồn cung cấp điểm yếu an toàn thông tin; phân nhóm và mức độ của điểm yếu cho các thành phần trong hệ thống đã xác định;
		c) Cơ chế phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin;

Stt	Nội dung công việc	Yêu cầu cơ bản
		d) Kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng;
		đ) Định kỳ kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống.
1.5.8	Quản lý sự cố an toàn thông tin	Chính sách, quy trình quản lý sự cố an toàn thông tin bao gồm:
		a) Phân nhóm sự cố an toàn thông tin mạng;
		b) Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng;
		c) Kế hoạch ứng phó sự cố an toàn thông tin mạng;
		d) Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin;
		đ) Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường;
		e) Quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng;
		g) Cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin;
		h) Định kỳ tổ chức diễn tập phương án xử lý sự cố an toàn thông tin.
1.5.9	Quản lý an toàn người sử dụng đầu cuối	Chính sách, quy trình quản lý an toàn người sử dụng đầu cuối bao gồm:
		a) Quản lý truy cập, sử dụng tài nguyên nội bộ;
		b) Quản lý truy cập mạng và tài nguyên trên Internet;
		c) Cài đặt và sử dụng máy tính an toàn.
1.6	Phương án Quản lý rủi ro an toàn thông tin	

Stt	Nội dung công việc	Yêu cầu cơ bản
1.7	Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ	
II	Yêu cầu kỹ thuật	
2.1	Bảo đảm an toàn mạng	
2.1.1	Thiết kế hệ thống	a) Thiết kế các vùng mạng trong hệ thống theo chức năng, các vùng mạng tối thiểu bao gồm:
		- Vùng mạng nội bộ;
		- Vùng mạng biên;
		- Vùng DMZ;
		- Vùng máy chủ nội bộ;
		- Vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác;
		- Vùng mạng máy chủ cơ sở dữ liệu;
		- Vùng quản trị;
		b) Phương án thiết kế bảo đảm các yêu cầu sau:
		- Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn;
		- Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập;
		- Có phương án cân bằng tải và dự phòng nóng cho các thiết bị mạng chính;
		- Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu;
		- Có phương án chặn lọc phần mềm độc hại trên môi trường mạng;
		- Có phương án phòng chống tấn công từ chối dịch vụ;

Stt	Nội dung công việc	Yêu cầu cơ bản
		- Có phương án giám sát hệ thống thông tin tập trung;
		- Có phương án giám sát an toàn hệ thống thông tin tập trung;
		- Có phương án quản lý sao lưu dự phòng tập trung;
		- Có phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung;
		- Có phương án phòng, chống thất thoát dữ liệu;
		- Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ;
		- Có phương án bảo đảm an toàn cho mạng không dây (nếu có).
2.1.2	Kiểm soát truy cập từ bên ngoài mạng	a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet;
		b) Kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép truy cập từ bên ngoài;
		c) Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng;
		d) Phân quyền và cấp quyền truy cập từ bên ngoài vào hệ thống theo từng người dùng hoặc nhóm người dùng căn cứ theo yêu cầu nghiệp vụ, yêu cầu quản lý;
		đ) Giới hạn số lượng kết nối đồng thời từ một địa chỉ nguồn và tổng số lượng kết nối đồng thời cho từng ứng dụng, dịch vụ được hệ thống cung cấp theo năng lực thực tế của hệ thống.
2.1.3	Kiểm soát truy cập từ bên trong mạng	a) Chỉ cho phép truy cập các ứng dụng, dịch vụ bên ngoài theo yêu cầu nghiệp vụ, chặn các dịch vụ khác không phục vụ hoạt động nghiệp vụ theo chính sách của tổ chức;
		b) Giới hạn truy cập các ứng dụng, dịch vụ bên ngoài theo thời gian (theo chính sách truy cập của tổ chức nếu có);

Stt	Nội dung công việc	Yêu cầu cơ bản
		c) Có phương án kiểm soát truy cập của người dùng vào các dịch vụ, các máy chủ nội bộ theo chức năng và chính sách của tổ chức.
2.1.4	Nhật kí hệ thống	a) Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị hệ thống (nếu hỗ trợ), bao gồm các thông tin sau:
		- Thời gian kết nối;
		- Thông tin kết nối mạng (địa chỉ IP, cổng kết nối);
		- Hành động đối với kết nối (cho phép, ngăn chặn);
		- Thông tin các thiết bị đầu cuối kết nối vào hệ thống theo địa chỉ vật lý và logic;
		- Thông tin cảnh báo từ các thiết bị;
		- Thông tin hiệu năng hoạt động của thiết bị và tài nguyên mạng.
		b) Sử dụng máy chủ thời gian trong hệ thống để đồng bộ thời gian giữa các thiết bị mạng, thiết bị đầu cuối và các thành phần khác trong hệ thống tham gia hoạt động giám sát;
		c) Lưu trữ và quản lý tập trung nhật ký hệ thống thu thập được từ các thiết bị hệ thống;
		đ) Lưu trữ nhật ký hệ thống của thiết bị tối thiểu 03 tháng.
2.1.5	Phòng chống xâm nhập	a) Có phương án phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống;
		b) Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng (Signatures);
		c) Bảo đảm năng lực hệ thống đáp ứng đủ theo yêu cầu, quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp.
2.1.6	Phòng chống phần mềm độc hại trên môi trường mạng	a) Có phương án phòng chống phần mềm độc hại trên môi trường mạng;
		b) Định kỳ cập nhật dữ liệu cho hệ thống phòng chống phần mềm độc hại;

Stt	Nội dung công việc	Yêu cầu cơ bản
		c) Bảo đảm năng lực hệ thống đáp ứng đủ theo yêu cầu, quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp.
2.1.7	Bảo vệ thiết bị hệ thống	a) Cấu hình chức năng xác thực trên các thiết bị hệ thống (nếu hỗ trợ) để xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa;
		b) Thiết lập cấu hình chỉ cho phép sử dụng các kết nối mạng an toàn (nếu hỗ trợ) khi truy cập, quản trị thiết bị từ xa;
		c) Cấu hình thiết bị (nếu hỗ trợ) chỉ cho phép hạn chế các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa;
		d) Hạn chế được số lần đăng nhập sai khi quản trị hoặc kết nối quản trị từ xa theo địa chỉ mạng;
		đ) Phân quyền truy cập, quản trị thiết bị đối với các tài khoản quản trị có quyền hạn khác nhau;
		e) Nâng cấp, xử lý điểm yếu an toàn thông tin của thiết bị hệ thống trước khi đưa vào sử dụng;
		g) Xóa bỏ thông tin cấu hình, dữ liệu trên thiết bị hệ thống khi thay đổi mục đích sử dụng hoặc gỡ bỏ khỏi hệ thống.
2.2	Bảo đảm an toàn máy chủ	
2.2.1	Xác thực	a) Thiết lập chính sách xác thực trên máy chủ để xác thực người dùng khi truy cập, quản lý và sử dụng máy chủ;
		b) Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa (nếu không sử dụng);
		c) Thiết lập cấu hình máy chủ để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau:
		- Yêu cầu thay đổi mật khẩu mặc định;
		- Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự;
		- Thiết lập thời gian yêu cầu thay đổi mật khẩu;
		- Thiết lập thời gian mật khẩu hợp lệ.

