HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

LÊ THỊ LÝ

XÂY DỰNG HỆ THỐNG GIÁM SÁT VÀ PHÁT HIỆN TẤN CÔNG TẠI CÔNG TY SAMSUNG DISPLAY VIỆT NAM

CHUYÊN NGÀNH: **HỆ THỐNG THÔNG TIN**

MÃ SỐ: **8.48.01.04**

TÓM TẮT ĐỀ ÁN TỐT NGHIỆP THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

HÀ NỘI – 2026

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: **TS. ĐINH TRƯỜNG DUY**

Phản biện 1:

Phản biện 2:

Luận văn này được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc:

Có thể tìm hiểu luận văn này tại:

Thư viện của Học viện Công nghệ Bưu chính Viễn thông

MỞ ĐẦU

Trước bối cảnh chuyển đổi số và sự phát triển mạnh mẽ của các hệ thống mạng, điện toán đám mây và Internet of Things (IoT), vấn đề an toàn và an ninh thông tin ngày càng trở nên cấp thiết. Các hệ thống thông tin hiện đại đang phải đối mặt với nhiều hình thức tấn công mạng ngày càng tinh vi có nguy cơ ảnh hưởng rất lớn đến các tổ chức doanh nghiệp. Công ty SAMSUNG DISPLAY VIETNAM thuộc tập đoàn SAMSUNG với ba mười nghìn nhân viên, đi đầu trong công nghệ lĩnh vực sản xuất mặt hàng điện thoại, màn hình TV mà còn là đối tác chiến lược quan trọng của nhiều tập đoàn lớn đang sở hữu một cơ sở hạ tầng CNTT rất lớn và có thể phát sinh nhiều lỗ hổng. Kho dữ liệu khổng lồ từ hệ thống thông tin này rất dễ trở thành mục tiêu hấp dẫn cho gián điệp kinh tế và tội phạm mạng.

Xuất phát từ những mối lo ngại đó, đề án "**XÂY DỰNG HỆ THỐNG GIÁM SÁT VÀ PHÁT HIỆN TẤN CÔNG TẠI CÔNG TY SAMSUNG DISPLAY VIỆT NAM"** được thực hiện nhằm nghiên cứu, xây dựng một hệ thống an toàn bảo mật không chỉ đáp ứng được việc kiểm soát an ninh mạng mà còn có khả năng mở rộng linh hoạt đồng thời tiết kiệm tối đa chi phí vận hành. Đề án sử dụng ứng dụng WAZUH kết hợp với các giải pháp bảo mật khác hiện có để xây dựng một hệ thống bảo mật hỗ trợ doanh nghiệp quản lý, kiểm tra, ngăn chặn những lỗ hổng có nguy cơ ảnh hưởng đến hệ thống mạng. Đề án được bố cục thành 03 chương, bao gồm:

Chương 1: Tổng quan về giám sát an toàn mạng.

Chương này trình bày về cơ sở hình thành đề án, giới thiệu tổng quan về giám sát an toàn mạng, mục tiêu và vai trò của giám sát an toàn mạng, các phương pháp phát hiện xâm nhập và vai trò của hai hệ thống cốt lõi trong giám sát an toàn mạng là IPS và IDS, đồng thời cũng trình bày nội dung về một số ứng dụng, công cụ phổ biến phục vụ cho cho giám sát và xâm nhập hiện nay.

Chương 2: GIỚI THIỆU VỀ HỆ THỐNG WAZUH

Chương này giới thiệu về cấu trúc và phương thức hoạt động và các chức năng của ứng dụng WAZUH, một giải pháp SIEM đang được sử dụng rất phổ biến hiện nay. Trên cơ sở đó đề án khai thác và tận dụng hết mức có thể những tính năng của WAZUH xây dựng một hệ thống an toàn bảo mật tối ưu phục vụ cho một công ty có hệ thống lớn và cơ sở hạ tầng phức tạp như SAMSUNG.

Chương 3: XÂY DỰNG HỆ THỐNG GIÁM SÁT

Chương này trình bày quá trình triển khai thực nghiệm trên mô hình thực tế, cấu hình môi trường thử nghiệm, thực hiện các phương thức kiểm tra để đánh giá tính hiệu quả của hệ thống. Từ những kết quả thu được, đề án phân tích được ưu nhược điểm của hệ thống để cải tiến và nâng cấp và xây dựng một hệ thống an toàn bảo mật tối ưu, nhằm củng cố tính an toàn, sẵn sàng và toàn vẹn của hệ thống bảo mật.

CHƯƠNG 1: TỔNG QUAN VỀ GIÁM SÁT AN TOÀN MẠNG

1.1 Tổng quan về giám sát an toàn mạng

Trong ATTT (An toàn thông tin), xây dựng tiến trình để giám sát, thực thi và quản lý hệ thống là một quy trình quan trọng. Giám sát và phát hiện an toàn thông tin là hai chức năng đóng vai trò quan trọng và IDS và IPS là các hệ thống bảo mật cốt lõi được sử dụng được dùng để giám sát, phát hiện và ngăn chặn các hành vi xâm nhập trái phép vào hệ thống thông tin.

Giám sát an toàn mạng là quá trình thu thập, phân tích và theo dõi liên tục các hoạt động diễn ra trên hệ thống mạng nhằm phát hiện, cảnh báo và ứng phó kịp thời với các mối đe dọa an ninh mạng. Đây là một công tác quan trọng bảo đảm an toàn thông tin trong các tổ chức, doanh nghiệp và cơ quan nhà nước. Thông qua hoạt động giám sát liên tục, tổ chức có thể nâng cao hiệu quả quản lý, bảo vệ tài sản thông tin và duy trì hoạt động ổn định của hệ thống.

