Phần 2. YÊU CẦU VỀ KỸ THUẬT
Chương V. YÊU CẦU VỀ KỸ THUẬT

Mục 1. Yêu cầu về kỹ thuật

I. Giới thiệu chung về dự án và gói thầu

1. Giới thiệu chung:

Tên gói thầu: Gói thầu số 03: Cung cấp, lắp đặt, cài đặt thiết bị và phần mềm dự án

Dự án: Đầu tư Trung tâm điều hành thông minh IOC - Giải pháp phòng chống tấn công APT và kiểm soát truy cập

Chủ đầu tư: Tổng công ty Công nghiệp Hóa chất mỏ - Vinacomin

Địa điểm thực hiện: Văn phòng Tổng công ty Công nghiệp Hóa chất mỏ - Vinacomin; Phố Phan Đình Giót, Phường Phương Liệt, TP. Hà Nội.

Giá gói thầu: **9.870.494.096 đồng** *(Chín tỷ, tám trăm bảy mươi triệu, bốn trăm chín mươi bốn nghìn, không trăm chín mươi sáu đồng - Đã bao gồm các khoản thuế, phí vận chuyển, lắp đặt, cài đặt và hướng dẫn sử dụng, bảo hành hàng hóa tại nơi sử dụng; trong đó có 287.490.119 đồng chi phí dự phòng).*

2. Mục tiêu dự án:

c) Mục tiêu chung

Đầu tư Trung tâm điều hành thông minh IOC - Giải pháp phòng chống tấn công APT và kiểm soát truy cập của Tổng công ty Công nghiệp Hóa chất mỏ - Vinacomin bảo đảm và đáp ứng các mục tiêu sau:

- Bảo đảm an toàn, bảo vệ thông tin, hệ thống thông tin tránh bị truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của hệ thống thông tin, hướng tới hiện thực hóa các mục tiêu chuyển đổi hầu hết các hoạt động của MICCO trên nền tảng số.

- Trung tâm điều hành thông minh (IOC) cung cấp một góc nhìn toàn diện và trực quan về các khía cạnh khác nhau của một hệ thống sản xuất để hỗ trợ việc đưa ra quyết định và quản lý hiệu quả.

d) Mục tiêu cụ thể

Trung tâm điều hành thông minh IOC - Giải pháp phòng chống tấn công APT

và kiểm soát truy cập của MICCO sau khi đầu tư phải đảm bảo đáp ứng được các yếu tố sau:

- Giám sát, theo dõi và điều hành được các hoạt động sản xuất của Tổng Công ty.

- Phát hiện các cuộc tấn công theo các dấu hiệu gián tiếp và bằng cách xác định những sai lệch trong công việc của người sử dụng và cơ sở hạ tầng mạng.

- Phòng chống tin tặc, mã độc cho các ứng dụng web, Web Application Firewall đưa ra một cách thức phòng vệ chống lại các hoạt động tin tặc, khai thác các lỗ hổng của Tổng công ty.

- Đảm bảo hiệu quả vận hành trên cơ sở sử dụng các công nghệ tiên tiến để thu thập, phân tích và chia sẻ dữ liệu; tăng tính kết nối, liên thông, đồng bộ và hiệu quả trong quản lý và điều hành.

- Đảm bảo tính bí mật của thông tin, tức là thông tin chỉ được phép truy cập bởi những đối tượng được cấp phép.

- Đảm bảo tính toàn vẹn của thông tin, tức là thông tin chỉ được phép xóa hoặc sửa bởi những đối tượng được phép và phải đảm bảo rằng thông tin vẫn còn chính xác khi được lưu trữ hay truyền đi.

- Đảm bảo độ sẵn sàng của thông tin, tức là thông tin có thể được truy xuất bởi những người được phép vào bất cứ khi nào họ muốn.

II. Yêu cầu về kỹ thuật

1. Yêu cầu chung:

1.1. Tiêu chí lựa chọn giải pháp công nghệ

Các giải pháp lựa chọn cần đáp ứng các tiêu chí sau để đảm bảo khả năng vận hành, mở rộng cũng như tích hợp của hệ thống. Cụ thể các tiêu chí lựa chọn công nghệ như sau:

- **Kiến trúc chuẩn**

Hệ thống phải được xây dựng dựa trên một kiến trúc chuẩn (mô hình chuẩn) về hệ thống mạng, hệ thống bảo mật an toàn dữ liệu CNTT. Đảm bảo khả năng chịu lỗi và tính sẵn sàng cao. Hỗ trợ tích hợp với các hệ thống CNTT hiện có. Đồng thời, kiến trúc phải có tính kế thừa và phù hợp với sự phát triển trong tương lai.

- **Tính mở và chuẩn hóa**

Bất kỳ sự thêm bớt nào các phần tử trong hệ thống đều có thể thực hiện một cách nhanh chóng và chính xác, tạo điều kiện thuận lợi cho việc phát triển, mở rộng hệ thống sau này. Cho phép tích hợp với các hệ thống tự động hóa và giám sát. Do vậy, hệ thống phải tuân thủ tối đa các chuẩn về công nghệ, về cấu trúc thông tin, trao đổi thông tin ... để đảm bảo khả năng tích hợp cao giữa các hệ thống, cũng như khả năng tương tác với các hệ thống khác.

Ngoài ra, hệ thống phải được xây dựng trên cơ sở nền tảng CNTT hiện đại với công nghệ tiên tiến nhất, phù hợp với xu thế phát triển và các tiêu chuẩn của CNTT trên thế giới.

- **Khả năng đáp ứng cao và khả năng mở rộng**

Hệ thống phải có khả năng hoạt động ổn định dưới tải cao. Dễ dàng mở rộng quy mô hệ thống khi cần thiết mà không làm thay đổi kiến trúc.

- **Tính sẵn sàng và độ tin cậy**

Hệ thống phải hỗ trợ dự phòng đảm bảo hoạt động liên tục trong trường hợp lỗi xảy ra.

Hỗ trợ khả năng phục hồi dữ liệu, khôi phục dữ liệu trong trường hợp bị mất mát. Ngoài ra, hệ thống phải đảm bảo chất lượng dịch vụ theo cam kết SLA (Service Level Agreement).

- **Khả năng quản trị**

Hệ thống cần có giao diện quản lý đơn giản, dễ dàng sử dụng và quản trị. Nhờ vậy, người quản trị hệ thống có thể quản trị tập trung toàn bộ hệ thống, theo dõi, phát hiện, cô lập và khắc phục sự cố một cách dễ dàng, nhanh chóng và hiệu quả, đồng thời cũng giúp giảm thiểu các chi phí đào tạo cũng như bảo trì hệ thống. Hỗ trợ tự động hóa, giúp tự động hóa các tác vụ quản lý. Đồng thời hỗ trợ cung cấp báo cáo về tình trạng hoạt động và bảo mật của hệ thống.

- **Khả năng an ninh, bảo mật**

Hệ thống phải có tính năng mã hóa dữ liệu, đảm bảo dữ liệu được bảo vệ khỏi truy cập trái phép trên đường truyền và khi lưu trữ. Kiểm soát truy cập: chỉ những người có quyền mới được truy cập. Mọi truy cập đều được kiểm soát bởi hệ thống.

Khả năng cập nhật phần mềm thường xuyên bằng cách vá các lỗ hổng bảo mật, cập nhật các dấu hiệu tấn công đã biết và khả năng học máy để ngăn ngừa các mối

nguy hiểm chưa biết.

- **Hỗ trợ giao thức IPv6**

Đảm bảo khả năng tương thích với mạng IPv6. Hỗ trợ các tính năng bảo mật nâng cao của IPv6.

1.2. Hệ thống phòng chống tấn công APT

Hệ thống phòng chống tấn công APT phát hiện các mối đe dọa tiên tiến, cho phép dò tìm, phân tích và hồi đáp các mối đe dọa, các cuộc tấn công có chủ đích. Giải pháp sử dụng các kỹ thuật dò đặc biệt, sandbox và Threat Intelligence để chống lại các cuộc tấn công.

Giải pháp phòng chống tấn công APT cung cấp cái nhìn toàn cảnh, sâu sắc và kiểm soát hệ thống mạng mà các doanh nghiệp và các tổ chức cần để làm giảm nguy cơ hứng chịu các tấn công APTs và các tấn công có chủ đích. Giúp phát hiện và xác định các mối đe dọa xâm nhập theo thời gian thực, và cung cấp sự phân tích sâu và các hành động cần thiết để phòng tránh, khám phá và ngăn chặn các tấn công vào các dữ liệu của doanh nghiệp.

Các tội phạm có tổ chức dựa vào các mã độc được cấu tạo tùy biến để tấn công vào một tổ chức nào đó, nó có thể biết được chính xác mội trường của máy trạm, ứng dụng, trình duyệt, dịch vụ … mà tổ chức đang hoạt động. Những mã độc này được thiết kế để khai thác chính xác vào các cấu đang hoạt động và việc sử dụng các môi trường sandbox chung chung không có khả năng nhận biết các dạng mã độc này. Vì thế cần một giáp pháp cung cấp môi trường sandbox được tùy biến giúp tổ chức có thể tạo dựng một môi trường ảo giống như thật để phát hiện các mã độc này.

Môi trường tùy chọn sandbox sẽ mô phỏng chính xách môi trường IT của tổ chức, cho phép tổ chức:

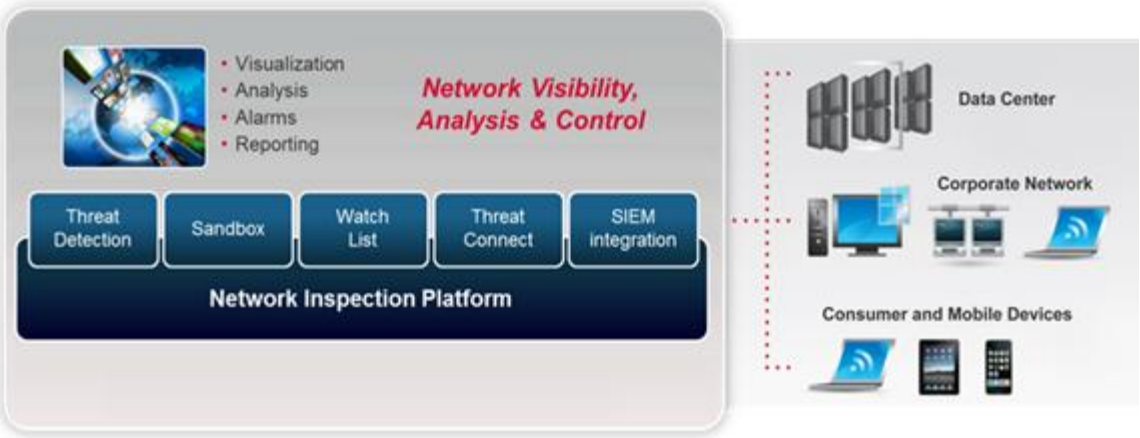
- Nhận dạng các mã độc nhắm đến tổ chức (mô phỏng môi trường Windows, ngôn ngữ, ứng dụng, môi trường desktop, …)
- Vô hiệu hóa kỹ thuật vượt mặt sandbox, dựa trên kỹ thuật phát hiện Windows license, ứng dụng chuẩn, hoặc ngôn ngữ đặc trưng.
- Bỏ qua các mã độc mà không ảnh hưởng tới tổ chức bởi vì hệ thống và ứng dụng của tổ chức không sử dụng.

Giải pháp phòng chống tấn công APT cần đáp ứng các tính năng sau:

- Giải pháp cung cấp cho các doanh nghiệp và các tổ chức chính phủ một **mức độ mới của tầm nhìn (visibility)** và giải pháp thông minh để phát hiện các tấn công APTs và các tấn công có chủ đích trên môi trường điện toán đang phát triển.
- Giải pháp cần đảm bảo giám sát tất cả các cổng (port) và giao thức cung cấp cho tổ chức một sự giám sát/bảo vệ rộng nhất. Các cơ chế phát hiện chuyên sâu cũng như các sandbox tùy biến giúp nhận diện và phân tích các chương trình mã độc, kết nối C&C nguy hiểm và các hoạt động tàng ẩn mình trong hệ thống mạng mà các giải pháp truyền thống không phát hiện được. Các thông tin chi tiết về các mối đe dọa sẽ giúp cho hệ thống tổ chức phản hồi

nhanh chóng trước mối đe dọa.

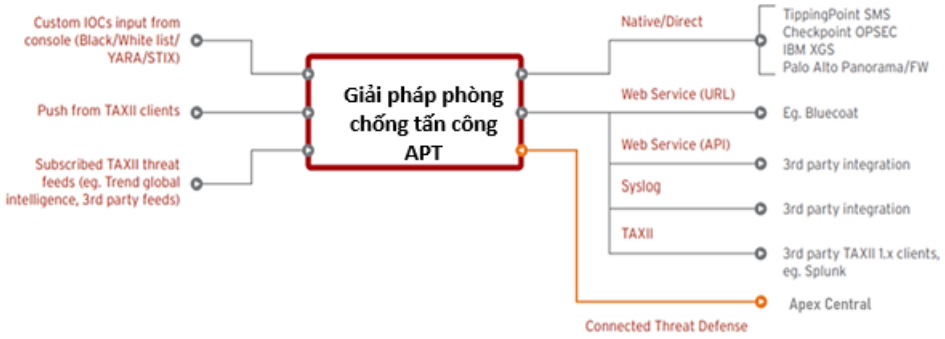
- **Giải pháp phát hiện đầy đủ các mối đe dọa mới:** Giám sát tất cả các port và các giao thức để phát hiện các tấn công trên toàn bộ mạng của tổ chức. Một vài cơ chế phát hiện đặc thù và tương quan các chính sách được thiết kế riêng để phát hiện các phần mềm mã độc, kết nối C&C và các hành vi nghi ngờ, độc hại trên toàn bộ mạng lưới, không chỉ giới hạn ở các giao thức chuẩn như HTTP và SMTP.