Stt	Nội dung công việc	Yêu cầu cơ bản
		d) Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với một tài khoản nhất định;
		đ) Thiết lập cấu hình để vô hiệu hóa tài khoản nếu tài khoản đó đăng nhập sai nhiều lần vượt số lần quy định.
2.2.2	Kiểm soát truy cập	a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa;
		b) Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi máy chủ không nhận được yêu cầu từ người dùng;
		c) Thay đổi cổng quản trị mặc định của máy chủ;
		d) Giới hạn địa chỉ mạng được phép truy cập, quản trị máy chủ từ xa.
2.2.3	Nhật ký hệ thống	a) Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau:
		- Thông tin kết nối mạng tới máy chủ (Firewall log);
		- Thông tin đăng nhập vào máy chủ;
		- Lỗi phát sinh trong quá trình hoạt động;
		- Thông tin thay đổi cấu hình máy chủ;
		- Thông tin truy cập dữ liệu và dịch vụ quan trọng trên máy chủ (nếu có).
		b) Đồng bộ thời gian giữa máy chủ với máy chủ thời gian;
		c) Giới hạn đủ dung lượng lưu trữ nhật ký hệ thống để không mất hoặc tràn nhật ký hệ thống;
		d) Quản lý và lưu trữ tập trung nhật ký hệ thống thu thập được từ máy chủ;
		đ) Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 03 tháng.
2.2.4	Phòng chống xâm nhập	a) Loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên máy chủ;

Stt	Nội dung công việc	Yêu cầu cơ bản
		b) Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ;
		c) Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng;
		d) Có phương án cập nhật bản vá, xử lý điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ;
		đ) Thực hiện nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng.
2.2.5	Phòng chống phần mềm độc hại	a) Cài đặt phần mềm phòng chống mã độc (hoặc có phương án khác tương đương) và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm;
		b) Có phương án kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt;
		c) Quản lý tập trung (cập nhật, cảnh báo và quản lý) các phần mềm phòng chống mã độc cài đặt trên máy chủ và các máy tính người sử dụng trong hệ thống.
2.2.6	Xử lý máy chủ khi chuyển giao	a) Có phương án xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng;
		b) Sao lưu dự phòng thông tin, dữ liệu trên máy chủ, bản dự phòng hệ điều hành máy chủ trước khi thực hiện xóa dữ liệu, hệ điều hành;
		c) Có biện pháp kiểm tra, bảo đảm dữ liệu không thể khôi phục sau khi xóa.
2.3	Bảo đảm an toàn ứng dụng	
2.3.1	Xác thực	a) Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng;
		b) Lưu trữ có mã hóa thông tin xác thực hệ thống;
		c) Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau:
		- Yêu cầu thay đổi mật khẩu mặc định;

Stt	Nội dung công việc	Yêu cầu cơ bản
		- Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự;
		- Thiết lập thời gian yêu cầu thay đổi mật khẩu;
		- Thiết lập thời gian mật khẩu hợp lệ.
		d) Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định;
		đ) Mã hóa thông tin xác thực trước khi gửi qua môi trường mạng;
		e) Thiết lập cấu hình ứng dụng để ngăn cản việc đăng nhập tự động đối với các ứng dụng, dịch vụ cung cấp và xử lý dữ liệu quan trọng trong hệ thống.
2.3.2	Kiểm soát truy cập	a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa;
		b) Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng;
		c) Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa;
		d) Phân quyền truy cập, quản trị, sử dụng tài nguyên khác nhau của ứng dụng với người sử dụng/nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau;
		đ) Giới hạn số lượng các kết nối đồng thời (kết nối khởi tạo và đã thiết lập) đối với các ứng dụng, dịch vụ máy chủ cung cấp.
2.3.3	Nhật kí hệ thống	a) Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau:
		- Thông tin truy cập ứng dụng;
		- Thông tin đăng nhập khi quản trị ứng dụng;
		- Thông tin các lỗi phát sinh trong quá trình hoạt động;
		- Thông tin thay đổi cấu hình ứng dụng.
		b) Quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý tập trung;

Stt	Nội dung công việc	Yêu cầu cơ bản
		c) Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 03 tháng.
2.3.4	Bảo mật thông tin liên lạc	a) Mã hóa thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trước khi truyền đưa, trao đổi qua môi trường mạng; sử dụng phương án mã hóa theo quy định về bảo vệ bí mật nhà nước đối với thông tin mật;
		b) Sử dụng kết nối mạng an toàn, bảo đảm an toàn trong quá trình khởi tạo kết nối kênh truyền và trao đổi thông tin qua kênh truyền.
2.3.5	Chống chối bỏ	Sử dụng chữ ký số khi trao đổi thông tin, dữ liệu quan trọng.
2.3.6	An toàn ứng dụng và mã nguồn	a) Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý;
		b) Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu ra trước khi gửi về máy yêu cầu;
		c) Có phương án bảo vệ ứng dụng chống lại những dạng tấn công phổ biến: SQL Injection, OS command injection, RFI, LFI, Xpath injection, XSS, CSRF;
		d) Có chức năng kiểm soát lỗi, thông báo lỗi từ ứng dụng.
2.4	Bảo đảm an toàn dữ liệu	
2.4.1	Nguyên vẹn dữ liệu	Có phương án quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn.
2.4.2	Bảo mật dữ liệu	a) Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ;
		b) Sử dụng các phương pháp mã hóa mạnh (chưa được các tổ chức quốc tế công bố điểm yếu an toàn thông tin) để mã hóa dữ liệu.
2.4.3	Sao lưu dự phòng	a) Thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ;
		b) Phân loại và quản lý các dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau;

Stt	Nội dung công việc	Yêu cầu cơ bản
		c) Có hệ thống/phương tiện lưu trữ độc lập để sao lưu dự phòng.

3.3.4.2.2. Kiểm tra đánh giá an toàn thông tin cho ứng dụng web

Các nhóm kiểm tra đánh giá bao gồm:

- Thăm dò, thu thập thông tin;
- Kiểm tra quản lý cấu hình & triển khai;
- Kiểm tra quản lý định danh;
- Kiểm tra xác thực;
- Kiểm tra phân quyền;
- Kiểm tra quản lý phiên;
- Kiểm tra sàng lọc dữ liệu đầu vào;
- Kiểm tra cơ chế xử lý lỗi;
- Kiểm tra thuật toán mã hóa;
- Kiểm tra logic nghiệp vụ;
- Kiểm tra xử lý phía người dùng;

Chi tiết bước thực hiện:

Nhóm	Bước thực hiện	Mô tả chi tiết
Thăm dò, thu thập thông tin	Conduct Search Engine Discovery and Reconnaissance for Information Leakage	Tận dụng các công cụ tìm kiếm như Google, Bing và các nguồn tương tự để tra cứu thông tin về mô hình mạng và cấu hình, tài khoản, thông báo lỗi, và nhiều thông tin khác.
	Fingerprint Web Server	Xác định phiên bản và loại máy chủ ứng dụng được sử dụng để phát hiện các lỗ hổng đã được công bố và xác định các mã khai thác có thể áp dụng.
	Review Webserver Metafiles for Information Leakage	Phân tích tập tin robots.txt và xác định các nhãn <META> của ứng dụng
		Tìm kiếm thông tin về các tập tin sao lưu có trên máy chủ.
	Enumerate Applications on Webserver	Tìm kiếm các ứng dụng đang tồn tại trên hệ thống (bao gồm host ảo, subdomain), các cổng không tiêu chuẩn (các cổng > 1024), chuyển vùng DNS.