1.2 Các hệ thống phát hiện xâm nhập

Trong lĩnh vực an toàn thông tin (ATTT), hệ thống phát hiện xâm nhập (Intrusion Detection System – IDS) và hệ thống ngăn chặn xâm nhập (Intrusion Prevention System – IPS) là những giải pháp bảo mật quan trọng giúp giám sát, phát hiện và bảo vệ hệ thống trước các hành vi truy cập trái phép hoặc các cuộc tấn công mạng.

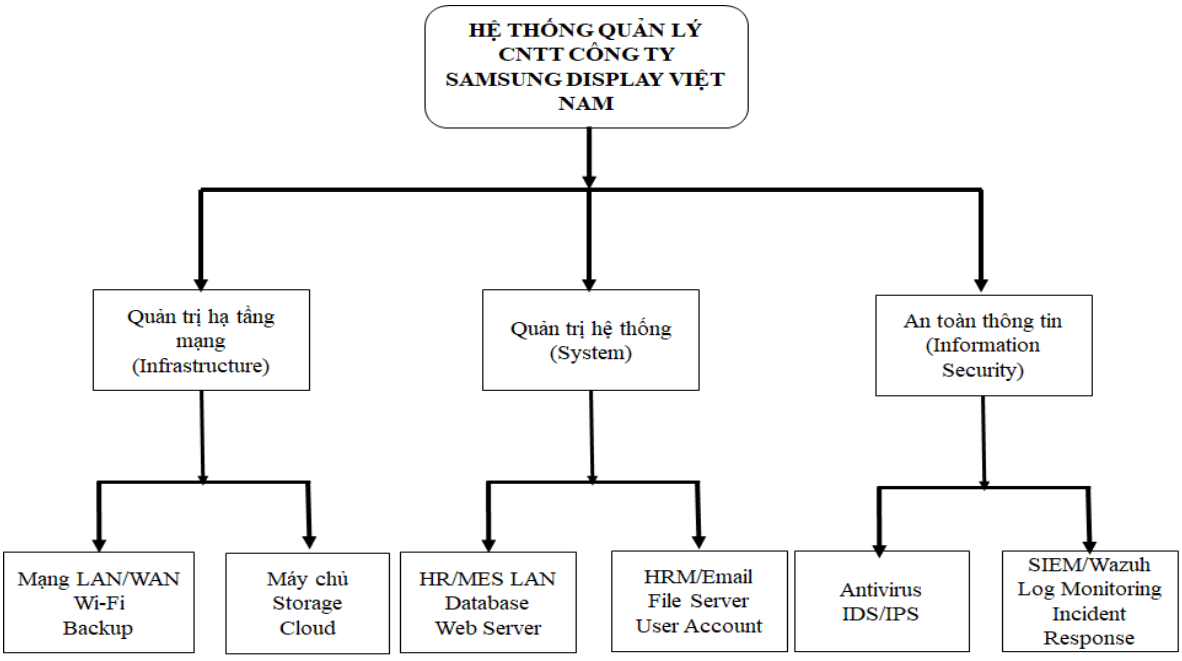
Hiện nay có nhiều giải pháp hỗ trợ giám sát an toàn thông tin, thu thập nhật ký, phát hiện xâm nhập và quản lý sự kiện bảo mật như WAZUH, SNORT, SURICATA, OSSEC… Trong số các giải pháp hiện nay, WAZUH đáp ứng toàn diện các yêu cầu về giám sát và bảo mật hệ thống trong một nền tảng thống nhất. Wazuh không chỉ tích hợp đồng thời nhiều chức năng quan trọng như phát hiện xâm nhập, giám sát tính toàn vẹn tập tin, quản lý lỗ hổng và cảnh báo theo thời gian thực, HIDS, SIEM và XDR**,** cho phép giám sát cả ở cấp độ máy chủ (host-based) lẫn dữ liệu nhật ký (log-based), ngoài ra Wazuh có khả năng tích hợp linh hoạt với nhiều công cụ khác giúp nâng cao khả năng phát hiện và phản ứng với

các mối đe dọa an ninh mạng. Wazuh được đánh giá là giải pháp cân bằng tốt giữa chi phí, tính năng và khả năng triển khai, phù hợp cho cả mục đích nghiên cứu và triển khai thực tế trong hệ thống giám sát an ninh mạng.

1.3 Giới thiệu về công ty TNHH Samsung Display Việt Nam

Công ty TNHH Samsung Display Việt Nam thuộc Tập đoàn Samsung của Hàn Quốc là công ty dẫn đầu trên thế giới về công nghệ màn hình. Công ty chuyên nghiên cứu và sản xuất các loại màn hình LCD, OLED với công nghệ hiện đại nhất cho điện thoại, tivi, máy tính bảng, máy tính xách tay…

SAMSUNG có một hạ tầng CNTT có lượng tài nguyên rất lớn, yêu cầu tính sẵn sàng cao, khả năng mở rộng linh hoạt và đáp ứng các yêu cầu nghiêm ngặt về bảo mật. Công ty triển khai hệ thống mạng nội bộ, các máy chủ, trung tâm lưu trữ dữ liệu và đặc biệt là các giải pháp giám sát hạ tầng CNTT hiện đại để phòng tránh và xử lý các sự cố an toàn thông tin có thể phát sinh.



Hình 1 Tổng quan sơ đồ cơ sở hạ tầng CNTT công ty Samsung Display Việt Nam

1.4 Kết luận chương 1

Chương 1 đã làm rõ các khái niệm về giám sát an toàn mạng, các giải pháp phát hiện ngăn chặn và xâm nhập, đồng thời cũng trình bày về bối cảnh và phương thức hoạt động của hệ thống mạng trông công ty SAMSUNG DISPLAY VIETNAM để nghiên cứu sâu hơn trong các chương tiếp theo.