- **Giải pháp giúp phát hiện các hành vi mã độc, kết nối C&C và các hành vi vi phạm khác**: Sử dụng các cơ chế phát hiện tối ưu, các rule tương quan, và tùy chỉnh sandbox để phát hiện tất cả các khía cạnh của tấn công có chủ đích, mà không chỉ tóm gọn ở việc phát hiện chương trình mã độc.
- **Hỗ trợ tùy chỉnh sandboxing:** Sử dụng các image phù hợp với cấu hệ thống của tổ chức để có thể phát hiện các mối đe dọa tiềm tàng. Việc phân tích được thực thi sử dụng sandbox tùy biến nhằm mô phỏng chính xác cấu hệ thống của tổ chức. Ngoài ra còn cò thể quét các file nghi ngờ và nội dung web. Sandbox tùy chỉnh có thể phát hiện chính xác các mối đe dọa chỉ nhắm vào tổ chức của bạn. Sandbox cho phép người quản trị tạo và import nhiều image khác nhau:
  - Windows Workstation: Windows 7, Windows 8, Windows 10…
  - Windows Server: 2012, 2016, 2019…
  - Linux
- **Hỗ trợ truy vấn thông tin mối đe dọa toàn cầu:** Giải pháp cho phép truy

vấn đa dạng các thông tin liên quan tới các mối đe dọa đã phát hiện thông qua portal.

- **Cung cấp khả năng bảo vệ hệ thống vượt trội**: Phát hiện tấn công với Windows, Mac OS X, Android, Linux và nhiều hệ thống khác.
- **Giải pháp có khả năng linh hoạt và đơn giản trong quá trình triển khai:** Triển khai giải pháp chỉ sử dụng một thiết bị, đã được tích hợp sẵn các chức năng và có thể triển khai với các cấu phần cứng hoặc ảo hóa.
- **Cung cấp khả năng chia sẻ các dấu hiệu nguy hiểm (SOC):** Chia sẻ các thông tin và các dấu vết nguy hiểm (IoC), tự động cập nhật cho các giải pháp khác của đơn vị và bên thứ ba. Giải pháp cho phép tổ chức chia sẻ các dấu hiệu nguy hiểm (IOC) được phát hiện bởi sandbox cho các giải pháp khác hoặc một bên thứ ba. Các thông tin chia sẻ này cho phép tổ chức tùy biên các lớp phòng thủ theo thời gian thực để chống lại các cuộc tấn công có chủ đích.



- **Cung cấp khả năng theo dõi Realtime:** Cho phép tổ chức trực quan toàn bộ các mối đe dọa theo thời gian thực và cung cấp các khả năng quét nâng cao trên cùng một giao diện, đồng thời hỗ trợ cung cấp các thông tin khẩn cấp, truy vấn nguồn gốc các mối đe dọa theo vị trí địa lý, giám sát các tài nguyên quan trọng của tổ chức.

1.3. Hệ thống tường lửa kiểm soát truy cập ứng dụng web - Web Applicaiton Firewall

Web Application Firewalls (WAF) là công nghệ được thiết kế để bảo vệ ứng dụng web trước các tấn công mức ứng dụng. WAF có khả năng ngăn chặn các tấn công mà hệ thống tường lửa và hệ thống phòng chống xâm nhập – IPS không ngăn

chặn được và cũng không yêu cầu việc sửa đổi các mã nguồn của ứng dụng. Tường lửa chỉ kiểm soát mức truy cập vào theo port mà không kiểm tra sâu nội dung trên cổng HTTP được mở để phát hiện tấn công. Hệ thống IPS thường có khả năng bảo vệ chủ yếu dựa trên mẫu (signature) tấn công cũng như các lỗ hổng đã biết. Các điểm yếu đặc thù của từng ứng dụng cụ thể có thể cho phép tấn công khai thác và dễ dàng vượt qua hệ thống firewall và IPS. Nhờ khả năng phân tích sâu vào ứng dụng Web, khả năng học và hiểu được cấu trúc dữ liệu cũng như logic hoạt động bình thường của ứng dụng, nên WAF có bảo vệ hiệu quả cho ứng dụng Web

Hệ thống Tường lửa ứng dụng Web chuyên dụng: Là các sản phẩm được thiết kế chuyên để bảo vệ ứng dụng Web, thị trường định nghĩa và gọi là Web Application Firewall.

1.4. Hệ thống trung tâm giám sát thông tin tập trung (IOC)

Hạ tầng trung tâm giám sát thông tin tập trung là hệ thống phần cứng đảm nhiệm chức năng thu thập, lưu trữ và hiển thị dữ liệu từ nhiều nguồn khác nhau trong cơ sở hạ tầng của tổ chức như hệ thống phòng chống tấn công APT, hệ thống kiểm soát truy cập NAC, hệ thống xác thực đa yếu tố MFA, hệ thống ngăn chặn xâm nhập IPS, hệ thống bảo mật Endpoint,... Hệ thống trung tâm giám sát thông tin tập trung hỗ trợ tổ chức theo dõi, quản lý và nâng cao hiệu quả hoạt động, đặc biệt trong các lĩnh vực sản xuất, kinh doanh và an toàn lao động. Nhờ khả năng giám sát trên diện rộng, dữ liệu được cập nhật liên tục, giúp ban lãnh đạo kịp thời đưa ra quyết định phù hợp.

Bên cạnh đó, giải pháp giám sát góp phần nâng cao mức độ an toàn bằng cách phát hiện sớm các nguy cơ tiềm ẩn, đồng thời kiểm soát chặt chẽ việc ra vào các khu vực quan trọng thông qua hệ thống camera giám sát. Điều này giúp giảm thiểu rủi ro trong quá trình vận hành và bảo vệ tài sản một cách hiệu quả.

Hệ thống cũng đóng vai trò quan trọng trong việc tối ưu hóa quy trình sản xuất thông qua phân tích dữ liệu, hạn chế thất thoát nguyên vật liệu. Việc ứng dụng công nghệ tự động hóa và giám sát từ xa giúp giảm sai sót do con người, đồng thời tiết kiệm chi phí vận hành.

Ngoài ra, hệ thống cung cấp dữ liệu phân tích hỗ trợ đánh giá hiệu suất sản xuất và vận hành. Qua đó, lãnh đạo có thể đưa ra các quyết định chiến lược dựa trên thông tin chính xác và đầy đủ.

Hạ tầng trung tâm giám sát thông tin tập trung cần đáp ứng các yêu cầu quan trọng để đảm bảo hệ thống hoạt động hiệu quả, an toàn và ổn định. Trước hết, hệ thống phải có khả năng giám sát dữ liệu liên tục, tiếp nhận thông tin từ nhiều nguồn. Dữ liệu cần được xử lý nhanh chóng, đảm bảo cập nhật liên tục, đồng thời hỗ trợ phân tích và cảnh báo khi phát hiện sự cố hoặc bất thường.

Tính linh hoạt và khả năng mở rộng cũng là một yêu cầu cần thiết, cho phép nâng cấp phần cứng khi nhu cầu giám sát tăng lên, đồng thời hỗ trợ tích hợp với các hệ thống hiện có. Hệ thống cần đảm bảo khả năng kết nối nhiều địa điểm giám sát trong cùng một nền tảng thống nhất.

Về mặt bảo mật, trung tâm giám sát cần áp dụng các giải pháp như tường lửa, VPN, hệ thống phát hiện và ngăn chặn xâm nhập nhằm bảo vệ mạng lưới. Cơ chế phân quyền người dùng giúp kiểm soát quyền truy cập dữ liệu, trong khi việc ghi log toàn bộ hoạt động hỗ trợ quá trình kiểm tra và truy vết khi cần thiết.

Hệ thống cần có giao diện trực quan, dễ sử dụng, hiển thị thông tin qua biểu đồ và bảng điều khiển để hỗ trợ giám sát hiệu quả. Các cảnh báo bằng âm thanh, hình ảnh hoặc tin nhắn giúp phản ứng kịp thời khi có sự cố. Khả năng truy cập từ xa

qua trình duyệt web hoặc ứng dụng di động cũng là một yếu tố quan trọng, giúp việc giám sát trở nên linh hoạt hơn.

Trung tâm giám sát đảm bảo tính ổn định và khả năng hoạt động liên tục 24/7. Việc tích hợp cơ chế dự phòng giúp tránh lỗi hệ thống, trong khi các giải pháp quản lý nguồn điện như UPS đảm bảo hệ thống vẫn vận hành ngay cả khi mất điện.

1.5. Hệ thống phần mềm văn phòng điện tử Portal Office

Hệ thống phần mềm văn phòng điện tử Portal Office 10 hiện tại Tổng công ty đang vận hành sử dụng chỉ đáp ứng được nhu cầu khai thác thông tin cơ bản, chưa được cập nhật bản vá lỗi. Nhằm khắc phục những hạn chế của những phiên bản trước đây, nhà sản xuất đã nâng cấp với các chức năng được tối ưu hơn. Cụ thể như:

Giao diện desktop trên nền bootstrap mới Admin LTE:

- Trang đăng nhập phần mềm:

+ Nền trong suốt có đính kèm hình ảnh.

+ Có chức năng xem mật khẩu đã lưu.

- Trang chủ sau khi đăng nhập giao diện mới:

Module Quy Trình:

+ Yêu cầu tôi xử lý: theo skin mới

+ Yêu cầu tôi gửi: theo skin mới

+ Tra cứu yêu cầu: theo skin mới

Module Lịch cơ quan:

+ Đăng ký lịch: theo skin mới

+ Hiển thị lịch: theo skin mới

+ Duyệt tài nguyên: theo skin mới

+ Tra cứu lịch: theo skin mới

Module Công Văn:

+ Công văn đến: theo skin mới

+ Công văn đi: theo skin mới

+ Công văn nội bộ: theo skin mới

+ Công văn nội bộ phòng: theo skin mới

Module Công Việc:

+ Giao việc: theo skin mới

+ Hiển thị công việc: theo skin mới

+ Tra cứu công việc: theo skin mới

+ Tương tác công việc: theo skin mới

Module Tin tức: theo skin mới

Module Tài liệu: theo skin mới

Module Lịch cá nhân: theo skin mới

Module Tin nhắn: theo skin mới

Tab Ký Số, Tab Danh bạ, Tab Tài khoản: theo skin mới

2. Tiêu chuẩn kỹ thuật áp dụng

- Quyết định số 19/2008/QĐ-BTTTT ngày 09/4/2008 của Bộ Thông tin và Truyền thông về việc ban hành Quy định áp dụng tiêu chuẩn về ứng dụng công nghệ thông tin, Thông tư 39/2017/TT-BTTTT ngày 15/12/2017 của Bộ trưởng Bộ Thông tin và Truyền thông ban hành Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong các ứng dụng.

- Tuân thủ Quyết định số 1729/QĐ-BTTTT ngày 09 tháng 10 năm 2024 của Bộ Thông tin và Truyền thông sửa đổi, bổ sung một số nội dung của Quyết định số 2568/QĐ-BTTTT ngày 29/12/2023 của Bộ trưởng Bộ Thông tin và Truyền thông ban hành Khung Kiến trúc Chính phủ điện tử Việt Nam, phiên bản 3.0 hoặc cao hơn, hướng tới Chính phủ số.

- Các chỉ tiêu kỹ thuật áp dụng trong triển khai lắp đặt, cài đặt, kiểm tra và hiệu chỉnh thiết bị:

TT	Tên Tiêu chuẩn	Ký hiệu
1	Công nghệ thông tin - Hệ thống quản lý an toàn thông tin - Các yêu cầu	TCVN ISO/IEC 27001:2019 ISO/IEC 27001:2013)
2	Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn triển khai hệ thống quản lý an toàn thông tin	TCVN 10541:2014 ISO/IEC 27003:2010
3	Trung tâm dữ liệu - Yêu cầu về hạ tầng kỹ	TCVN 9250:2021

TT	Tên Tiêu chuẩn	Ký hiệu
	thuật viễn thông	

3. Các giải pháp thiết kế và yêu cầu kỹ thuật tối thiểu của hàng hóa:

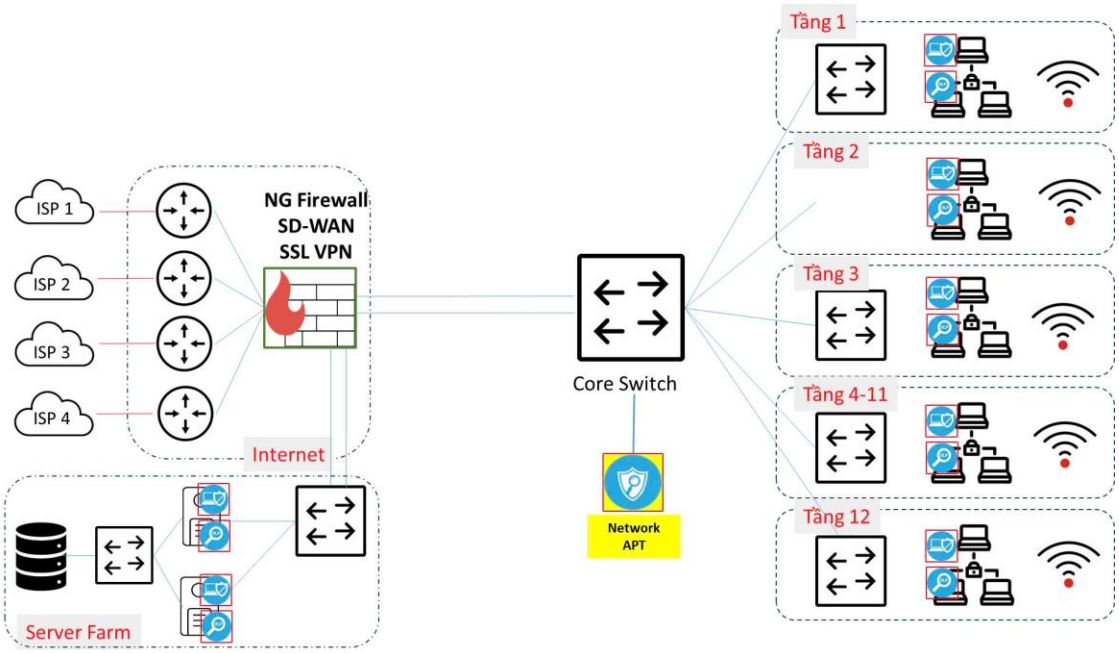
3.1. Giải pháp hệ thống phòng chống tấn công APT