Nhóm	Bước thực hiện	Mô tả chi tiết
	Review Webpage Comments and Metadata for Information Leakage	Tìm kiếm các thông tin nhạy cảm từ các chú thích và metadata có trong mã nguồn (chức năng view-source của trình duyệt).
	Identify application entry points	Xác định các trường, tham số đầu vào được ẩn đi, các phương thúc gọi HTTP.
	Map execution paths through application	Ánh xạ các chức năng của ứng dụng và hiểu được luồng xử lý chính của ứng dụng.
	Fingerprint Web Application Framework	Xác định framework/CMS ứng dụng sử dụng thông qua các HTTP header, cookie, mã nguồn và các tập tin/thư mục
		Xác định các thông tin về File Extension được thực thi như php, aspx, jsp, …
	Fingerprint Web Application	Xác định phiên bản và nền tảng của ứng dụng để xác định các lỗ hổng đã biết và các mã khai thác thích hợp.
	Map Network and Application Architecture	Xác định kiến trúc của ứng dụng bao gồm ngôn ngũ lập trình, WAF, Reverse proxy, máy chủ ứng dụng, CSDL.
Kiểm tra quản lý cấu hình & triển khai	Test Network/Infrastructure Configuration	Tìm hiểu cấu hình network và cấu hình của cơ sở hạ tầng, máy chủ CSDL, WebDAV, FTP để xác định các lỗ hổng đã biết.
	Test Application Platform Configuration	Xác định các tập tin/thư mục cài đặt mặc định, cách thức xử lý lỗi máy chủ (40*, 50*), cách thức phân quyền, ghi log ứng dụng.
		Kiểm tra các lỗ hổng đã biết về cấu hình nền tảng hoặc hệ thống.
	Test File Extensions Handling for Sensitive Information	Kiểm tra thông tin về định dạng, đuôi file (File Extention) thông qua kỹ thuật Fuzzing, sử dụng Wordlist:
		Tìm các tập tin, thông tin quan trọng (.asa, .inc, .sql, .zip, .tar, .pdf, .txt, …).
	Backup and Unreferenced Files for Sensitive Information	Kiểm tra mã nguồn Javascript, tập tin cache, tập tin backup (.old, .bak, .inc, .src) và dự đoán tên các tập tin có thể có
		Kiểm tra các thư mục cài đặt, tập tin sao lưu của

Nhóm	Bước thực hiện	Mô tả chi tiết
		framework còn sót lại trong quá trình cài đặt ứng dụng.
	Enumerate Infrastructure and Application Admin Interfaces	Thực hiện liệt kê tập tin và thư mục, tìm kiếm các chú thích và đường dẫn chứa thông tin đến trang quản trị trong mã nguồn (/admin, /administrator, /backoffice, /backend, ...), các cổng dịch vụ khác (Tomcat/8080).
		Tìm kiếm các thông tin về hạ tầng và ứng dụng như đường dẫn quản trị.
	Test HTTP Methods	Xác định các phương thức được phép gọi đến máy chủ bằng phương thức OPTIONS. Kiểm tra khả năng quản lý truy cập thông qua phương thức HEAD và TRACE.
	Test HTTP Strict Transport Security	Xác định header HSTS trên máy chủ ứng dụng thông qua header của gói tin HTTP response
		curl -s -D- https://<url>/ | grep Strict".
	Test RIA cross domain policy	Phân tích các quyền được phép thông qua các tập tin chính sách (crossdomain.xml/clientaccesspolicy.xml) và header allow-access-from.
Kiểm tra quản lý định danh	Test Role Definitions	Sử dụng ma trận phân quyền để xác nhận các vài trò được định nghĩa trong hệ thống.
		Tìm cách bypass cơ chế phân quyền trên hệ thống.
	Test User Registration Process	Trong quá trình đăng ký người dùng, kiểm tra xem các yêu cầu định danh có phù hợp với yêu cầu nghiệp vụ và bảo mật không.
	Test Account Provisioning Process	Xác định cơ chế ủy quyền để tạo người dùng và loại tài khoản được phép tạo.
	Testing for Account Enumeration and Guessable User Account	Kiểm tra thông báo lỗi, status code và mọi thông tin liên quan đến user có thể bị rò rỉ thông qua chức năng đăng nhập, quên mật khẩu.
		Xác định các tài khoản mặc định, tài khoản khách (Guest).
	Testing for Weak or	Xác định các nguyên tắc đặt tên tài khoản để dự

Nhóm	Bước thực hiện	Mô tả chi tiết
	unenforced username policy	đoán các tài khoản có thể đoán được.
		Tìm kiếm và cố gắng khai thác các policy yếu.
Kiểm tra xác thực	Testing for Credentials Transported over an Encrypted Channel	Kiểm tra các gói tin chứa tài khoản đăng nhập có thể được thực hiện trên giao thức HTTP thay vì HTTPS.
	Testing for Default Credentials	Kiểm tra các tài khoản mặc định của các ứng dụng/CMS thông dụng, mật khẩu mặc định cho tài khoản mới tạo (nếu có).
		Xác định các tài khoản mặc định được tạo, khả năng đoán được tên tài khoản hoặc có được tài khoản.
	Testing for Weak Lock Out Mechanism	Đánh giá cơ chế khóa tài khoản để ngăn chặn tấn công vét cạn mật khẩu. Đánh giá cơ chế kiểm soát việc mở khóa tài khoản để ngăn chặn việc mở khóa trái phép.
	Testing for Bypassing Authentication Schema	Kiểm tra khả năng vượt qua cơ chế xác thực của ứng dụng thông qua thay đổi tham số nếu việc xác thực dựa trên tham số, thay đổi giá trị phiên làm việc, lỗ hổng SQL Injection.
	Test Remember Password Functionality	Xác định lỗ hổng có thể có trong chức năng "Gợi nhớ mật khẩu".
		Kiểm tra thông tin lưu trong cookie, tìm kiếm mật khẩu nếu có. Xác định mật khẩu được lưu dưới dạng cleartext hoặc mã hóa.
	Testing for Browser Cache Weakness	Kiểm tra lỗ hổng trong phương thức đăng xuất, có thể truy cập lại các trang trước mặc dù đã đăng xuất.
		Kiểm tra cơ chế quản lý bộ nhớ đệm của trình duyệt thông qua cơ chế Back sau khi đã đăng xuất. Kiểm tra header Cache-Control trong HTTP response.
	Testing for Weak Password Policy	Xác định cơ chế ngăn chặn tấn công vét cạn mật khẩu trong ứng dụng và kiểm tra các chính sách liên quan đến mật khẩu, bao gồm độ dài tối thiểu, độ phức tạp và yêu cầu thay đổi mật khẩu định kỳ,...