CHƯƠNG 2 GIỚI THIỆU VỀ HỆ THỐNG WAZUH

2.1. Giới thiệu về Wazuh

Wazuh là một nền tảng giám sát an toàn thông tin mã nguồn mở cung cấp các chức năng giám sát bảo mật tập trung, phát hiện xâm nhập, quản lý sự kiện bảo mật (SIEM), giám sát thiết bị đầu cuối (XDR), đánh giá lỗ hổng và hỗ trợ tuân thủ các tiêu chuẩn an toàn thông tin. Mục tiêu chính của Wazuh là giúp tổ chức thu thập, phân tích và tương quan dữ liệu bảo mật từ nhiều nguồn khác nhau nhằm phát hiện sớm các mối đe dọa, giảm thiểu rủi ro và nâng cao khả năng ứng phó sự cốWazuh hiện là một trong những giải pháp SIEM/XDR phổ biến được triển khai trong doanh nghiệp, tổ chức giáo dục và các trung tâm điều hành an ninh mạng (SOC).

Các chức năng chính của Wazuh bao gồm: thu thập và phân tích nhật ký tập trung, phát hiện xâm nhập trên máy chủ, giám sát tính toàn vẹn tập tin, phát hiện Rootkit và phần mềm độc hại, quản lý lỗ hổng bảo mật, kiểm tra tuân thủ các tiêu chuẩn an toàn thông tin, cảnh báo và hỗ trợ ứng phó sự cố và trực quan hóa dữ liệu và điều tra sự kiện bảo mật.

Hệ thống Wazuh bao gồm bốn thành phần chính: Wazuh Agent**,** Wazuh Manager**,** Wazuh Indexer **và** Wazuh Dashboard**.** Trong đó, Wazuh Agent được cài đặt trên các máy cần giám sát để thu thập nhật ký (log) và thông tin bảo mật; Wazuh Manager tiếp nhận, phân tích dữ liệu và phát hiện các mối đe dọa dựa trên bộ luật (rules); Wazuh Indexer có nhiệm vụ lưu trữ và đánh chỉ mục dữ liệu nhằm tối ưu việc tìm kiếm; còn Wazuh Dashboard cung cấp giao diện trực quan giúp quản trị viên theo dõi, phân tích cảnh báo và quản lý toàn bộ hệ thống. Sự kết hợp của các thành phần này tạo thành một nền tảng giám sát an toàn thông tin tập trung, hỗ trợ phát hiện, phân tích và ứng phó với các sự cố bảo mật một cách hiệu quả.

Luồng xử lý của Wazuh diễn ra theo các bước sau: Wazuh Agent thu thập nhật ký và thông tin bảo mật từ các máy được giám sát, sau đó gửi dữ liệu đến Wazuh Manager**.** Tại đây, dữ liệu được giải mã, phân tích và đối chiếu với các quy tắc để phát hiện các hành vi bất thường hoặc mối đe dọa. Các cảnh báo được tạo ra sẽ được lưu trữ

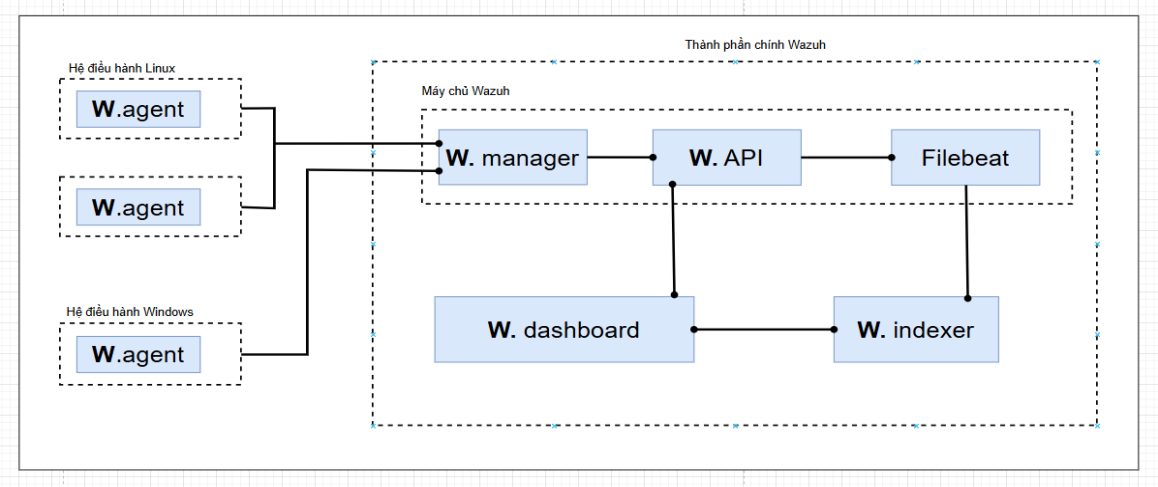
và đánh chỉ mục **trên** Wazuh Indexer**,** đồng thời hiển thị trên Wazuh Dashboard để quản trị viên theo dõi, phân tích và xử lý sự cố bảo mật.

2.2. Cài đặt và kết nối Wazuh tới máy chủ

Trong mô hình triển khai cơ bản, hệ thống bao gồm:

01 máy chủ cài đặt Wazuh Server và ba thành phần trung tâm: Wazuh Server (còn được gọi là Manager), Wazuh Indexer (dựa trên Elasticsearch) và Wazuh Dashboard (dựa trên Kibana) phục vụ quản trị và giám sát ...

Các máy Agent (Windows/Linux) gửi dữ liệu về Server.