Cơ sở tính toán hệ thống

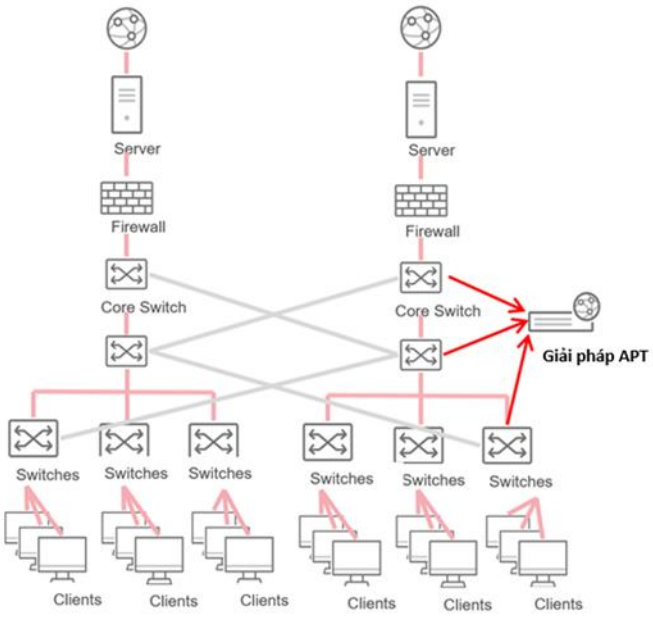
Căn cứ hiện trạng hệ thống mạng phục vụ ứng dụng hiện tại của Micco đang sử dụng các kết nối 1Gbps, vì vậy giải pháp phòng chống tấn công APT trang bị cần đáp ứng thông lượng tối thiểu 1Gbps và có khả năng mở rộng thông lượng mà không cần thay thế thiết bị phần cứng đảm bảo tối ưu hóa việc sử dụng thiết bị đáp ứng nhu cầu hiện tại và mở rộng trong tương lai. Vì vậy, đề xuất sử dụng giải pháp có thông lượng tối thiểu >= 1 Gbps.

Mô hình hệ thống

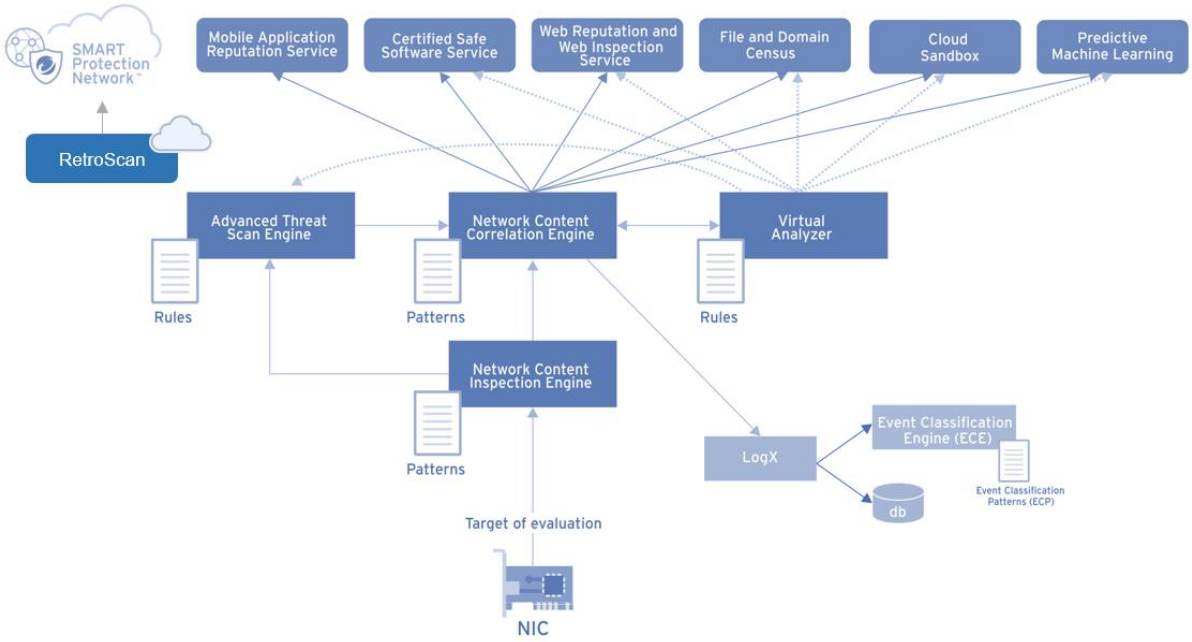
Dựa trên mô hình hệ thống mạng hiện có, mô hình triển khai APT như sau:



Giải pháp đề xuất triển khai ở chế độ Out of Band, cho phép giải pháp có thể thu thập đầy đủ lưu lượng trong hệ thống mạng từ các mirror port/ span port để phân tích, tương quan và phát hiện các mối đe dọa APT.



Giải pháp phòng chống, tấn công APT sẽ thực hiện quan trắc nhiều đoạn mạng sử dụng nhiều cổng (Data Port) input lưu lượng được mirror từ hạ tầng mạng. Việc thực hiện phân tích phát hiện các mối đe dọa được thực hiện như sau:



Lưu lượng mạng được ghi nhận trên cổng Data Port của giải pháp APT sẽ lần lượt được xử lý, phân tích chuyên sâu bởi một số module thành phần của giải pháp như:

- Thành phần phát hiện các mối đe dọa mạng dựa trên thông tin của giao thức
- Thành phần tương quan, thực hiện phân tích tất cả những dữ liệu telemetry thu thập được từ một kết nối cụ thể, và sẽ ra quyết định về mức độ rủi ro an toàn thông tin của kết nối đó
- Thành phần Sandboxing: Môi trường ảo tách biệt với mạng Production để đánh giá hành vi của mã độc
- Một số thành phần đánh giá thống kê mức độ phổ biến của hình mẫu file cũng như danh tiếng của files/URL/app

Giải pháp dựa trên các kết quả thu thập để xác định mức độ nguy hiểm của tệp tin dựa trên ngữ cảnh cũng như các thông tin liên quan khác, từ đó đưa ra các cảnh bảo, thông tin về các hành vi, mối đe dọa đối với hệ thống.

Yêu cầu kỹ thuật:

STT	Tên hàng hoá	Yêu cầu kỹ thuật tối thiểu hoặc tương đương
I	**Hệ thống phòng chống tấn công APT**	
1	**Phần cứng**	
	Kiểu dáng	Rackmount
	Băng thông (Throughput)	≥ 1 Gbps
	Số lượng sandbox/VM hỗ trợ	≥ 4
	Cổng quản trị	≥ 1x 100/1000 BaseT RJ45
	Cổng dữ liệu	≥ 5x 100/1000 BaseT RJ45
	Storage	≥ 2 x 1TB
	Nguồn điện	Redundant
2	**Các tính năng bảo mật**	
	Tính năng phát hiện các mối đe dọa	Phát hiện các cuộc tấn công có chủ đích và các hành vi của mã độc
		Phát hiện các mã độc mã hóa dữ liệu (ransomware)
		Phát hiện mã độc Zero-day và các khai thác lỗ hổng (Zero-day malware)
		Phát hiện hành vi của attacker và các hoạt động mạng khả nghi
		Phát hiện các hiểm họa trên nền Web, bao gồm cả khai thác lỗ hổng, tự động

STT	Tên hàng hoá	Yêu cầu kỹ thuật tối thiểu hoặc tương đương
		tải malware
		Phát hiện phishing, spear phishing và các mối đe dọa khác trên email
		Phát hiện các hành vi đánh cắp dữ liệu truyền ra ngoài (Data exfiltration)
		Phát hiện các phần mềm mã độc: Bots, Trojans, Worms, keyloggers...
		Phát hiện các ứng dụng gây rối, gây hại cho máy tính
		Có khả năng phát hiện các mối đe dọa đã biết hay chưa biết tới như: advanced malware, unknown malware, ransomware, zero-day, command and control (C&C)...
		Giải pháp có khả năng phát hiện các ứng dụng mạng trái phép: Các ứng dụng mạng trái phép dạng peer-to-peer, instant messaging hoặc streaming media khiến người sử dụng bị đánh lạc hướng, chiếm băng thông và có các rủi ro bảo mật.
	Khả năng chia sẻ thông tin	Có khả năng chia sẻ thông tin với các thiết bị khác hoặc các giải pháp của hãng thứ 3 để phục vụ công tác điều tra, đảm bảo an toàn an ninh thông tin
	Giám sát và phân tích mối đe dọa theo thời gian thực	Cung cấp giao diện giám sát có khả năng cung cấp thông tin về các mối đe dọa theo thời gian thực. Thông tin được tổ chức dưới dạng tab
	Hỗ trợ giám sát đa giao thức và ứng dụng mạng	Giải pháp có thể hỗ trợ giám sát $\geq$ 100 giao thức mạng trên tất cả các cổng mạng nhằm phát hiện mã độc

STT	Tên hàng hoá	Yêu cầu kỹ thuật tối thiểu hoặc tương đương
	Hệ thống cho phép cho phép cung cấp các thông tin điều tra	Hệ thống có khả năng cung cấp thông tin điều tra đối với các file nghi ngờ như File name File Type File Size SHA-1 MD5 Risk level Threat Đồng thời cho phép download file bị phát hiện ở dạng nén có password
	Có khả năng phát hiện mã độc với nhiều cơ chế	Có khả năng áp dụng các cơ chế kiểm tra của file, web, IP, ứng dụng moblie, tổng hợp thông tin mối đe dọa nhằm phát hiện ransomeware, zero-day, advanced malware và các hành vi của attacker
	Có khả năng phân tích các file nén được bảo vệ bởi mật khẩu	- Có khả năng phân tích các file nén được bảo vệ bởi password - Hỗ trợ giải mã các file nén có mật khẩu đến tiến hành kiểm tra, dựa vào danh sách mật khẩu được cung cấp sẵn
	Hỗ trợ-phân tích phát hiện rò rỉ thông tin, các lỗ hổng bảo mật và các ứng dụng di động bị sửa đổi	Hỗ trợ-phân tích để phát hiện các rò rỉ thông tin, các lỗ hổng bảo mật và các ứng dụng di động bị sửa đổi
	Cung cấp giải pháp sandbox riêng	Cho phép tự tạo môi trường giả lập (sandbox) riêng. Người dùng có thể tự tạo riêng sandbox theo tiêu chuẩn OVA format,
		Môi trường giả lập hỗ trợ các HĐH - Windows 7/8/10/11 - Windows Server 2016 - Windows Server 2019 - Windows Server 2022

STT	Tên hàng hoá	Yêu cầu kỹ thuật tối thiểu hoặc tương đương
	Định dạng file hỗ trợ phân tích trong môi trường giả lập	Hệ thống phải hỗ trợ phân tích trong môi trường giả lập các file EXE, Office, các file dạng đặc biệt như Javascript, PDF, CHM, XML, MOV, …
	Khả năng phân tích traffic	Hỗ trợ phân tích traffic trên cả 2 chiều inbound và outbound nhằm phát hiện các cuộc tấn công của attacker, advanced threats, ransomeware
	Khả năng ghi nhận và ngăn chặn lây lan mã độc	Khi phát hiện mối đe dọa, giải pháp cho phép ghi nhận (log) và ngăn chặn (block) network traffic
	Có cơ chế phát hiện hoạt động nguy hại của attacker sau khi đã vào hệ thống	Giải pháp có khả năng phát hiện các hành vi của attacker sau khi đã xâm nhập được hệ thống như - Thu thập thông tin xác thực - Leo thang đặc quyền - Tìm cách kiểm soát thêm các máy khác
	Có khả năng phát hiện các ứng dụng và dịch vụ trái phép trong hệ thống mạng	Có khả năng phát hiện những dịch vụ trái phép hoặc chưa được đăng ký đang hoạt động trong hệ thống mạng: AD, kerberos, database, DNS, WSUS, Webserver, SMTP Open Relay
3	**Quản trị và báo cáo**	
	Tính năng quản trị	Giao diện quản trị có khả năng hiển thị các thông tin - Trạng thái hệ thống - Thông tin về các mối đe dọa và thông tin phân tích tương ứng - Các biểu đồ tổng quát
	Tính năng báo cáo	Cho phép tạo nhiều loại báo cáo khác nhau như - Tổng quan về phát hiện các mối đe dọa trên hệ thống - Report chi tiết cho từng máy bị tấn

STT	Tên hàng hoá	Yêu cầu kỹ thuật tối thiểu hoặc tương đương
		công hoặc có nguy cơ bị tấn công - Tạo report theo yêu cầu hoặc theo lập lịch ngày, tuần, tháng
4	**Bản quyền đi kèm**	Bản quyền sử dụng, cập nhật phần mềm tối thiểu 1 năm kèm theo thiết bị
5	**Bảo hành**	≥ 1 năm chính hãng

3.2. Hệ thống tường lửa kiểm soát truy cập ứng dụng WAF-WEB

Cơ sở tính toán hệ thống

Hiện nay hệ thống đang sử dụng thiết bị FortiWeb 400D, vì vậy cơ sở định cỡ cấu hình hệ thống WAF, được sizing theo các nguyên tắc sau:

- Có cấu hình tối thiểu > thiết bị hiện tại đảm bảo khả năng chịu tải của toàn bộ hệ thống.