Nhóm	Bước thực hiện	Mô tả chi tiết
	Testing for Weak Security Question/Answer	Kiểm tra các câu hỏi bảo mật được sử dụng, khả năng tấn công vét cạn câu trả lời.
	Testing for Weak Password Change or Reset Functionalities	Kiểm tra chức năng reset mật khẩu, xác định kênh gửi thông tin là email hay SMS, đường dẫn reset được tạo ngẫu nhiên hoặc có thể đoán được, thời gian hiểu lực của đường dẫn.
	Testing for Weaker Authentication in Alternative Channel	Kiểm tra chức năng thay đổi mật khẩu, xác định việc thay đổi có cần mật khẩu cũ, khả năng tạo request để thay đổi mật khẩu người dùng khác trái phép (CSRF)".
Kiểm tra phân quyền	Testing Directory Traversal/File Include	Xác định các chức năng tải tập tin trên hệ thông như hình ảnh, file tài liệu,... và kiểm tra các lỗ hổng trong chức năng đó bằng các kỹ thuật như thêm các ký tự "../" vào tên tập tin.
	Testing for Bypassing Authorization Schema	Xác định các tài nguyên cần xác thực để truy cập nhưng có thể bị truy cập trái phép, đặc biệt là các trang quản trị.
		Xác định các tính năng mà người dùng có thể truy cập trái phép vào các thông tin trên hệ thống.
		Sử dụng các kỹ thuật bypass cơ chế xác thực như thay đổi tham số định danh, tái sử dụng session.
	Testing for Privilege Escalation	Thực hiện leo quyền bằng việc thay đổi các giá trị trong cookie hoặc đường dẫn đã được xác định.
		Kiểm tra khả năng leo quyền hoặc truy cập trái phép đến các tài nguyên khác.
	Testing for Insecure Direct Object References	Thay đổi các tham số có thể là id của 1 đối tượng như tài khoản, vật phẩm để truy cập thông tin của đối tượng khác (?invoice=123 -> ?invoice=456).
		Kiểm tra khả năng leo quyền ở ứng dụng này từ ừng dụng khác.
Kiểm tra quản lý phiên	Testing for Bypassing Session Management Schema	Xác định khả năng decode cookie, sessionid và thử leo quyền bằng cách thay đổi các giá trị đó.
	Testing for Cookies	Kiểm tra biến cookie của ứng dụng đã được bật

Nhóm	Bước thực hiện	Mô tả chi tiết
	Attributes	các cờ httponly, secure, expire time và có chứa các thông tin nhạy cảm không.
	Testing for Session Fixation	Thử nghiệm đăng nhập lại bằng cookie cũ để kiểm tra cookie có bị hủy sau khi đăng xuất không.
	Testing for Exposed Session Variables	Kiểm tra khả năng giải mã của giá trị phiên làm việc hoặc cùng 1 giá trị được sử dụng nhiều lần, xác định các biến sessionid được gửi theo phương thức GET.
	Testing for Cross Site Request Forgery	Xác định các chức năng có thể bị tấn công Cross Site Request Forgery – CSRF.
		Kiểm tra các chức năng nhạy cảm, cần người dùng xác thực có được kèm theo các token bảo vệ, khả năng giả mạo người dùng để thực hiện các chức năng này.
	Testing for Logout Functionality	Kiểm tra session cookie có còn khả năng sử dụng khi phiên làm việc đã kết thúc không.
	Test Session Timeout	Kiểm tra thời gian hết hạn của session cookie, nếu hết hạn thì session cookie có bị hủy không.
	Testing for Session Puzzling	Xác định các yếu tố ảnh hưởng đến việc khởi tạo session cookie, từ đó kiểm tra xem có thể khởi tạo các session cookie giống nhau bằng cách giữ nguyên các yếu tố đó.
Kiểm tra sàng lọc dữ liệu đầu vào	Testing for Reflected Cross Site Scripting	Sử dụng các kỹ thuật trong tấn công reflected XSS bằng việc thêm các đoạn mã Javascript vào các trường nhập dữ liệu.
	Testing for Stored Cross Site Scripting	Sử dụng các kỹ thuật trong tấn công stored XSS bằng việc thêm các đoạn mã Java script vào các trường nhập dữ liệu.
	Testing for HTTP Verb Tampering	Thực hiện thay đổi phương thức của các chức năng, từ GET thành POST và ngược lại.
		Thay đổi các phương thức HTTP thông thường như GET/POST bằng các phương thức PUT/DELETE/TRACE/HEAD.
	Testing for HTTP Parameter pollution	Tiến hành ghi nhận kết quả trả về khi nhập giá trị tham số đúng, thay đổi giá trị tham số, và lặp

Nhóm	Bước thực hiện	Mô tả chi tiết
		lại việc thay đổi giá trị tham số nhiều lần để xác định có sự tồn tại của lỗ hổng hay không.
	Testing for SQL Injection	Sử dụng các kỹ thuật trong tấn công SQL Injection như thêm dấu nháy đơn ('), dấu nháy kép (") vào câu truy vấn và kiểm tra kết quả trả về để xác định khả năng tồn tại lỗ hổng.
	Testing for LDAP Injection	Thực hiện tìm kiếm lỗ hổng bằng cách chèn các câu truy vấn LDAP.
	Testing for ORM Injection	Sử dụng kỹ thuật trong tấn công ORM Injection bằng cách nhập các ký tự đặc biệt trong câu truy vấn và kiểm tra kết quả trả về để xác định khả năng tồn tại lỗ hổng.
	Testing for XML Injection	Sử dụng các kỹ thuật trong tấn công XML Injection bằng cách chèn các ký tự Meta của XML vào các tham số và kiểm tra kết quả để xác định khả năng tồn tại lỗ hổng.
	Testing for SSI Injection	Sử dụng các kỹ thuật trong tấn công SSI Injection bằng cách chèn các ký tự đặc biết, exploit code vào tham số để kiểm tra khả năng tồn tại của lổ hổng.
	Testing for XPath Injection	Chèn dấu nháy vào các giá trị tham số để kiểm tra sự tồn tại của lổ hổng.
	IMAP/SMTP Injection	Chèn các ký tự đặc biệt vào tham số để kiểm tra sự tồn tại của lổ hổng.
	Testing for Code Injection	Chèn các câu câu lệnh hệ thống sau dấu chấm phẩy để kiểm tra khả năng tồn tại của lổ hổng.
	Testing for Local File Inclusion	Discovery local file bằng cách thêm các ký tự "../" vào tên file.
	Testing for Remote File Inclusion	Chèn các exploit code vào url để kiểm tra khả năng tồn tại của lổ hổng.
	Testing for Command Injection	Xác định OS, cấu trúc thư mục, path,... từ đó thực thi câu lệnh hệ thống trên máy chủ.
	Testing for Buffer overflow	Nhập các giá trị có độ dài lớn hoặc các giá trị không hợp lệ (số quá lớn) để làm tràn bộ đệm, từ đó kiểm tra sự tồn tại của lổ hổng.