Hình 13 Các thành phần chính của hệ thống giám sát Wazuh

Cách cài đặt

Linux:

Cài đặt WAZUH SERVER và AGENT bằng Script chính thức trên Terminal trên hệ điều hành UBUNTU của LINUX:

Windows

Tải Agent từ trang Wazuh sau đó chạy file cài đặt và nhập địa chỉ IP Wazuh Server.

Sau đó tiến hành thu thập dữ liệu từ các file log mạng, USB, nhật ký truy cập hệ thống...

Sau khi thu thập log, WAZUH tiến hành kiểm tra, phân tích và phát hiện dữ liệu bất thường, lỗ hổng bảo mật. Người sử dụng có thể sử dụng các tính năng của WAZUH để phân tích cảnh báo bảo mật, phát hiện tấn công Brute Force SSH, phát hiện thay đổi tập tin, phát hiện Malware và Rootkit và phân tích lỗ hổng bảo mật.

2.3. Tìm hiểu về cấu hình nâng cao và tích hợp giải pháp

Trong hệ thống Wazuh, **Decoder** và **Rules** đóng vai trò quan trọng trong việc phân tích và phát hiện các sự kiện an ninh. Decoder được sử dụng để xử lý và trích xuất thông tin từ log thô, trong khi Rules được áp dụng để so khớp dữ liệu đã được chuẩn hóa nhằm phát hiện các hành vi bất thường hoặc dấu hiệu tấn công.

Decoder có nhiệm vụ phân tích cấu trúc của log trước khi dữ liệu được đưa vào hệ thống Rules. Thông qua Decoder, các trường thông tin quan trọng trong log sẽ được tách và chuẩn hóa, giúp quá trình xử lý dữ liệu trở nên chính xác và hiệu quả hơn.

Sau khi dữ liệu được xử lý bởi Decoder, hệ thống sử dụng Rules để phát hiện các hành vi bất thường dựa trên các điều kiện đã được định nghĩa trước. Rule này sẽ kích hoạt cảnh báo khi phát hiện các log đã được Decoder xử lý theo định dạng “apache-access”, đồng thời gán mức độ nghiêm trọng tương ứng.

Active Response là cơ chế cho phép hệ thống Wazuh tự động thực hiện các hành động phản ứng khi phát hiện hành vi tấn công hoặc sự kiện bảo mật nghiêm trọng. Cơ chế này giúp rút ngắn thời gian phản ứng và giảm thiểu thiệt hại do các cuộc tấn công gây ra. Wazuh Active Response có thể được cấu hình để thực hiện nhiều hành động khác nhau, bao gồm: Chặn địa chỉ IP thông qua Firewall, vô hiệu hóa tài khoản người dùng bị nghi ngờ hay ngắt kết nối thiết bị hoặc tiến trình đang bị tấn công hoặc cấu hình trên cho phép hệ thống tự động thực thi hành động chặn truy cập.

Wazuh hỗ trợ tích hợp với nhiều nguồn **Threat Intelligence** bên ngoài nhằm nâng cao khả năng phát hiện và phân tích các mối đe dọa an ninh mạng. Việc tích hợp này giúp hệ thống đối chiếu dữ liệu nội bộ với các nguồn thông tin về mối đe dọa đã được công bố.

2.4. Kết luận chương 2

Chương 2 đã giới thiệu về cách hoạt động, chức năng và các thành phần cơ bản của hệ thống WAZUH, qua đó hiểu hơn về cơ chế hoạt động của một hệ thống an ninh mạng và là cơ sở để xây dựng và triển khai một hệ thống an ninh mạng.

CHƯƠNG 3. XÂY DỰNG HỆ THỐNG GIÁM SÁT

3.1. Tìm hiểu hệ thống giám sát hiện tại tại công ty

Trong môi trường doanh nghiệp sản xuất quy mô lớn, hệ thống công nghệ thông tin bao gồm nhiều thành phần khác nhau, mỗi thành phần có đặc điểm hoạt động và mức độ rủi ro riêng. Vì vậy, việc phân loại đối tượng cần giám sát là cơ sở để xây dựng các biện pháp bảo vệ phù hợp.

Hệ thống mạng CNTT: Bao gồm các máy chủ, thiết bị mạng, dịch vụ nội bộ, hệ thống thư điện tử và các ứng dụng phục vụ hoạt động doanh nghiệp.

Hệ thống máy tính nhân sự: Bao gồm máy tính của nhân viên sử dụng để: tổng hợp, xử lý và phân tích dữ liệu phục vụ công việc, trao đổi thông tin, gửi và nhận thư điện tử (Email), họp trực tuyến và phối hợp công việc với các cá nhân hoặc phòng ban.

Hệ thống vận hành sản xuất: Cấu trúc của hệ thống bao gồm: các máy tính điều khiển, máy chủ vận hành, hệ thống SCADA, PLC hoặc các thiết bị phục vụ dây chuyền sản xuất. Các mini agent này truyền tải data, dữ liệu tới một máy chủ đóng vai trò như một Wazuh Agent giao tiếp và truyền tải dữ liệu.

Dữ liệu và tài liệu kinh doanh: Đóng vai trò cốt lõi trong hoạt động vận hành, sản xuất và quản trị. Các loại dữ liệu này thường bao gồm nhiều nhóm thông tin có giá trị cao,

Thiết bị và công cụ lưu trữ thông tin: là các phương tiện được sử dụng để lưu trữ, sao lưu và truyền tải dữ liệu trong hệ thống công nghệ thông tin. Đây là nhóm thiết bị tiềm ẩn nhiều rủi ro về an toàn thông tin.