  Trong đó:

  - Thiết bị FortiWeb 400D hiện tại đang đang bảo vệ cho 2 ứng dụng (EAM và Portal) của Micco. Trong thời gian tới, Micco sẽ đưa thêm các hệ thống ứng dụng qua thiết bị bảo vệ ứng dụng Web bao gồm:

  + Phần mềm KPI

  + Phần mềm An Toàn

  + Phần mềm Môi Trường

  + Phần mềm Elearning

  + Phần mềm eMicco

  …

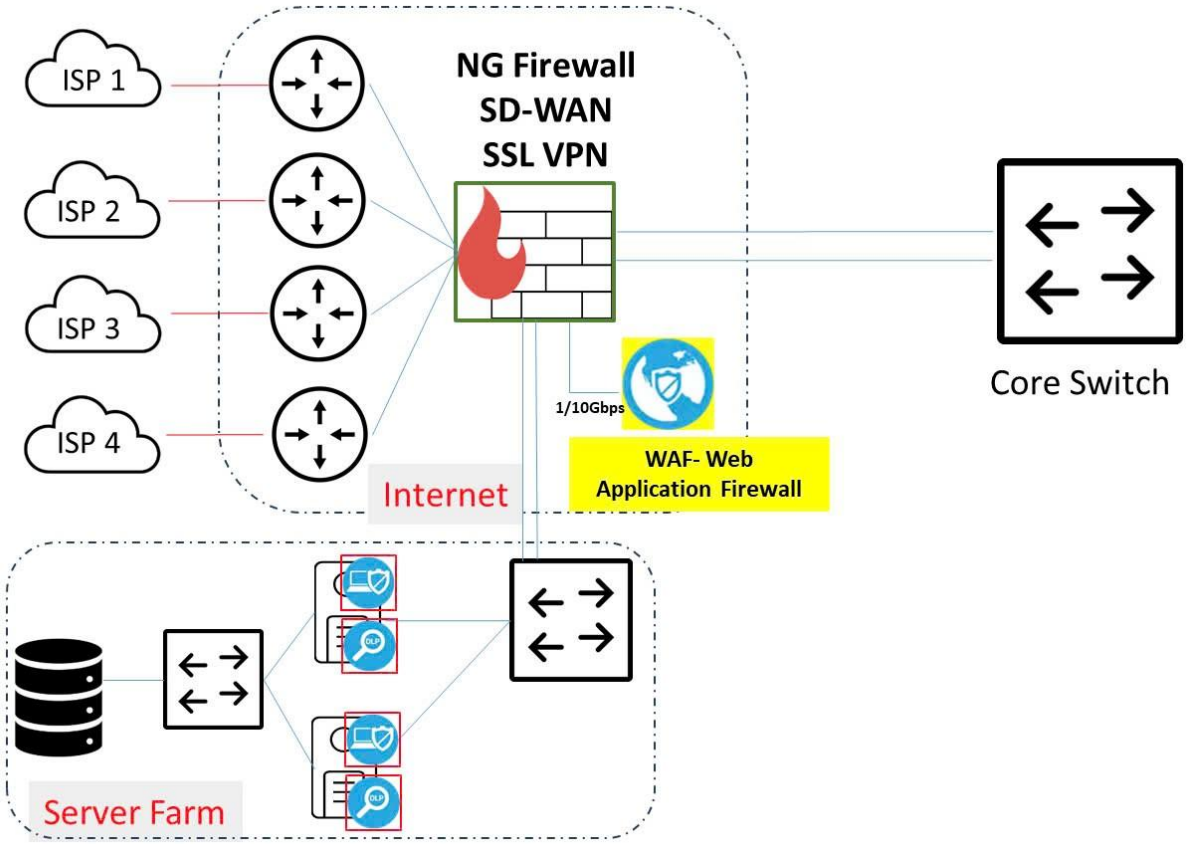
  - Hiện nay throughput của FortiWeb 400D 100Mbps không đáp ứng hiệu năng bảo vệ cho các hệ thống ứng dụng dự kiến của MICCO, để đảm bảo hiệu năng hoạt động cũng như có tính dự phòng mở rộng, đề xuất throughput tối thiểu ≥ 1Gbps.

- Tính dự phòng tăng trưởng hệ thống.
- Về kết nối đảm bảo tương thích với hệ thống hiện tại và có tính dự phòng kết nối 1/10GbE phục vụ khả năng mở rộng trong tương lai.

Giải pháp triển khai

Hệ thống triển khai đề xuất mô hình out-of-band để đảm bảo không ảnh hưởng đến hoạt động, cũng như làm thay đổi kiến trúc hệ thống hiện tại.

Mô hình hệ thống được mô tả như sau:



Thiết bị WAF đóng vai trò bảo vệ các hệ thống ứng dụng luồng truy cập các ứng dụng được mô tả như sau:

(1) Người dùng ứng dụng → (2) truy cập các ứng dụng MICCO qua thiết bị tường lửa public → (3) luồng truy cập ứng dụng được đẩy qua thiết bị bảo vệ ứng dụng Web –WAF để kiểm tra các luồng access theo các rule chính sách bảo mật được định nghĩa sẵn → (4) Nếu luồng access đáp ứng yêu cầu sẽ được

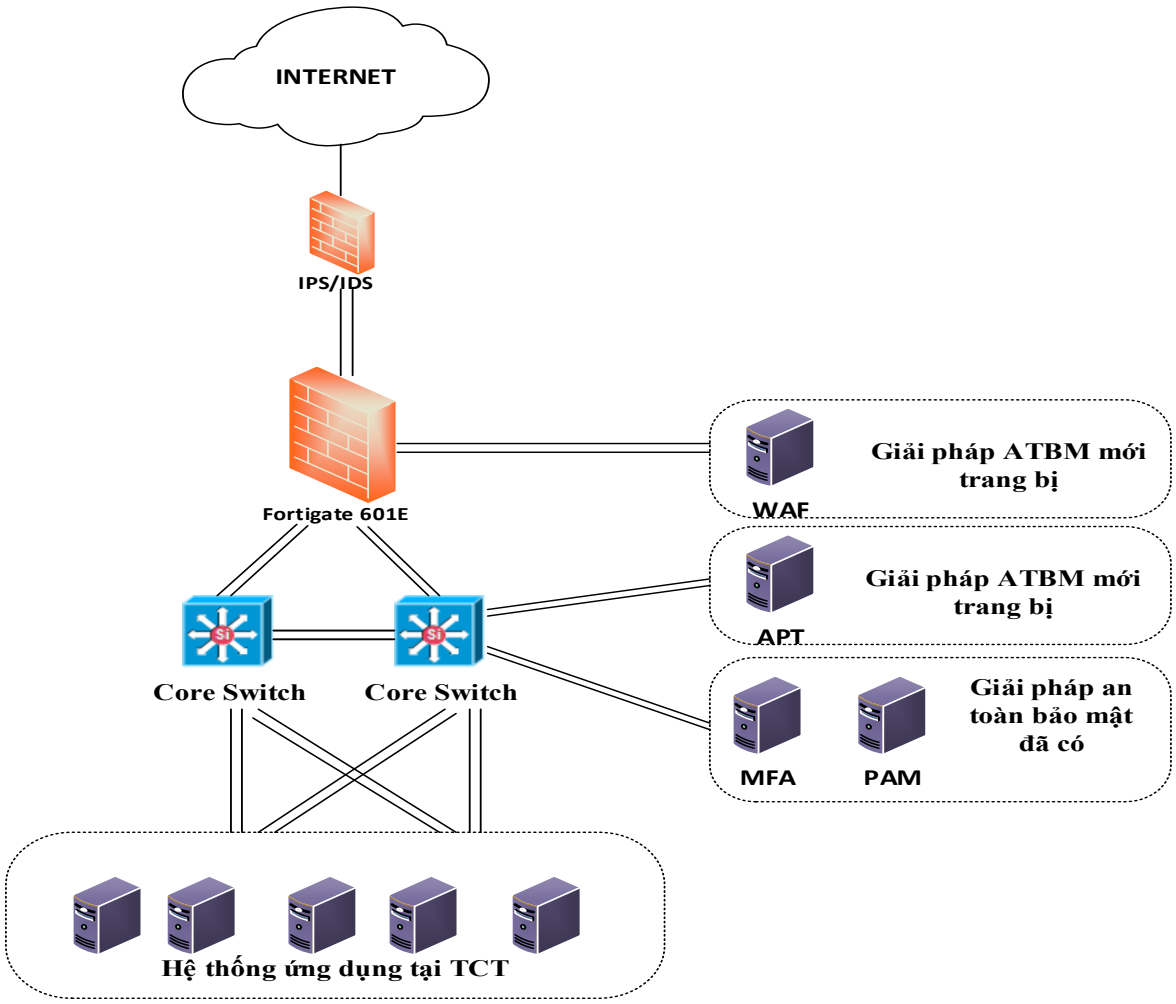
allow access các backend server, với luồng access trên người dùng chỉ thấy được địa chỉ IP của thiết bị WAF và không thấy được địa chỉ priv của các máy chủ backend phía trong → (5) Nếu luồng access không đáp ứng các rule chính sách sẽ bị block và gửi cảnh báo đến quản trị viên.

Yêu cầu kỹ thuật:

STT	Tên hàng hoá	Yêu cầu kỹ thuật tối thiểu hoặc tương đương
II	Hệ thống kiểm soát truy cập ứng dụng Web- WAF	
	Kiểu dáng	Rackmount
	Thông lượng	≥ 1 Gbps
	Độ trễ	< 5,5 ms
	Giao diện kết nối bypass	Tối thiểu 4 cổng GE RJ45
	Giao diện kết nối	Tối thiểu 4 cổng SFP
	Storage	≥ 480GB SSD
	Nguồn điện	02 nguồn
	Xử lý mã hóa SSL/TLS	Hỗ trợ xử lý SSL/TLS offloading bằng phần cứng xử lý chuyên dụng của hãng sản xuất thiết bị
	Các tính năng bảo mật ứng dụng Web	- Hỗ trợ machine learning - Hỗ trợ chặn lọc dựa trên IP reputation - Hỗ trợ chặn lọc dựa trên vị trí địa lý của IP - Hỗ trợ ngăn ngừa khai thắc lỗ hổng trên ứng dụng web/API theo OWASP Top 10 - Hỗ trợ phòng chống tấn công Brute force - Hỗ trợ tích hợp các công cụ dò quét lỗ hổng scanner của bên thứ 3 - Hỗ trợ phòng chống

STT	Tên hàng hoá	Yêu cầu kỹ thuật tối thiểu hoặc tương đương
		DoS/DDoS - Hỗ trợ phòng chống thay đổi giao diện Web (Web Defacement Protection)
	Các tính năng xác thực	- Hỗ trợ SSL client certificate - Hỗ trợ LDAP, RADIUS
	Hỗ trợ kiểm soát phát hiện theo ngưỡng	- Hỗ trợ kiểm soát phát hiện theo ngưỡng
	Tính sẵn sàng	Cho phép triển khai active/passive và active/active clustering
	TÍnh năng quản trị và giám sát	- Quản trị qua giao diện Web - Quản trị qua giao diện CLI - Khả năng phân quyền quản trị cho từng tài khoản - Giám sát đồ họa real-time - Phân tích dữ liệu và báo cáo - Hỗ trợ Syslog, SNMP, Email Logging
	Bản quyền	Bản quyền cập nhật trong vòng 1 năm các tính năng bảo mật cho thiết bị bao gồm: - Anti Virus - Tính năng bảo mật ứng dụng Web - Tính năng định danh IP
	Bảo hành	1 năm chính hãng

Mô hình tổng thể hệ thống sau khi triển khai



- Giải pháp phòng chống tấn công APT giúp nhận diện các mối đe dọa ẩn nấp mà các hệ thống tường lửa, antivirus hiện tại không phát hiện được, giúp ngăn chặn các mối tấn công nguy hiểm, ngăn chặn rò rỉ dữ liệu, kiểm soát phát hiện nhanh các vùng bị lây nhiễm mã độc, giảm thiểu rủi ro và thời gian downtime của hệ thống. Đồng thời cho phép tích hợp vơi các hệ thống giám sát tập trung giúp tự động hóa phản hồi và nâng cao khả năng phân tích sự kiện trong hệ thống.