Nhóm	Bước thực hiện	Mô tả chi tiết
	Testing for incubated vulnerabilities	Tìm kiếm các lổ hổng tồn tại lâu trên hệ thống như upload webshell, Stored XSS, hay các lỗi configuration cho phép cài đặt các thành phần trái phép (Tomcat, Plesk, Cpanel). Từ đó kiểm tra sự tồn tại của lổ hổng.
	Testing for HTTP Splitting/Smuggling	Sử dụng các kỹ thuật trong tấn công HTTP splitting/smuggling như chèn thêm vào HTTP header của request nhiều đoạn request khác nhau hoặc break các header bằng ký hiệu xuống dòng CRLF, từ đó kiểm tra sự tồn tại của lổ hổng.
Kiểm tra cơ chế xử lý lỗi	Analysis of Error Codes	Thu thập các thông tin nhạy cảm về máy chủ, ứng dụng,... từ error code và thông báo lỗi.
	Analysis of Stack Traces	Thực hiện nhập các giá trị có thể gây lỗi vào các trường tham số, từ đó phân tích Stack Trace có thể được trả về:
		- Giá trị không hợp lệ, không phù hợp với logic của ứng dụng;
		- Giá trị chứa các ký tự đặc biệt không thuộc bảng mã ASCII thông dụng;
		- Truy cập các trang nội bộ mà không xác thực;
		- Bypass luồng xác thực của ứng dụng.
Kiểm tra thuật toán mã hóa	Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection	Xác định ứng dụng SSL đang sử dụng, các thuật toán/giao thức mã hóa yếu được phép sử dụng có thể dẫn đến các lỗ hổng như RC4, BEAST, CRIME, POODLE.
	Testing for Padding Oracle	So sánh kết quả giải mã khi thay đổi dữ liệu đầu vào của quá trình mã hóa, từ đó kiểm tra sự tồn tại của lổ hổng:
		- Dữ liệu được giải mã và kết quả trả về đúng;
		- Dữ liệu được giải mã và kết quả trả về gây lỗi hoặc ngoại lệ;
		- Dữ liệu không thể giải mã do lỗi padding;
	Testing for Sensitive information sent via	Kiểm tra các thông tin được truyền không qua mã hóa:

Nhóm	Bước thực hiện	Mô tả chi tiết
	unencrypted channels	- Thông tin dùng để xác thực như tài khoản/mật khẩu, mã PIN, giá trị định danh phiên làm việc, token, cookie…);
		- Thông tin được bảo vệ bởi pháp luật, quy định hay chính sách của tổ chức cụ thể như thẻ tín dụng, dữ liệu khách hàng, ...
Kiểm tra logic nghiệp vụ	Test Business Logic Data Validation	Nhập các giá trị không phù hợp logic xử lý của ứng dụng, vd như nhập số tiền âm, số lượng âm, ...
	Test Ability to Forge Requests	Kiểm tra các trường/tham số/chức năng ẩn có khả năng truy cập mà không cần tuân theo luồng xử lý của ứng dụng.
	Test Integrity Checks	Kiểm tra khả năng nhập vào các thông tin/dữ liệu trái với logic của ứng dụng, các thao tác dữ liệu có thể được thực hiện trái phép.
	Test for Process Timing	Xác định các chức năng phụ thuộc vào thời gian và thực hiện các trường hợp có thể phá vỡ luồng xử lý của ứng dụng.
	Test Number of Times a Function Can be Used Limits	Kiểm tra các chức năng chỉ nên được thực hiện 1 lần hoặc với số lần nhất định trong 1 khoảng thời gian như OTP bằng cách thực thi liên tục nhiều lần.
	Testing for the Circumvention of Work Flows	Xác định luồng thực thi của các chức năng và kiểm tra khả năng phá vỡ luồng xử lý, có thể bỏ qua các bước.
	Test Defenses Against Application Mis-use	Kiểm tra, đánh giá các cơ chế bảo vệ của ứng dụng như ngăn chặn truy cập, khóa tài khoản, token/captcha.
	Test Upload of Unexpected File Types	Kiểm tra khả năng sàng lọc file upload bằng cách tải lên các tập tin không không phù hợp với ứng dụng như đăng tải tập tin chứa mã nguồn thay vì hình ảnh.
	Test Upload of Malicious Files	Kiểm tra khả năng sàng lọc file upload bằng cách tải lên các tập tin thực thi chứa mã nguồn độc hại như .php, .asp, .jsp, …
Kiểm tra xử	Testing for DOM based	Sử dụng các kỹ thuật trong tấn công XSS như chèn các đoạn mã Javascript vào các trường nhập

Nhóm	Bước thực hiện	Mô tả chi tiết
lý phía người dùng	Cross Site Scripting	dữ liệu để kiểm tra sự tồn tại của lổ hổng.
	Testing for JavaScript Execution	Kiểm tra lỗ hổng bằng cách chèn các mã thực thi Javascript vào đường dẫn.
	Testing for HTML Injection	Kiểm tra lỗ hổng bằng cách chèn các mã HTML vào đường dẫn.
	Testing for Client-Side URL Redirect	Kiểm tra lỗ hổng bằng cách chèn các đường dẫn độc hại vào đường dẫn.
	Testing for CSS Injection	Kiểm tra lỗ hổng bằng cách chèn các mã CSS vào đường dẫn.
	Testing for Client-Side Resource Manipulation	Kiểm tra lỗ hổng bằng cách tải tài nguyên chứa mã thực thi Javascript vào đường dẫn.
	Test Cross Origin Resource Sharing	Kiểm tra các header quy định khả năng chia sẻ tài nguyên như:
		- Origin & Access-Control-Allow-Origin;
		- Access-Control-Request-Method & Access-Control-Allow-Method;
		- Access-Control-Request-Headers & Access-Control-Allow-Headers;
		- Access-Control-Allow-Credentials.
	Testing for Cross Site Flashing	Kiểm tra khả năng khai thác ứng dụng Flash thông đánh giá mã nguồn ActionScript của ứng dụng.
	Testing for Clickjacking	Kiểm tra lỗ hổng bằng cách tải ứng dụng vào một iframe trong một ứng dụng khác.
	Testing Web Sockets	Kiểm tra khả năng bảo mật của WebSockets nếu ứng dụng có sử dụng.
	Test Web Messaging	Kiểm tra cách ứng dụng triển khai và xử lý dữ liệu Web Messaing nếu có.
	Test Local Storage	Kiểm tra các thông tin được lưu trữ trong Local Storage của trình duyệt, khả năng chèn mã khai thác.

3.3.4.3. Đánh giá an toàn thông tin cho máy chủ

3.3.4.3.1. Rà soát lỗ hổng bảo mật, điểm yếu

Nhà cung cấp dịch vụ sẽ chịu trách nhiệm thu thập thông tin máy chủ như địa chỉ IP và địa chỉ MAC; thông tin về hệ điều hành, phiên bản và cấu hình hệ thống; các ứng dụng và dịch vụ chạy trên máy chủ sau đó sẽ kết nối tới máy chủ mục tiêu qua tài khoản, mật khẩu được cung cấp bởi cơ quan chủ quản.

Nhà cung cấp dịch vụ sẽ thực hiện việc dò quét, phát hiện các điểm yếu bảo mật trên hệ thống máy chủ, đưa ra phân tích, cảnh bảo cũng như các biện pháp khắc phục kịp thời.

Nhà cung cấp dịch vụ sẽ tiến hành rà quét lỗ hổng bảo mật trên phạm vị đã được định nghĩa, thu thập và phân tích kết quả rà quét.

3.3.4.3.2. Kiểm tra, rà soát cấu hình

Nhà cung cấp dịch vụ sẽ chịu trách nhiệm thu thập thông tin máy chủ như Địa chỉ IP và địa chỉ MAC; thông tin về hệ điều hành, phiên bản và cấu hình hệ thống; các ứng dụng và dịch vụ chạy trên máy chủ sau đó sẽ kết nối tới máy chủ mục tiêu qua tài khoản, mật khẩu được cung cấp bởi cơ quan chủ quản.