3.2. Xây dựng hệ thống giám sát và phát hiện xâm nhập dựa trên Wazuh

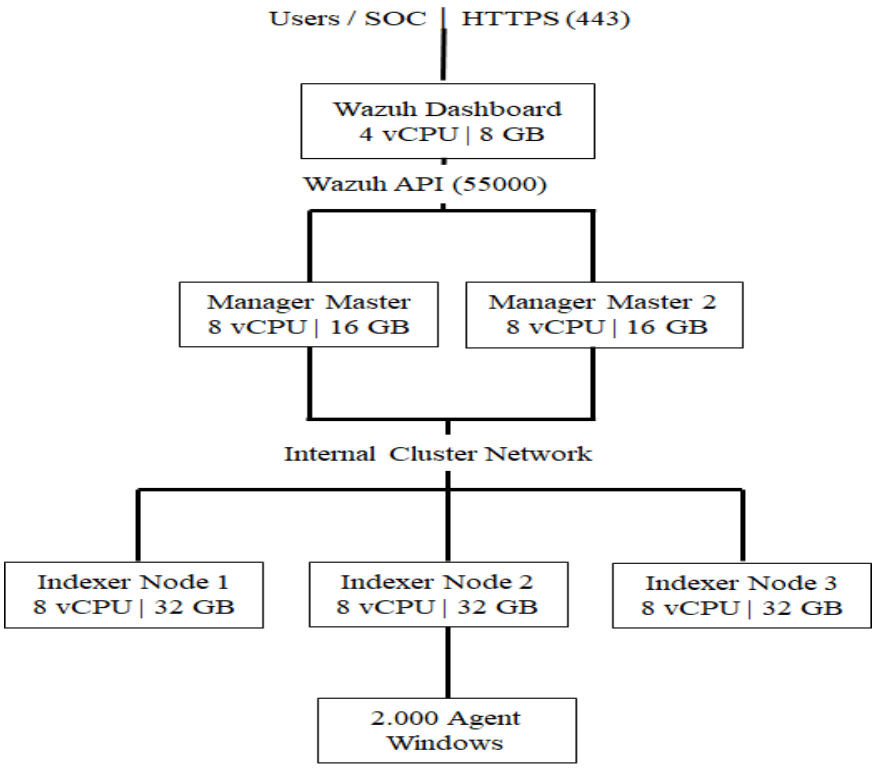
Xây dựng hệ thống quản lý cho khối sản xuất

. Các nguy cơ bị tấn công đối với hệ thống này bao gồm:

- Đăng nhập trái phép trên thiết bị từ tác nhân bên ngoài, ngăn chặn thay đổi thiết bị dẫn đến gián đoạn sản xuất.
- Kết nối thiết bị ngoại vi bất thường: Việc kết nối USB, ổ cứng lây nhiễm virus có thể dẫn đến lây nhiễm mã độc, phá hủy chương trình thiết bị.
- Phát hiện cài đặt phần mềm trái phép: Các phần mềm không có bản quyền có thể chứa virus có thể gây ra lây nhiễm mã độc hoặc vô hiệu hóa đến hệ thống.

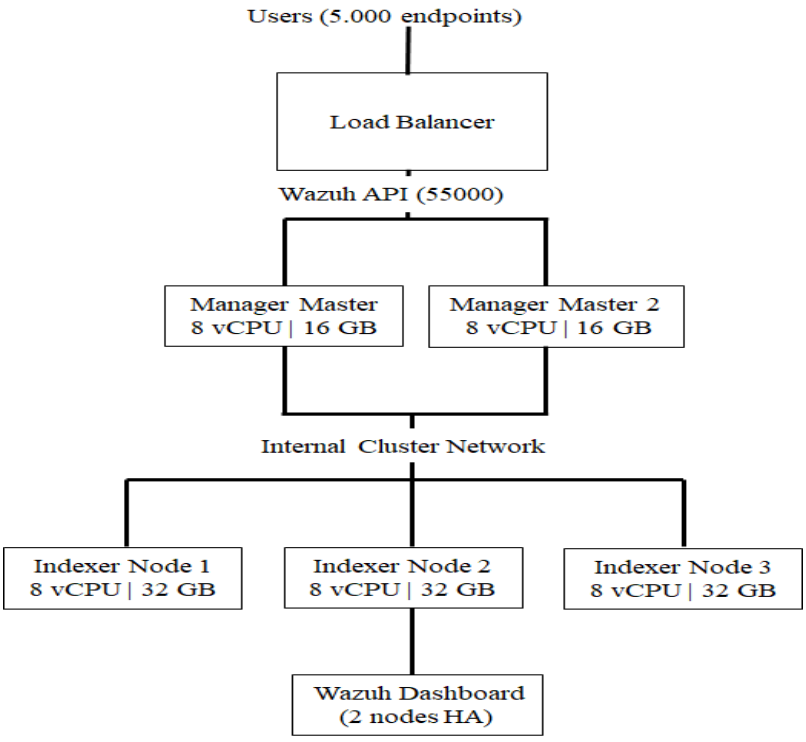
- Quản lý lưu trữ tài liệu trong thư mục, giám sát tính toàn vẹn tập tin: Quản lý các tài liệu kỹ thuật, bí mật kinh doanh… quan trọng,

Xây dựng hệ thống quản lý cho khối sản xuất 2000 Agent



Hình 43: Sơ đồ mô phỏng cấu hình cho 2000 máy Agent

Xây dựng hệ thống quản lý cho khối văn phòng 5000 Agent



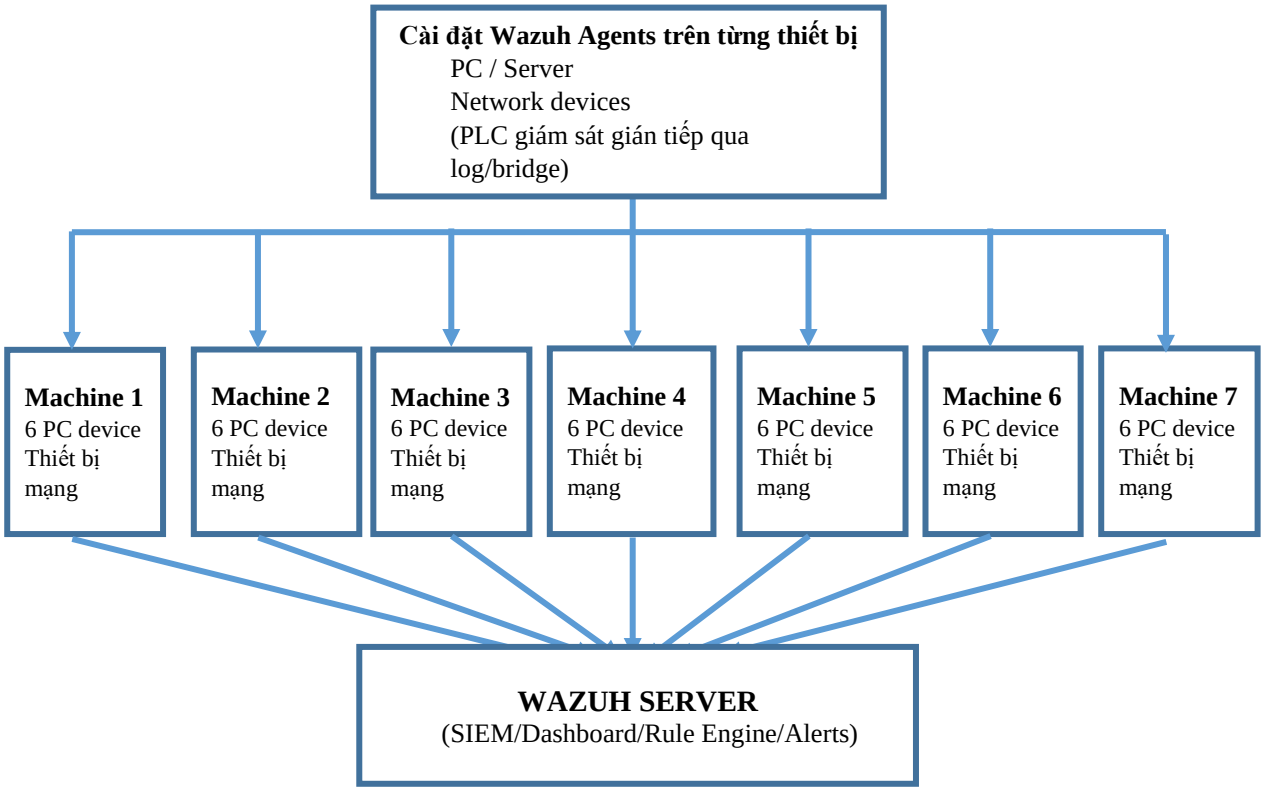
Sơ đồ mô phỏng cấu hình cho 5000 máy Agent

Xây dựng các kịch bản tấn công và phòng chống

Mô hình triển khai thử nghiệm

Hiện tại phạm vi quản lý của WAZUH mới tập trung vào máy chủ của từng line, trong khi các thiết bị khác như máy trạm, thiết bị mạng và các thiết bị đầu cuối chưa được giám sát và quản lý một cách đầy đủ. Điều này tạo ra những khoảng trống trong hệ thống giám sát an ninh, tiềm ẩn nguy cơ phát sinh các lỗ hổng bảo mật, từ đó có thể bị khai thác để thực hiện các cuộc tấn công mạng hoặc xâm nhập trái phép vào hệ thống. Do vậy, trong thời gian tới, đề án đang tiến hành xây dựng và triển khai quy trình bảo mật nhằm nâng cấp phạm vi quản lý, mở rộng từ các máy CIM hiện tại sang toàn bộ hệ thống máy tính trong công đoạn.

Mô tả triển khai mô hình như sau: Công đoạn bao gồm 20 line, mỗi line gồm 7~8 thiết bị, mỗi thiết bi bao gồm 6 máy tính và thiết bị mạng, thiết bị đầu cuối, PLC



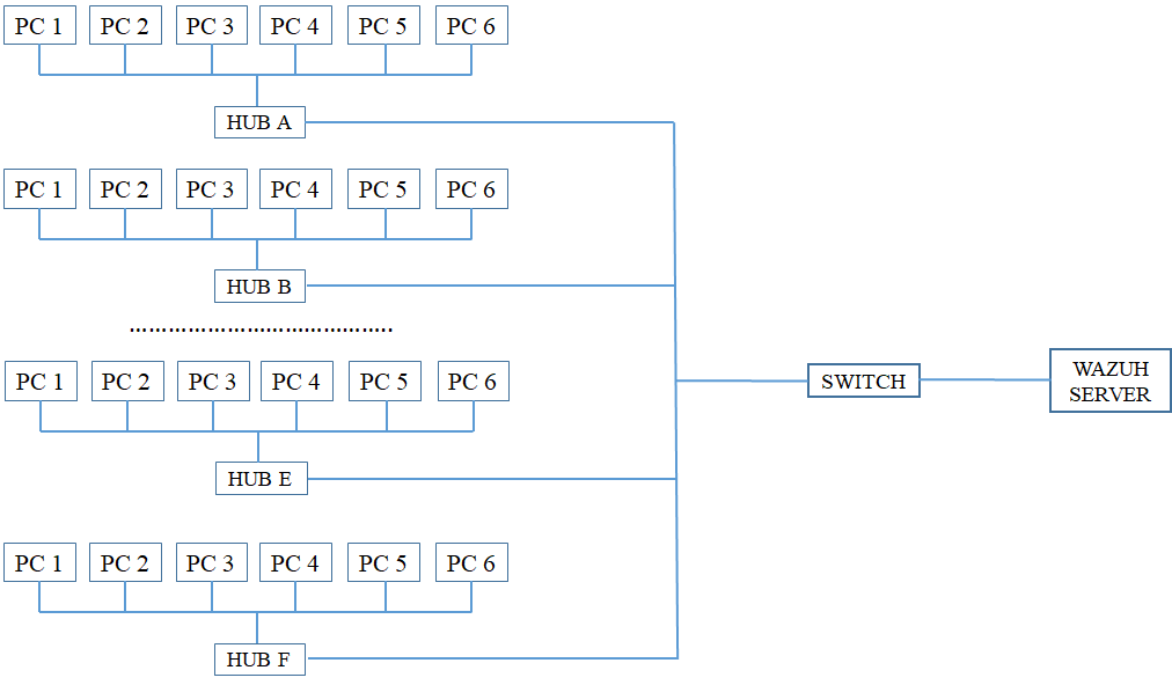
Hình 45: Mô phỏng hệ thống setup cho từng line.

Phương thức kết nối:

Các máy tính và module PLC trong hệ thống này được kết nối với nhau qua hub mạng LAN, sau đó các hub này sẽ được kết nối chung vào một switch tổng. Các máy Agent đều cài Window 10 và cài đặt chung dải IP. VD: 192.168.100.xyz để tiến hành liên kết mạng



Hình 46: Kết nối mạng Lan trên từng thiết bị



Hình 47: Kết nối mạng giữa các thiết bị trên cùng hệ thống

Mô hình cài đặt cho hệ thống này

WAZUH SERVER: Do số lượng thiết bị từ 40~50 nên cụm máy chủ có thể chạy tất cả thành phần (all-in-one): Wazuh Manager, Indexer, Dashboard

WAZUH AGENT: Cài đặt Wazuh Agents trên từng thiết bị: PC / Server, Network devices, Endpoint, (PLC giám sát gián tiếp qua log/bridge)

Cơ chế hoạt động trong mô hình

Thu thập dữ liệu: Wazuh Agent được cài trên máy tính, server, endpoint trong từng line, thiết bị mạng và PLC có thể gửi log qua Syslog hoặc gateway trung gian. Toàn bộ log được gửi về Wazuh Server (Manager)

Phương thức kiểm thảo:

Để kiểm thảo tấn công cho hệ thống này, đề án sẽ giả lập một **Wazuh Agent** được kết nối trong hệ thống **Wazuh**. Sau đó đề án sẽ mô phỏng/ giả lập các trường hợp Agent này bị tấn công bằng nhiều phương thức, cách thức cấu hình và cách Wazuh phát hiện ra xâm nhập

Kịch bản 1: Phát hiện đăng nhập trái phép

Kịch bản này nhằm kiểm tra khả năng phát hiện các hành vi đăng nhập không hợp lệ hoặc truy cập trái phép vào hệ thống. và tạo cảnh báo khi phát hiện số lần đăng nhập sai bất thường tấn công dò mật khẩu. WAZUH cảnh báo đăng nhập thất bại sau 3 lần

Biện pháp phòng chống: Kích hoạt cơ chế Active Response chặn kết nối IP

```
C:\Windows\system32>netsh advfirewall firewall show rule name=all | findstr Wazuh
Rule Name:                            Wazuh Block 192.168.28.28
Rule Name:                            Wazuh Block
Rule Name:                            Wazuh Block IP
```

Kịch bản 2: Thay đổi trái phép tập tin hệ thống

Kịch bản này kiểm tra khả năng giám sát và phát hiện thay đổi trái phép đối với các tập tin quan trọng trong hệ thống. Cấu hình Wazuh theo dõi một thư mục chứa dữ liệu quan trọng, sau đó thực hiện các hành động như tạo mới, chỉnh sửa hoặc xóa tập tin và kiểm tra cảnh báo

☞ Kiểm tra trên Dashboard bằng cách truy cập mục **Endpoint Security** - > **File Integrity Monitoring** - > **Event** sẽ thấy sự kiện add (thêm) file và modified file

	syscheck.path	syscheck.event	rule.description
	c:\wazuhtest\fim-test.txt	modified	Integrity checksum changed.

Hình 56: Sự kiện thay đổi file trên Dashboard.

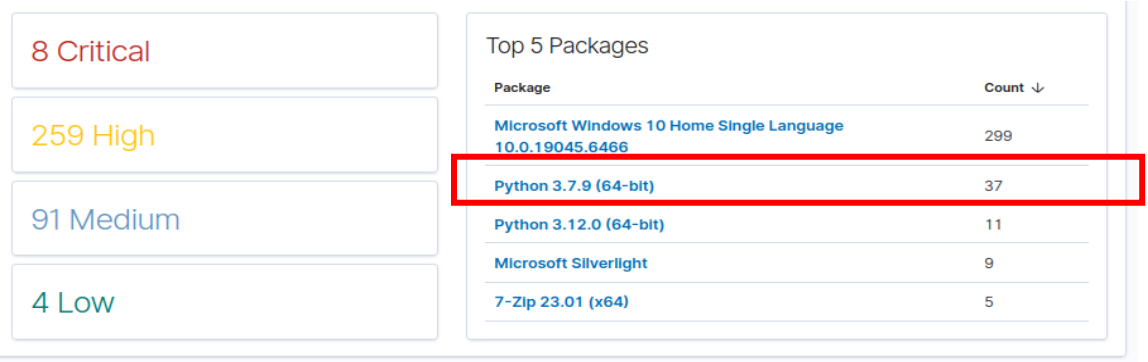
Hình 61: Cảnh báo kết nối USB

Kịch bản 3: Phát hiện cài đặt phần mềm có chứa lỗ hổng

Thực hiện: Cài đặt phiên bản phần mềm cũ chứa lỗ hổng đã biết.

VD: Cài đặt phần mềm Python 3.7.9 là phiên bản cũ có nhiều lỗ hổng.

Kết quả: Kiểm tra tại tính năng trên Dashboard bằng cách truy cập **Threat Intelligence → Vulnerability Detection** để theo dõi các lỗ hổng được phát hiện.



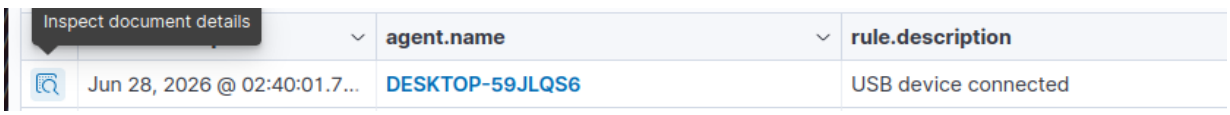
Hình 58: Phát sinh cảnh báo.

Kịch bản 4: Phát hiện kết nối thiết bị ngoại vi trái phép

Thực hiện: cắm USB vào máy Agent.

Cấu hình trên file /var/ossec/etc/rules/local_rules.xml để tạo rule cảnh bảo cắm thiết bị USB

Hệ thống sinh alert cảnh báo có USB cắm vào máy tính Agent.



Đánh giá kết quả

Kết quả thực nghiệm cho thấy Wazuh có khả năng thu thập dữ liệu tập trung, phát hiện các hành vi bất thường và hỗ trợ phản ứng sự cố hiệu quả. Các kịch bản thử nghiệm như brute-force, quét cổng, thay đổi tập tin và phát hiện lỗ hổng đều được hệ thống ghi nhận và cảnh báo kịp thời. Điều này chứng minh Wazuh là một giải pháp giám sát và phát hiện xâm nhập hiệu quả, đáp ứng tốt yêu cầu về quản lý an ninh

mạng trong môi trường doanh nghiệp và là một công cụ hữu ích giúp xây dựng nên một hệ thống giám sát an toàn toàn diện.

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

1. Kết luận

Đề án đã xây dựng được một hệ thống SIEM bằng Wazuh, với các chức năng như: thu thập thông tin như các log và event, thông qua các chức năng được tích hợp trên hệ thống nhằm phát hiện sớm các sự cố an toàn thông tin.

Qua đề án không chỉ hiểu sâu hơn về cơ chế thu thập log – xử lý – ngăn chặn các mối đe dọa, mà còn biết cách phân tích, đánh giá và phản ứng trước các rủi ro bảo mật một cách hiệu quả.

Qua quá trình tìm hiểu và triển khai, có thể thấy Wazuh đáp ứng hiệu quả các yêu cầu của một hệ thống giám sát an toàn mạng hiện đại nhờ khả năng mở rộng, chi phí triển khai thấp và hỗ trợ đa nền tảng. Bên cạnh đó, các tính năng nâng cao như Active Response, Decoder và Rule tùy chỉnh, cùng khả năng tích hợp với Suricata, Zeek, các nguồn Threat Intelligence và môi trường điện toán đám mây giúp nâng cao khả năng phát hiện và ứng phó với các mối đe dọa an ninh mạng.

2. Hướng phát triển

Trong bối cảnh các mối đe dọa an ninh mạng ngày càng tinh vi và khó lường, việc nâng cấp và mở rộng hệ thống giám sát an toàn thông tin là yêu cầu tất yếu. Định hướng trong tương lai của hệ thống Wazuh không chỉ dừng lại ở việc thu thập và quản lý log truyền thống, mà còn hướng tới tích hợp các công nghệ AI và Machine Learning nhằm nâng cao khả năng phân tích hành vi, phát hiện bất thường và tự động hóa phản ứng trước các sự cố bảo mật. Qua đề án này có thể dự đoán và cảnh báo sớm các nguy cơ tiềm ẩn mà các phương pháp truyền thống khó có thể nhận diện kịp thời. Bên cạnh đó, việc triển khai và vận hành hệ thống Wazuh trong môi trường thực tế – chẳng hạn tại các doanh nghiệp vừa và nhỏ, trung tâm dữ liệu, hoặc các tổ chức giáo dục – sẽ là bước tiếp theo quan trọng nhằm đánh giá hiệu quả hoạt động.

Wazuh là một nền tảng giám sát an toàn thông tin mã nguồn mở mạnh mẽ, tích hợp các chức năng của hệ thống SIEM, HIDS và XDR trong cùng một giải pháp. Hệ thống cho phép thu thập và phân tích log tập trung, phát hiện các hành vi bất thường, giám sát

tính toàn vẹn tập tin, đánh giá lỗ hổng bảo mật và hỗ trợ phản ứng sự cố theo thời gian thực.

Mặc dù vẫn tồn tại một số hạn chế như yêu cầu tài nguyên hệ thống tương đối lớn trong các môi trường quy mô lớn và cần kiến thức chuyên môn để tối ưu luật phát hiện, Wazuh vẫn là một lựa chọn phù hợp cho các doanh nghiệp, tổ chức và đơn vị nghiên cứu muốn xây dựng trung tâm giám sát an toàn thông tin (SOC) với chi phí hợp lý góp phần nâng cao năng lực giám sát, phát hiện sớm và giảm thiểu rủi ro đối với hệ thống thông tin của tổ chức.