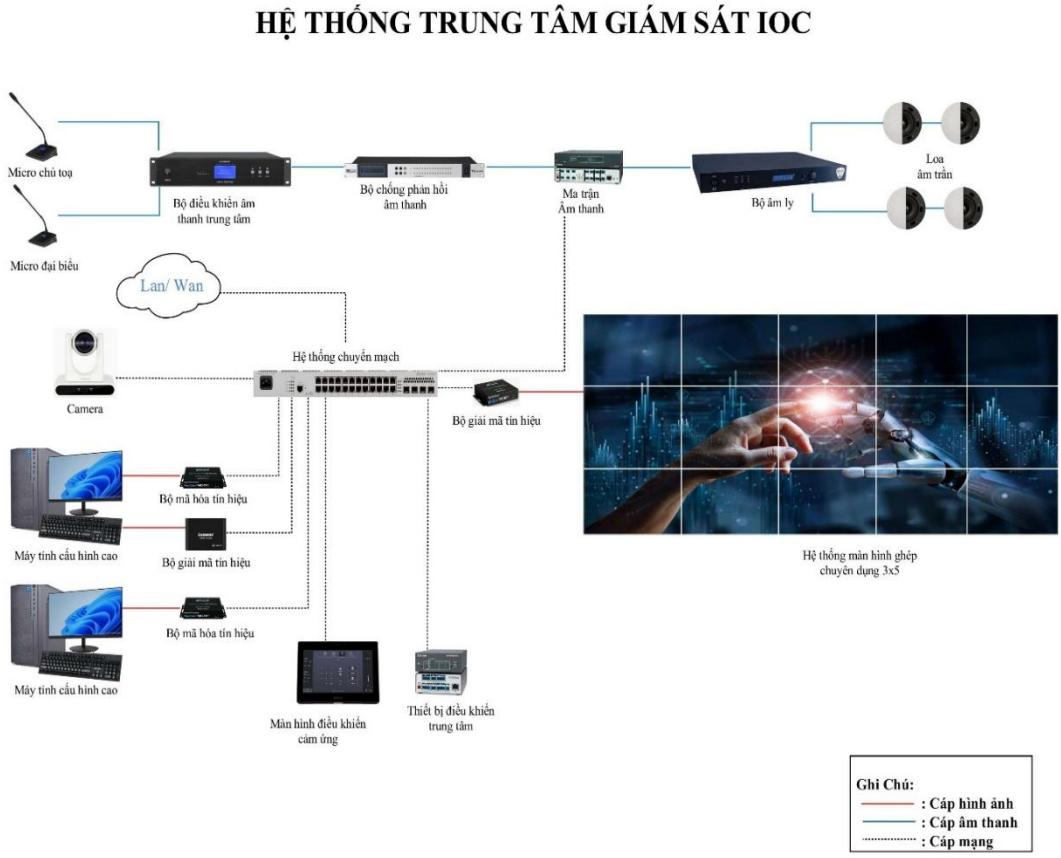
- Giải pháp WAF giúp ngăn chặn khai thác các lỗ hổng qua các ứng dụng web hiện tại- nơi dễ bị tấn công và khai thác nhất. Giúp bảo vệ các dữ liệu, tránh bị đánh cắp thông tin qua các trình duyệt web.

3.3.Hạ tầng trung tâm giám sát thông tin tập trung IOC

Cơ sở tính toán hệ thống:

Dựa trên quy mô hoạt động vận hành của Tổng công ty, số lượng thiết bị, hệ thống cần theo dõi và yêu cầu về giám sát an ninh, vận hành sản xuất. Đơn vị có nhiều hệ thống bảo mật, an toàn thông tin được phân bố tại các khu vực khác nhau, yêu cầu một hệ thống giám sát tập trung có khả năng thu thập dữ liệu từ nhiều nguồn khác nhau, bao gồm các hệ thống bảo mật (như tường lửa, hệ thống phát hiện xâm nhập), hệ thống an toàn thông tin (như hệ thống quản lý danh tính và truy cập), hệ thống vận hành sản xuất, và các thiết bị khác (như máy chủ, máy trạm, thiết bị mạng). Hệ thống cần có khả năng trực quan hóa dữ liệu để người quản trị có thể dễ dàng theo dõi và hiểu được tình hình của hệ thống. Hệ thống cần có khả năng tùy chỉnh để phù hợp với các yêu cầu cụ thể của đơn vị, ví dụ như tùy chỉnh các quy tắc phát hiện bất thường, tùy chỉnh các cảnh báo, hoặc tùy chỉnh giao diện. Hệ thống giám sát cũng cần đáp ứng các yêu cầu về hiệu suất, độ tin cậy, và tính sẵn sàng. Hệ thống cần hoạt động ổn định và liên tục để đảm bảo giám sát toàn diện và kịp thời các hoạt động của đơn vị.

Sơ đồ kết nối hệ thống trung tâm điều hành giám sát IOC



Giải pháp triển khai

Hệ thống IOC được bố trí triển khai và lắp đặt tại tầng 4 Tổng công ty Hóa chất mỏ - Vinacomin (Ngõ 1, Phố Phan Đình Giót, Quận Thanh Xuân, TP Hà Nội).

Hệ thống IOC đóng vai trò trung tâm trong việc thu thập, phân tích và hiển thị dữ liệu từ nhiều nguồn khác nhau, hỗ trợ ra quyết định nhanh chóng, chính xác và hiệu quả hơn. Để đáp ứng yêu cầu này, việc triển khai hạ tầng thiết bị cho phòng IOC cần được thực hiện theo một giải pháp tổng thể, đảm bảo tính đồng bộ, hiện đại, bảo mật cao và có khả năng mở rộng trong tương lai.

Hệ thống phòng IOC được triển khai trong mạng LAN nội bộ, với toàn bộ các thiết bị trong hệ thống được kết nối và quản lý tập trung thông qua bộ điều khiển trung tâm. Hệ thống bao gồm các thành phần chính như thiết bị chuyển mạch mạng,

máy trạm, hệ thống hiển thị, hệ thống âm thanh và hệ thống giám sát hình ảnh.

Hệ thống màn hình giám sát chuyên dụng

Hệ thống màn hình ghép chuyên dụng

Màn hình ghép được thiết kế để hiển thị đồng bộ, liên tục các luồng thông tin giám sát, dữ liệu, bản đồ số, và hình ảnh camera từ nhiều nguồn khác nhau, qua đó cung cấp cái nhìn tổng thể phục vụ công tác điều hành. Để đáp ứng yêu cầu vận hành liên tục 24/7 tại Trung tâm IOC, hệ thống cần sử dụng các màn hình chuyên dụng ghép viền mỏng với kích thước từ 49 inch trở lên, đạt độ phân giải tối thiểu Full HD (1920x1080). Tấm nền IPS đảm bảo góc nhìn rộng và khả năng hiển thị ổn định, còn khe ghép ≤ 3.5mm giúp giảm thiểu tối đa khoảng cách giữa các tấm, đảm bảo tính liên tục của hình ảnh tổng thể. Độ sáng tối thiểu 500 nits là cần thiết để hình ảnh luôn rõ ràng trong mọi điều kiện ánh sáng, đặc biệt là trong môi trường ánh sáng mạnh hoặc chiếu sáng toàn phòng. Thiết bị phải có tuổi thọ tối thiểu 50.000 giờ.

Khung giá treo và chân đế

Khung giá treo và chân đế giúp cố định chắc chắn, đảm bảo sự ổn định và an toàn cho toàn bộ hệ thống màn hình ghép, đồng thời tối ưu hóa không gian lắp đặt và tạo sự linh hoạt trong bảo trì. Khung treo dạng pop-out được lựa chọn nhằm hỗ trợ việc lắp đặt và bảo trì thuận tiện, cho phép thao tác đẩy – kéo từng màn hình riêng lẻ khi cần thay thế hoặc kiểm tra kỹ thuật. Chân đế và khung cần đảm bảo khả năng cố định đồng bộ toàn bộ hệ thống màn hình ghép, đồng thời phải có tính thẩm mỹ cao và phù hợp với kiến trúc không gian trung tâm.

Bộ giải mã tín hiệu

Bộ giải mã tín hiệu đóng vai trò tiếp nhận và chuyển đổi các luồng tín hiệu video, âm thanh từ hệ thống điều khiển trung tâm và các nguồn khác sang định dạng phù hợp để hiển thị trên hệ thống màn hình ghép, đồng thời đảm bảo chất lượng hình ảnh và bảo mật dữ liệu. Thiết bị này yêu cầu hỗ trợ đầu ra HDMI độ phân giải ≥

4K60, cùng các giao tiếp cần thiết như cổng mạng RJ45 1GbE và RS232. Khả năng mã hóa chuẩn AES-256 là bắt buộc để đảm bảo an toàn dữ liệu truyền dẫn. Độ sâu màu ≥ 36-bit hỗ trợ hiển thị hình ảnh trung thực, không vỡ màu, đặc biệt quan trọng với các nội dung đồ họa hoặc bản đồ số. Bộ giải mã là thành phần trung gian thiết yếu giữa máy trạm điều khiển và hệ thống hiển thị.

Thiết bị chuyển mạch mạng (switch)

Thiết bị chuyển mạch mạng có nhiệm vụ quản lý và điều phối luồng dữ liệu giữa các thiết bị trong hệ thống mạng, đảm bảo kết nối thông suốt, ổn định, cung cấp nguồn điện cho thiết bị đầu cuối qua PoE, và phân tách lưu lượng để tối ưu băng thông cho từng loại dữ liệu (video, âm thanh, điều khiển). Yêu cầu tối thiểu 24 cổng RJ-45 hỗ trợ PoE/PoE+ để cấp nguồn trực tiếp cho các thiết bị như camera, bộ giải mã, màn hình điều khiển. 04 cổng uplink tốc độ 10G phục vụ kết nối với hệ thống máy chủ điều khiển hoặc mạng lõi. Tính năng L3 switching và hỗ trợ VLAN là cần thiết để phân tách lưu lượng theo từng dịch vụ và đảm bảo băng thông riêng biệt cho video, dữ liệu và điều khiển.

Thiết bị cấp nguồn chuyên dụng

Thiết bị cấp nguồn chuyên dụng có chức năng cung cấp nguồn điện ổn định, liên tục và đủ công suất cho tất cả các thiết bị quan trọng của hệ thống màn hình giám sát, đảm bảo chúng hoạt động hiệu quả và bền bỉ. Yêu cầu tối thiểu 8 kênh độc lập, công suất ≥ 2000W/kênh để đảm bảo khả năng chịu tải liên tục. Việc trang bị màn hình LCD là cần thiết để hiển thị thông số vận hành và hỗ trợ giám sát tình trạng nguồn từ xa.

Hệ thống điều khiển trung tâm

Thiết bị điều khiển trung tâm

Thiết bị điều khiển trung tâm tích hợp và quản lý toàn bộ các hệ thống phụ trợ và thông tin trong Trung tâm IOC, cho phép người vận hành điều khiển, giám sát và tự động hóa các tác vụ một cách hiệu quả, tập trung, từ đó nâng cao khả năng phản

ứng và điều phối. Thiết bị này cần hỗ trợ các giao thức công nghiệp để kết nối và điều khiển các hệ thống điện, điều hòa, ánh sáng, an ninh, video... từ một điểm tập trung. Việc hỗ trợ giao tiếp qua cổng Ethernet 1GbE và khả năng phân quyền dựa trên vai trò người dùng (RBAC) là yếu tố then chốt nhằm nâng cao tính bảo mật và dễ quản trị trong các môi trường nhạy cảm như Trung tâm điều hành.

Màn hình điều khiển cảm ứng

Màn hình điều khiển cảm ứng cung cấp giao diện trực quan, dễ sử dụng cho người vận hành để tương tác trực tiếp với hệ thống điều khiển trung tâm, thực hiện các lệnh điều khiển, giám sát trạng thái hệ thống và truy cập nhanh các chức năng thiết yếu. Cần trang bị màn hình cảm ứng điện dung với độ phân giải tối thiểu 1024x600, phù hợp với các thao tác giám sát và điều khiển trong môi trường vận hành thời gian thực. Thiết bị yêu cầu phải có chứng nhận đảm bảo an toàn thông tin, đủ điều kiện sử dụng trong các môi trường đặc biệt như chính phủ, cơ quan nhà nước hoặc quốc phòng.

Bộ mã hóa tín hiệu

Bộ mã hóa tín hiệu có chức năng chuyển đổi các tín hiệu video, âm thanh từ các nguồn đầu vào (như máy tính, camera) thành các luồng dữ liệu số được mã hóa và truyền qua mạng IP, đảm bảo an toàn và hiệu quả trong việc truyền tải thông tin đến bộ giải mã và hệ thống hiển thị. Cần có khả năng mã hóa các luồng tín hiệu hình ảnh đầu vào (HDMI) ở độ phân giải ≥ 4K60, bảo vệ an toàn dữ liệu bằng chuẩn mã hoá AES-256 và hỗ trợ truyền qua mạng IP (RJ45). Cổng RS232 phục vụ giám sát và điều khiển từ xa. Đây là thiết bị đầu vào quan trọng trước khi dữ liệu được truyền tới bộ giải mã ở hệ thống hiển thị.

Switch và thiết bị cấp nguồn

Tương tự hệ thống hiển thị, các thiết bị chuyển mạch ≥ 24 cổng PoE/PoE+ với uplink 10G và hỗ trợ L3 được sử dụng đồng bộ nhằm đảm bảo tương thích và dễ vận hành toàn hệ thống. Các thiết bị này đảm bảo kết nối mạng ổn định, cung cấp đủ

nguồn điện cho các thiết bị điều khiển, mã hóa, và các thiết bị ngoại vi khác, từ đó duy trì hoạt động không gián đoạn của toàn bộ hệ thống điều khiển trung tâm. Thiết bị cấp nguồn chuyên dụng ≥ 8 kênh, ≥ 2000W/kênh có chức năng cấp nguồn cho hệ thống và màn hình trạng thái trực quan.

Máy tính cấu hình cao

Máy tính văn phòng cấu hình cao phục vụ điều khiển, giám sát và xử lý dữ liệu từ các luồng video, âm thanh và cảnh báo, chạy các ứng dụng điều khiển, phần mềm quản lý thông minh, và hỗ trợ người vận hành thực hiện các tác vụ phức tạp một cách nhanh chóng, hiệu quả. Cấu hình bao gồm CPU Core i7 thế hệ 14 hoặc tương đương, RAM ≥ 16GB DDR5, ổ SSD ≥ 256GB + SSD ≥ 1TB, GPU rời ≥ 4GB nhằm đảm bảo khả năng xử lý đồ họa và đa nhiệm. Màn hình kích thước tối thiểu 27 inch, hỗ trợ Full HD, có chống chói và các cổng giao tiếp hỗ trợ (VGA/HDMI/DisplayPort) để tối ưu trải nghiệm vận hành.

Hệ thống phục vụ vận hành, giám sát

Thiết bị ma trận xử lý âm thanh kỹ thuật số

Thiết bị ma trận xử lý âm thanh kỹ thuật số có nhiệm vụ tiếp nhận, xử lý, và định tuyến linh hoạt các tín hiệu âm thanh từ nhiều nguồn khác nhau đến các thiết bị đầu ra (loa, ghi âm), đảm bảo chất lượng âm thanh tối ưu. Thiết bị cần đáp ứng dải tần 20Hz – 20kHz, hỗ trợ chống nhiễu và điều chỉnh âm lượng đầu vào từng kênh, giúp tinh chỉnh chất lượng âm thanh tùy theo từng nguồn. Khả năng điều khiển qua Serial, USB, Ethernet phục vụ cấu hình linh hoạt, phù hợp với quy mô mở rộng và tích hợp nhiều nguồn vào/ra.

Bộ chống phản hồi âm thanh

Bộ chống phản hồi âm thanh giúp loại bỏ hiện tượng hú, rít (feedback) thường gặp trong các hệ thống âm thanh có microphone và loa, từ đó cải thiện đáng kể chất lượng âm thanh trong các cuộc họp, đảm bảo lời nói luôn rõ ràng và dễ nghe. Thiết bị cần tích hợp chức năng phát hiện tự động các tín hiệu phản hồi (microphone–loa),

sử dụng màn hình LCD để hiển thị trạng thái.

Bộ điều khiển âm thanh trung tâm

Bộ điều khiển âm thanh trung tâm có nhiệm vụ quản lý và điều phối toàn bộ hệ thống micro và loa trong phòng họp, cho phép điều khiển qua RS232 và cung cấp đầu ra âm thanh dạng XLR/RCA. Thiết bị này hỗ trợ các chế độ hội nghị khác nhau như: Chủ tịch kiểm soát, chế độ tự động, chế độ tự do – giúp đáp ứng nhiều tình huống tổ chức hội họp linh hoạt, đồng thời tăng khả năng tổ chức và kiểm soát phát biểu theo vai trò.

Micro chủ tọa và micro đại biểu

Micro chủ tọa có chức năng phát biểu ưu tiên, tự động ngắt các micro còn lại khi cần phát biểu điều hành, đảm bảo quyền kiểm soát tối cao của người chủ trì. Thiết bị này hỗ trợ lắp đặt tại bất kỳ vị trí nào trong vòng mạch âm thanh.

Micro đại biểu là loại micro tụ điện cổ dài, có chỉ báo trạng thái LED tại phần đế, phục vụ cho phát biểu cá nhân, giúp các thành viên tham gia thảo luận một cách dễ dàng và hiệu quả, dễ quan sát và sử dụng.

Camera PTZ và bộ giải mã đi kèm

Camera PTZ có chức năng thu lại hình ảnh chất lượng cao của các hoạt động trong phòng họp hoặc khu vực giám sát, với khả năng điều khiển xoay, nghiêng, phóng to/thu nhỏ linh hoạt để tập trung vào các điểm quan trọng hoặc cung cấp cái nhìn tổng thể. Thiết bị này hỗ trợ hiệu quả cho việc ghi hình cuộc họp, giám sát từ xa hoặc truyền hình hội nghị. Camera yêu cầu độ phân giải 1080p60 với khả năng xoay ngang, dọc, zoom 12x và hỗ trợ lưu sẵn ≥ 256 vị trí quan sát. Kèm theo là bộ giải mã tín hiệu để đảm bảo truyền tải hình ảnh đến hệ thống hiển thị mà không suy giảm chất lượng. Ngoài ra, camera cần hỗ trợ chế độ toàn cảnh với độ phân giải tối thiểu 720p để bao quát không gian chung của phòng IOC.*Âm ly và loa âm trần*

Âm ly có chức năng khuếch đại tín hiệu âm thanh từ bộ xử lý để đưa ra loa, đảm bảo âm lượng đủ lớn và rõ ràng; trong khi loa âm trần có chức năng tái tạo âm

thanh, phân tán đều khắp không gian, mang lại trải nghiệm nghe tối ưu cho tất cả người tham dự, không gây chói tai hay khó chịu. Âm ly cần hỗ trợ định tuyến tín hiệu đầu vào đến từng kênh đầu ra theo chế độ ma trận. Loa âm trần với công nghệ phân vùng âm thanh và độ nhạy ≥ 89dB giúp âm thanh phủ đều trong không gian, không bị méo tiếng hay dội âm.

Thiết bị cấp nguồn

Tương tự các hệ thống trên, thiết bị cấp nguồn có nhiệm vụ cung cấp dòng điện ổn định và liên tục cho toàn bộ hệ thống âm thanh, đảm bảo các thiết bị hoạt động với hiệu suất cao nhất và duy trì sự ổn định. Thiết bị cấp nguồn yêu cầu ≥ 8 kênh, công suất ≥ 2000W/kênh, và màn hình LCD hiển thị trạng thái hoạt động.

Máy tính cấu hình cao

Máy tính văn phòng cấu hình cao phục vụ điều khiển, giám sát và xử lý dữ liệu từ các luồng video, âm thanh và cảnh báo, chạy các ứng dụng điều khiển, phần mềm quản lý thông minh, và hỗ trợ người vận hành thực hiện các tác vụ phức tạp. Cấu hình bao gồm CPU Core i7 thế hệ 14 hoặc tương đương, RAM ≥ 16GB DDR5, ổ SSD ≥ 256GB + SSD ≥ 1TB, GPU rời ≥ 4GB đảm bảo khả năng xử lý đồ họa và đa nhiệm. Màn hình kích thước tối thiểu 27 inch, hỗ trợ Full HD, có chống chói và các cổng giao tiếp hỗ trợ (VGA/HDMI/DisplayPort) để tối ưu trải nghiệm vận hành.

Yêu cầu kỹ thuật:

STT	Tên hàng hoá	Yêu cầu kỹ thuật tối thiểu hoặc tương đương	Đơn vị tính	Số lượng
III	Hệ thống trung tâm giám sát IOC			
3.1	Hệ thống màn hình giám sát chuyên dụng			
3.1.1	Màn hình ghép chuyên dụng	- Kích thước màn hình: ≥ 49 inch - Độ phân giải: ≥ 1,920 x 1,080	Chiếc	15

STT	Tên hàng hoá	Yêu cầu kỹ thuật tối thiểu hoặc tương đương	Đơn vị tính	Số lượng
		(FHD) - Công nghệ tấm nền: IPS - Cổng kết nối: HDMI, DP, RS-232C, RJ45, IR, USB - Khe ghép: ≤ 3.5mm - Độ sáng: ≥ 500 nits - Độ tương phản: ≥ 1,000:1 - Tuổi thọ tối thiểu: ≥ 50,000 giờ - Hoạt động: 24/7 - Bảo hành ≥ 02 năm		
3.1.2	Hệ thống khung giá treo kèm chân đứng cho toàn bộ màn hình ghép	- Loại khung giá treo pop-out - Đảm bảo thiết kế thẩm mỹ, phù hợp không gian lắp đặt	Hệ thống	1
3.1.3	Bộ giải mã tín hiệu	- Độ phân giải: ≥ 4K60 @ 4:4:4 - Cổng: ≥ 1x RJ45 (1GbE), 1x HDMI out, RS232 - Điều khiển endpoints với IR, RS232 - Băng thông: ≥ 850 Mbps - Mã hóa AES256 - Bảo hành ≥ 01 năm	Bộ	15
3.1.4	Cáp HDMI chuyên dụng	- Dài ≥ 0,9 m (3ft) - Cáp HDMI 2.0, tuân thủ HDCP 2.2 - Băng thông 18Gbps - Độ phân giải: 4K@60Hz-4:4:4 - Bảo hành ≥ 01 năm	Sợi	15
3.1.5	Thiết bị chuyển mạch	- ≥ 24 cổng 10/100/1000BASE-T (RJ-45) PoE/PoE+ - ≥ 4 cổng 10GBASE-R (SFP+)/1000BASE-X (SFP) - Hỗ trợ chức năng L3 - Băng thông: ≥ 128 Gbps - Thông lượng (64 bytes): ≥ 93,1 MPPS	Bộ	1

STT	Tên hàng hoá	Yêu cầu kỹ thuật tối thiểu hoặc tương đương	Đơn vị tính	Số lượng
		- Bảng địa chỉ MAC: ≥ 16K - VLAN: ≥ 4K - Bảo hành ≥ 01 năm		
3.1.6	Thiết bị cấp nguồn	- Nguồn đầu vào AC: 90-260V 50-60 Hz - Số kênh: ≥ 08 - Khả năng cấp nguồn: ≥ 2000W/kênh - Hỗ trợ màn hình hiển thị LCD - Bảo hành ≥ 01 năm	Bộ	2
3.2	Hệ thống điều khiển trung tâm			
3.2.1	Thiết bị điều khiển trung tâm	- Bộ nhớ: SDRAM ≥ 1 GB, Flash ≥ 8 GB - Hỗ trợ các giao thức cho phép giám sát và kiểm soát tập trung các hệ thống cơ và điện bao gồm HVAC, chiếu sáng, điện, phòng cháy chữa cháy và an ninh - Cổng Ethernet tốc độ ≥ 1Gbps, half/full duplex với autodetect - Giao thức Ethernet: ARP, DHCP, DNS, HTTP, HTTPS, ICMP - Hỗ trợ các giao thức truyền thông tiêu chuẩn công nghiệp an toàn - Hỗ trợ cổng Serial, cổng Digital I/O, IR, Relay, eBUS, Volume control - Cho phép thiết lập bảo mật dựa trên vai trò của người dùng - Bảo hành ≥ 01 năm	Bộ	1
3.2.2	Màn hình điều khiển cảm ứng	- Kích thước ≥ 7 inch - Loại cảm biến: Điện dung - Độ phân giải: ≥ 1024x600 - Độ sáng: ≥ 350 nits - Chứng nhận đảm bảo thông tin	Chiếc	1

STT	Tên hàng hoá	Yêu cầu kỹ thuật tối thiểu hoặc tương đương	Đơn vị tính	Số lượng
		để sử dụng trong các ứng dụng của chính phủ và các môi trường quan trọng khác - Bộ nhớ: ≥ 2GB SDRAM, ≥ 8GB Flash - Bảo hành ≥ 01 năm		
3.2.3	Bộ mã hóa tín hiệu	- Độ phân giải: ≥ 4K60 @ 4:4:4 - Cổng: ≥ 1x RJ45 (1GbE), 1x HDMI in, RS232 - Băng thông ≥ 850 Mbps - Mã hóa AES256 - Bảo hành ≥ 01 năm	Bộ	8
3.2.4	Cáp HDMI chuyên dụng	- Dài ≥ 0,9 m (3ft) - Cáp HDMI 2.0, tuân thủ HDCP 2.2 - Băng thông 18Gbps - Độ phân giải: 4K@60Hz-4:4:4 - Bảo hành ≥ 01 năm	Sợi	8
3.2.5	Dây nhảy mạng chuyên dụng	- Chiều dài: ≥ 7ft - Loại: Cat6A UTP, ≥ 500 MHz	Sợi	13
3.2.6	Thiết bị chuyển mạch	- ≥ 24 cổng 10/100/1000BASE-T (RJ-45) PoE/PoE+ - ≥ 4 cổng 10GBASE-R (SFP+)/1000BASE-X (SFP) - Hỗ trợ chức năng L3 - Băng thông: ≥ 128 Gbps - Thông lượng (64 bytes): ≥ 93,1 MPPS - Bảng địa chỉ MAC: ≥ 16K - VLAN: ≥ 4K - Bảo hành ≥ 01 năm	Bộ	1
3.2.7	Thiết bị cấp nguồn	- Nguồn đầu vào AC: 90-260V 50-60 Hz - Số kênh: ≥ 08 - Khả năng cấp nguồn: ≥ 2000W/kênh - Hỗ trợ màn hình hiển thị LCD	Bộ	1

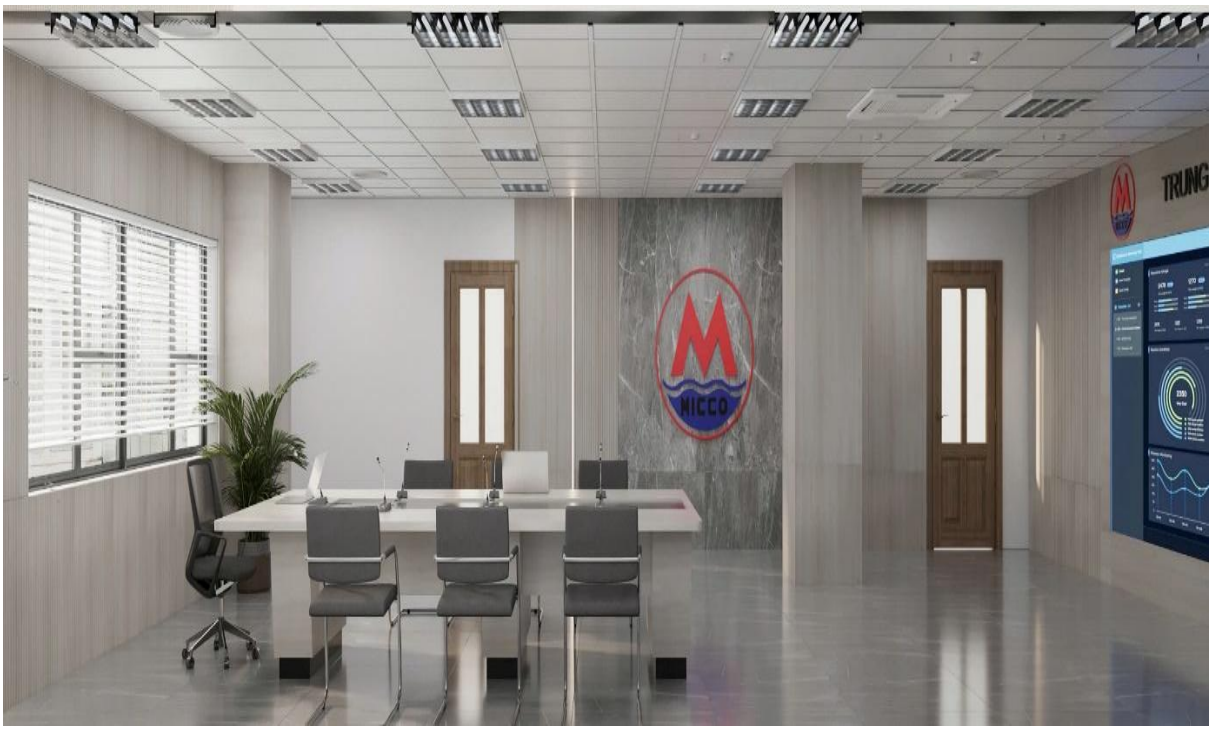
STT	Tên hàng hoá	Yêu cầu kỹ thuật tối thiểu hoặc tương đương	Đơn vị tính	Số lượng
		- Bảo hành ≥ 01 năm		
3.2.8	Tủ rack	- Tủ ≥ 27U, D: 800 mm - Có khóa, kèm khay, quạt tản nhiệt, ổ nguồn - Bảo hành ≥ 01 năm	Chiếc	1
3.2.9	Máy tính văn phòng cấu hình cao	- Loại máy trạm (Workstation) - Bộ vi xử lý: Core i7 thế hệ 14 hoặc tương đương - RAM ≥ 16GB DDR5 - Ổ cứng ≥ 256GB SSD + ≥ 1TB SSD - Card đồ hoạ rời, dung lượng bộ nhớ ≥ 4GB - Windows 11 Pro - Bàn phím, chuột kèm theo - Bảo hành ≥ 03 năm	Bộ	1
3.2.10	Màn hình máy tính	- Kích thước ≥ 27 inch - Độ phân giải: Full HD 1920 x 1080 - Tỉ lệ màn hình: 16:9 - Độ sáng: ≥ 300 cd/m² - Công nghệ chống chói (Anti-glare) - Giao diện hỗ trợ VGA/ DisplayPort/ HDMI - Bảo hành ≥ 03 năm	Chiếc	2
3.3	Hệ thống phục vụ vận hành, giám sát			
3.3.1	Thiết bị ma trận xử lý âm thanh kỹ thuật số	- Khuếch đại âm thanh cân bằng đầu ra: 0 dB, không cân bằng đầu ra: -6 dB - Tần số đáp ứng: 20 Hz đến 20 kHz, ± 0.2 dB - Độ hội tụ triệt vọng: 60 dB/giây - Khử nhiễu lên tới: 20 dB - Hỗ trợ điều chỉnh âm lượng: -	Bộ	1

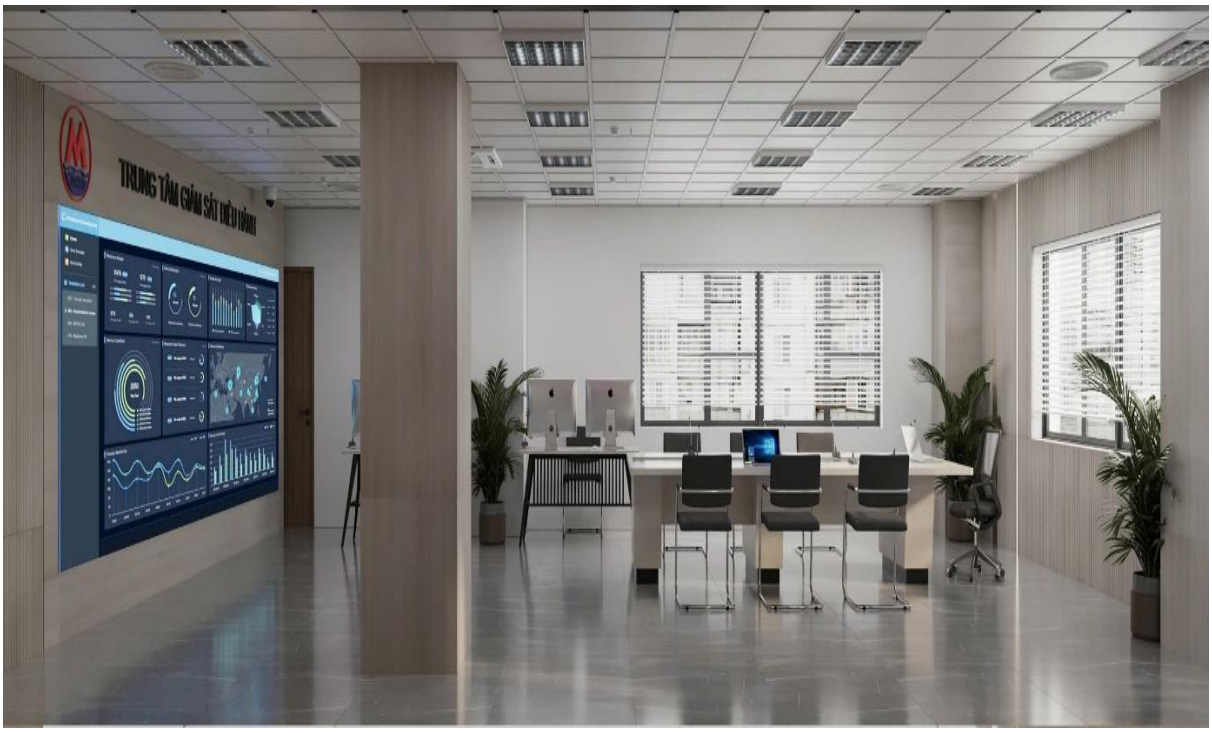
STT	Tên hàng hoá	Yêu cầu kỹ thuật tối thiểu hoặc tương đương	Đơn vị tính	Số lượng
		100 dB đến 0 dB - Số cổng đầu vào: ≥ 6 - Số cổng đầu ra: ≥ 4 - Điều chỉnh khuếch đại âm thanh đầu vào: 0 dB tới +60 dB - Hỗ trợ điều khiển qua RS-232 - Bảo hành ≥ 01 năm		
3.3.2	Bộ chống phản hồi âm thanh	- Tỷ lệ lấy mẫu: ≥ 96kHz - Độ phân giải: ≥ 24 bit - Kênh vào/ra: 02 kênh, cân bằng - Trở kháng đầu vào/ra (cân bằng): ≥ 47K Ω / 600 Ω - Màn hình hiển thị LCD - Phát hiện phản hồi âm tự động - Bảo hành ≥ 01 năm	Bộ	1
3.3.3	Bộ điều khiển âm thanh trung tâm	- Tần số đáp ứng: 50Hz-16kHz - Độ méo: <0.5% - Tỷ lệ tín hiệu trên nhiễu:>65dB - Cổng kết nối micro: RJ45 và 8 Pin Din - Cổng đầu ra âm thanh: XLR,RCA		1
3.3.4	Micro chủ tọa	- Tần số đáp ứng: 100 Hz – 16kHz - Nút ấn để nói - Chức năng phát biểu ưu tiên sẽ ngắt phát biểu các micro trong hệ thống - Chiều dài cần: ≥ 420mm - Cổng kết nối: RJ45 và 8 Pin		1
3.3.5	Micro đại biểu	- Tần số đáp ứng: 100 Hz – 16kHz - Nút ấn để nói - Chiều dài cần: ≥ 420mm - Cổng kết nối: RJ45 và 8 Pin		8
3.3.6	Camera PTZ	- Cảm biến: 1 / 2.8” 2.16MP		1

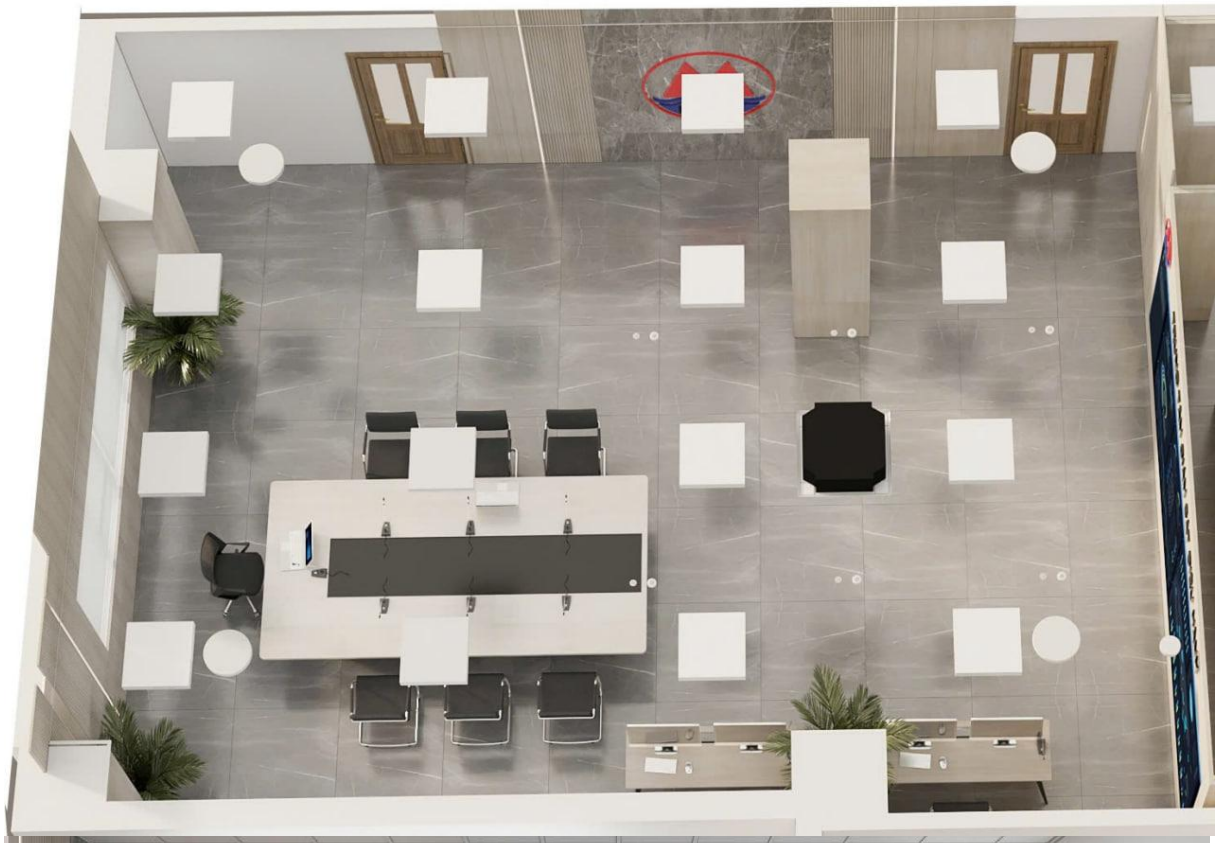
STT	Tên hàng hoá	Yêu cầu kỹ thuật tối thiểu hoặc tương đương	Đơn vị tính	Số lượng
		CMOS - Độ phân giải: camera PTZ 1080P 60fps; camera toàn cảnh: 720p30 - Zoom quang: 12x - Góc quay: +170 ~ -170° - Góc ngẩng: +90 ~ -30° - Số vị trí lưu sẵn: 256 - Bảo hành ≥ 01 năm		
3.3.7	Bộ giải mã dành cho camera PTZ	- Hỗ trợ triển khai hệ thống màn hình ghép - Cổng đầu ra: HDMI - Cổng USB: Type-C - Giao thức IP: UDP/ RTSP - Độ phân giải: 2160p60 - Giải mã video: H.264 / HEVC(H.265) - Bảo hành ≥ 01 năm		1
3.3.8	Bộ âm ly	Âm ly công suất: - Đầu vào: 02 - Số kênh đầu ra: 2 - Công suất đầu ra: 500W/kênh - Tương thích với hệ thống loa 4/8 ohm và 100V - Chế độ ma trận cho phép mọi nguồn có thể định tuyến đến bất kỳ kênh đầu ra nào - Bảo hành ≥ 01 năm		1
3.3.9	Loa âm trần	- Loại loa: ≥ 2 dải - Công nghệ xử lý âm thanh theo vùng - Lựa chọn công suất (70/100V) - Tần số đáp ứng: 48 Hz – 24 kHz - Độ nhạy: ≥ 88 dB - Công suất xử lý: ≥120W - Bảo hành ≥ 01 năm	Cái	4
3.3.10	Dây nhảy mạng	- Chiều dài: ≥ 7ft	Sợi	5

STT	Tên hàng hoá	Yêu cầu kỹ thuật tối thiểu hoặc tương đương	Đơn vị tính	Số lượng
	chuyên dụng	- Loại: Cat6A UTP, ≥ 500 MHz		
3.3.11	Thiết bị cấp nguồn	- Nguồn đầu vào AC: 90-260V 50-60 Hz - Số kênh: ≥ 08 - Khả năng cấp nguồn: ≥ 2000W/kênh - Hỗ trợ màn hình hiển thị LCD - Bảo hành ≥ 01 năm	Bộ	1
3.3.12	Máy tính văn phòng cấu hình cao	- Loại máy trạm (Workstation) - Bộ vi xử lý: Core i7 thế hệ 14 hoặc tương đương - RAM ≥ 16GB DDR5 - Ổ cứng ≥ 256GB SSD + ≥ 1TB SSD - Card đồ hoạ rời, dung lượng bộ nhớ ≥ 4GB - Windows 11 Pro - Bàn phím, chuột kèm theo - Bảo hành ≥ 03 năm	Bộ	1
3.3.13	Màn hình máy tính	- Kích thước ≥ 27 inch - Độ phân giải: Full HD 1920 x 1080 - Tỉ lệ màn hình: 16:9 - Độ sáng: ≥ 300 cd/m² - Công nghệ chống chói (Anti-glare) - Giao diện hỗ trợ VGA/ DisplayPort/ HDMI - Bảo hành ≥ 03 năm	Chiếc	2

Mô hình thiết kế 3D trung tâm giám sát IOC







3.4. Nâng cấp phần mềm văn phòng điện tử Portal Office

Nâng cấp giao diện phần mềm Văn phòng điện tử - **PORTAL OFFICE 10** với đầy đủ các tính năng:

<table>
<tr><th colspan="3">DANH SÁCH CHỨC NĂNG</th></tr>
<tr><td>Lịch công ty -
Lịch xe</td><td>Quản lý Công văn</td><td>App Mobile
Android/IOS</td></tr>
<tr><td>Tin nhắn nội bộ</td><td>Công việc/Dự án</td><td>Quản lý tài liệu</td></tr>
<tr><td>Nhân sự Express</td><td>Quản trị hệ thống/Danh bạ</td><td>Quản lý tin tức</td></tr>
<tr><td colspan="2">Giao diện Desktop trên nền bootstrap mới Admin LTE:
- Trang đăng nhập phần mềm:
o Mới nền trong suốt có đính kèm hình ảnh.
o Có chức năng xem mật khẩu đã lưu.
- Trang chủ sau khi đăng nhập giao diện mới:
- Module Quy Trình:
o Yêu cầu tôi xử lý: theo skin mới
o Yêu cầu tôi gửi: theo skin mới
o Tra cứu yêu cầu: theo skin mới
- Module Lịch cơ quan:
o Đăng ký lịch: theo skin mới
o Hiển thị lịch: theo skin mới
o Duyệt tài nguyên: theo skin mới
o Tra cứu lịch: theo skin mới
- Module Công Văn:
o Công văn đến: theo skin mới
o Công văn đi: theo skin mới
o Công văn nội bộ: theo skin mới
o Công văn nội bộ phòng: theo skin mới
- Module Công Việc:
o Giao việc: theo skin mới</td><td></td></tr>
</table>

o Hiển thị công việc: theo skin mới o Tra cứu công việc: theo skin mới o Tương tác công việc: theo skin mới - **Module Tin tức:** theo skin mới - **Module Tài liệu:** theo skin mới - **Module Lịch cá nhân:** theo skin mới - **Module Tin nhắn:** theo skin mới - **Tab Ký Số, Tab Danh bạ, Tab Tài khoản:** theo skin mới (Không bao gồm phần quản trị Module & quản trị hệ thống)	
Xác thực LDAP: - User đăng nhập kết nối LDAP kiểm tra password nhập trùng với LDAP thì cấp token đăng nhập	

<u>Yêu cầu kỹ thuật chi tiết:</u>

*** Nâng cấp LDAP:**

- Chỉnh sửa phần mềm:

+ Giao diện người dùng có thông tin tài khoản LDAP để khi kết nối sẽ dùng thông tin này để xác thực với Windows.

+ Cấu hình cách xác thực: Cho phép người dùng dùng hình thức xác thực chỉ LDAP hay chỉ Local bằng văn phòng điện tử hoặc cả 2 hình thức hoặc bắt buộc chỉ LDAP.

+ Giải pháp chuyển đổi nhanh nếu kết nối LDAP của Window có sự cố.

+ Thông báo lỗi về Log Admin để xem tình trạng lỗi, để xác định nguyên nhân và có hướng khắc phục.

+ Lập trình kết nối và các thủ tục liên quan dựa vào hiện trạng kết nối của Công ty.

- Cấu hình kết nối Server và LDAP: tạo Connection thông số LDAP tùy trường hợp một Site hay nhiều Site theo Công ty.

*** Giao diện phần mềm:**

- Trang đăng nhập phần mềm:

+ Mới nền trong suốt có đính kèm hình ảnh

+ Có chức năng xem mật khẩu đã lưu.

- Module Công văn:

+ Công văn đến: theo skin mới
+ Hiển thị danh sách văn bản
+ Hiển thị chi tiết văn bản
+ Các thao tác Ghi bút phê, phân phát, … Pop-up
+ Công văn đi: theo skin mới
+ Công văn nội bộ: theo skin mới
+ Công văn nội bộ phòng: theo skin mới

- Module Công việc:

+ Giao việc: theo skin mới
+ Hiển thị công việc: theo skin mới
+ Tra cứu công việc: theo skin mới
+ Tương tác công việc: theo skin mới, các thao tác dạng Pop-up.

- Module Quy trình:

+ Yêu cầu tôi xử lý: theo skin mới
+ Tra cứu và lọc yêu cầu
+ Hiển thị phiếu theo skin mới
+ Yêu cầu tôi gửi: theo skin mới
+ Tra cứu yêu cầu: theo skin mới

- Module Lịch cơ quan:

+ Hiển thị lịch: theo skin mới
+ Đăng ký lịch: theo skin mới
+ Duyệt tài nguyên: theo skin mới
+ Tra cứu lịch: theo skin mới

- Module Tin tức:

+ Xem tin mới
+ Tra cứu tin tức

- Module Tài liệu:

+ Xem tài liệu: theo skin mới
+ Thêm tài liệu: theo skin mới
+ Tra cứu tài liệu: theo skin mới

- Module Lịch cá nhân:

+ Thêm sự kiện: theo skin mới

+ Hiển thị sự kiện: theo skin mới

- Module Tin nhắn:

+ Xem tin nhắn: theo skin mới

+ Trả lời tin nhắn: theo skin mới

- Tab Ký Số, Tab Danh bạ, Tab Tài khoản: theo skin mới

3.5. Trang thiết bị nội thất

STT	Danh mục	Đơn vị tính	Số lượng
I	**Trang thiết bị nội thất**	**Gói**	**1**
1	**Vách màn led**	Gói	1
	- Vách phẳng: Vách phẳng bề mặt gỗ MDF lõi xanh chống ẩm; gia cố lắp màn led - Kích thước : Rộng 6.5m x cao 2.75m		
	- Vật lam: Vách lam bề mặt gỗ MDF lõi xanh chống ẩm; gia cố lắp màn led - Kích thước: Rộng 1.2m x cao 2.75m		
2	**Bàn họp**	Bộ	1
	- Bàn họp chữ U - Vật liệu: gỗ MDF lõi xanh chống ẩm; - Kích thước: Dài 7.8m x rộng 0.6m x cao 0.75m		
3	**Bàn làm việc**	Bộ	2
	- Vật liệu: gỗ MDF lõi xanh chống ẩm An Cường kết hợp sắt; - Kích thước: Dài 1.6m x rộng 0.6m x cao0.75m		
4	**Ghế ngồi họp**	Bộ	10
	- Chất liệu nhựa và kim loại phổ thông tiêu chuẩn. Kiểu dáng đảm bảo thẩm mỹ phòng họp		
5	**Ghế chủ tọa**	Bộ	1
	- Chất liệu nhựa và kim loại phổ thông tiêu		

	chuẩn. Kiểu dáng đảm bảo thẩm mỹ phòng họp		

4. Yêu cầu chi tiết về việc đào tạo hướng dẫn sử dụng; triển khai, hỗ trợ, quản trị, vận hành sản phẩm hoặc hạng mục công việc của dự án trước khi nghiệm thu bàn giao (nếu có); yêu cầu về bảo hành và bảo trì

4.1. Mục đích đào tạo

Mục đích của việc đào tạo là nhằm chuyển giao được hệ thống, đảm bảo cán bộ quản trị và cán bộ nghiệp vụ sử dụng hệ thống và vận hành khai thác được hệ thống.

4.2. Các yêu cầu cụ thể

Mục tiêu khóa học: Các cán bộ CNTT của MICCO có thể nắm các khái niệm, kiến thức về công nghệ và sản phẩm được bàn giao cũng như có khả năng vận hành, thao tác, sử dụng sản phẩm hệ thống.

Việc triển khai đào tạo phải cần tuân thủ quá trình sau:

- Chuẩn bị Đào tạo:
  + Chuẩn bị bài giảng.
  + Lập kế hoạch đào tạo chi tiết;
  + Chuẩn bị nội dung và tài liệu đào tạo;
  + Thống nhất về kế hoạch và nội dung đào tạo;
- Thực hiện Đào tạo:
  + Phát tài liệu đào tạo cho học viên.
  + Hướng dẫn và khai thác tài liệu hướng dẫn khai thác sử dụng phần mềm chuyển giao.
  + Hướng dẫn các nghiệp vụ thực tế do phần mềm đảm nhiệm.
  + Hướng dẫn thực hành khai thác sử dụng các chức năng phần mềm chuyển giao.
  + Hướng dẫn cách thức kiểm tra, đối chiếu số liệu.
  + Mô tả một số tình huống thường gặp trong quá trình khai thác sử dụng phần mềm chuyển giao.
  + Giải đáp thắc mắc trong quá trình hướng dẫn khai thác sử dụng phần mềm chuyển giao.
  + Hỗ trợ giải đáp cho học viên.

5. Yêu cầu triển khai chi tiết

STT	Yêu cầu triển khai
1	Khảo sát chi tiết hệ thống mạng trong TTDL tại Micco và DR (Sơ đồ kết nối vật lý, địa chỉ IP, máy chủ, hệ thống lưu trữ dữ liệu, hệ thống ứng dụng, hệ thống máy chủ, hệ thống mạng LAN, hệ thống kết nối Micco và các đơn vị thành viên, hệ thống SSL VPN…) để làm cơ sở xây dựng phương án và kịch bản triển khai. Phân tích các yêu cầu về triển khai - Triển khai hệ thống APT, tích hợp cùng các hệ thống ATBM hiện tại của MICCO như Firewall, IPS, PAM, MFA, Endpoint Security…, thiết lập các chính sách phát hiện, phân tích, kiểm soát và phản ứng trước các mối đe dọa, các chính sách bảo vệ đảm bảo không ảnh hưởng đến hoạt động hiện tại của hệ thống CNTT và tuân thủ các quy định chính sách bảo mật của MICCO. - Triển khai hệ thống tường lửa kiểm soát truy cập ứng dụng Web tích hợp với các hệ thống ứng dụng hiện có của MICCO, thiết lập các chính sách an toàn thông tin. - Triển khai trung tâm giám sát thông tin tập trung IOC theo yêu cầu của MICCO. - Triển khai nâng cấp hệ thống phần mềm Portal Office đảm bảo nhanh chóng và hiệu quả, không ảnh hưởng đến dữ liệu của phần mềm. - Triển khai trang thiết bị nội thất đảm bảo kỹ thuật và mỹ quan.
2	Xây dựng kịch bản triển khai chi tiết, tránh ảnh hưởng tới hoạt động của hệ thống hiện tại, có phương án dự phòng hệ thống
3	Xây dựng bản vẽ và tài liệu hoàn công, kịch bản kiểm thử, tài liệu vận hành, quản trị hệ thống, tài liệu hướng dẫn
4	Đào tạo vận hành cho kỹ sư hệ thống của Micco.

6. Lưu ý:

- Đối với các công nghệ được nhà thầu cho là ưu việt hơn thì cần phải chứng minh bằng các tài liệu của cơ quan kiểm định độc lập hoặc các dẫn chứng khoa học cụ thể từ các cơ quan kiểm định có uy tín.

- Tổ chuyên gia sẽ căn cứ theo ký mã hiệu hoặc tên thương mại để tìm kiếm thông tin hàng hoá chào thầu từ trang thông tin chính thức của nhà sản xuất. Đối với các thông tin sai lệch giữa tuyên bố của nhà thầu với thông tin từ nhà sản xuất sẽ

được làm rõ. Nhà thầu phải làm rõ các thông tin khi có yêu cầu. Trong trường hợp nhà thầu không trả lời yêu cầu làm rõ, thông tin từ trang tin nhà sản xuất sẽ là cơ sở để đánh giá E-HSDT.

- Nhà thầu phải chịu trách nhiệm trước pháp luật về tính chính xác của các văn bản có yếu tố nước ngoài, văn bản và catalô của Nhà sản xuất. Mọi gian lận về văn bản, hồ sơ, các thông số kỹ thuật của hàng hóa của Nhà thầu là căn cứ để Bên mời thầu đề nghị cấm tham gia hoạt động đấu thầu đối với các gói thầu do Tổng Công ty hóa chất mỏ - Vinacomin làm chủ đầu tư, tạo cảnh báo trên Hệ thống Mạng đấu thầu quốc gia hoặc yêu cầu cơ quan chức năng chuyển diện quản lý cơ bản đối với pháp nhân.

Mục 2. Bản vẽ

Không có bản vẽ

Mục 3. Kiểm tra và thử nghiệm

Việc kiểm tra, nghiệm thu tuân thủ thông tư 16/2024/TT-BTTTT ngày 30/12/2024 của Bộ Thông tin và Truyền thông Quy định chi tiết nội dung công tác triển khai, giám sát công tác triển khai, nghiệm thu đối với dự án đầu tư ứng dụng công nghệ thông tin; xác định yêu cầu về chất lượng dịch vụ và các nội dung đặc thù của hợp đồng thuê dịch vụ đối với thuê dịch vụ công nghệ thông tin theo yêu cầu riêng.