Checklist thực hiện:

- Kiểm tra cấu hình hệ điều hành: Kiểm tra các dịch vụ, ứng dụng và giao thức không cần thiết trên máy chủ, các dịch vụ, ứng dụng, giao thức mạng không sử dụng.
- Kiểm tra cấu hình chứng thực: Đánh giá các tài khoản mặc định và các tài khoản không còn sử dụng. Kiểm tra các tài khoản đặc quyền trên máy chủ và các tài khoản dịch vụ. Xem xét chính sách mật khẩu và cơ chế ngăn chặn tấn công mật khẩu.
- Kiểm tra cấu hình log và giám sát: Đánh giá chính sách ghi và quản lý log của hệ thống. Kiểm tra cơ chế ghi nhật ký máy chủ đang sử dụng và các thông tin được ghi lại.
- Kiểm tra, đánh giá cấu hình chính sách tài khoản: Xác định chính sách tài khoản như tài khoản không sử dụng, tài khoản mặc định và chính sách mật khẩu mạnh.
- Kiểm tra chính sách kết nối quản trị: Đánh giá chính sách quản trị từ xa qua các kênh truyền an toàn và mã hóa, giới hạn tài khoản truy cập quản trị từ xa.

3.3.4.4. Đánh giá an toàn thông tin cho các thiết bị mạng

3.3.4.4.1. Rà soát lỗ hổng bảo mật, điểm yếu

Nhà cung cấp dịch vụ sẽ thu thập thông tin thiết bị như địa chỉ IP, địa chỉ MAC, nhận dạng thiết bị mạng: Router, Firewall, Switch sau đó thực hiện việc dò quét, kiểm tra hệ thống mạng, phát hiện các dịch vụ đang mở của các thiết bị, giao thức mạng truyền tải trên hệ thống được coi là các điểm yếu, phát hiện các điểm yếu bảo mật trên các thiết bị mạng, và lập báo cáo kiểm tra, đánh giá đối với các lỗ hổng bảo mật đó.

Nhà cung cấp dịch vụ sẽ tiến hành rà quét lỗ hổng bảo mật trên phạm vi đã được định nghĩa, thu thập và phân tích kết quả rà quét.

3.3.4.4.2. Kiểm tra, rà soát cấu hình

Nhà cung cấp dịch vụ sẽ chịu trách nhiệm thu thập thông tin thiết bị như địa chỉ IP và địa chỉ MAC; thông tin về firmware, phiên bản và cấu hình hệ thống; các dịch vụ chạy trên thiết bị sau đó sẽ kết nối tới thiết bị mục tiêu qua tài khoản, mật khẩu được cung cấp bởi cơ quan chủ quản.

Checklist thực hiện:

- Kiểm tra cấu hình hệ điều hành: Kiểm tra các dịch vụ và giao thức không cần thiết trên thiết bị, các dịch vụ, giao thức mạng không sử dụng.
- Kiểm tra cấu hình chứng thực: Đánh giá các tài khoản mặc định và các tài khoản không còn sử dụng. Kiểm tra các tài khoản đặc quyền trên thiết bị. Xem xét chính sách mật khẩu và cơ chế ngăn chặn tấn công mật khẩu.
- Kiểm tra cấu hình log và giám sát: Đánh giá chính sách ghi và quản lý log của hệ thống. Kiểm tra cơ chế ghi nhật ký thiết bị đang sử dụng và các thông tin được ghi lại.
- Kiểm tra, đánh giá cấu hình chính sách tài khoản: Xác định chính sách tài khoản như tài khoản không sử dụng, tài khoản mặc định và chính sách mật khẩu mạnh.
- Kiểm tra chính sách kết nối quản trị: Đánh giá chính sách quản trị từ xa qua các kênh truyền an toàn và mã hóa, giới hạn tài khoản truy cập quản trị từ xa.

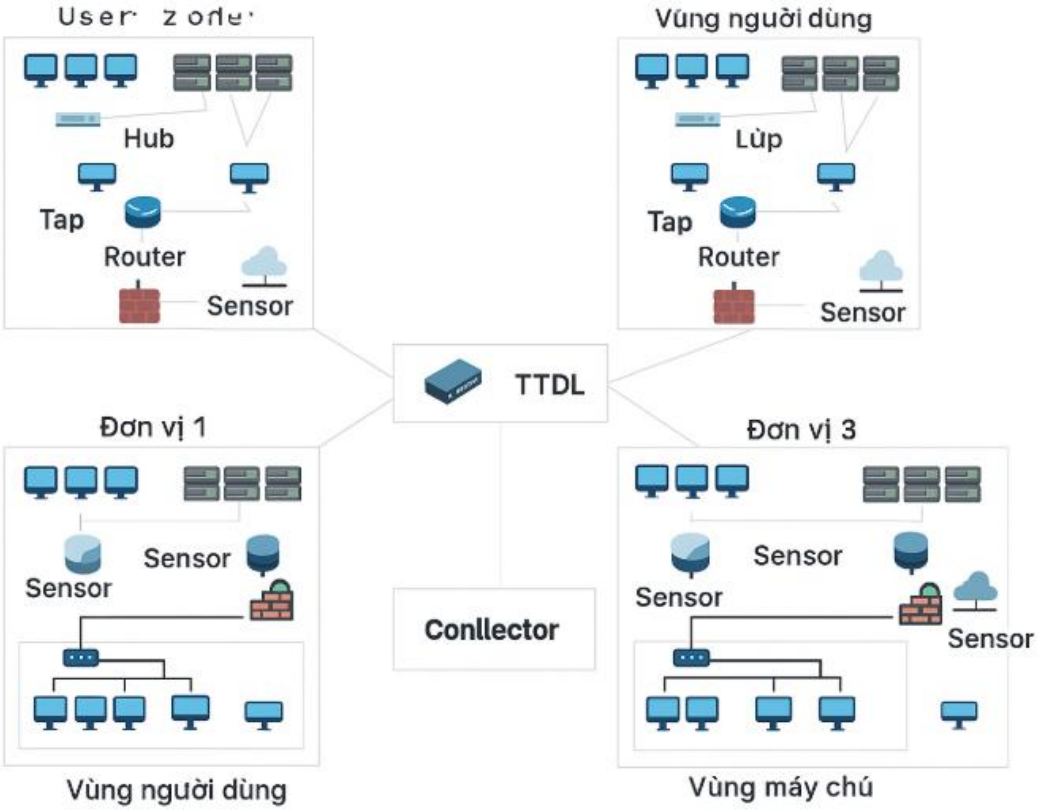
3.3.5. Phương án triển khai rà quét, bóc tách mã độc tại các cơ quan đơn vị trên địa bàn thành phố

3.3.5.1. Mô hình triển khai

Mô hình triển khai được thiết kế phù hợp với hiện trạng hạ tầng mạng và điều kiện vận hành của các cơ quan, đơn vị trên địa bàn Thành phố, với các đặc điểm chính như sau:

- Cấu trúc hai lớp: Hệ thống được tổ chức theo mô hình 2 tầng, bao gồm lớp Trung tâm tại TTDL và lớp đơn vị tại 15 cơ quan, được kết nối thông qua mạng riêng VPN/MPLS nhằm đảm bảo an toàn, bảo mật trong quá trình truyền tải dữ liệu.
- Triển khai trong môi trường cách ly an toàn: Giải pháp được triển khai hoàn toàn trong phạm vi mạng Metronet, không kết nối Internet hoặc hạ tầng Cloud của bên thứ ba, nhằm bảo vệ tuyệt đối tính bí mật của thông tin thu thập. Toàn bộ dữ liệu sau khi hoàn thành quá trình phân tích, rà quét và bóc tách mã độc sẽ được xóa khỏi thiết bị tại Trung tâm và các đơn vị, đảm bảo tuân thủ yêu cầu bảo mật dữ liệu.
- Không can thiệp hệ thống hiện hữu: Phương án triển khai được thiết kế theo nguyên tắc non-invasive, không cài đặt phần mềm lên máy người dùng, không làm thay đổi kiến trúc hay cấu hình mạng hiện có tại các đơn vị.
- Khả năng mở rộng và linh hoạt: Hệ thống có thể dễ dàng mở rộng quy mô, điều chỉnh linh hoạt theo đặc thù hạ tầng mạng của từng đơn vị, bảo đảm khả năng ứng dụng rộng rãi trong các cơ quan nhà nước có quy mô và mô hình vận hành khác nhau.

- Phân tích và phát hiện mã độc theo tầng mạng: Thiết bị tại mỗi đơn vị sẽ thu thập, phân tích và phát hiện dấu hiệu mã độc trên luồng lưu lượng mạng. Các kết quả được tổng hợp, đồng bộ và hiển thị trên hệ thống quản lý tập trung tại Trung tâm, phục vụ điều tra, khoanh vùng, cô lập và loại bỏ các mối đe dọa đã phát hiện.
- Đề xuất và hỗ trợ xử lý mã độc: Sau quá trình rà quét, hệ thống sẽ cung cấp báo cáo chi tiết, đồng thời đề xuất phương án bóc tách, xử lý mã độc, cùng với các khuyến nghị tăng cường biện pháp bảo mật để ngăn ngừa tái diễn sự cố trong tương lai.
- Hỗ trợ triển khai Out-of-Band: Mô hình triển khai theo phương thức Out-of-Band, đảm bảo tách biệt hoàn toàn khỏi luồng truyền dữ liệu sản xuất, tránh ảnh hưởng đến hoạt động thường nhật của các cơ quan.
- Thời gian triển khai: Tổng thời gian triển khai dự án không vượt quá 15 ngày, trong đó mỗi đơn vị được triển khai, rà soát và hoàn thành báo cáo trong thời gian tối đa 10 ngày, tính từ thời điểm thiết lập hệ thống đến khi có kết quả và phương án xử lý



Hình 6: Mô hình triển khai

3.3.5.2. Yêu cầu thiết bị rà quét mã độc

Máy chủ xử lý, phân tích, tổng hợp đặt tại Trung tâm dữ liệu Thành phố có cấu hình tối thiểu 96 core CPU, 512 GB RAM, 2 TB SSD 8TB HDD.

Máy chủ không cho phép kết nối Internet ra bên ngoài hoặc các cơ quan, đơn vị khác không nằm trong phạm vi rà soát trong quá trình thực hiện. Trường hợp thay đổi chính sách kết nối phải được sự chấp thuận của đơn vị chủ đầu tư

3.3.5.3. Yêu cầu thiết bị thu thập thông tin luồng mạng tại đơn vị

Hệ thống thu thập dữ liệu tại đơn vị có cấu hình tối thiểu là 24 core CPU, 96 GB RAM, 1 TB SSD 8TB HDD, 02 NIC 1Gbps; có khả năng tiếp nhận dữ liệu mạng (thông qua SPAN/TAPPING) tối thiểu 1GB; có khả năng thu thập thông tin tương ứng đồng thời tối thiểu 400 thiết bị đầu cuối.

Số lượng thiết bị: 15 thiết bị

3.3.5.4. Cơ chế phát hiện đa lớp

Giải pháp được thiết kế theo mô hình phát hiện đa lớp, kết hợp nhiều kỹ thuật phân tích và tương quan nhằm tối ưu hiệu quả nhận diện mối đe dọa, đảm bảo khả năng phát hiện toàn diện trên nhiều lớp dữ liệu:

Phát hiện kết nối C&C và Botnet:

- Nhận diện các kết nối tới máy chủ điều khiển (Command & Control) dựa trên mẫu hành vi đã được xác định (known behavioral patterns).
- Đối chiếu lưu lượng với cơ sở dữ liệu IP độc hại (malicious IP database) được cập nhật liên tục từ các nguồn Threat Intelligence uy tín quốc tế.
- Phát hiện hành vi lạm dụng giao thức (protocol abuse) như HTTP/HTTPS tunneling, DNS tunneling, ICMP tunneling – các phương thức phổ biến để ẩn giấu lưu lượng C&C.
- Phân tích đặc trưng lưu lượng mạng nhằm phát hiện các nhóm máy trạm có hành vi kết nối đồng loạt, biểu hiện đặc trưng của Botnet

Phát hiện truy vấn tên miền độc hại:

- Giám sát và phân tích toàn bộ truy vấn DNS trong mạng nội bộ để nhận diện truy cập đáng ngờ.
- Ứng dụng Machine Learning nhằm phát hiện tên miền sinh tự động (DGA domains) ngay cả khi chưa có trong cơ sở dữ liệu blacklists

Phát hiện vi phạm chính sách và hành vi bất thường:

- Phát hiện sử dụng dịch vụ trái phép: truy cập cổng không được phép, sử dụng giao thức bất thường, hoặc truyền tải lượng dữ liệu đột biến.
- Phát hiện nguy cơ nội gián (insider threat): người dùng truy cập dữ liệu nhạy cảm ngoài giờ làm việc, tải xuống lượng lớn dữ liệu, hoặc kết nối tới IP lạ không nằm trong danh sách tin cậy

Phát hiện tấn công khai thác theo thời gian thực:

- Dò quét mạng (Network Scanning): nhận diện hoạt động của các công cụ quét như Nmap, Masscan và hành vi quét cổng hoặc quét lỗ hổng.
- Tấn công Brute-force: phát hiện nỗ lực đăng nhập liên tục vào các dịch vụ (HTTP, SSH, RDP, FTP, SMB) với tần suất cao trong thời gian ngắn.
- Khai thác lỗ hổng (Exploitation): phân tích payload và signature để nhận diện hành vi khai thác các lỗ hổng đã biết.
- Di chuyển ngang (Lateral Movement): giám sát các hoạt động di chuyển nội bộ trong mạng như Pass-the-Hash, Pass-the-Ticket, Remote Service Creation,

WMI execution, PowerShell remoting – những dấu hiệu đặc trưng của mã độc giai đoạn lan truyền.

Phát hiện tấn công APT (Advanced Persistent Threat):

- Cảnh báo sớm các dấu hiệu tấn công có chủ đích (Targeted Attack) ở tầng mạng.
- Áp dụng MITRE ATT&CK Framework để nhận diện đầy đủ các giai đoạn trong chuỗi tấn công (Kill Chain): Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command & Control, Exfiltration, Impact.
- Tương quan và phân tích các sự kiện liên quan nhằm phát hiện các chiến dịch tấn công kéo dài hoặc đa giai đoạn (Multi-Stage Attacks).
- Nhận diện các nhóm APT đã biết thông qua phân tích hành vi và đặc trưng TTPs (Tactics, Techniques & Procedures)

Phân tích tự động tại đơn vị:

- Thiết bị triển khai tại từng đơn vị có khả năng phân tích cục bộ các dấu hiệu mã độc, hành vi bất thường và lỗ hổng bị khai thác mà không phụ thuộc vào hệ thống trung tâm.
- Cơ chế phân tích tại chỗ giúp giảm tải cho hạ tầng TTDL, tiết kiệm băng thông và duy trì hiệu suất ổn định trong môi trường phân tán.
- Chỉ các sự kiện nghiêm trọng (Critical Events), cảnh báo mức cao (High-Severity Alerts) và dữ liệu tổng hợp mới được gửi về trung tâm.
- Mô hình này cho phép hệ thống mở rộng quy mô tới hàng trăm đơn vị mà vẫn đảm bảo hiệu năng, tính sẵn sàng và tốc độ xử lý cao

3.3.5.5. Yêu cầu kết quả đạt được

Mục tiêu của giải pháp là đảm bảo hệ thống thông tin vận hành ổn định, liên tục và an toàn, chủ động phòng ngừa, phát hiện và xử lý các rủi ro an ninh mạng trong quá trình ứng dụng công nghệ thông tin tại các đơn vị. Giải pháp đồng thời bảo vệ an toàn khi truy cập các ứng dụng, dịch vụ và website được triển khai tại Trung tâm dữ liệu thành phố.

Bên cạnh đó, hệ thống giúp giảm thiểu nguy cơ lộ lọt thông tin, mất an toàn dữ liệu, góp phần làm sạch mã độc trong không gian mạng, bảo vệ an toàn cho các giao dịch điện tử của cơ quan, doanh nghiệp và người dân. Đây là bước đi quan trọng trong tiến trình chuyển đổi số, hướng tới Chính phủ số, kinh tế số và xã hội số an toàn, bền vững.

3.4. Yêu cầu về sở hữu các thông tin, dữ liệu hình thành trong quá trình cung cấp dịch vụ

Sở hữu các thông tin, dữ liệu hình thành trong quá trình cung cấp dịch vụ tuân thủ quy định tại Điều 48 Nghị định 73/2019/NĐ-CP ngày 05/9/2019 cụ thể như sau:

"Thông tin, dữ liệu hình thành trong quá trình thực hiện dịch vụ công nghệ thông tin thuộc sở hữu của chủ đầu tư. Nhà cung cấp dịch vụ có trách nhiệm bảo đảm an ninh, an toàn thông tin, chuyển giao đầy đủ cho chủ đầu tư các thông tin, dữ liệu khi kết thúc hợp đồng cung cấp dịch vụ công nghệ thông tin".

3.5. Yêu cầu về quản lý, chuyển giao dữ liệu trong quá trình thuê

Đơn vị thuê dịch vụ có quyền sử dụng dịch vụ đã thuê để phục vụ công việc của đơn vị và có quyền tải về thông tin, dữ liệu do chính đơn vị tạo lập trong thời gian sử dụng dịch vụ.

Nhà cung cấp dịch vụ có trách nhiệm đảm bảo tính an toàn bảo mật thông tin, dữ liệu do đơn vị thuê dịch vụ tạo lập, đảm bảo hệ thống có thể khôi phục lại dữ liệu khi xảy ra các sự cố ngoại trừ những trường hợp bất khả kháng.

Nhà cung cấp dịch vụ có trách nhiệm cung cấp công cụ quản lý, giám sát hệ thống dịch vụ cho đơn vị thuê dịch vụ sau khi đã hoàn tất thủ tục cung cấp dịch vụ cho bên thuê.

Nhà cung cấp dịch vụ có trách nhiệm chuyển giao toàn bộ thông tin, dữ liệu phát sinh cho các đơn vị thuê dịch vụ khi hết hạn thuê dịch vụ mà bên thuê không gia hạn sử dụng dịch vụ nữa hoặc khi có yêu cầu bằng văn bản của bên thuê dịch vụ.

3.6. Sở hữu thông tin, dữ liệu

Các đơn vị sử dụng dịch vụ có quyền sở hữu, tải về phần dữ liệu do chính đơn vị tạo lập trong suốt quá trình sử dụng.

Nhà cung cấp có trách nhiệm bảo mật mọi thông tin về dữ liệu của các đơn vị thuê dịch vụ và không được phép tiết lộ cho bất kỳ bên thứ 3 nào khác ngoại trừ yêu cầu của cơ quan có thẩm quyền của nhà nước.

Nhà cung cấp dịch vụ có trách nhiệm chuyển giao toàn bộ thông tin, dữ liệu phát sinh cho các đơn vị thuê dịch vụ khi hết hạn thuê dịch vụ mà bên thuê không gia hạn sử dụng dịch vụ nữa hoặc khi có yêu cầu bằng văn bản của bên thuê dịch vụ.

Nếu như Chủ trì thuê dịch vụ không tiếp tục thuê mà muốn đầu tư xây dựng hệ thống cho riêng mình, thì nhà thầu phải hỗ trợ Chủ trì thuê dịch vụ tối đa trong việc sao chép hệ thống và back up dữ liệu về máy chủ của Chủ trì thuê dịch vụ chỉ định. Bao gồm:

- Chuẩn bị nhân lực thực hiện chuyển dữ liệu.
- Thời gian thực hiện tối thiểu 7-10 ngày làm việc hoặc theo kế hoạch của Chủ trì thuê dịch vụ.
- Sao chép và di chuyển dữ liệu theo yêu cầu của Chủ trì thuê dịch vụ
- Kiểm tra tính toàn vẹn dữ liệu của dữ liệu.
- Kiểm tra độ ổn định và chính xác của các ứng dụng sau khi được phục hồi.
- Đảm bảo 100% dữ liệu được chuyển giao cho Chủ trì thuê dịch vụ, giảm toàn bộ thời gian gián đoạn dịch vụ đến 99,999%.

Tài sản hình thành trong quá trình sử dụng 100% thuộc quyền sở hữu hợp pháp của Chủ trì thuê dịch vụ. Nhà thầu không can thiệp vào quyền quản trị hệ thống và quyền quản trị của Chủ trì thuê dịch vụ sau khi bàn giao và nghiệm thu khi hết thời hạn thuê dịch vụ. Nhà cung cấp có trách nhiệm bảo mật mọi thông tin về dữ liệu của Chủ trì thuê dịch vụ và không được phép tiết lộ cho bất kỳ bên thứ 3 nào khác ngoại trừ yêu cầu của cơ quan có thẩm quyền của nhà nước.

4. Giải pháp và phương pháp luận

Nhà thầu chuẩn bị đề xuất giải pháp, phương pháp luận tổng quát thực hiện dịch vụ theo các nội dung quy định tại Mục 3 Chương này, gồm các phần như sau:

1. Giải pháp và phương pháp luận;
2. Kế hoạch công tác.

5. Quy định về kiểm tra, nghiệm thu sản phẩm.

Quy định kiểm tra, nghiệm thu sản phẩm được áp dụng theo Thông tư số 16/2024/TT-BTTTT ngày 30/12/2024 của Bộ Thông tin và Truyền thông quy định về công tác triển khai, giám sát công tác triển khai và nghiệm thu dự án đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước.