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

ĐỀ ÁN TỐT NGHIỆP THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

HÀ NỘI – 2026

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**

ĐỀ ÁN TỐT NGHIỆP THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

NGƯỜI HƯỚNG DẪN KHOA HỌC

TS. ĐINH TRƯỜNG DUY

HÀ NỘI – 2026

LỜI CAM ĐOAN

Tên tôi là Lê Thị Lý, mã số học viên: B23CHIS018. Học viên lớp cao học B23HTTT01-B Khóa 2023-2025, Khoa Công nghệ Thông tin Học viện Công nghệ Bưu chính Viễn thông, xin cam đoan:

1. Đây là luận văn do bản thân tôi trực tiếp thực hiện dưới sự hướng dẫn của TS. Đinh Trường Duy.

2. Luận văn này không trùng lặp với bất kỳ nghiên cứu nào khác đã được công bố tại Việt Nam.

3. Các số liệu, dữ liệu và thông tin trong nghiên cứu là hoàn toàn trung thực và khách quan.

Tôi xin hoàn toàn chịu trách nhiệm trước pháp luật về những cam kết này.

Hà Nội, ngày 07 tháng 07 năm 2026.

TÁC GIẢ LUẬN VĂN



Lê Thị Lý

LỜI CẢM ƠN

Sau hai năm học tập và nghiên cứu khoa học, trải qua nhiều khó khăn, đến nay em đã hoàn thành bản đề án thạc sĩ của mình. Với tất cả tấm lòng, em xin bày tỏ sự biết ơn sâu sắc tới:

Ban Giám hiệu, Phòng Đào tạo Sau đại học, Khoa Sau đại học Học viện Công nghệ Bưu chính Viễn thông đã tạo điều kiện thuận lợi và cho phép em được học tập, nghiên cứu để đạt được những thành quả về kiến thức, kỹ năng nghề nghiệp và nâng cao năng lực công tác trong suốt thời gian học tập vừa qua.

Các thầy các cô giáo, các giảng viên Khoa Sau đại học Học viện Công nghệ Bưu chính Viễn thông đã tận tâm hướng dẫn em trong suốt quá trình học tập, nghiên cứu và hoàn thành đề án này.

Em cũng xin bày tỏ lòng kính trọng và biết ơn sâu sắc tới thầy giáo, TS. ĐINH TRƯỜNG DUY, người đã tận tâm hướng dẫn, ân cần chỉ bảo và nhiều lần cho ý kiến quý báu về phương pháp nghiên cứu, kiến thức tư duy khoa học trong suốt quá trình học tập, nghiên cứu đề tài, chỉnh sửa và hoàn thiện đề án này.

HỌC VIÊN

Lê Thị Lý

MỤC LỤC

LỜI CAM ĐOAN i
LỜI CẢM ƠN ii
MỤC LỤC iii
DANH SÁCH BẢNG v
DANH SÁCH HÌNH VẼ vi
MỞ ĐẦU 1
II. NỘI DUNG 8
CHƯƠNG 1 CƠ SỞ LÝ LUẬN 8
1.1 Tổng quan về giám sát an toàn mạng 8
1.1.1 Giám sát an toàn mạng là gì? 8
1.1.2. Mục tiêu của giám sát an toàn mạng 8
1.1.3. Các thành phần chính của hệ thống giám sát an toàn mạng 10
1.1.4 Vai trò của giám sát an toàn mạng 12
1.2. Các hệ thống phát hiện xâm nhập 13
1.2.1. Hệ thống phát hiện xâm nhập (IDS) 13
1.2.2. Hệ thống ngăn chặn xâm nhập (IPS) 14
1.2.3. Các phương pháp phát hiện xâm nhập 16
1.2.4. Vai trò của IDS/IPS trong hệ thống an toàn thông tin 17
1.2.5. Giới thiệu một số hệ thống, công cụ phục vụ cho giám sát và phát hiện xâm nhập 18
1.3. Giới thiệu về công ty TNHH Samsung Display Việt Nam 30
1.3.1 Việc quản lý cơ sở hạ tầng CNTT tại công ty Samsung Display Việt Nam 32
1.3.2. Hệ thống quản lý CNTT của công ty Samsung Display VietNam 32
CHƯƠNG 2 GIỚI THIỆU VỀ HỆ THỐNG WAZUH 35
2.1. Giới thiệu về Wazuh 35
2.1.1. Wazuh là gì? 35
2.1.3. Luồng xử lý dữ liệu và cấu tạo luật trong Wazuh 42
2.1.4. Lợi ích và hạn chế của Wazuh 46

2.1.5. Các công cụ nền tảng sử dụng để triển khai và thử nghiệm giải pháp...48
2.2. Cài đặt và kết nối Wazuh tới máy chủ 49
2.2.1. Cài đặt Wazuh Server và kết nối Wazuh tới máy chủ [4][8]. *50*
2.2.2. Cấu hình Wazuh Agent.....*52*
2.2.3. Thu thập dữ liệu *53*
2.2.4 Cách kiểm tra, phân tích và phát hiện dữ liệu bất thường, lỗ hổng bảo mật bằng Wazuh [5].....*54*
2.2.5. Một số tính năng cơ bản khác *57*
2.3. Tìm hiểu về cấu hình nâng cao và tích hợp giải pháp.....64
2.3.1. Tùy chỉnh Decoder và Rules.....*64*
2.3.2. Tích hợp Active Response.....*65*
2.3.3. Tích hợp Threat Intelligence.....*65*
CHƯƠNG 3. XÂY DỰNG HỆ THỐNG GIÁM SÁT 67
3.1. Tìm hiểu hệ thống giám sát hiện tại tại công ty 67
3.1.1. Phân loại đối tượng cần giám sát và bảo vệ.....*67*
3.1.2. Phân tích các dạng tấn công an toàn thông tin *72*
3.2. Xây dựng hệ thống giám sát và phát hiện xâm nhập dựa trên Wazuh.....74
3.2.1. Mô hình đề xuất cho hệ thống.....*74*
3.3. Thực hiện mô phỏng tấn công và kết quả 83
KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN 92
TÀI LIỆU THAM KHẢO 94

DANH SÁCH BẢNG

Bảng 1.1 Bảng so sánh giữa các công cụ quét bảo mật 29
Bảng 1.2: Số liệu doanh thu công ty Samsung Display VietNam 31
Bảng 2.1: Các level cảnh báo 46
Bảng 3.1: Cấu hình đề xuất cho các máy trên hệ thống 74
Bảng 3.2: Cấu hình đề xuất cho các máy trên hệ thống sản xuất 75

DANH SÁCH HÌNH VẼ

Hình 1.1: Phương thức hoạt động của WAZUH [1] 19
Hình 1.2: Phương thức hoạt động của Snort [8] 20
Hình 1.3: Các bước hoạt động của Suricata [9] 21
Hình 1.4: Các bước hoạt động của OSSEC [10] 23
Hình 1.5: Sơ đồ hoạt động của ELK [12] 24
Hình 1.6: Mô hình hoạt động của Zeek [13] 25
Hình 1.7: Mô hình hoạt động của Slunk [11] 26
Hình 1.8: Mô hình hoạt động của IBM Qradar [14] 28
Hình 1.9. Sơ đồ cơ cấu tổ chức công ty Samsung Display Việt Nam 31
Hình 1.10. Tổng quan sơ đồ cơ sở hạ tầng CNTT công ty Samsung Display Việt Nam 34
Hình 2.1: Sơ đồ hệ thống Wazuh 38
Hình 2.2: Ví dụ cơ bản về cấu tạo luật trong WAZUH 45
Hình 2.3. Các thành phần chính của hệ thống giám sát Wazuh 49
Hình 2.4: Cấu hình hệ điều hành trước khi cài đặt trên VM 50
Hình 2.5: Update hệ điều hành 50
Hình 2.6: Bash cài đặt 51
Hình 2.7: Cài đặt các gói quan trọng 51
Hình 2.8: Cài đặt các gói quan trọng 52
Hình 2.9: Cấu hình Wazuh Agent 53
Hình 2.10: Thông tin Agent 53
Hình 2.11: Endpoint security 57
Hình 2.12: Threat Intelligence 57
Hình 2.13: Server management 58
Hình 2.14: Indexer management 59
Hình 2.15: Dashboard management 59
Hình 2.16: Giám sát log 60
Hình 2.17: Menu FIM 61
Hình 2.18: Lọc FIM log 61

Hình 2.19: Chức năng quản lý lỗ hổng bảo mật 62
Hình 2.20: Chọn log 62
Hình 2.21: Thông tin log 62
Hình 2.22: local_rules 63
Hình 2.23: Tạo cảnh báo 63
Hình 2.24: Truy cập web và bị ngắt truy cập 63
Hình 3.1: Hệ thống máy tính văn phòng 67
Hình 3.2: Hệ thống máy tính nhà xưởng 69
Hình 3.3: Sơ đồ mô phỏng cấu hình cho 2000 máy Agent 75
Hình 3.4: Sơ đồ mô phỏng cấu hình cho 5000 máy Agent 76
Hình 3.5: Mô phỏng hệ thống setup cho từng line. 79
Hình 3.6: Kết nối mạng Lan trên từng thiết bị 80
Hình 3.7. Kết nối mạng giữa các thiết bị trên cùng hệ thống 80
Hình 3.8. Cấu hình trên máy WAZUH SERVER 82
Hình 3.9. Cấu hình trên máy WAZUH AGENT 82
Hình 3.10: Thêm rule để Wzuh phát hiện đăng nhập thất bại 84
Hình 3.111: Cảnh báo đăng nhập thất bại sau 3 lần 85
Hình 3.12: Thông tin đăng nhập 85
Hình 3.13: Thông tin IP đăng nhập bị block 87
Hình 3.14: Tạo file trên Window Agent 88
Hình 3.15: Sự kiện phát hiện thêm file trên Dashboard 88
Hình 3.16: Thêm dữ liệu vào file. 88
Hình 3.17: Sự kiện thay đổi file trên Dashboard. 88
Hình 3.18: Cài đặt phần mềm phiên bản cũ. 89
Hình 3.19: Phát sinh cảnh báo. 89
Hình 3.20: Hiển thị mức độ nghiêm trọng và nguy cơ 89
Hình 3.21: Cấu hình để phát hiện kết nối USB trên thiết bị 90
Hình 3.22: Cảnh báo kết nối USB 90
Hình 3.23: Thông tin truy cập 90

MỞ ĐẦU

1. Lý do nghiên cứu đề tài

Trong thời đại công nghệ 4.0 hiện nay, 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 như tấn công từ chối dịch vụ (DoS/DDoS), xâm nhập trái phép, mã độc, khai thác lỗ hổng zero-day, v.v.

Công ty SAMSUNG DISPLAY VIETNAM thuộc tập đoàn SAMSUNG – tập đoàn hàng đầu Hàn Quốc với ba mười nghìn nhân viên, không chỉ đang 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 như APPLE, HUAWEI, OPPO, DELL… do vậy để điều hành hiệu quả, công ty SAMSUNG DISPLAY VIETNAM không chỉ phải có cơ sở hạ tầng CNTT rất lớn và có dữ liệu nội bộ quy mô lớn (nhân sự, hợp đồng, đối tác) hay dữ liệu khách hàng (thông tin cá nhân, tài chính, dữ liệu kinh doanh của khách hàng) lớn mà quan trọng hơn là dữ liệu kinh doanh, chiến lược, các bí mật công nghệ. Kho dữ liệu khổng lồ này rất dễ trở thành mục tiêu hấp dẫn cho hacker, gián điệp kinh tế và tội phạm mạng. Các hệ thống dễ bị tấn công trong doanh nghiệp hiện nay:

Máy tính cá nhân/Điện thoại: Máy tính cá nhân (PC/Laptop) và thiết bị di động: Đây là các thiết bị được sử dụng hàng ngày để xử lý công việc, lưu trữ dữ liệu và trao đổi thông tin. Các thiết bị và dữ liệu này nếu không được cài đặt bảo mật tốt thì rất dễ tấn công dưới các hình thức như: lây nhiễm mã độc, đánh cắp dữ liệu, chiếm quyền điều khiển... Không những vậy, khi một thiết bị đầu cuối bị xâm nhập, kẻ tấn công có thể lợi dụng để truy cập trái phép vào hệ thống nội bộ và mở rộng phạm vi tấn công toàn hệ thống.

Mạng nội bộ (LAN/WAN): Mạng nội bộ là hạ tầng kết nối các máy tính, máy chủ và thiết bị mạng trong doanh nghiệp, đóng vai trò quan trọng trong việc trao đổi dữ liệu và vận hành các hệ thống thông tin. Nếu không được cấu hình và bảo vệ đúng cách, mạng nội bộ có thể trở thành mục tiêu của các cuộc tấn công như truy cập trái

phép, nghe lén lưu lượng mạng, đánh cắp dữ liệu, lây lan mã độc. Một số hình thức tấn công tiêu biểu bao gồm ransomware giữa các thiết bị, tấn công giả mạo địa chỉ , tấn công từ chối dịch vụ và khai thác lỗ hổng trên các thiết bị mạng. Những sự cố này có thể gây gián đoạn hoạt động của hệ thống, làm suy giảm hiệu suất mạng, ảnh hưởng đến quá trình sản xuất, đồng thời gây thiệt hại về dữ liệu và tài chính cho doanh nghiệp.

Máy chủ Web và ứng dụng Web: Các hệ thống cung cấp dịch vụ trực tuyến thường đối mặt với các hình thức tấn công như SQL Injection, Cross-Site Scripting (XSS), Remote Code Execution (RCE), Directory Traversal và Brute Force nhằm đánh cắp dữ liệu hoặc chiếm quyền điều khiển hệ thống. Cơ sở dữ liệu bị truy cập trái phép, đánh cắp dữ liệu nhạy cảm.

Hệ thống cơ sở dữ liệu (Database): Chứa nhiều thông tin quan trọng như dữ liệu kinh doanh, thông tin khách hàng, nhân sự và tài chính. Kho dữ liệu này dễ trở thành mục tiêu khai thác để đánh cắp thông tin và thực hiện tống tiền. Các nguy cơ phổ biến bao gồm truy cập trái phép, rò rỉ và đánh cắp dữ liệu, tấn công SQL Injection.

Máy chủ (Server): Máy chủ lưu trữ cơ sở dữ liệu, ứng dụng và các dịch vụ quan trọng của doanh nghiệp. Nếu không được cập nhật bản vá bảo mật hoặc cấu hình đúng cách, máy chủ có thể bị khai thác lỗ hổng, leo thang đặc quyền, cài đặt mã độc hoặc chiếm quyền điều khiển.

Hệ thống thư điện tử (Email): Email là kênh giao tiếp chính trong doanh nghiệp nhưng cũng là mục tiêu của nhiều cuộc tấn công như Phishing, Business Email Compromise (BEC), phát tán mã độc và thư rác. Một tài khoản email bị xâm nhập có thể gây ảnh hưởng đến toàn bộ hệ thống.

Ngoài ra đối với một công ty có hệ thống sản xuất theo dây chuyền lớn như Samsung, công ty Samsung Display Việt Nam còn phải đối mặt với nhiều rủi ro về an toàn thông tin cơ cấu hạ tầng CNTT phức tạp, bao gồm nhiều nhà máy, nhiều chi nhánh, phòng ban, trung tâm dữ liệu và hệ thống kết nối trên diện rộng khó kiểm soát và có thể phát sinh nhiều lỗ hổng. Do vây một khi xảy ra sự cố, thiệt hại mang tới là rất lớn. Bao gồm:

Ngừng hoạt động sản xuất, kinh doanh: Các cuộc tấn công mạng như mã độc tống tiền (Ransomware) hoặc tấn công từ chối dịch vụ có thể làm gián đoạn các hệ thống mạng, khiến hệ thống phải dừng hoạt động, mất nhiều thời gian để khôi phục và khắc phục hậu quả.

Mất hoặc mã hóa dữ liệu quan trọng: Việc ngăn chặn bị đánh cắp công nghệ và dữ liệu là ưu tiên hàng đầu đối với bất cứ công ty nào. Nếu những tài liệu quan trọng như: bí mật kinh doanh, tài liệu kỹ thuật sản xuất hoặc dữ liệu hoạt động của công ty rơi vào tay hacker hoặc đối thủ, công ty sẽ phải đối mặt với nguy cơ tống tiền, cạnh tranh không lành mạnh, ảnh hưởng trực tiếp đến uy tín và hoạt động kinh doanh của doanh nghiệp.

Gián đoạn chuỗi cung ứng: Khi các hệ thống quản lý đơn hàng, kho vận hoặc kết nối với nhà cung cấp bị gián đoạn, toàn bộ chuỗi cung ứng có thể bị ảnh hưởng, dẫn đến chậm tiến độ sản xuất và giao hàng.

Ảnh hưởng đến thông tin cá nhân của nhân viên: Dữ liệu cá nhân của hàng nghìn nhân viên như thông tin định danh, thông tin cá nhân có thể bị truy cập trái phép hoặc rò rỉ nếu hệ thống bị xâm nhập, kẻ xấu có thể lừa đảo và tống tiền.

Rò rỉ dữ liệu của khách hàng và đối tác: Các thông tin về hợp đồng, dữ liệu khách hàng, bí mật kinh doanh hoặc tài liệu kỹ thuật nếu bị lộ có thể làm suy giảm uy tín của doanh nghiệp, gây mất lòng tin từ khách hàng và đối tác, đồng thời có thể dẫn đến tranh chấp pháp lý hoặc các yêu cầu bồi thường thiệt hại.

Vì vậy, việc triển khai các giải pháp giám sát an toàn thông tin và ứng phó kịp thời với các sự cố bảo mật là cần thiết đối với các doanh nghiệp. Hiện tại có rất nhiều nền tảng SIEM giúp thu thập và phân tích dữ liệu từ nhiều hệ thống, hỗ trợ phát hiện tấn công mạng, cảnh báo theo thời gian thực và nâng cao hiệu quả quản lý an toàn thông tin trong doanh nghiệp. Mặc dù các giải pháp bảo mật truyền thống như tường lửa (Firewall) hay cơ chế xác thực đã được triển khai rộng rãi, nhưng các giải pháp này chủ yếu mang tính phòng ngừa và không đủ khả năng phát hiện các hành vi tấn công phức tạp. Do đó, việc xây dựng một hệ thống phát hiện xâm nhập (IDS) đóng vai trò quan trọng trong việc giám sát, phân tích và cảnh báo sớm các hành vi xâm nhập mạng và hệ thống bất thường. Tuy nhiên các hệ thống IDS hiện nay vẫn còn tồn

tại nhiều hạn chế như: Tỷ lệ cảnh báo sai còn cao hoặc khó phát hiện các cuộc tấn công mới, chưa có mẫu (signature) và hiệu năng chưa tối ưu khi triển khai trong môi trường dữ liệu lớn hoặc thời gian thực

Xuất phát từ những vấn đề trên, việc nghiên cứu và phát triển một hệ thống phát hiện xâm nhập hiệu quả, chính xác và có khả năng để tự làm chủ là cần thiết, đặc biệt với một hệ thống sản xuất có quy mô lớn như SAMSUNG rất cần một hệ thống giám sát và phát hiện tấn công toàn diện.

2. Mục đích nghiên cứu

Hiện tại trên thế giới có rất nhiều các loại hình tấn công với nhiều mục tiêu khác nhau: đánh cắp thông tin gây gián đoạn hệ thống hoặc kiểm soát tài nguyên mạng. Một số hình thức tấn công phổ biến bao gồm [6]:

Malware (Phần mềm độc hại): Malware là thuật ngữ dùng để chỉ các chương trình hoặc đoạn mã được thiết kế nhằm xâm nhập, gây hư hại hoặc chiếm quyền kiểm soát hệ thống thông tin người dùng. Malware bao gồm nhiều loại như virus, worm, trojan, ransomware, spyware và rootkit. Sau khi xâm nhập vào hệ thống, phần mềm độc hại có thể đánh cắp dữ liệu, mã hóa tệp tin nhằm mục đích tống tiền, làm gián đoạn hoạt động hệ thống hoặc tạo cửa hậu (backdoor) duy trì quyền truy cập trái phép.

Phishing (Tấn công lừa đảo): Phishing là hình thức tấn công sử dụng các phương tiện như thư điện tử, tin nhắn hoặc trang web giả mạo nhằm đánh lừa người sử dụng cung cấp các thông tin nhạy cảm bao gồm tên đăng nhập, mật khẩu, mã xác thực hoặc thông tin cá nhân hoặc tài khoản ngân hàng.

Tấn công từ chối dịch vụ phân tán (Distributed Denial of Service - DDoS): Tấn công DDoS là hình thức sử dụng một số lượng lớn thiết bị hoặc máy tính bị kiểm soát để đồng thời gửi lưu lượng truy cập lớn đến hệ thống mục tiêu. Mục đích của cuộc tấn công là gây gián đoạn, treo hệ thống và cạn kiệt tài nguyên xử lý của người dùng.

Man-in-the-Middle (MITM): Tấn công trung gian là hình thức tấn công chen vào quá trình trao đổi dữ liệu giữa hai thực thể nhằm nghe lén, thu thập hoặc thay đổi nội dung thông tin truyền tải mà các bên không nhận biết được. Hình thức tấn công này thường xuất hiện trong các môi trường mạng không được mã hóa hoặc mạng công cộng.

SQL Injection: SQL Injection là kỹ thuật tấn công khai thác các lỗ hổng trong quá trình xử lý dữ liệu đầu vào của hệ thống. Kẻ tấn công chèn các câu lệnh SQL độc hại vào các trường nhập liệu nhằm thao túng cơ sở dữ liệu, từ đó truy xuất, chỉnh sửa hoặc xóa dữ liệu trái phép.

Cross-Site Scripting (XSS): Cross-Site Scripting là hình thức tấn công trong đó kẻ tấn công chèn các đoạn mã độc vào nội dung của ứng dụng web. Khi người dùng truy cập trang web, đoạn mã sẽ cho phép kẻ tấn công đánh cắp thông tin phiên đăng nhập (session), cookie hoặc thực hiện các thao tác trái phép dưới quyền của người dùng.

Zero-day Attack: Zero-day Attack là hình thức khai thác các lỗ hổng bảo mật chưa được nhà phát triển phần mềm phát hiện hoặc chưa phát hành bản vá khắc phục. Do chưa có giải pháp phòng vệ tương ứng, các cuộc tấn công dạng này thường gây ra mức độ rủi ro rất cao và khó bị phát hiện trong giai đoạn đầu.

Password Attack (Tấn công mật khẩu): Tấn công mật khẩu là nhóm các kỹ thuật nhằm thu thập hoặc chiếm đoạt thông tin xác thực của người dùng để truy cập trái phép vào hệ thống. Các phương pháp thường được sử dụng bao gồm dò đoán mật khẩu, sử dụng cơ sở dữ liệu mật khẩu bị rò rỉ, tấn công từ điển hoặc kết hợp với các hình thức lừa đảo khác.

Brute Force Attack: Brute Force Attack là một phương pháp tấn công mật khẩu trong đó kẻ tấn công sử dụng các công cụ tự động để thử lần lượt tất cả các tổ hợp mật khẩu có thể cho đến khi tìm được thông tin xác thực chính xác.

Drive-by Download: Là hình thức phát tán phần mềm độc hại thông qua các trang web bị nhiễm mã độc hoặc bị giả mạo. Người dùng có thể vô tình tải xuống và thực thi mã độc chỉ bằng việc truy cập vào trang web mà không cần thực hiện bất kỳ thao tác tải tệp nào.

Social Engineering (Tấn công kỹ thuật xã hội): Tấn công kỹ thuật xã hội là phương thức khai thác yếu tố con người nhằm đạt được quyền truy cập hoặc thu thập thông tin nhạy cảm. Kẻ tấn công sử dụng các thủ đoạn tâm lý như giả mạo danh tính, lợi dụng sự thiếu cảnh giác hoặc tâm lý chủ quan của người dùng để đánh cắp thông tin.

Trước những nguy cơ tiềm ẩn như trên, việc xây dựng một hệ thống giám sát bảo mật đối với một hệ thống có cơ sở hạ tầng CNTT phức tạp như công ty SAMSUNG là một thách thức vô cùng lớn. Hiện tại trong công ty đã sử dụng nhiều dịch vụ quản lý và kiểm soát hệ thống như Knox, Nasca... hầu hết chúng đều hoạt động tốt, độ an toàn bảo mật cao, cung cấp khả năng thu thập và phân tích log ưu việt, ngăn chặn nhiều nguy cơ xâm nhập, tuy nhiên những phần mềm trả tiền này có phí duy trì rất cao hoặc khi phát sinh sự cố cần bảo trì gấp việc mời chuyên gia nước ngoài ngay tức thì rất khó khăn, không kịp thời ứng phó sự cố theo thời gian thực do phần mềm thường được update định kỳ (từ 3 đến 6 tháng một lần). Do vậy các phần mềm này chỉ hỗ trợ một phần trong việc quản lý để hệ thống mạng tránh lây nhiễm mã độc, nhưng chưa toàn diện trong việc hỗ trợ doanh nghiệp xây dựng một hệ thống an toàn bảo mật toàn diện.

Mục đích nghiên cứu chính của đề án là xây dựng một hệ thống để giám sát các hoạt động kết nối hệ thống CNTT nhằm theo dõi và kiểm tra liên tục, phát hiện và ngăn chặn xâm nhập bất thường trên các hệ thống mạng, ngoài ra còn có thể giám sát log các phần mềm quan trọng, kiểm tra tính toàn vẹn của hệ thống và khả năng tích hợp cao.

3. Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu của đề tài là hệ thống công nghệ thông tin và các tài sản thông tin đang được triển khai và sử dụng tại Công ty Samsung Display Việt Nam. Nội dung nghiên cứu tập trung vào các thành phần có vai trò quan trọng trong việc bảo đảm an toàn thông tin, bao gồm:

Hệ thống hạ tầng mạng và các thiết bị phân phối mạng phục vụ kết nối, truyền dẫn và trao đổi dữ liệu trong doanh nghiệp.

Hệ thống máy tính phục vụ khối văn phòng, bao gồm các máy trạm và các thiết bị đầu cuối được sử dụng trong hoạt động quản lý, điều hành và xử lý công việc.

Hệ thống máy tính và thiết bị công nghệ phục vụ hoạt động sản xuất, bao gồm các máy tính điều khiển, giám sát và vận hành dây chuyền sản xuất.

Các tài liệu, dữ liệu và thông tin liên quan đến hoạt động sản xuất, kinh doanh và quản trị doanh nghiệp, bao gồm cả dữ liệu có cấu trúc và phi cấu trúc.

Hệ thống quản lý các phương tiện kết nối mạng và thiết bị lưu trữ thông tin nhằm giám sát, kiểm soát việc truy cập, sử dụng và trao đổi dữ liệu, góp phần ngăn ngừa nguy cơ rò rỉ, thất thoát hoặc đánh cắp thông tin.

Dựa trên việc giám sát hoạt động phân tích dữ liệu các phần mềm quan trọng để phát hiện ra điểm thay đổi, phát hiện các rủi ro bảo mật tiềm ẩn và đưa ra cảnh báo. Hiện tại WAZUH chính là một phương án cung cấp các tính năng cần thiết để phát hiện và xây dựng một hệ thống CNTT trước các mối đe dọa phổ biến hiện nay.

4. Phương pháp nghiên cứu

Đề án được nghiên cứu dựa trên cả lý thuyết và thực nghiệm. Xây dựng giao diện giám sát và kiểm tra hệ thống dựa trên dữ liệu WAZUH cung cấp.

Công cụ và thư viện: Cài đặt và cấu hình chương trình WAZUH để làm công cụ giảm sát và quản lý.

Thu thập dữ liệu: Thu thập log, dữ liệu, nhật ký hoạt động từ các thiết bị đầu cuối, các ứng dụng, trình duyệt, tường lửa, các máy chủ sử dụng mạng.

Phân tích dữ liệu: Phân tích dựa trên các log và sự kiện đã thu thập được từ các thiết bị mạng, thiết bị đầu cuối, nhật ký chương trình (logs)...

Giám sát và cảnh báo tới người quản trị hệ thống.

Xây dựng hệ thống giám sát, phát hiện và ngăn chặn xâm nhập.

Phương pháp nghiên cứu cho đề án:

Nghiên cứu tài liệu: nghiên cứu các tài liệu hướng dẫn về cách cài đặt, nắm bắt được cách sử dụng, các tình năng, hiểu sâu và chi tiết hơn về cách hoạt động của WAZUH.

Tiến hành giả lập hệ thống, trực tiếp cài đặt, mô phỏng, thiết lập cấu hình hệ thống.

Nghiên cứu thực tiễn: tiến hành thực nghiệm vận hành hệ thống trong môi trường ảo hóa để đưa ra đánh giá, nhận xét.

Xây dựng demo một chương trình quản lý và giám sát mạng dùng WAZUH để quản lý và kiểm tra tính ổn định.

II. NỘI DUNG

CHƯƠNG 1 CƠ SỞ LÝ LUẬN

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.

1.1 Tổng quan về giám sát an toàn mạng

1.1.1 Giám sát an toàn mạng là gì?

Giám sát an toàn mạng (Network Security Monitoring - NSM) 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.

Trong bối cảnh các cuộc tấn công mạng ngày càng tinh vi và phức tạp, việc giám sát an toàn mạng giúp các đơn vị chủ động phát hiện các hành vi bất thường, truy cập trái phép, nguy cơ rò rỉ dữ liệu và nhiều vấn đề khác trước khi chúng gây ra thiệt hại nghiêm trọng.

1.1.2. Mục tiêu của giám sát an toàn mạng

Giám sát an toàn mạng được triển khai nhằm đảm bảo khả năng phát hiện, theo dõi, đánh giá và ứng phó kịp thời đối với các nguy cơ và sự cố an ninh mạng trong hệ thống thông tin của tổ chức. 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. Các mục tiêu chính của giám sát an toàn mạng bao gồm:

Phát hiện sớm các sự cố và nguy cơ mất an toàn thông tin

Một trong những mục tiêu quan trọng của hệ thống giám sát an toàn mạng là phát hiện sớm các sự cố và các nguy cơ có thể ảnh hưởng đến an toàn thông tin của tổ chức. Việc giám sát liên tục giúp nhận diện các dấu hiệu tấn công ngay từ giai đoạn đầu, qua đó kịp thời để triển khai các biện pháp xử lý trước khi sự cố lan rộng. Bên

cạnh đó, hệ thống giám sát còn hỗ trợ phát hiện các lỗ hổng bảo mật tồn tại trong hạ tầng mạng, hệ điều hành hoặc các ứng dụng, từ đó giúp tổ chức chủ động khắc phục trước khi các lỗ hổng này bị khai thác đồng thời cảnh báo kịp thời về các nguy cơ mất an toàn thông tin, góp phần giảm thiểu rủi ro đối với hệ thống mạng.

Theo dõi trạng thái hoạt động của hệ thống mạng và các thiết bị mạng

Giám sát an toàn mạng cho phép theo dõi liên tục trạng thái hoạt động của hệ thống mạng và máy chủ nhằm đảm bảo hệ thống luôn vận hành ổn định và liên tục. Thông qua việc giám sát, tổ chức có thể nhanh chóng phát hiện các dấu hiệu bất thường, xác định nguyên nhân gây ra sự cố qua đó triển khai các biện pháp khắc phục kịp thời.

Thu thập và lưu trữ nhật ký hệ thống (Log)

Thu thập và lưu trữ nhật ký hệ thống sẽ ghi nhận toàn bộ quá trình hoạt động của hệ điều hành, ứng dụng, thiết bị mạng, các thiết bị đầu cuối, tạo nguồn dữ liệu phục vụ cho công tác giám sát, điều tra và phân tích sự cố, cho phép truy vết các hoạt động đã diễn ra, qua đó xác định nhanh chóng nguyên nhân gây ra sự cố cũng như hỗ trợ quá trình khôi phục sau sự cố.

Hỗ trợ đánh giá mức độ tuân thủ các chính sách và quy định về an toàn thông tin

Hệ thống giám sát an toàn mạng hỗ trợ tổ chức trong việc đánh giá mức độ tuân thủ các chính sách, quy trình và quy định về an toàn thông tin đã được ban hành. Thông qua việc thu thập và phân tích dữ liệu giám sát, tổ chức có thể kiểm tra việc thực hiện các chính sách bảo mật, đánh giá mức độ đáp ứng các tiêu chuẩn an toàn thông tin và phát hiện các điểm chưa phù hợp trong quá trình vận hành hệ thống.

Bên cạnh đó, dữ liệu thu thập từ hệ thống giám sát cung cấp cơ sở để xây dựng các phương án ứng cứu sự cố, cải thiện năng lực phòng thủ và nâng cao khả năng phục hồi của hệ thống sau tấn công. Điều này góp phần giảm thiểu thiệt hại đối với tài sản thông tin, dữ liệu, hạ tầng mạng và các dịch vụ công nghệ thông tin, đồng thời bảo đảm các thuộc tính cốt lõi của an toàn thông tin, bao gồm **tính bí mật (Confidentiality)**, **tính toàn vẹn (Integrity)** và **tính sẵn sàng (Availability)** của hệ thống.

1.1.3. Các thành phần chính của hệ thống giám sát an toàn mạng

Nguồn dữ liệu giám sát là thành phần đầu vào quan trọng của hệ thống giám sát an toàn mạng, cung cấp các thông tin cần thiết để theo dõi trạng thái hoạt động, phát hiện các hành vi bất thường và phân tích các sự cố an ninh mạng. Thành phần chính của hệ thống giám sát bao gồm:

Thiết bị mạng

Các thiết bị mạng như router, switch và firewall là nguồn cung cấp dữ liệu quan trọng phục vụ giám sát an toàn mạng. Các thiết bị này liên tục ghi nhận thông tin về trạng thái hoạt động, lưu lượng truyền tải, các phiên kết nối, thay đổi cấu hình, cũng như các sự kiện liên quan đến chính sách kiểm soát truy cập và bảo mật. Việc thu thập và phân tích dữ liệu từ các thiết bị mạng giúp theo dõi tình trạng hoạt động của hạ tầng mạng, phát hiện các dấu hiệu bất thường hoặc các hành vi vi phạm chính sách bảo mật. Đồng thời, đây cũng là cơ sở để đánh giá hiệu quả hoạt động của hệ thống mạng và kịp thời xử lý các sự cố phát sinh.

Hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS)

Hệ thống phát hiện xâm nhập (Intrusion Detection System – IDS) và hệ thống ngăn chặn xâm nhập (Intrusion Prevention System – IPS) là các thành phần chuyên dụng trong việc giám sát và bảo vệ hệ thống mạng trước các hành vi tấn công. IDS có chức năng phân tích lưu lượng và phát hiện các dấu hiệu xâm nhập hoặc hành vi bất thường, trong khi IPS có khả năng tự động thực hiện các biện pháp ngăn chặn đối với các mối đe dọa đã được xác định. Dữ liệu do IDS/IPS cung cấp bao gồm thông tin về địa chỉ IP nguồn và đích, phương thức tấn công, mức độ nghiêm trọng và các hành động xử lý đã được thực hiện, giúp hệ thống giám sát nhanh chóng nhận diện các mối đe dọa và hỗ trợ đưa ra các biện pháp ứng phó kịp thời.

Dữ liệu lưu lượng mạng (Network Traffic)

Dữ liệu lưu lượng mạng phản ánh toàn bộ quá trình trao đổi thông tin giữa các thiết bị trong hệ thống mạng mạng bao gồm các gói tin, lưu lượng truyền tải và hành vi giao tiếp giữa các thiết bị, qua đó có thể phát hiện các dấu hiệu bất thường mà dữ liệu nhật ký thông thường không thể hiện đầy đủ. Phân tích lưu lượng mạng giúp nhận diện các hoạt động như quét cổng (Port Scanning), truyền dữ liệu bất thường,

giao tiếp với máy chủ điều khiển từ xa, tấn công từ chối dịch vụ (DDoS), hoặc hành vi rò rỉ dữ liệu ra bên ngoài. Đây là nguồn dữ liệu có giá trị đặc biệt trong việc phát hiện các mối đe dọa nâng cao (Advanced Persistent Threat - APT) và các cuộc tấn công có chủ đích.

Hệ thống thu thập và lưu trữ dữ liệu: Thành phần này có chức năng thu thập dữ liệu từ nhiều nguồn như: log chương trình, ứng dụng, nhật ký hoạt động từ các thiết bị đầu cuối, trình duyệt, tường lửa, các máy chủ sử dụng mạng, nhật ký hệ điều hành… sau đó chuẩn hóa và lưu trữ dữ liệu từ nhiều nguồn khác nhau nhằm phục vụ cho quá trình phân tích và truy vấn. Dữ liệu sau khi thu thập được xử lý và tổ chức theo cấu trúc phù hợp để đảm bảo hiệu quả khai thác.

Hệ thống phân tích và phát hiện: Từ những dữ liệu, data log đầu vào để kiểm tra và đưa ra các số liệu, data theo các tiêu chuẩn bảo mật nhằm hỗ trợ người sử dụng kiểm soát và đánh giá về hệ thống CNTT đang sử dụng. sau đó dùng giải pháp phát hiện hành vi bất thường dựa trên luật hoặc trí tuệ nhân tạo để cảnh báo về các lỗ hổng, nguy cơ mất an toàn mạng có thể xảy ra. Hệ thống cũng thu thập dữ liệu tương quan sự kiện từ nhiều nguồn dữ liệu để đảm bảo tính bao quát và khách quan.

Hệ thống cảnh báo và ứng phó

Gửi cảnh báo khi phát hiện nguy cơ hoặc sự cố: Giám sát liên tục các sự kiện, nhật ký (logs) và hoạt động trên mạng. Khi phát hiện các dấu hiệu bất thường dựa trên các quy tắc và chỉ báo đã được cấu hình, hệ thống sẽ tự động tạo và gửi cảnh báo đến đội ngũ quản trị thông qua các kênh như email, tin nhắn hoặc bảng điều khiển (dashboard). Điều này giúp phát hiện sớm và kịp thời triển khai các biện pháp xử lý.

Hỗ trợ điều tra và xử lý sự cố: Sau khi thu thập, lưu trữ và tổng hợp dữ liệu từ nhiều nguồn để phục vụ quá trình điều tra, hệ thống sẽ chuẩn hóa, liên kết các dữ liệu và cung cấp thông tin nhằm hỗ trợ người sử dụng nhanh chóng xác định nguyên nhân, phạm vi ảnh hưởng, phương thức tấn công và đưa ra biện pháp khắc phục phù hợp, đồng thời hỗ trợ truy vết và điều tra.

Tự động hóa một số quy trình ứng phó:

Hiện nay các doanh nghiệp đều có các phương án cho phép tự động thực hiện các quy trình tự sửa chữa lỗi hoặc áp dụng quy trình ứng phó được xây dựng sẵn khi

phát sinh lỗi hệ thống, sự cố hoặc đứng trước các mối đe dọa an toàn thông tin. Các phương pháp thường được sử dụng nhất bao gồm: Cô lập thiết bị, chặn kết nối độc hại, thông báo cho quản trị viên và tự động khởi động các phương án sao lưu và khôi phục (Backup & Recovery).

Việc tự động hóa giúp giảm hạn chế sự phụ thuộc vào thao tác thủ công và giảm thiểu sai sót trong quá trình xử lý, đồng thời giảm thiểu thời gian gián đoạn và thiệt hại cho doanh nghiệp.

Việc kết hợp dữ liệu từ nhiều nguồn khác nhau giúp hệ thống giám sát xây dựng được bức tranh toàn diện về trạng thái hoạt động của hạ tầng công nghệ thông tin. Các nguồn dữ liệu này không chỉ cung cấp các dữ liệu hoạt động của hệ thống mà còn phục vụ hiệu quả cho việc phát hiện ra các nguy cơ và rủi ro tiềm ẩn trong hệ thống, qua đó góp phần ứng phó với các sự cố an toàn thông tin, đảm hoạt động ổn định và an toàn của hệ thống thông tin trong doanh nghiệp.

1.1.4 Vai trò của giám sát an toàn mạng

Giám sát an toàn mạng đóng vai trò quan trọng trong việc bảo vệ hệ thống công nghệ thông tin của doanh nghiệp trước các mối đe dọa an ninh mạng ngày càng gia tăng và phức tạp. Đối với doanh nghiệp, giám sát an toàn mạng góp phần bảo vệ các tài sản thông tin quan trọng như dữ liệu khách hàng, dữ liệu sản xuất, tài liệu nội bộ và các hệ thống nghiệp vụ trọng yếu. Việc giám sát liên tục giúp giảm thiểu rủi ro từ các cuộc tấn công mạng như mã độc, mã độc tống tiền, truy cập trái phép và đánh cắp dữ liệu. Đồng thời, giải pháp này giúp đảm bảo ba mục tiêu cốt lõi của an toàn thông tin là **tính bí mật (Confidentiality), tính toàn vẹn (Integrity)** và **tính sẵn sàng (Availability)**. Bên cạnh đó, hệ thống giám sát an toàn mạng còn hỗ trợ hiệu quả cho công tác quản trị, vận hành và kiểm toán hệ thống thông tin. Ngoài vai trò phát hiện và cảnh báo, giám sát an toàn mạng còn góp phần nâng cao năng lực phòng thủ chủ động của doanh nghiệp. Khi được kết hợp với các giải pháp như SIEM, IDS/IPS, EDR và các nền tảng tự động hóa phản ứng sự cố (SOAR), hệ thống có thể phát hiện sớm các mối đe dọa, hỗ trợ ứng phó nhanh chóng và giảm thiểu tối đa thiệt hại do các cuộc tấn công mạng gây ra. Đây là một trong những thành phần không thể thiếu trong chiến lược bảo đảm an toàn thông tin của các doanh nghiệp hiện đại.

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. IDS tập trung vào việc phát hiện và cảnh báo các sự kiện bất thường, trong khi IPS không chỉ phát hiện mà còn có khả năng tự động ngăn chặn các mối đe dọa trong thời gian thực.

1.2.1. Hệ thống phát hiện xâm nhập (IDS)

Hệ thống phát hiện xâm nhập (Intrusion Detection System – IDS) là một giải pháp an toàn thông tin được sử dụng để giám sát, phát hiện và cảnh báo các hoạt động bất thường hoặc có dấu hiệu tấn công vào hệ thống mạng và máy chủ. IDS không trực tiếp ngăn chặn các cuộc tấn công mà có nhiệm vụ phát hiện sớm, ghi nhận thông tin, khi phát hiện sự kiện bất thường, IDS sẽ ghi nhận và gửi cảnh báo cho quản trị viên để tiến hành điều tra và xử lý. IDS có chức năng giám sát liên tục lưu lượng mạng và các hoạt động diễn ra trên máy chủ, ứng dụng cũng như các thiết bị đầu cuối nhằm phát hiện kịp thời những hành vi bất thường hoặc các hoạt động vi phạm chính sách bảo mật. IDS hoạt động dựa trên tập luật (Rules) được xây dựng sẵn hoặc các mô hình phân tích để so sánh với dữ liệu thu thập được, từ đó nhận diện các dấu hiệu của các cuộc tấn công mạng.

Bên cạnh chức năng giám sát, IDS còn có khả năng phân tích dữ liệu nhằm phát hiện các hành vi xâm nhập thông qua nhiều phương pháp khác nhau như so khớp chữ ký (Signature-based Detection), phát hiện bất thường (Anomaly-based Detection) và phân tích hành vi (Behavior-based Detection). Nhờ đó, hệ thống có thể nhận diện nhiều hình thức tấn công phổ biến như quét cổng (Port Scanning), tấn công Brute Force, khai thác lỗ hổng bảo mật, phát tán mã độc, truy cập trái phép và nhiều mối đe dọa khác. Khi phát hiện một sự kiện đáng ngờ, IDS sẽ ghi nhận đầy đủ các thông tin liên quan như: thời gian xảy ra, địa chỉ IP nguồn và đích, loại tấn công, mức độ nghiêm trọng và các thông tin kỹ thuật khác đồng thời hệ thống sẽ tạo cảnh báo và gửi đến quản trị viên thông qua giao diện quản lý, email hoặc các phương thức

thông báo khác, giúp bộ phận quản trị có thể nhanh chóng xác minh và xử lý sự cố trước khi chúng gây ảnh hưởng đến hệ thống. Ngoài ra, dữ liệu nhật ký (Log) do IDS thu thập còn đóng vai trò quan trọng trong công tác điều tra và phân tích sự cố an toàn thông tin. Các bản ghi này giúp xác định nguyên nhân, thời điểm và phạm vi ảnh hưởng của cuộc tấn công, đồng thời hỗ trợ quá trình điều tra số, đánh giá mức độ thiệt hại và cải thiện các chính sách bảo mật. Nhờ đó, doanh nghiệp có thể nâng cao khả năng phát hiện sớm, tăng cường năng lực phòng thủ và chủ động ứng phó với các mối đe dọa an ninh mạng trong tương lai. Việc triển khai IDS giúp doanh nghiệp nâng cao khả năng giám sát an toàn thông tin, phát hiện sớm các nguy cơ bảo mật và hỗ trợ xây dựng một môi trường CNTT an toàn, ổn định và đáng tin cậy.

PHÂN LOẠI IDS

1. Hệ thống phát hiện xâm nhập dựa trên mạng (Network-based IDS – NIDS)

NIDS được triển khai tại các vị trí trọng yếu trong mạng để giám sát và phân tích lưu lượng truyền qua mạng. NIDS có thể giám sát được nhiều thiết bị cùng lúc và phát hiện các cuộc tấn công từ bên ngoài mạng tuy nhiên chúng khó phân tích dữ liệu đã được mã hóa và hiệu quả có thể giảm trong môi trường có lưu lượng lớn.

Ví dụ: Snort, Suricata.

2. Hệ thống phát hiện xâm nhập dựa trên máy chủ (Host-based IDS – HIDS)

HIDS được cài đặt trực tiếp trên máy chủ hoặc máy trạm để giám sát hoạt động nội bộ của hệ thống giúp theo dõi chi tiết các hoạt động trên thiết bị và phát hiện thay đổi tập tin, tiến trình và cấu hình hệ thống, tuy nhiên nhược điểm của hệ thống là gây tiêu tốn tài nguyên của thiết bị và cần triển khai trên từng máy cần giám sát.

Ví dụ: Wazuh, OSSEC.

1.2.2. Hệ thống ngăn chặn xâm nhập (IPS)

Hệ thống ngăn chặn xâm nhập (Intrusion Prevention System – IPS) là giải pháp bảo mật có khả năng giám sát lưu lượng mạng theo thời gian thực, được triển khai trực tiếp trên đường truyền mạng hoặc tích hợp vào các thiết bị bảo mật nhằm phát hiện và tự động ngăn chặn các hành vi tấn công ngay khi chúng xảy ra. Khác với

IDS chỉ có chức năng phát hiện và cảnh báo, IPS được triển khai trực tiếp có khả năng chủ động thực hiện các hành động phòng vệ và xử lý các nguy cơ độc hại ngay khi phát hiện như chặn gói tin, ngắt kết nối hoặc cô lập thiết bị bị tấn công. Điều này giúp giảm thiểu nguy cơ bị xâm nhập và hạn chế tối đa thiệt hại do các mối đe dọa an ninh mạng gây ra.

Một trong những chức năng quan trọng của IPS là giám sát và phân tích liên tục lưu lượng mạng đi qua hệ thống. IPS kiểm tra nội dung, đặc điểm và hành vi của các gói tin để phát hiện những hoạt động bất thường hoặc các hành vi vi phạm chính sách bảo mật. Hệ thống sử dụng nhiều kỹ thuật phát hiện khác nhau như so khớp chữ ký (Signature-based Detection), phát hiện bất thường (Anomaly-based Detection) và phân tích hành vi (Behavior-based Detection) nhằm nhận diện các hình thức tấn công phổ biến như quét cổng (Port Scanning), Brute Force, SQL Injection, Cross-Site Scripting (XSS), khai thác lỗ hổng, phát tán mã độc và các hành vi truy cập trái phép. Khi phát hiện lưu lượng có dấu hiệu nguy hiểm, IPS sẽ tự động thực hiện các biện pháp phòng vệ mà không cần sự can thiệp của quản trị viên. Tùy theo chính sách được cấu hình, hệ thống có thể chặn các gói tin độc hại, hủy kết nối đang diễn ra, khóa địa chỉ IP nguồn, giới hạn lưu lượng hoặc áp dụng các quy tắc bảo mật nhằm ngăn chặn cuộc tấn công tiếp tục lan rộng. Khả năng phản ứng tự động này giúp rút ngắn thời gian xử lý sự cố và giảm thiểu nguy cơ ảnh hưởng đến các hệ thống quan trọng.

Nhờ kết hợp khả năng phát hiện và ngăn chặn theo thời gian thực, IPS góp phần bảo vệ hệ thống mạng trước nhiều hình thức tấn công hiện đại, đảm bảo tính sẵn sàng, duy trì hoạt động ổn định và giảm thiểu rủi ro mất mát dữ liệu cho doanh nghiệp. Khi được triển khai cùng với các giải pháp bảo mật khác như Firewall, IDS và hệ thống SIEM, IPS giúp hình thành mô hình phòng thủ nhiều lớp (Defense in Depth), nâng cao hiệu quả giám sát và tăng cường khả năng bảo vệ toàn diện cho hạ tầng công nghệ thông tin của doanh nghiệp.

Một trong những biện pháp phổ biến là **chặn địa chỉ IP nguồn tấn công**. Khi xác định một địa chỉ IP có hành vi độc hại như quét cổng, Brute Force hoặc khai thác lỗ hổng, IPS sẽ tự động đưa địa chỉ IP đó vào danh sách chặn để ngăn mọi kết nối tiếp theo đến hệ thống. Bên cạnh đó, IPS có khả năng **hủy bỏ các gói tin độc hại**

trước khi chúng đến máy chủ hoặc thiết bị đích. Các gói tin chứa mã khai thác, mã độc hoặc dữ liệu vi phạm chính sách bảo mật sẽ bị loại bỏ ngay trên đường truyền. Trong trường hợp phát hiện các phiên kết nối có dấu hiệu bất thường hoặc nguy hiểm, IPS có thể **đóng các phiên kết nối đáng ngờ** nhằm ngăn chặn kẻ tấn công tiếp tục khai thác hệ thống hoặc đánh cắp dữ liệu. Biện pháp này đặc biệt hiệu quả đối với các cuộc tấn công đang diễn ra theo thời gian thực.

Ngoài các hành động ngăn chặn tự động, IPS còn **gửi cảnh báo đến quản trị viên** thông qua giao diện quản lý, email hoặc các hệ thống giám sát tập trung như SIEM. Các cảnh báo này cung cấp thông tin chi tiết về thời gian xảy ra sự kiện, địa chỉ IP liên quan, loại tấn công và mức độ nghiêm trọng, giúp quản trị viên nhanh chóng đánh giá và đưa ra phương án xử lý phù hợp.

Cuối cùng, IPS có thể **cập nhật danh sách đen (Blacklist)** bằng cách bổ sung các địa chỉ IP, tên miền hoặc nguồn phát tán mã độc đã được xác định là nguy hiểm giúp hệ thống chủ động ngăn chặn các kết nối từ những nguồn độc hại trong tương lai.

1.2.3. Các phương pháp phát hiện xâm nhập

1. Phát hiện dựa trên chữ ký (Signature-based Detection)

Phát hiện dựa trên chữ ký là phương pháp nhận diện các mối đe dọa bằng cách so sánh dữ liệu thu thập được với cơ sở dữ liệu chứa các mẫu nhận dạng (signature) đã được biết trước. Các mẫu nhận dạng này được xây dựng dựa trên đặc điểm của các cuộc tấn công đã được phân tích và xác định trước đó. Khi hệ thống phát hiện dữ liệu hoặc hành vi có sự trùng khớp với một chữ ký trong cơ sở dữ liệu, sự kiện sẽ được đánh dấu là nguy cơ mất an toàn thông tin và phát sinh cảnh báo để phục vụ quá trình xử lý. .

2. Phát hiện dựa trên bất thường (Anomaly-based Detection)

Phát hiện dựa trên bất thường là phương pháp xây dựng mô hình hành vi bình thường của hệ thống, người dùng hoặc lưu lượng mạng, sau đó so sánh các hoạt động thực tế với mô hình đã thiết lập để phát hiện các dấu hiệu khác biệt. Những hành vi có mức độ sai lệch vượt quá ngưỡng cho phép sẽ được xem là có khả năng là dấu hiệu của một cuộc tấn công hoặc sự cố an toàn thông tin. Phương pháp này thường

ứng dụng các kỹ thuật thống kê, học máy (Machine Learning) hoặc trí tuệ nhân tạo (Artificial Intelligence) nhằm phân tích dữ liệu và xác định các mẫu hành vi bất thường trong hệ thống.

1.2.4. Vai trò của IDS/IPS trong hệ thống an toàn thông tin

IDS và IPS đóng vai trò quan trọng trong chiến lược phòng thủ nhiều lớp của tổ chức:

1. Phát hiện sớm các cuộc tấn công mạng

Hệ thống có khả năng giám sát và phân tích các dữ liệu được cung cấp từ các nguồn dữ liệu có sẵn qua đó phát hiện sớm được các dấu hiệu bất thường, rủi ro hoặc nguy cơ tiềm ẩn đối với hệ thống mạng của doanh nghiệp. Việc phát hiện kịp thời giúp hệ thống bảo vệ an ninh nhanh chóng triển khai các biện pháp ngăn chặn, hạn chế tối đa ảnh hưởng và rủi ro tới hệ thống.

2. Giảm thiểu nguy cơ xâm nhập trái phép

Dựa vào việc phân tích, đối chiếu dữ liệu đầu vào với các hành vi, quy tắc có sẵn hoặc chữ ký áp dụng vào các cơ chế phát hiện, hệ thống ATTT có thể giúp nhận diện sớm các hoạt động truy cập trái phép, khai thác lỗ hổng hoặc các điểm yếu bảo mật. Khi phát hiện các dấu hiệu xâm nhập bất thường, hệ thống sẽ gửi cảnh báo hoặc phối hợp với các giải pháp bảo mật khác để kịp thời ngăn chặn các rủi ro an toàn thông tin và góp phần giảm thiểu nguy cơ và rủi ro xâm nhập vào hệ thống dẫn đến việc bị đánh cắp dữ liệu thông tin hoặc lây nhiễm mã độc ...

3. Hỗ trợ giám sát liên tục hệ thống thông tin

Hệ thống thực hiện giám sát 24/7 đối với các thiết bị mạng, máy chủ, ứng dụng và các thành phần trong hạ tầng công nghệ thông tin. Dữ liệu được thu thập và phân tích liên tục nhằm theo dõi trạng thái hoạt động, phát hiện bất thường và hỗ trợ đánh giá mức độ an toàn của hệ thống, giúp nâng cao khả năng quản trị và vận hành.

4. Cung cấp dữ liệu phục vụ điều tra và phân tích sự cố

Hệ thống ATTT sẽ thu thập, lưu trữ và chuẩn hóa các dữ liệu từ các nguồn cung cấp khác nhau như nhật ký hệ thống (log), ứng dụng lưu lượng mạng, các thiết bị đầu cuối và các sự kiện bảo mật. Khi xảy ra sự cố, các dữ liệu này chính là các yếu tố quan trọng được sử dụng để phân tích và tìm ra nguyên nhân gây phát sinh sự cố,

truy vết quá trình tấn công, đánh giá được phạm vi ảnh hưởng và hỗ trợ quá trình điều tra, xử lý sự cố cũng như lưu trữ bằng chứng số khi cần thiết.

5. Nâng cao khả năng ứng phó trước các mối đe dọa an ninh mạng

Thông qua việc cung cấp thông tin cảnh báo kịp thời, hỗ trợ phân tích sự cố và tích hợp với các giải pháp ứng phó như SOAR, tường lửa hoặc hệ thống quản lý sự kiện bảo mật (SIEM), hệ thống giúp rút phát hiện và xử lý sự cố trong thời gian nhanh nhất, nâng cao hiệu quả ứng phó trước các mối đe dọa an ninh mạng, đồng thời giảm thiểu tối đa ảnh hưởng tiêu cực tác động đến hoạt động của tổ chức.

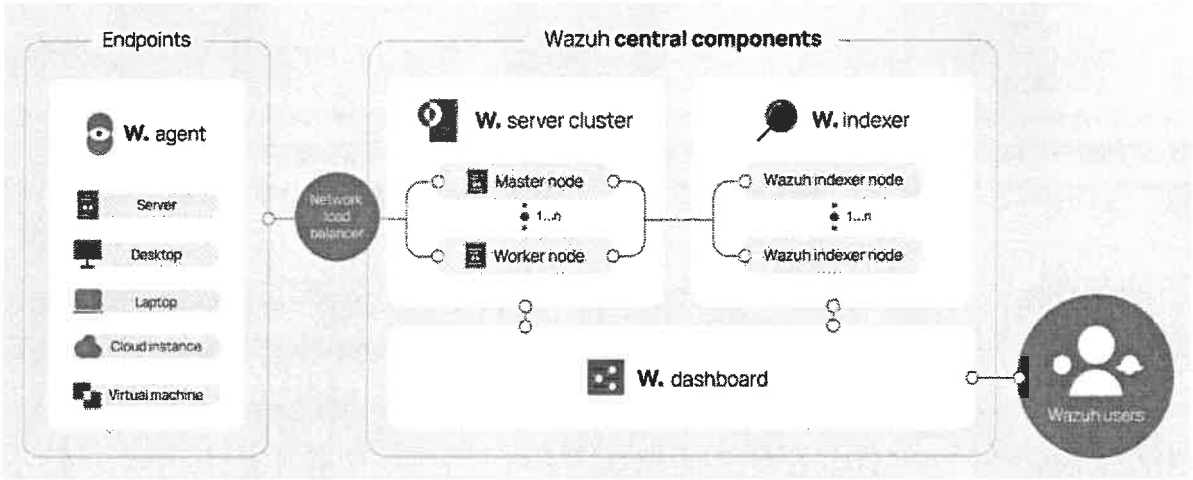
1.2.5. Giới thiệu một số hệ thống, công cụ phục vụ cho giám sát và phát hiện xâm nhập

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. Các công cụ này có thể được triển khai độc lập hoặc kết hợp để xây dựng hệ thống giám sát an toàn mạng hoàn chỉnh. Dưới đây là một số giải pháp phổ biến.

1. Wazuh

Wazuh là một nền tảng mã nguồn mở được phát triển nhằm hỗ trợ giám sát, phát hiện và ứng phó với các mối đe dọa an ninh mạng. Nền tảng này tích hợp nhiều chức năng như Hệ thống phát hiện xâm nhập trên máy chủ, quản lý thông tin và sự kiện an ninh và phát hiện và phản ứng mở. Nhờ đó, Wazuh cho phép giám sát tập trung các máy chủ và thiết bị đầu cuối, đồng thời thu thập, phân tích và trực quan hóa dữ liệu nhật ký phục vụ công tác giám sát an toàn thông tin.

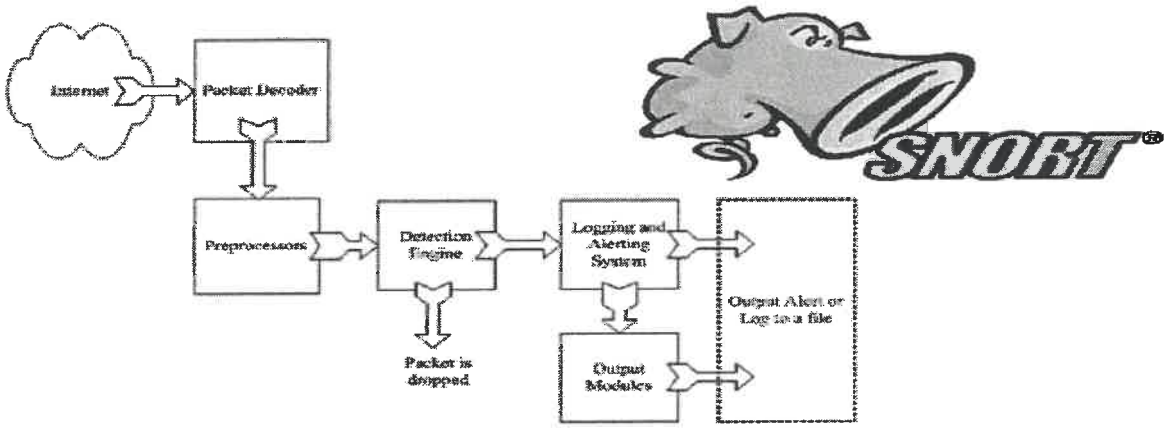
Với khả năng tích hợp với các nền tảng như ELK Stack hoặc OpenSearch, Wazuh được triển khai rộng rãi trong các doanh nghiệp, tổ chức và trung tâm điều hành an ninh mạng (Security Operations Center - SOC) nhằm nâng cao hiệu quả phát hiện, điều tra và ứng phó với các sự cố an ninh mạng.



Hình 1.1: Phương thức hoạt động của WAZUH [1]

2. Snort

Snort là một hệ thống **Phát hiện và Ngăn chặn Xâm nhập Mạng (Intrusion Detection and Prevention System - IDS/IPS)** mã nguồn mở được phát triển nhằm giám sát lưu lượng mạng và phát hiện các hoạt động bất thường hoặc các cuộc tấn công mạng. Snort cung cấp nhiều chức năng quan trọng trong việc giám sát và bảo vệ an ninh mạng, bao gồm: Giám sát lưu lượng mạng theo thời gian thực, Phát hiện xâm nhập dựa trên chữ ký, ngăn chặn tấn công (IPS), ghi nhật ký và tạo cảnh báo, Snort có thể nhận diện nhiều loại mối đe dọa như quét cổng, tấn công từ chối dịch vụ (DoS), khai thác lỗ hổng, tấn công ứng dụng web và các hành vi xâm nhập khác. Cấu trúc luồng xử lý của Snort bao gồm 4 thành phần chính: Bộ bắt gói tin (**Packet Decoder**): Lấy các gói tin thô (Raw Packets) từ giao diện mạng.Bóc tách, phân tích các lớp giao thức (IP, TCP, UDP, ICMP) và chuẩn bị dữ liệu cho các bước tiếp theo. **Preprocessors** (Tiền xử lý): Sửa đổi/chuẩn hóa dữ liệu mạng và phát hiện các điểm bất thường trước khi đối chiếu quy tắc. Giúp chống lại các kỹ thuật tấn công lẩn tránh (evasion techniques). **Detection Engine** (Bộ phát hiện): Trái tim của Snort. Nó so sánh từng gói tin với các Quy tắc (Rule Base) được định nghĩa từ trước.Nếu gói tin khớp với quy tắc độc hại, nó sẽ chuyển sang bước tạo cảnh báo (Alert).Bộ **Output Modules / Logger** (ghi log và xuất cảnh báo):Ghi lại nhật ký các gói tin vi phạm.Gửi cảnh báo đến quản trị viên qua email, cơ sở dữ liệu (MySQL), Syslog, hoặc kích hoạt khối IP trên firewall.



Hình 1.2: Phương thức hoạt động của Snort [8]

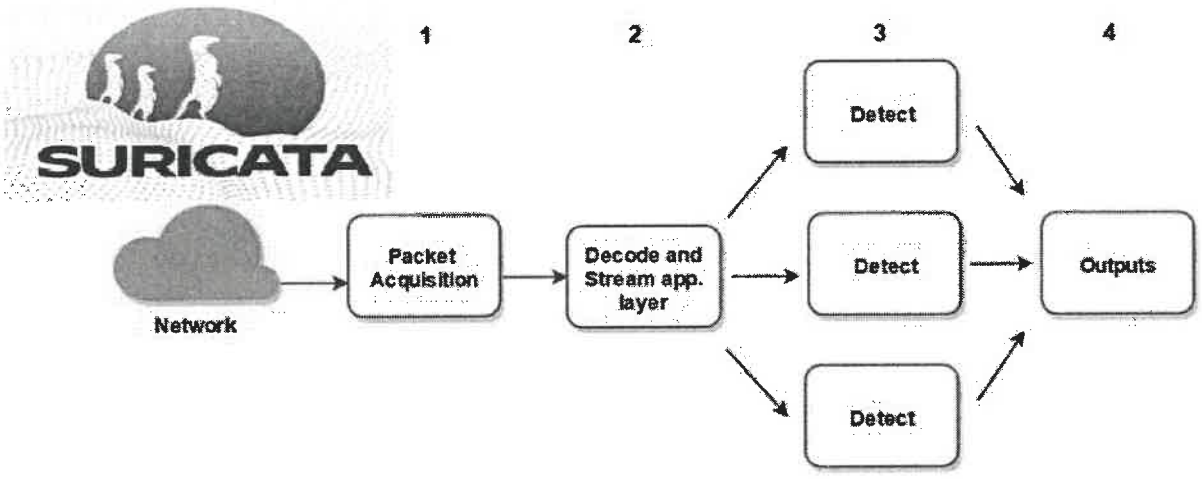
Snort có khả năng mở rộng và tùy chỉnh cho phép người quản trị xây dựng và cập nhật các quy tắc phát hiện phù hợp với đặc điểm của hệ thống, đồng thời tích hợp với các nền tảng SIEM như Wazuh, ELK Stack, Splunk và IBM QRadar để nâng cao hiệu quả giám sát và phân tích an ninh. Nhờ tính linh hoạt, hiệu quả và cộng đồng người dùng lớn, Snort được triển khai rộng rãi trong các hệ thống mạng của doanh nghiệp, tổ chức giáo dục, cơ quan chính phủ cũng như các trung tâm điều hành an ninh mạng (Security Operations Center - SOC).

3. Suricata

Suricata là một hệ thống **Phát hiện và Ngăn chặn Xâm nhập Mạng** mã nguồn mở thế hệ mới, được phát triển bởi **Open Information Security Foundation (OISF)**. Công cụ được thiết kế nhằm giám sát lưu lượng mạng theo thời gian thực, phát hiện các hành vi tấn công và hỗ trợ ngăn chặn các mối đe dọa an ninh mạng. Suricata được xây dựng trên kiến trúc xử lý đa luồng cho phép tận dụng hiệu quả tài nguyên của các bộ xử lý đa nhân, từ đó nâng cao hiệu suất xử lý lưu lượng mạng tốc độ cao. Bên cạnh cơ chế phát hiện dựa trên chữ ký, Suricata còn hỗ trợ phân tích giao thức ứng dụng, phát hiện bất thường và trích xuất siêu dữ liệu (Metadata), giúp tăng cường khả năng giám sát và điều tra các sự kiện an ninh.

Hoạt động của Suricata được vận hành theo mô hình đường ống tuyến tính đa luồng, phân tách dữ liệu thô từ tầng vật lý đến tầng ứng dụng qua 5 giai đoạn độc lập như sau: Ban đầu, Sutricara sẽ thực hiện thu thập gói tin **(Packet Acquisition)** bằng cách khai thác các bộ thư viện hiệu năng cao (AF_PACKET, PF_RING, DPDK) để

sao chép trực tiếp các gói tin thô (raw packets) từ tầng liên kết dữ liệu (Network Interface Card) vào bộ nhớ đệm của hệ thống, giảm thiểu tối đa tỷ lệ bỏ sót gói tin ở băng thông lớn, sau đó Suricata sẽ tiến hành giải mã và chuẩn hóa **(Decode & Normalize)**, sau đó trích xuất cấu trúc các trường thông tin trong Header (IP, TCP, UDP). Giai đoạn này thực hiện chuẩn hóa dữ liệu (như giải mã URL mã hóa, xử lý khoảng trắng) nhằm phá vỡ các kỹ thuật ngụy trang, che giấu mã độc của kẻ tấn công. Tiếp theo, hệ thống sẽ thực hiện theo dõi luồng và tái ráp **(Stream & Flow Tracking)** để thực hiện quản lý trạng thái kết nối dựa trên cơ chế bắt tay 3 bước (TCP Three-way Handshake). Các gói tin đơn lẻ được sắp xếp và tái ráp lại theo đúng trình tự thời gian tạo thành một phiên giao dịch (Session) hoàn chỉnh, chống lại các kỹ thuật tấn công phân mảnh (Fragmentation Attacks). Tại bước tiếp theo, Suricata thực hiện chức năng phân tích giao thức ứng dụng (Protocol Parsing): Áp dụng kỹ thuật phân tích sâu gói tin (Deep Packet Inspection - DPI) để định danh các giao thức tầng ứng dụng (HTTP, DNS, TLS, SMB) dựa trên đặc tính nội dung thay vì số cổng (Port). Từ đó trích xuất các siêu dữ liệu (Metadata) quan trọng như tên miền, tệp tin đính kèm hoặc chứng thư số, sau đó hệ thống sẽ sử dụng các thuật toán tìm kiếm chuỗi song song tốc độ cao **(Detection Engine)** để đối chiếu toàn bộ dữ liệu đã xử lý với tập luật định sẵn (Signatures/Rules), từ đó đưa ra quyết định xử lý lưu lượng theo cấu hình.



Hình 1.3: Các bước hoạt động của Suricata [9]

Ngoài những tính năng như hỗ trợ giám sát theo thời gian thực và có thể định danh nhiều giao thức, Suricata cũng có chức năng ghi nhật ký và tạo cảnh báo và có

thể tích hợp với các nền tảng SIEM như Wazuh, ELK Stack, Splunk và IBM Qradar để góp phần xây dựng hệ thống giám sát an ninh mạng tập trung và nâng cao hiệu quả phát hiện, phân tích cũng như ứng phó với các mối đe dọa.

4. OSSEC

OSSEC (Open Source Security Event Correlator) là một hệ thống **Phát hiện Xâm nhập trên Máy chủ** mã nguồn mở, được phát triển nhằm giám sát và bảo vệ các máy chủ trước các mối đe dọa an ninh mạng. Hệ thống hoạt động dựa trên mô hình máy chủ – tác nhân (Manager – Agent), cho phép thu thập và phân tích dữ liệu từ nhiều máy chủ tập trung, từ đó phát hiện các hành vi bất thường và các dấu hiệu xâm nhập. Quy trình hoạt động của OSSEC như sau:

Bước 1: Phát hiện tại Agent: OSSEC Agent quét liên tục hệ thống, phát hiện sự thay đổi file (FIM) hoặc hành vi đăng nhập sai nhiều lần tại tệp cục bộ /var/log/auth.log.

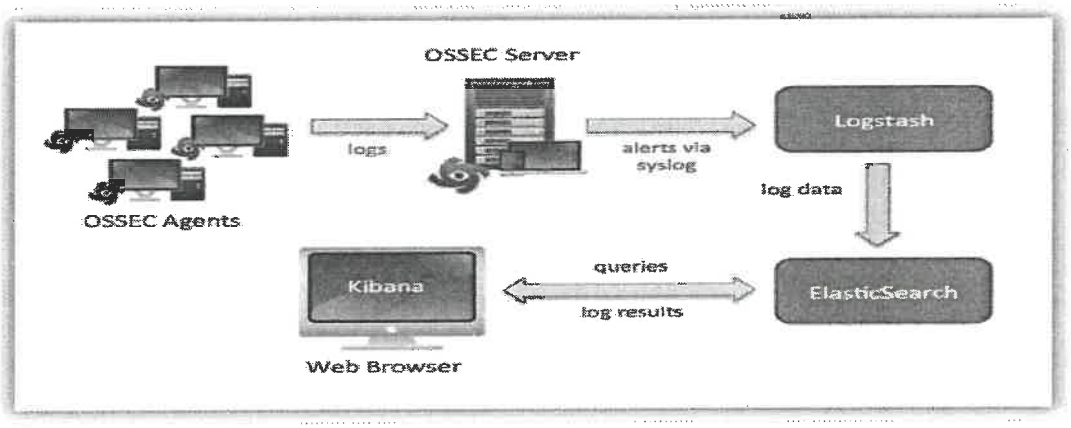
Bước 2: Xử lý tập trung tại Server: Toàn bộ log thô được gửi về **OSSEC Server**. Server khớp rule, nếu phát hiện tấn công sẽ kích hoạt *Active Response* (ví dụ: chặn IP) đồng thời ghi nhận cảnh báo vào file nhật ký dạng cấu trúc đặt tại thư mục /var/ossec/logs/alerts.

Bước 3: Thu thập bằng Logstash: Logstash **đọc** trực tiếp tệp alerts.json này. Nó thực hiện bóc tách, bổ sung thêm các trường dữ liệu hữu ích (ví dụ: gắn tọa độ địa lý GeoIP dựa trên IP của kẻ tấn công) để tăng độ phong phú cho log.

Bước 4: Lưu trữ tại Elasticsearch: Logstash đẩy dữ liệu đã làm sạch sang **Elasticsearch**. Tại đây, dữ liệu được đánh chỉ mục (indexing) siêu nhanh, giúp việc truy vấn hàng triệu bản ghi diễn ra trong vài phần giây.

Bước 5: Trực quan hóa tại Kibana: Quản trị viên không cần đọc file log text thủ công. **Kibana** sẽ kéo dữ liệu từ Elasticsearch để hiển thị biểu đồ tròn (phân loại biểu đồ mã lỗi), biểu đồ cột (tần suất tấn công theo giờ), hoặc bản đồ thế giới ghi nhận vị trí nguồn tấn công. Với khả năng phân tích nhật ký, giám sát tính toàn vẹn của tệp tin và phát hiện rootkit, OSSEC được triển khai rộng rãi trong các hệ thống doanh nghiệp nhằm nâng cao khả năng giám sát và bảo vệ an toàn thông tin. Ngoài ra OSSEC có khả năng tích hợp với các nền tảng SIEM như ELK Stack, Splunk và

IBM QRadar để tập trung dữ liệu nhật ký, nâng cao khả năng giám sát, phân tích và điều tra các sự kiện an ninh mạng và hỗ trợ giám sát nhiều hệ điều hành như Windows, Linux và macOS.



Hình 1.4: Các bước hoạt động của OSSEC [10]

5. ELK Stack

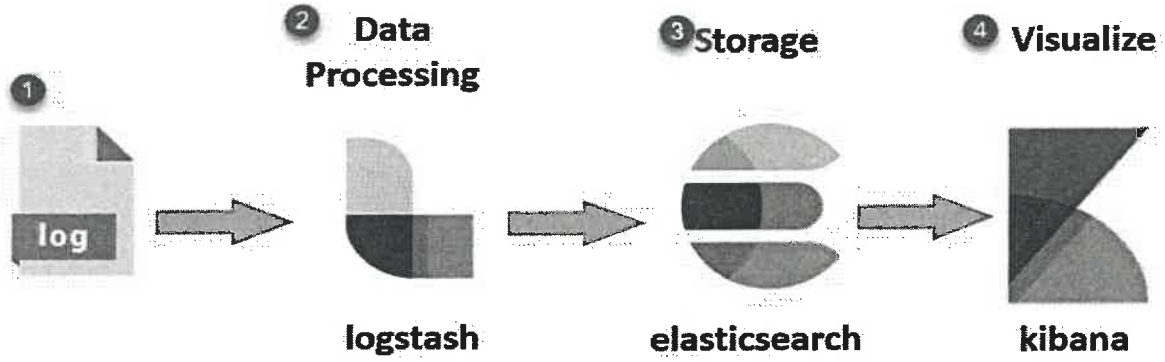
ELK Stack là một bộ công cụ mã nguồn mở được sử dụng để thu thập, xử lý, lưu trữ, tìm kiếm và trực quan hóa dữ liệu nhật ký (log). Bộ công cụ này bao gồm ba thành phần chính là **Elasticsearch**, **Logstash** và **Kibana**, phối hợp với nhau để xây dựng một nền tảng quản lý và phân tích dữ liệu tập trung.

Bước 1: Thu thập dữ liệu: Logstash thu thập log từ nhiều nguồn khác nhau và chuẩn hóa dữ liệu.

Bước 2: Xử lý dữ liệu: Logstash tiền xử lý dữ liệu bằng cách phân tích, chuyển đổi và làm giàu thông tin trước khi lưu trữ.

Bước 3: Lưu trữ dữ liệu: Dữ liệu sau xử lý được lưu vào Elasticsearch dưới dạng các chỉ mục (Index), giúp tìm kiếm và truy vấn nhanh chóng.

Bước 4: Truy vấn và trực quan hóa (Data Query & Visualization)



Hình 1.5: Sơ đồ hoạt động của ELK [12]

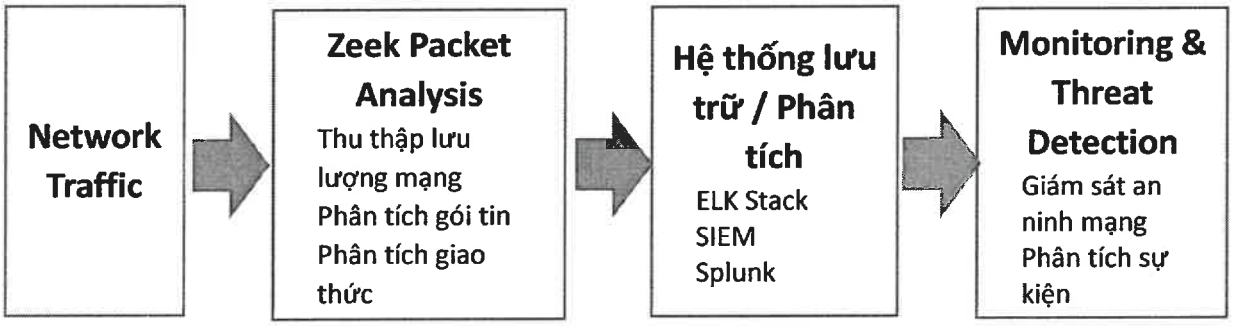
Kibana kết nối với Elasticsearch để truy vấn, phân tích và trực quan hóa dữ liệu thông qua các biểu đồ, bảng thống kê và dashboard. Nhờ đó, người dùng dễ dàng giám sát hệ thống, qua phân tích log có thể đánh giá hiệu năng và nhận diện các dấu hiệu bất thường trong hoạt động của hệ thống và theo dõi sự kiện, phát hiện bất thường một cách trực quan, nhanh chóng và hiệu quả.

Nhờ khả năng xử lý khối lượng dữ liệu lớn theo thời gian thực, ELK Stack được ứng dụng rộng rãi trong quản trị hệ thống, giám sát hạ tầng công nghệ thông tin, phân tích hiệu năng ứng dụng và giám sát an toàn thông tin. Trong lĩnh vực an ninh mạng, ELK Stack thường được tích hợp với các công cụ như Wazuh, Suricata hoặc Filebeat để xây dựng hệ thống SIEM. ELK Stack cũng hỗ trợ giám sát an ninh mạng và có thể mở rộng linh hoạt để đáp ứng nhu cầu xử lý và lưu trữ dữ liệu trong các hệ thống có quy mô từ nhỏ đến rất lớn.

6. Zeek

Zeek là một nền tảng giám sát an toàn mạng mã nguồn mở, được thiết kế để phân tích chuyên sâu lưu lượng mạng và phát hiện các hoạt động bất thường. Khác với các hệ thống IDS truyền thống chủ yếu dựa trên chữ ký, Zeek tập trung vào việc phân tích hành vi, trạng thái của các kết nối mạng và các giao thức ứng dụng, từ đó cung cấp thông tin chi tiết phục vụ công tác giám sát, điều tra và ứng phó sự cố an ninh mạng. Với khả năng phân tích lưu lượng mạng ở mức độ chi tiết, Zeek được triển khai rộng rãi trong các trung tâm điều hành an ninh mạng (Security Operations Center - SOC), các tổ chức nghiên cứu, doanh nghiệp và cơ quan chính phủ. **Cơ chế hoạt động của Zeek như sau:** Zeek Packet Analysis thu thập lưu lượng mạng, phân

tích các gói tin và giao thức để tạo ra các sự kiện (Events). Các sự kiện này được xử lý bằng Zeek Script nhằm tạo các tệp log có cấu trúc (như conn.log, dns.log, http.log) và phát hiện bất thường. Cuối cùng, các log được lưu trữ hoặc gửi đến các hệ thống như ELK Stack hoặc SIEM để phục vụ giám sát, phân tích và phát hiện mối đe dọa.



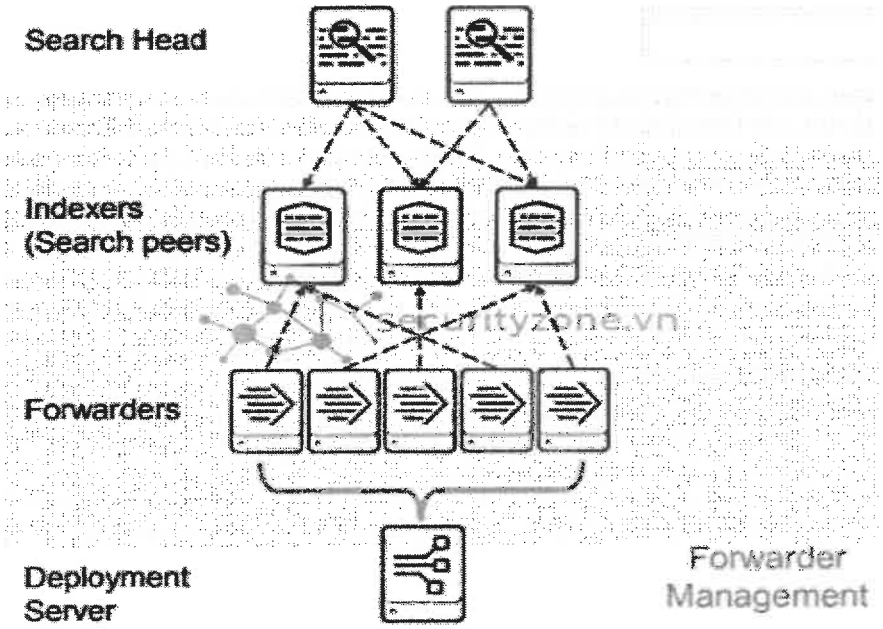
Hình 1.6: Mô hình hoạt động của Zeek [13]

Zeek cung cấp nhiều chức năng quan trọng trong việc giám sát và phân tích an ninh mạng như: Giám sát lưu lượng mạng theo thời gian thực, phân tích hành vi mạng, ngoài ra Zeek còn hỗ trợ phân tích nhiều giao thức phổ biến như HTTP, HTTPS, DNS, SMTP, FTP, SSH, TLS và DHCP giúp nhận diện các dấu hiệu bất thường ở nhiều tầng ứng dụng. Zeek cũng ghi nhật ký chi tiết để cung cấp dữ liệu phục vụ quá trình điều tra và phân tích sự cố. Zeek cũng được sử dụng để hỗ trợ phát hiện mối đe dọa và xâm nhập bất thường. Ngoài ra Zeek có thể tích hợp với các nền tảng SIEM và các công cụ phân tích bảo mật như Wazuh, ELK Stack, Splunk và IBM QRadar, góp phần xây dựng hệ thống giám sát an ninh mạng tập trung và nâng cao hiệu quả phát hiện, điều tra cũng như ứng phó với các sự cố bảo mật.

7. Splunk

Splunk là một nền tảng phân tích dữ liệu máy được thiết kế để thu thập, lưu trữ, lập chỉ mục và phân tích dữ liệu được tạo ra từ các hệ thống công nghệ thông tin. Dữ liệu này bao gồm nhật ký hệ thống (logs), sự kiện (events), lưu lượng mạng và các dữ liệu vận hành khác phát sinh từ máy chủ, thiết bị mạng, ứng dụng và môi trường điện toán đám mây. Nhờ khả năng xử lý và phân tích dữ liệu theo thời gian thực, Splunk được ứng dụng rộng rãi trong nhiều lĩnh vực như quản trị hạ tầng công nghệ thông tin (IT Operations), giám sát hiệu năng ứng dụng (Application Monitoring), DevOps và an toàn thông tin. Trong lĩnh vực an ninh mạng, Splunk cung

cấp giải pháp Splunk Enterprise Security (Splunk ES), một nền tảng SIEM hỗ trợ giám sát, phát hiện và điều tra các sự kiện an ninh mạng. Các bước tiến hành:



Hình 1.7: Mô hình hoạt động của Slunk [11]

Bước 1: Thu thập dữ liệu: Splunk thu thập dữ liệu từ nhiều nguồn thông qua các thành phần như **Universal Forwarder**, **Heavy Forwarder** hoặc nhận trực tiếp từ các giao thức như Syslog, HTTP Event Collector (HEC), API… Dữ liệu thu thập có thể là log hệ thống, log ứng dụng, sự kiện bảo mật, lưu lượng mạng hoặc dữ liệu hiệu năng.

Bước 2: Chuyển tiếp dữ liệu (Data Forwarding) Các Forwarder gửi dữ liệu về máy chủ Splunk, trong quá trình này, dữ liệu có thể được lọc, định tuyến hoặc chuyển đổi định dạng trước khi truyền lại đến Indexer.

Bước 3: Lập chỉ mục và lưu trữ (Indexing) tiếp nhận dữ liệu, thực hiện: phân tích cú pháp, trích xuất các trường dữ liệu (Field Extraction), gắn dấu thời gian (Timestamping) sau đó nén và lưu dữ liệu vào các chỉ mục. Việc lập chỉ mục giúp Splunk tìm kiếm dữ liệu nhanh và hiệu quả.

Bước 4: Tìm kiếm và phân tích (Search & Analytics): Search Head sử dụng ngôn ngữ truy vấn SPL (Search Processing Language) để tìm kiếm dữ liệu, phân tích các sự kiện, thống kê và trực quan hóa dữ liệu, sau đó tạo Dashboard và báo cáo.

Bước 5: Cảnh báo và giám sát (Alerting & Monitoring) Dựa trên các truy vấn SPL hoặc điều kiện được cấu hình trước, Splunk có thể phát hiện các hành vi bất thường, gửi cảnh báo qua email hoặc các hệ thống tích hợp, sau đó hỗ trợ điều tra sự cố và giám sát an ninh mạng theo thời gian thực.

Splunk có khả năng tích hợp với nhiều giải pháp và thiết bị bảo mật khác nhau như Firewall, IDS/IPS, Endpoint Detection and Response (EDR), hệ thống quản lý danh tính (IAM) và các nền tảng điện toán đám mây, góp phần xây dựng một hệ sinh thái giám sát và bảo vệ an toàn thông tin toàn diện.

8. IBM QRadar

IBM QRadar là một nền tảng Quản lý Thông tin và Sự kiện An ninh (SIEM) do IBM phát triển, được thiết kế nhằm hỗ trợ các tổ chức trong việc giám sát, phát hiện và ứng phó với các mối đe dọa an ninh mạng. Hệ thống cho phép thu thập, lưu trữ và phân tích dữ liệu nhật ký từ nhiều nguồn khác nhau, từ đó cung cấp khả năng giám sát an ninh tập trung và theo thời gian thực. Hệ thống có thể tự động đánh giá mức độ nghiêm trọng của các sự kiện bảo mật và ưu tiên các cảnh báo theo mức độ rủi ro, giúp đội ngũ vận hành an ninh tập trung xử lý các mối đe dọa có ảnh hưởng lớn trước. Ngoài ra Qradar còn có chức năng phân tích hành vi của người dùng, thiết bị và các hoạt động trên mạng nhằm phát hiện các dấu hiệu bất thường, góp phần nhận diện các hành vi xâm nhập hoặc lạm dụng quyền truy cập.

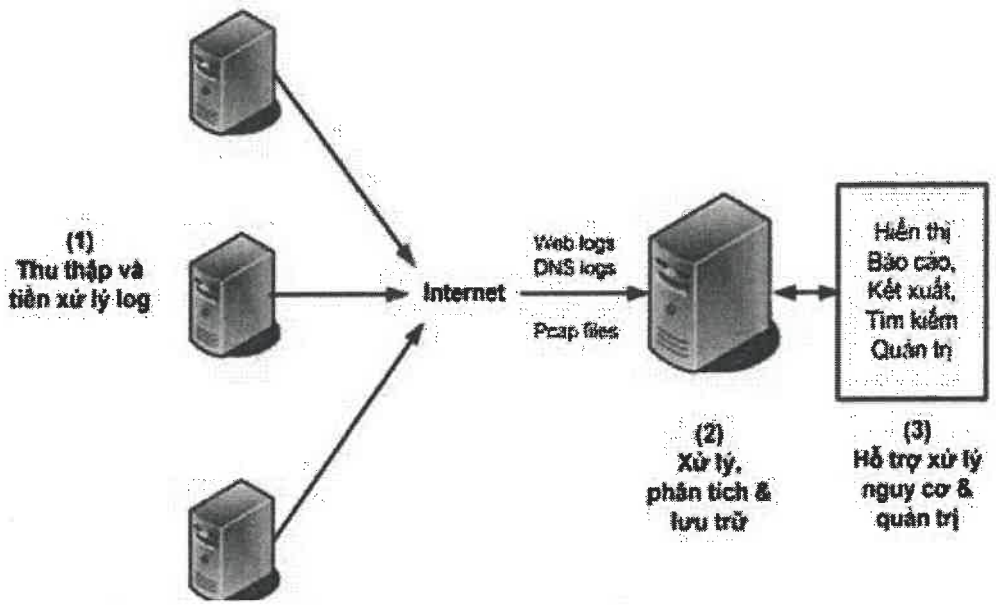
IBM QRadar hoạt động theo 4 bước chính:

Bước 1: Thu thập dữ liệu hệ thông nhận log và luồng mạng (flow) từ firewall, server, IDS/IPS, ứng dụng ...

Bước 2: Xử lý dữ liệu hệ thống chuẩn hóa dữ liệu về cùng định dạng, sau đó tiến hành phân tích và trích xuất thông tin quan trọng

Bước 3: Tương quan sự kiện (Correlation) Kết hợp nhiều sự kiện để phát hiện hành vi tấn công hoặc bất thường, đông thời áp dụng luật (rules) và thông tin tài sản (asset)

Bước 4: Hiển thị & cảnh báo Tạo Offense (sự cố bảo mật), hiển thị dashboard và gửi cảnh báo cho SOC



Hình 1.8: Mô hình hoạt động của IBM Qradar [14]

Nhờ khả năng phân tích chuyên sâu và tích hợp với nhiều giải pháp bảo mật khác nhau, IBM QRadar được triển khai rộng rãi trong các tổ chức có yêu cầu cao về an toàn thông tin như ngân hàng, cơ quan chính phủ, doanh nghiệp lớn và các trung tâm điều hành an ninh mạng (Security Operations Center - SOC). Đồng thời, QRadar hỗ trợ tạo các báo cáo phục vụ yêu cầu tuân thủ các tiêu chuẩn và quy định về an toàn thông tin như PCI DSS, ISO/IEC 27001, HIPAA và GDPR.

Công cụ	**Nhóm chức năng**	**Mã nguồn**	**Phạm vi giám sát**	**Khả năng SIEM**	**IDS/IPS**	**Phân tích log**	**Quản lý lỗ hổng**	**Mức độ triển khai**
Wazuh	HIDS + SIEM + XDR	Mã nguồn mở	Host + log + cloud	Có	Có (HIDS-based)	Mạnh	Có	Trung bình
ELK Stack	Log management	Mã nguồn mở	Log tập trung	Không (cần tích hợp)	Không	Rất mạnh	Không	Trung bình

Công cụ	Nhóm chức năng	Mã nguồn	Phạm vi giám sát	Khả năng SIEM	IDS/IPS	Phân tích log	Quản lý lỗ hổng	Mức độ triển khai
Splunk Enterprise Security	SIEM thương mại	Có phí	Toàn hệ thống	Rất mạnh	Không trực tiếp	Rất mạnh	Có (qua add-on)	Dễ–Trung bình
IBM QRadar	SIEM doanh nghiệp	Có phí	Enterprise SOC	Rất mạnh	Không trực tiếp	Mạnh	Có	Khó
Snort	IDS/IPS	Mã nguồn mở	Network	Không	Có	Hạn chế	Không	Trung bình
Suricata	IDS/IPS	Mã nguồn mở	Network	Không	Có	Hạn chế	Không	Trung bình
Zeek	Network Security Monitoring	Mã nguồn mở	Network behavior	Không	Không	Mạnh (behavior-based)	Không	Trung bình
OSSEC	HIDS	Mã nguồn mở	Host	Hạn chế	Có (HIDS)	Mạnh	Không	Thấp–Trung bình

Bảng 1.1 Bảng so sánh giữa các công cụ quét bảo mật

Lý do lựa chọn Wazuh

Trong số các công cụ được phân tích, Wazuh được lựa chọn làm giải pháp chính do khả năng đáp ứng toàn diện các yêu cầu về giám sát và bảo mật hệ thống trong một nền tảng thống nhất.

Trước hết, Wazuh tích hợp đồng thời nhiều chức năng quan trọng như HIDS, SIEM và XDR, cho phép giám sát cả ở cấp độ máy chủ (host-based) lẫn dữ liệu nhật ký (log-based). Điều này giúp giảm sự phụ thuộc vào nhiều công cụ riêng lẻ như OSSEC (HIDS), ELK Stack (log management) hay các hệ thống SIEM thương mại như Splunk và IBM QRadar. Thứ hai, Wazuh là giải pháp mã nguồn mở, giúp giảm

chi phí triển khai nhưng vẫn cung cấp đầy đủ các tính năng cần thiết cho một hệ thống giám sát an ninh mạng hiện đại. Đây là yếu tố quan trọng trong môi trường nghiên cứu, đào tạo hoặc các tổ chức có ngân sách hạn chế. Thứ ba, Wazuh có khả năng tích hợp linh hoạt với nhiều công cụ khác như ELK Stack, Suricata, Zeek và các hệ thống cloud. Nhờ đó, nó có thể mở rộng thành một kiến trúc SIEM hoàn chỉnh, đáp ứng nhu cầu thu thập, phân tích và trực quan hóa dữ liệu an ninh mạng một cách hiệu quả. Cuối cùng, Wazuh hỗ trợ đầy đủ các 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, giúp nâng cao khả năng phát hiện và phản ứng với các mối đe dọa an ninh mạng. Từ các phân tích trên, 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.

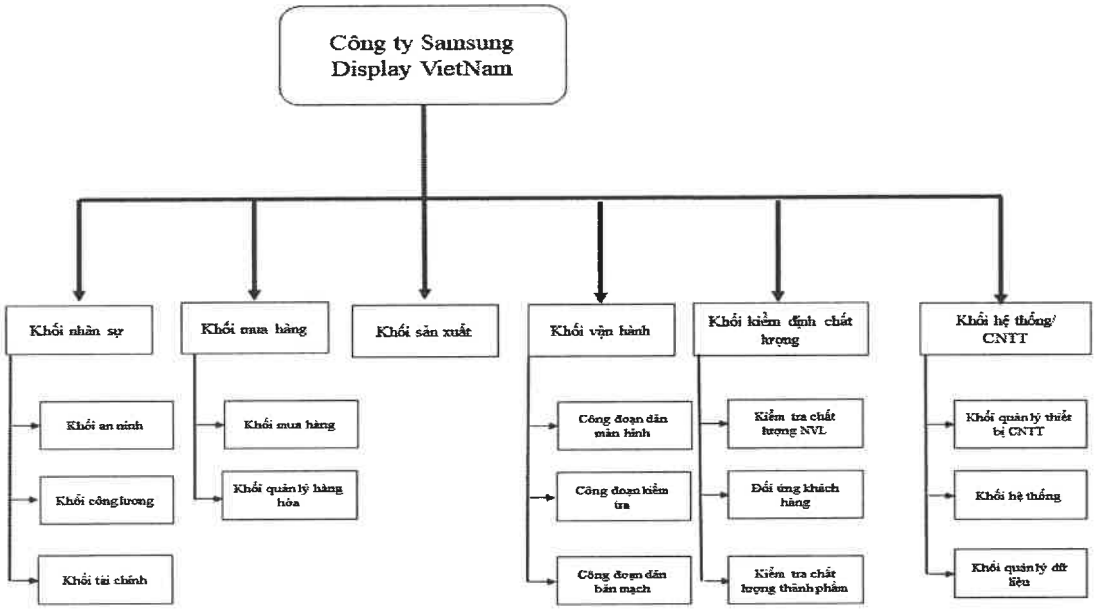
1.3. Giới thiệu về công ty TNHH Samsung Display Việt Nam

Công ty TNHH Samsung Display Việt Nam thuộc Tập đoàn Samsung của Hàn Quốc, là công ty sản xuất có quy mô lớn nhất trong hệ thống Tập đoàn Sam Sung và cũng 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…

Được thành lập tại Việt Nam từ năm 2014. Hiện tại Công ty có nhà máy sản xuất tại KCN Yên Phong, Yên Trung, Bắc Ninh với cơ cấu nhân lực là hơn 30000 nhân viên. Là một doanh nghiệp tiên phong trong lĩnh vực sản xuất màn hình, sản phẩm màn hình của công ty Samsung Display VietNam không chỉ nổi tiếng thế giời về những chiêc điện thoại có hình ảnh sống động, rõ nét mà Samsung Display VietNam còn thực hiện nhiều dự án với những đối tác quan trọng như: Apple, XiaoMi, OPPO… Tính đến năm 2026, mặc dù kinh tế thế giới đang trải qua nhiều thời kỳ thăng trầm, tình hình chính trị thế giới nhiều biến động phức tạp, các hoạt động sản xuất tại Việt Nam vẫn được duy trì tương đối ổn định. Tổng doanh thu năm 2023 (tính đến tháng 12) của SDV đạt xấp xỉ 15 tỷ USD.

Năm [1, 2, 3, 4, 5, 6]	Doanh thu (Tỷ USD)	Lợi nhuận ròng (Triệu USD)	Đặc điểm tình hình kinh doanh
2025	**~15,0**	**~650**	Giảm nhẹ 1,8% doanh thu nhưng lợi nhuận tăng trưởng ổn định trở lại.
2024	**14,28**	**588,7**	Thị trường màn hình toàn cầu bão hòa, sụt giảm cả doanh thu và lợi nhuận.
2023	**18,14**	**860**	Giai đoạn kinh tế thế giới gặp khó khăn, nhu cầu thiết bị điện tử suy giảm.
2022	**~19,9**	**~1.000**	**Đỉnh lịch sử** về doanh thu nhờ dòng màn hình OLED cao cấp bùng nổ.
2021	**19,0**	**~900**	Vượt qua dịch Covid-19 xuất sắc, ghi nhận doanh thu vượt cả nhà máy SEV Bắc Ninh.
2020	**16,3**	**500**	Chịu ảnh hưởng gián đoạn chuỗi cung ứng giai đoạn đầu dịch bệnh.

Bảng 1.2: Số liệu doanh thu công ty Samsung Display VietNam



Hình 1.9. Sơ đồ cơ cấu tổ chức công ty Samsung Display Việt Nam

1.3.1 Việc quản lý cơ sở hạ tầng CNTT tại công ty Samsung Display Việt Nam

Cơ sở hạ tầng công nghệ thông tin luôn là yếu tố đóng vai trò cốt lõi trong việc đảm bảo hoạt động sản xuất, kinh doanh và quản trị doanh nghiệp tại Công ty Samsung Display Việt Nam. Với quy mô hàng chục nghìn nhân viên cùng hệ thống dây chuyền sản xuất hiện đại, công ty phải vận hành 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. Một trong những thách thức lớn nhất của Samsung Display Việt Nam là quản lý hệ thống phục vụ đồng thời nhiều hoạt động khác nhau cùng lúc như điều hành sản xuất, chia sẻ và lưu trữ dữ liệu, quản lý tài liệu nội bộ cũng như đảm bảo an toàn thông tin. Các hệ thống này phải đảm bảo hoạt động liên tục, không có sai sót nhằm đáp ứng yêu cầu sản xuất 24/7 không gián đoạn và hỗ trợ hàng nghìn người dùng truy cập đồng thời. Để đáp ứng các yêu cầu trên, 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. Bên cạnh đó, công ty áp dụng các chính sách quản lý tài khoản người dùng, phân quyền truy cập, giám sát nhật ký hệ thống nhằm nâng cao mức độ an toàn và giảm thiểu rủi ro mất mát dữ liệu. Ngoài việc duy trì tính ổn định của hạ tầng CNTT, Samsung Display Việt Nam còn chú trọng đến công tác an toàn thông tin thông qua việc triển khai các giải pháp giám sát bảo mật, phát hiện sớm các hành vi bất thường và xử lý kịp thời các sự cố có nguy cơ ảnh hưởng đến hệ thống. Điều này giúp đảm bảo tính bảo mật, toàn vẹn và sẵn sàng của dữ liệu, đồng thời đáp ứng các tiêu chuẩn quản lý an toàn thông tin trong doanh nghiệp.

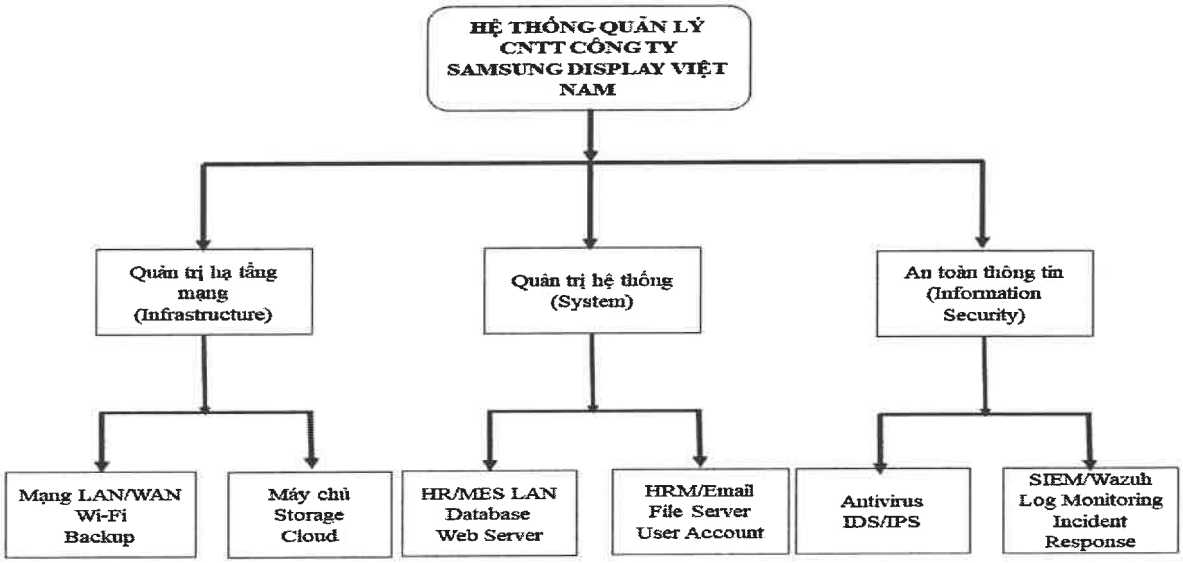
Nhờ việc đầu tư và quản lý hiệu quả cơ sở hạ tầng CNTT, Samsung Display Việt Nam có thể duy trì hoạt động sản xuất ổn định, nâng cao hiệu quả quản lý và tạo nền tảng cho quá trình chuyển đổi số trong doanh nghiệp.

1.3.2. Hệ thống quản lý CNTT của công ty Samsung Display VietNam

Một hệ thống cơ sở hạ tầng đáp ứng cho hàng nghìn người với hàng ngàn nhu cầu sử dụng khác nhau phải là giải pháp tổng thể được thiết kế và xây dựng để áp dụng cho từng đặc thù riêng biệt của mỗi tổ chức sử dụng nó. Qua phương thức vận hành có thể giúp cho từng nhân viên trong từng phòng ban với công việc khác nhau

có thể dễ dàng theo dõi thông tin, dữ liệu công việc, dữ liệu cá nhân của chính mình. Đồng thời hệ thống cũng cần có khả năng lưu trữ những dữ liệu này theo tiêu chuẩn, có khả năng chỉnh sửa và lưu trữ dữ liệu nhưng vẫn đảm bảo tính bảo mật của công việc. Tuy nhiên một cơ sở hạ tầng công nghệ thông tin rất lớn như vậy sẽ có rất nhiều lỗ hổng dễ khai thác, do vậy việc áp dụng các biện pháp an toàn thông tin để ngăn chặn xâm nhập và khai thác thông tin là điều tối cần thiết.

Hệ thống quản lý công nghệ thông tin (CNTT) tại Công ty Samsung Display Việt Nam được xây dựng theo mô hình tập trung, nhằm đáp ứng yêu cầu quản lý, vận hành và hỗ trợ hoạt động sản xuất quy mô lớn. Bộ phận Hệ thống/CNTT chịu trách nhiệm quản lý toàn bộ hạ tầng kỹ thuật, hệ thống máy chủ, mạng nội bộ, các công cụ/ ứng dụng nội bộ... Công ty áp dụng quy trình quản lý theo các tiêu chuẩn và quy định nội bộ của Tập đoàn Samsung, bao gồm quản lý tài sản CNTT, tài khoản người dùng, định danh nhân viên... Mọi hoạt động triển khai, bảo trì hoặc nâng cấp hệ thống đều được thực hiện theo quy trình kiểm soát chặt chẽ nhằm hạn chế tối đa ảnh hưởng đến hoạt động sản xuất. Hệ thống CNTT được chia ra thành hai hệ thống cơ bản là: hệ thống quản lý sản xuất (MES) và hệ thống dịch vụ văn phòng (OFFICE), hệ thống thư điện tử, lưu trữ dữ liệu, chia sẻ tài liệu giữa MES và OFFICE và các ứng dụng phục vụ mọi hoạt động tìm kiếm, tra cứu các số liệu được quản lý, các hệ thống này được kết nối thông qua mạng nội bộ tốc độ cao và được giám sát liên tục để đảm bảo hiệu suất và tính sẵn sàng. Bên cạnh công tác quản trị hệ thống, Samsung Display Việt Nam đặc biệt chú trọng đến quản lý an toàn thông tin. Công ty triển khai nhiều giải pháp bảo mật như tường lửa, hệ thống phát hiện và ngăn chặn xâm nhập, phần mềm chống mã độc, mã hóa dữ liệu, xác thực người dùng và giám sát nhật ký hệ thống. Đồng thời, các công cụ giám sát tập trung (SIEM) được sử dụng để thu thập, phân tích nhật ký từ nhiều thiết bị và phát hiện sớm các nguy cơ mất an toàn thông tin. Ngoài ra, bộ phận CNTT thường xuyên thực hiện sao lưu dữ liệu, kiểm tra khả năng khôi phục hệ thống và xây dựng các phương án dự phòng nhằm đảm bảo hoạt động của doanh nghiệp. Việc quản lý CNTT theo quy trình giúp Samsung Display Việt Nam duy trì hệ thống ổn định, nâng cao hiệu quả quản lý và đáp ứng yêu cầu phát triển trong môi trường sản xuất công nghệ cao.



Hình 1.10. Tổng quan sơ đồ cơ sở hạ tầng CNTT công ty Samsung Display Việt Nam

CHƯƠNG 2 GIỚI THIỆU VỀ HỆ THỐNG WAZUH

2.1. Giới thiệu về Wazuh

2.1.1. Wazuh là gì?

Wazuh là một nền tảng giám sát an toàn thông tin mã nguồn mở được phát triển từ dự án OSSEC. Wazuh 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 cố. Nhờ tính mã nguồn mở, miễn phí và khả năng mở rộng cao, Wazuh 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[7]:

Thu thập và phân tích nhật ký tập trung (Centralized Log Collection and Analysis)

Wazuh hỗ trợ thu thập nhật ký (log) từ nhiều nguồn dữ liệu khác nhau như hệ điều hành, máy chủ, ứng dụng, cơ sở dữ liệu, thiết bị mạng và các giải pháp bảo mật. Dữ liệu sau khi thu thập được chuẩn hóa, lưu trữ và phân tích tập trung, giúp người quản trị có cái nhìn tổng thể về trạng thái hoạt động của toàn bộ hệ thống. Thông qua cơ chế phân tích theo luật kết hợp với tương quan sự kiện, Wazuh có khả năng phát hiện các hành vi bất thường, các dấu hiệu tấn công và sinh cảnh báo theo thời gian thực, hỗ trợ quá trình điều tra và xử lý sự cố.

Phát hiện xâm nhập trên máy chủ (Host-based Intrusion Detection System - HIDS)

Wazuh tích hợp hệ thống phát hiện xâm nhập trên máy chủ, cho phép giám sát hoạt động của các máy chủ và thiết bị đầu cuối thông qua các tác nhân (Agent) được cài đặt trên từng thiết bị.

Hệ thống theo dõi các sự kiện như đăng nhập thất bại, thay đổi quyền truy cập, thay đổi cấu hình hệ thống, leo thang đặc quyền và các hành vi bất thường khác. Khi

phát hiện dấu hiệu xâm nhập hoặc vi phạm chính sách bảo mật, Wazuh sẽ sinh cảnh báo để người quản trị kịp thời xử lý.

Giám sát tính toàn vẹn tập tin (File Integrity Monitoring - FIM) Chức năng giám sát tính toàn vẹn tập tin cho phép theo dõi các thay đổi xảy ra đối với tệp tin và thư mục quan trọng trong hệ thống. Wazuh sử dụng các thuật toán băm (Hash) để kiểm tra tính toàn vẹn của tập tin, đồng thời ghi nhận các sự kiện như tạo mới, chỉnh sửa, đổi tên hoặc xóa tập tin. Khi phát hiện sự thay đổi ngoài mong muốn hoặc trái với chính sách bảo mật, hệ thống sẽ phát sinh cảnh báo để hỗ trợ điều tra và ngăn chặn nguy cơ xâm nhập hoặc phá hoại dữ liệu.

Phát hiện Rootkit và phần mềm độc hại (Malware Detection)

Wazuh cung cấp khả năng phát hiện rootkit, malware và các dấu hiệu bất thường trên hệ thống thông qua việc kiểm tra tiến trình đang chạy, dịch vụ hệ thống, cổng mạng, module nhân hệ điều hành và các thành phần quan trọng khác. Ngoài các cơ chế phát hiện tích hợp, Wazuh còn có khả năng tích hợp với nhiều công cụ chống mã độc và nền tảng phân tích mã độc nhằm nâng cao hiệu quả phát hiện và xử lý các mối đe dọa.

Quản lý lỗ hổng bảo mật (Vulnerability Management)

Wazuh hỗ trợ quản lý lỗ hổng bảo mật bằng cách thu thập thông tin về hệ điều hành, phần mềm và các gói cài đặt trên thiết bị đầu cuối, sau đó đối chiếu với các cơ sở dữ liệu lỗ hổng bảo mật đã được công bố. Thông qua quá trình này, hệ thống có thể xác định các lỗ hổng còn tồn tại, đánh giá mức độ nghiêm trọng và đưa ra cảnh báo để hỗ trợ người quản trị xây dựng kế hoạch cập nhật bản vá và giảm thiểu rủi ro đối với hệ thống.

Kiểm tra tuân thủ các tiêu chuẩn an toàn thông tin (Security Compliance Monitoring)

Wazuh hỗ trợ đánh giá mức độ tuân thủ của hệ thống đối với các tiêu chuẩn và khung quản lý an toàn thông tin thông qua chức năng Security Configuration Assessment (SCA). Hệ thống có khả năng kiểm tra cấu hình bảo mật của máy chủ và thiết bị đầu cuối, từ đó xác định các điểm chưa đáp ứng yêu cầu của các tiêu chuẩn

đã thiết lập. Kết quả đánh giá giúp tổ chức nâng cao mức độ tuân thủ và giảm thiểu các nguy cơ phát sinh từ việc cấu hình hệ thống chưa phù hợp.

Cảnh báo và hỗ trợ ứng phó sự cố

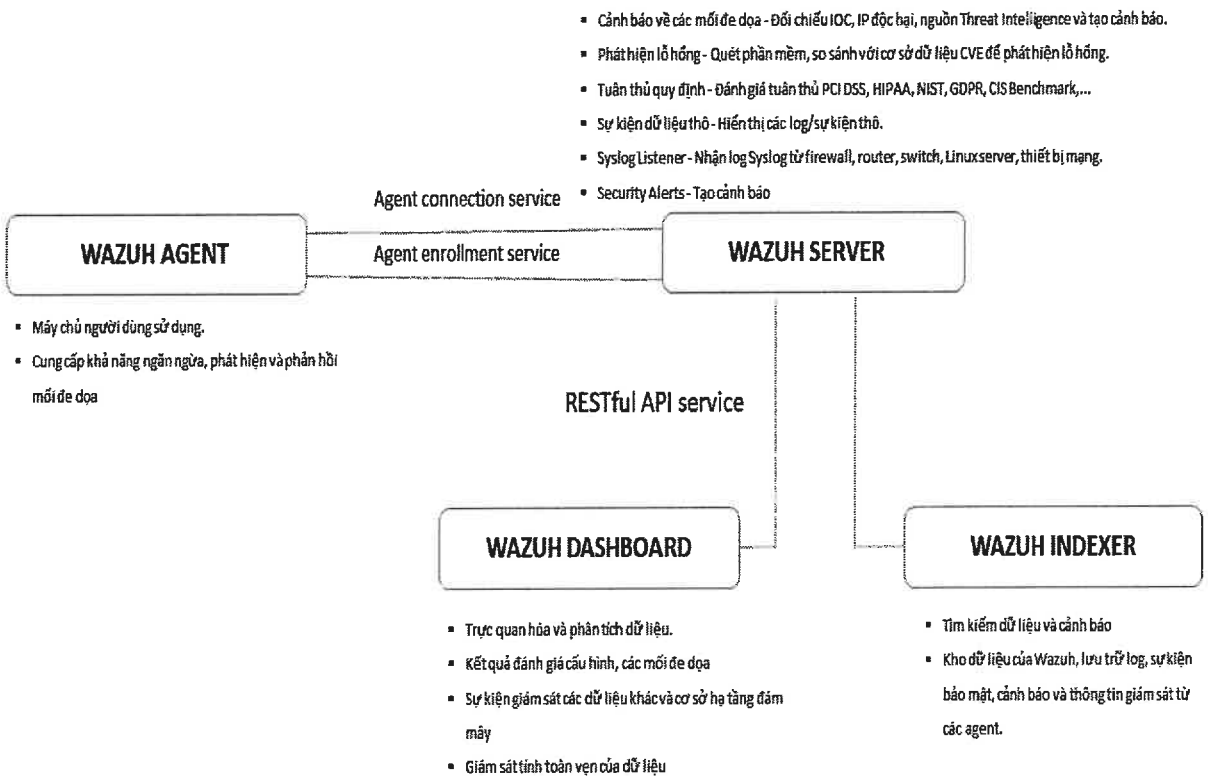
Khi phát hiện các hành vi bất thường hoặc các dấu hiệu tấn công, Wazuh sẽ sinh cảnh báo theo thời gian thực với nhiều mức độ nghiêm trọng khác nhau, giúp đội ngũ quản trị nhanh chóng nhận biết và xử lý sự cố. Ngoài khả năng cảnh báo, Wazuh còn hỗ trợ cơ chế Active Response, cho phép tự động thực hiện các hành động như chặn địa chỉ IP, khóa tài khoản người dùng, dừng tiến trình độc hại hoặc cô lập thiết bị bị xâm nhập. Việc tự động hóa quá trình ứng phó góp phần giảm thời gian xử lý và hạn chế tác động của các cuộc tấn công đối với hệ thống.

Trực quan hóa dữ liệu và điều tra sự kiện bảo mật

Wazuh cung cấp giao diện quản trị trực quan thông qua Dashboard, cho phép hiển thị thông tin về trạng thái hệ thống, cảnh báo an ninh, tình hình lỗ hổng bảo mật và kết quả giám sát dưới dạng biểu đồ, bảng thống kê và báo cáo. Các công cụ tìm kiếm và phân tích dữ liệu giúp người quản trị dễ dàng truy vấn nhật ký, tương quan sự kiện và điều tra nguyên nhân của các sự cố an ninh mạng. Điều này góp phần nâng cao hiệu quả giám sát, hỗ trợ quá trình ra quyết định và cải thiện khả năng quản lý an toàn thông tin trong doanh nghiệp.

2.1.2. Kiến trúc tổng thể của Wazuh [7][8]

Kiến trúc Wazuh được xây dựng theo mô hình phân tán gồm nhiều thành phần phối hợp với nhau để thu thập, xử lý, lưu trữ và hiển thị dữ liệu bảo mật.



Hình 2.1: Sơ đồ hệ thống Wazuh

Wazuh Agent

Wazuh Agent là thành phần được cài đặt trên các thiết bị đầu cuối nhằm thu thập dữ liệu và giám sát hoạt động của hệ thống. Agent có vai trò như một cầu nối giữa các máy được giám sát và Wazuh Server, giúp thu thập thông tin về trạng thái hệ thống, các sự kiện bảo mật và gửi dữ liệu về máy chủ để phân tích, phát hiện các dấu hiệu bất thường hoặc nguy cơ tấn công. Wazuh Agent có thể được cài đặt trên nhiều loại thiết bị và hệ điều hành khác nhau như Linux, Windows, máy trạm (Workstation) của người dùng. hoặc máy ảo trên nền tảng điện toán đám mây (Cloud). Sau khi được cài đặt, Wazuh Agent thực hiện các nhiệm vụ chính sau:

Thu thập nhật ký hệ thống (System Logs): Thu thập các bản ghi từ hệ điều hành và ứng dụng để phục vụ việc giám sát và phân tích các sự kiện bảo mật.

Giám sát tiến trình (Process Monitoring): Theo dõi các tiến trình đang hoạt động trên hệ thống nhằm phát hiện các tiến trình bất thường hoặc có dấu hiệu độc hại.

Giám sát Registry trên Windows (Registry Monitoring): Theo dõi các thay đổi trong Windows Registry để phát hiện những hành vi chỉnh sửa trái phép hoặc các thay đổi có thể ảnh hưởng đến tính bảo mật của hệ thống.

Thu thập thông tin phần mềm (Inventory): Ghi nhận danh sách phần mềm đã cài đặt trên thiết bị, hỗ trợ quản lý tài sản CNTT và phát hiện các phần mềm không được cấp phép hoặc tồn tại lỗ hổng bảo mật.

Truyền dữ liệu về Wazuh Server: Dữ liệu sau khi được thu thập sẽ được mã hóa và gửi đến Wazuh Server để lưu trữ, phân tích, đối chiếu với các quy tắc phát hiện mối đe dọa và sinh cảnh báo khi phát hiện các dấu hiệu bất thường.

Trong kiến trúc Wazuh, Agent đóng vai trò là thành phần thu thập dữ liệu tại các điểm cuối (Endpoint). Mọi thông tin về hoạt động của hệ thống được Agent ghi nhận và chuyển đến Wazuh Server để xử lý tập trung. Nhờ đó, quản trị viên có thể giám sát trạng thái của toàn bộ hệ thống, phát hiện sớm các sự cố bảo mật và đưa ra biện pháp xử lý kịp thời.

Wazuh Server

Là thành phần trung tâm trong kiến trúc Wazuh, chịu trách nhiệm tiếp nhận, xử lý và phân tích dữ liệu được gửi từ các Wazuh Agent. Dựa trên các quy tắc phát hiện đã được cấu hình, máy chủ có khả năng nhận diện các hành vi bất thường, phát hiện các mối đe dọa an ninh mạng và tạo cảnh báo để hỗ trợ quản trị viên giám sát hệ thống một cách tập trung.

Wazuh Server thực hiện các chức năng chính sau:

Tiếp nhận dữ liệu từ Wazuh Agent: Nhận các bản ghi sự kiện (log), thông tin giám sát và dữ liệu bảo mật từ các Agent được triển khai trên các thiết bị đầu cuối.

Giải mã log (Log Decoding): Phân tích cấu trúc của các bản ghi bằng các Decoder để trích xuất các trường thông tin quan trọng như địa chỉ IP, tài khoản người dùng, tiến trình, mã sự kiện và các thuộc tính liên quan.

So khớp luật phát hiện (Rules Engine): So sánh dữ liệu sau khi giải mã với tập hợp các quy tắc (Rules) nhằm phát hiện các hành vi bất thường, vi phạm chính sách bảo mật hoặc dấu hiệu tấn công.

Sinh cảnh báo (Alert Generation): Khi dữ liệu thỏa mãn điều kiện của một quy tắc, hệ thống sẽ tạo cảnh báo với các mức độ nghiêm trọng khác nhau để hỗ trợ quá trình giám sát và ứng phó sự cố.

Tương quan sự kiện (Event Correlation): Phân tích mối liên hệ giữa nhiều sự kiện xảy ra trên cùng hoặc nhiều thiết bị nhằm phát hiện các cuộc tấn công phức tạp mà một sự kiện đơn lẻ khó có thể nhận biết.

Quản lý Agent: Quản lý quá trình đăng ký, xác thực, kết nối và giám sát trạng thái hoạt động của các Wazuh Agent trong hệ thống.

Để thực hiện các chức năng trên, Wazuh Server được xây dựng từ nhiều module chuyên biệt, trong đó các module quan trọng gồm:

Analysisd: Analysisd thực hiện việc giải mã log, áp dụng các quy tắc phát hiện và tạo cảnh báo khi phát hiện các dấu hiệu bất thường hoặc hành vi đáng ngờ.

Remoted: Chịu trách nhiệm tiếp nhận dữ liệu được gửi từ các Wazuh Agent thông qua kết nối an toàn, đồng thời chuyển dữ liệu đến các module xử lý phía sau.

Authd: Quản lý quá trình đăng ký và xác thực Agent mới trước khi cho phép kết nối với Wazuh Server.

Syscheckd: Điều phối chức năng giám sát tính toàn vẹn của tập tin (File Integrity Monitoring – FIM), theo dõi các thay đổi đối với tập tin để phát hiện các hành vi chỉnh sửa trái phép.

Logcollector: Thu thập nhật ký từ các nguồn log trên chính máy chủ Wazuh hoặc các thành phần cục bộ, sau đó chuyển dữ liệu đến Analysisd để phân tích và xử lý.

Wazuh Server đóng vai trò là trung tâm điều phối và phân tích của toàn bộ hệ thống giám sát an ninh. Thành phần này tiếp nhận dữ liệu từ các Agent, xử lý thông tin bằng các bộ giải mã và tập luật, sau đó tạo cảnh báo và lưu trữ kết quả để phục vụ việc giám sát, điều tra và ứng phó sự cố. Nhờ cơ chế xử lý tập trung, Wazuh Server giúp quản trị viên theo dõi trạng thái an toàn của toàn bộ hạ tầng CNTT, phát hiện sớm các mối đe dọa và nâng cao hiệu quả quản lý an ninh mạng.

Wazuh Indexer

Wazuh Indexer là thành phần chịu trách nhiệm lưu trữ, lập chỉ mục và quản lý toàn bộ dữ liệu do Wazuh Server xử lý. Wazuh Indexer được xây dựng trên nền tảng

OpenSearch, cho phép lưu trữ khối lượng lớn dữ liệu nhật ký (log) và hỗ trợ tìm kiếm, truy vấn với hiệu năng cao. Đây là thành phần quan trọng giúp hệ thống có thể lưu giữ lịch sử sự kiện bảo mật, phục vụ công tác giám sát, điều tra và phân tích. Chức năng chính của Wazuh Indexer bao gồm:

Lưu trữ dữ liệu nhật ký (Log Storage): Tiếp nhận và lưu trữ các bản ghi sự kiện được xử lý bởi Wazuh Server, bao gồm log hệ thống, log ứng dụng, cảnh báo bảo mật và các dữ liệu giám sát khác.

Đánh chỉ mục dữ liệu (Data Indexing): Tổ chức và lập chỉ mục dữ liệu theo cấu trúc của OpenSearch, giúp tối ưu hóa quá trình truy xuất và quản lý dữ liệu.

Tìm kiếm dữ liệu tốc độ cao (High-performance Search): Cho phép tìm kiếm và truy vấn dữ liệu nhanh chóng thông qua nhiều tiêu chí như thời gian, địa chỉ IP, tên máy, mức độ cảnh báo hoặc loại sự kiện, ngay cả khi dữ liệu có dung lượng rất lớn.

Hỗ trợ phân tích dữ liệu lớn (Big Data Analytics): Xử lý và phân tích khối lượng lớn dữ liệu bảo mật được thu thập từ nhiều Agent, hỗ trợ phát hiện xu hướng, thống kê sự kiện và phục vụ điều tra sau sự cố (Forensics).

Trong kiến trúc Wazuh, Wazuh Indexer đóng vai trò là **kho lưu trữ dữ liệu tập trung**. Sau khi Wazuh Server phân tích và tạo cảnh báo, toàn bộ dữ liệu sẽ được chuyển đến Indexer để lưu trữ và lập chỉ mục. Nhờ nền tảng OpenSearch, hệ thống có khả năng truy vấn dữ liệu theo thời gian thực, đồng thời hỗ trợ mở rộng để đáp ứng nhu cầu lưu trữ và xử lý dữ liệu của các hệ thống có quy mô lớn. Đây cũng là nguồn dữ liệu để Wazuh Dashboard khai thác, trực quan hóa và hiển thị các cảnh báo, biểu đồ thống kê và báo cáo phục vụ công tác giám sát an toàn thông tin.

Wazuh Dashboard

Wazuh Dashboard là giao diện quản trị và giám sát của hệ thống Wazuh, được xây dựng trên nền tảng **OpenSearch Dashboards**. Thành phần này cung cấp môi trường trực quan để quản trị viên theo dõi trạng thái an toàn thông tin, quản lý các thiết bị được giám sát và phân tích các sự kiện bảo mật theo thời gian thực. Thông qua Dashboard, người dùng có thể dễ dàng truy cập, tìm kiếm và trực quan hóa dữ

liệu được lưu trữ trong Wazuh Indexer. Wazuh Dashboard cung cấp các chức năng chính bao gồm:

Giám sát cảnh báo (Alert Monitoring): Hiển thị các cảnh báo bảo mật do Wazuh Server tạo ra, bao gồm thông tin về mức độ nghiêm trọng, thời gian xảy ra, thiết bị bị ảnh hưởng và nội dung sự kiện.

Quản lý Agent: Cho phép theo dõi trạng thái hoạt động của các Wazuh Agent, kiểm tra kết nối, phiên bản phần mềm và thông tin của các thiết bị đang được giám sát.

Phân tích sự kiện (Event Analysis): Hỗ trợ tìm kiếm, lọc và phân tích các sự kiện bảo mật theo nhiều tiêu chí như thời gian, địa chỉ IP, tài khoản người dùng, loại sự kiện hoặc mức độ cảnh báo, giúp xác định nguyên nhân và phạm vi ảnh hưởng của sự cố.

Trực quan hóa dữ liệu (Data Visualization): Cung cấp các biểu đồ, bảng thống kê và báo cáo trực quan về tình trạng an toàn thông tin, xu hướng cảnh báo, mức độ rủi ro và các chỉ số bảo mật của hệ thống.

Điều tra sự cố (Incident Investigation): Hỗ trợ truy vết các sự kiện, phân tích chuỗi hoạt động và đối chiếu dữ liệu lịch sử nhằm phục vụ quá trình điều tra, đánh giá và xử lý các sự cố an ninh mạng.

Trong kiến trúc Wazuh, Wazuh Dashboard đóng vai trò là **giao diện tương tác giữa người quản trị và hệ thống giám sát**. Dashboard khai thác dữ liệu được lưu trữ trong Wazuh Indexer để hiển thị thông tin dưới dạng trực quan, đồng thời cho phép quản trị viên thực hiện các thao tác quản lý, theo dõi và phân tích sự kiện bảo mật một cách tập trung. Wazuh Dashboard mang lại khả năng tìm kiếm nhanh, trực quan hóa dữ liệu và hỗ trợ quá trình giám sát, phát hiện cũng như ứng phó với các mối đe dọa an toàn thông tin.

2.1.3. Luồng xử lý dữ liệu và cấu tạo luật trong Wazuh

1. Luồng xử lý dữ liệu

Quá trình xử lý dữ liệu của Wazuh được thực hiện theo một quy trình khép kín, bắt đầu từ việc thu thập dữ liệu trên các thiết bị đầu cuối, sau đó truyền về máy chủ để phân tích, phát hiện mối đe dọa sau đó lưu trữ, hiển thị kết quả trên giao diện

quản trị. Quy trình này giúp hệ thống giám sát tập trung, phát hiện sớm các sự kiện bất thường và hỗ trợ điều tra sự cố an toàn thông tin.

Bước 1: Thu thập dữ liệu

Tại các thiết bị được giám sát, Wazuh Agent thực hiện việc thu thập các thông tin và sự kiện bảo mật từ nhiều nguồn khác nhau trong hệ điều hành. Các loại dữ liệu chính bao gồm:

Nhật ký hệ điều hành, Nhật ký các ứng dụng đang sử dụng trên thiết bị, Windows Event Logs hoặc Syslog trên Linux, giám sát thay đổi tập tin, thông tin lỗ hổng bảo mật **về các phần mềm đã cài đặt.** Sau khi thu thập, dữ liệu sẽ được chuẩn hóa và chuẩn bị để gửi đến Wazuh Server.

Bước 2: Gửi dữ liệu về Wazuh Server

Dữ liệu thu thập từ Wazuh Agent được truyền đến **Wazuh Server** thông qua kết nối mạng được mã hóa nhằm đảm bảo tính bảo mật và toàn vẹn của dữ liệu trong quá trình truyền tải. Máy chủ tiếp nhận dữ liệu từ nhiều Agent khác nhau và đưa vào quy trình phân tích tập trung. Việc truyền dữ liệu theo thời gian thực giúp hệ thống nhanh chóng phát hiện các sự kiện bất thường, giảm thời gian phản ứng khi xảy ra sự cố an toàn thông tin.

Bước 3: Giải mã dữ liệu (Decoder)

Sau khi tiếp nhận dữ liệu, Wazuh Server sử dụng **Decoder** để phân tích và chuẩn hóa các bản ghi nhật ký. Đây là bước quan trọng nhằm chuyển đổi các bản ghi có định dạng khác nhau thành dữ liệu có cấu trúc thống nhất để phục vụ quá trình phân tích. Decoder thực hiện các chức năng sau:

Phân tích cú pháp log (Log Parsing): Xác định cấu trúc của từng loại log và nhận diện các trường thông tin chứa trong bản ghi.

Tách trường dữ liệu (Field Extraction): Trích xuất các thông tin quan trọng như địa chỉ IP, tài khoản người dùng, tiến trình, cổng mạng, mã sự kiện, thời gian xảy ra và các thuộc tính liên quan.

Chuẩn hóa dữ liệu (Normalization): Chuyển đổi các dữ liệu thu thập từ nhiều nguồn khác nhau về một định dạng thống nhất, tạo điều kiện cho quá trình so khớp luật (Rules Engine), tương quan sự kiện và phân tích bảo mật ở các bước tiếp theo.

Nhờ cơ chế Decoder, Wazuh có khả năng xử lý dữ liệu từ nhiều hệ điều hành, ứng dụng và thiết bị khác nhau, đồng thời nâng cao độ chính xác trong việc phát hiện các hành vi bất thường và các mối đe dọa an ninh mạng.

Bước 4: Rules Engine

Sau khi giải mã, dữ liệu được đối chiếu với tập luật phát hiện.

Ví dụ:

<rule id="5710" level="5">
<if_sid>5700</if_sid>
<match>Failed password</match>
<description>SSH authentication failed</description>
</rule>

Nếu log khớp với điều kiện của luật, hệ thống sẽ sinh cảnh báo.

Bước 5: Sinh cảnh báo

Mỗi cảnh báo được tạo ra đều chứa các thông tin quan trọng sau:

Mức độ nghiêm trọng (Alert Level): Wazuh sử dụng thang điểm từ Level 0 đến Level 15 để đánh giá mức độ nguy hiểm của sự kiện. Mức điểm càng cao thì mức độ rủi ro và mức độ ưu tiên xử lý càng lớn.

Mô tả cảnh báo (Description): Cung cấp nội dung mô tả về sự kiện được phát hiện, giúp quản trị viên nhanh chóng hiểu được bản chất của cảnh báo và nguyên nhân phát sinh.

Thời gian xảy ra (Timestamp): Ghi nhận chính xác thời điểm sự kiện được phát hiện hoặc thời điểm cảnh báo được tạo, hỗ trợ việc phân tích theo dòng thời gian và điều tra sự cố.

Nguồn phát sinh (Source): Xác định thiết bị hoặc Agent đã gửi dữ liệu tạo nên cảnh báo, bao gồm các thông tin như tên máy, địa chỉ IP, hệ điều hành hoặc dịch vụ liên quan. Điều này giúp nhanh chóng xác định vị trí xảy ra sự cố để thực hiện các biện pháp xử lý phù hợp.

Bước 6: Lưu trữ và hiển thị

Cảnh báo được gửi tới Indexer và hiển thị trên dịch vụ OpenSearch Dashboard của WAZUH.

2. Cấu tạo luật (Rules) trong Wazuh

Luật trong Wazuh được viết bằng XML được lưu trong đường dẫn: /var/ossec/etc/rules/local_rules.xml trên máy Wazuh Server. Ví dụ:

```
<group name="windows,network,">

  <!-- WFP blocked connection -->
  <rule id="100300" level="5">
    <field name="win.system.eventID">5157</field>
    <description>WFP blocked connection detected</description>
  </rule>

  <!-- Port scan detection -->
  <rule id="100301" level="12">

    <if_matched_sid>100300</if_matched_sid>

    <same_source_ip />
    <frequency>5</frequency>
    <timeframe>10</timeframe>

    <description>Possible port scan detected (WFP based)</description>

    <mitre>
      <id>T1046</id>
    </mitre>

  </rule>

</group>
```

Hình 12: Ví dụ cơ bản về cấu tạo luật trong WAZUH

Thành phần	Chức năng
rule id	Mã định danh luật
level	Mức độ cảnh báo
match	Nội dung cần phát hiện
regex	Biểu thức chính quy
if_sid	Kế thừa luật khác
frequency	Số lần xuất hiện
timeframe	Khoảng thời gian
description	Mô tả cảnh báo
group	Nhóm luật

Bảng 2.1: Các thành phần cơ bản của luật

Mức cảnh báo

Level	Ý nghĩa
Level 0–2:	Thông tin hoặc sự kiện không đáng lo ngại.
Level 3–7:	Cảnh báo mức thấp đến trung bình, phản ánh các hoạt động bất thường hoặc cần theo dõi.
Level 8–11:	Cảnh báo mức cao, có khả năng liên quan đến hành vi tấn công hoặc vi phạm chính sách bảo mật.
Level 12–15:	Cảnh báo mức rất nghiêm trọng hoặc khẩn cấp, thường liên quan đến các cuộc tấn công đang diễn ra hoặc các sự cố an ninh cần được xử lý ngay lập tức.

Bảng 2.2: Các level cảnh báo

2.1.4. Lợi ích và hạn chế của Wazuh

Lợi ích của Wazuh

Wazuh là một nền tảng giám sát và quản lý an toàn thông tin mã nguồn mở được sử dụng rộng rãi trong các tổ chức và doanh nghiệp. Với khả năng tích hợp nhiều chức năng bảo mật trong cùng một hệ thống, Wazuh mang lại nhiều lợi ích trong việc giám sát, phát hiện và ứng phó với các mối đe dọa an ninh mạng với chi phí triển khai thấp. Một trong những ưu điểm nổi bật của Wazuh là được phát triển theo mô hình mã nguồn mở (Open Source). Người dùng có thể tải xuống, cài đặt và sử dụng mà không phải trả chi phí bản quyền phần mềm. Điều này giúp các doanh nghiệp, đặc biệt là các tổ chức có ngân sách hạn chế, dễ dàng triển khai hệ thống giám sát an toàn thông tin với chi phí thấp nhưng vẫn đáp ứng được các yêu cầu về bảo mật. Ngoài ra Wazuh có thể tích hợp nhiều tính năng quan trọng trong cùng một nền tảng, giúp giảm nhu cầu sử dụng nhiều giải pháp riêng lẻ. Bao gồm:

SIEM (Security Information and Event Management): Thu thập, lưu trữ, phân tích nhật ký và quản lý các sự kiện bảo mật tập trung.

HIDS (Host-based Intrusion Detection System): Giám sát các thiết bị đầu cuối nhằm phát hiện các hành vi bất thường hoặc dấu hiệu xâm nhập.

XDR (Extended Detection and Response): Hỗ trợ mở rộng khả năng phát hiện và phản ứng với các mối đe dọa trên nhiều nguồn dữ liệu khác nhau.

FIM (File Integrity Monitoring): Theo dõi tính toàn vẹn của tập tin và phát hiện các thay đổi trái phép.

Vulnerability Detection: Kiểm tra phần mềm và hệ điều hành để phát hiện các lỗ hổng bảo mật dựa trên cơ sở dữ liệu CVE.

Nhờ sự tích hợp này, Wazuh giúp đơn giản hóa việc triển khai và quản lý hệ thống bảo mật.

Hỗ trợ đa nền tảng: Wazuh có khả năng hoạt động trên nhiều hệ điều hành và môi trường triển khai khác nhau như Linux, Windows, macOS, Docker và các nền tảng container và các dịch vụ điện toán đám mây (Cloud) như AWS, Azure và Google Cloud Platform. Khả năng tương thích đa nền tảng giúp Wazuh dễ dàng triển khai trong các hệ thống CNTT có môi trường hỗn hợp.

Khả năng mở rộng cao do được thiết kế để đáp ứng nhu cầu của cả các hệ thống nhỏ và các doanh nghiệp có quy mô lớn. Hệ thống có khả năng quản lý đồng thời hàng nghìn Wazuh Agent và hỗ trợ triển khai theo mô hình Cluster, cho phép phân tải và tăng khả năng xử lý khi số lượng thiết bị hoặc lượng dữ liệu giám sát ngày càng tăng.

Hỗ trợ hiệu quả cho Trung tâm điều hành an ninh (SOC): do Wazuh cung cấp đầy đủ các chức năng cần thiết cho hoạt động của Trung tâm điều hành an ninh (Security Operations Center – SOC), bao gồm: thu thập và quản lý nhật ký tập trung từ nhiều nguồn dữ liệu, phân tích sự kiện và phát hiện các mối đe dọa theo thời gian thực, sinh cảnh báo tự động khi phát hiện các hành vi bất thường và ỗ trợ điều tra, truy vết và ứng phó với các sự cố an toàn thông tin. Nhờ đó, Wazuh giúp nâng cao hiệu quả giám sát và rút ngắn thời gian phát hiện cũng như xử lý các sự cố bảo mật.

Hạn chế của Wazuh

Bên cạnh những ưu điểm nổi bật, Wazuh vẫn tồn tại một số hạn chế cần được cân nhắc trong quá trình triển khai và vận hành.

Yêu cầu tài nguyên hệ thống lớn khi số lượng Agent và lượng dữ liệu nhật ký tăng lên, Wazuh cần nhiều tài nguyên phần cứng hơn để đảm bảo hiệu năng hoạt động. Đặc biệt mức sử dụng CPU tăng do phải xử lý và phân tích nhiều sự kiện hoặc hu cầu RAM tăng để phục vụ việc xử lý dữ liệu theo thời gian thực và dung lượng

lưu trữ cần được mở rộng nhằm đáp ứng yêu cầu lưu giữ khối lượng lớn dữ liệu nhật ký và cảnh báo.

Quản trị và cấu hình tương đối phức tạp: Việc triển khai và tối ưu Wazuh đòi hỏi quản trị viên phải có kiến thức về hệ điều hành Linux, quản trị mạng và bảo mật. Ngoài ra, để xây dựng các chính sách phát hiện phù hợp với từng môi trường, người quản trị cần hiểu rõ cách hoạt động cũng như có khả năng tùy chỉnh các quy tắc nhằm nâng cao hiệu quả phát hiện và giảm cảnh báo không cần thiết.

Phát sinh cảnh báo giả (False Positive): Nếu tập luật chưa được tinh chỉnh phù hợp với môi trường thực tế, hệ thống có thể tạo ra nhiều cảnh báo không phản ánh các mối đe dọa thực sự. Điều này dẫn đến: gia tăng số lượng cảnh báo không cần thiết (False Positive). Do đó, việc tối ưu hóa các quy tắc phát hiện và loại bỏ các cảnh báo không cần thiết là yêu cầu quan trọng sau khi triển khai hệ thống.

Khả năng ứng dụng Machine Learning còn hạn chế: So với các giải pháp SIEM thương mại hiện đại như Microsoft Sentinel, IBM QRadar hay Splunk Enterprise Security, Wazuh vẫn còn hạn chế về các tính năng ứng dụng Machine Learning (ML) và User and Entity Behavior Analytics (UEBA). Việc phát hiện các hành vi bất thường chủ yếu dựa trên các quy tắc được định nghĩa sẵn, do đó khả năng nhận diện các cuộc tấn công mới hoặc các hành vi chưa có mẫu vẫn chưa mạnh bằng các giải pháp thương mại có tích hợp trí tuệ nhân tạo.

Kết luận:

Với ưu điểm là mã nguồn mở, chi phí triển khai thấp, tích hợp nhiều tính năng bảo mật và khả năng mở rộng tốt, Wazuh là một giải pháp phù hợp cho các tổ chức, doanh nghiệp và cơ sở đào tạo muốn xây dựng hệ thống giám sát an toàn thông tin tập trung. Tuy nhiên, để khai thác hiệu quả nền tảng này, cần có đội ngũ quản trị có chuyên môn, đồng thời thường xuyên tối ưu các quy tắc phát hiện và đầu tư hạ tầng phù hợp nhằm đảm bảo hiệu năng và giảm thiểu các cảnh báo giả.

2.1.5. Các công cụ nền tảng sử dụng để triển khai và thử nghiệm giải pháp

Để xây dựng mô hình giám sát an toàn mạng bằng Wazuh, có thể sử dụng bộ công cụ sau:

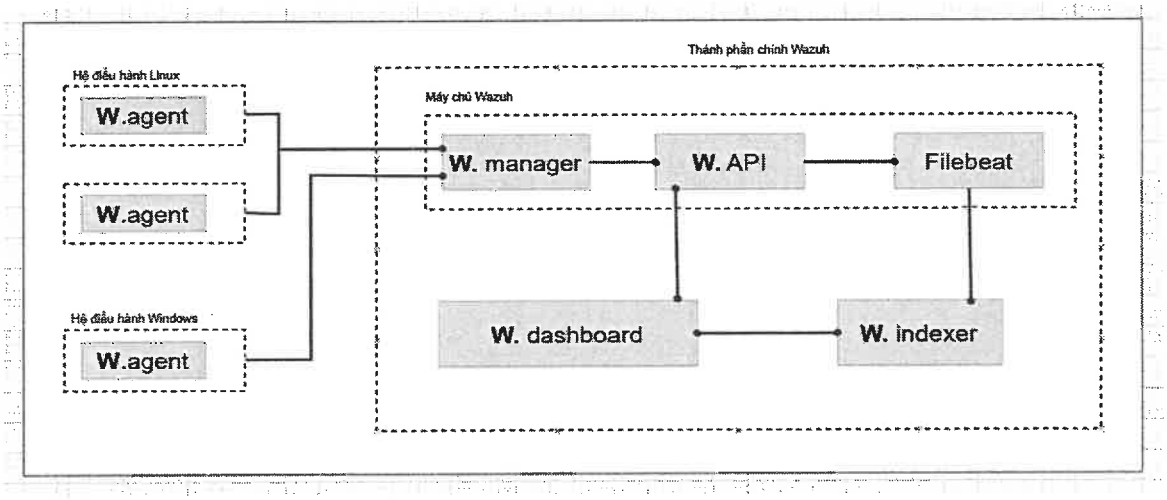
Thành phần	Công cụ sử dụng
Hệ điều hành máy chủ	Ubuntu Server 22.04 LTS
Hệ thống SIEM	Wazuh
Máy Agent Linux	Ubuntu
Máy Agent Windows	Microsoft Windows 10 hoặc Microsoft Windows 11
Môi trường ảo hóa	VMware Workstation hoặc Oracle VM VirtualBox
Sinh log và tấn công thử nghiệm	Nmap, Hydra
Giám sát mạng	Wireshark
Kiểm thử bảo mật	Kali Linux

Mô hình trên cho phép mô phỏng các cuộc tấn công như quét cổng, brute-force SSH, đăng nhập sai nhiều lần hoặc thay đổi tập tin hệ thống để đánh giá khả năng phát hiện và cảnh báo của Wazuh trong môi trường thực tế.

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.

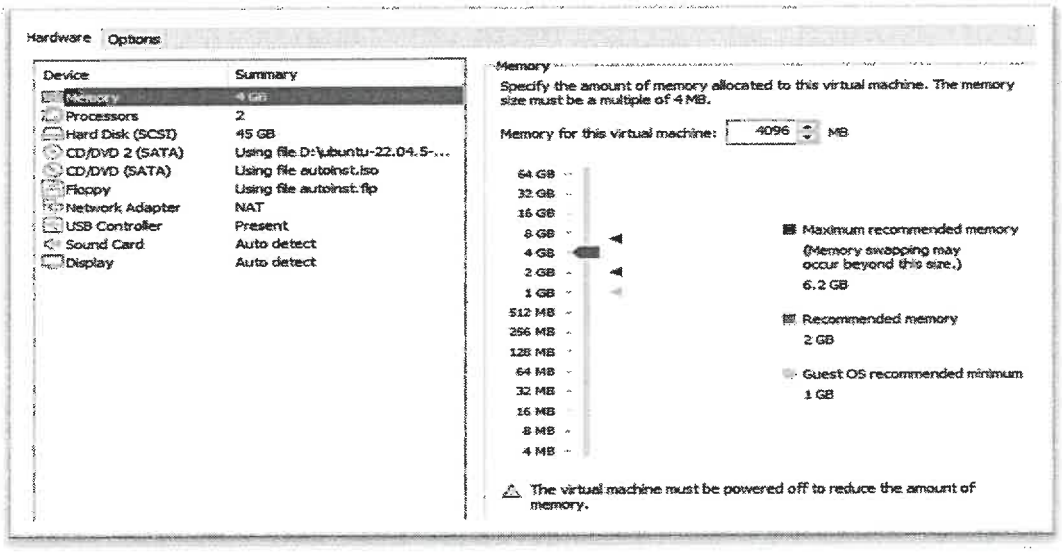


Hình 2.3. Các thành phần chính của hệ thống giám sát Wazuh

2.2.1. Cài đặt Wazuh Server và kết nối Wazuh tới máy chủ [4][8].

Môi trường đề xuất:

Thành phần	Cấu hình
Hệ điều hành	Ubuntu Server 22.04
CPU	4 Core trở lên
RAM	8 GB trở lên
Storage	40 GB trở lên



Hình 2.4: Cấu hình hệ điều hành trước khi cài đặt trên VM

Update hệ điều hành trên WAZUH SERVER

Trên Terminal bash:

sudo apt update && sudo apt upgrade -y

```
lee@lee-virtual-machine: $ sudo apt update && sudo apt upgrade -y
[sudo] password for lee:
Hit:1 http://vn.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://vn.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://vn.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu jammy-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
```

Hình 2.5: Update hệ điều hành

Cài đặt nhanh bằng Script chính thức:

curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh

sudo bash wazuh-install.sh –a

```
lee@lee-virtual-machine: $ curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh
lee@lee-virtual-machine: $ sudo bash wazuh-install.sh -a
18/06/2026 01:09:17 INFO: Starting Wazuh installation assistant. Wazuh version: 4.14.5
18/06/2026 01:09:17 INFO: Verbose logging redirected to /var/log/wazuh-install.log
18/06/2026 01:09:26 INFO: --- Dependencies ----
18/06/2026 01:09:26 INFO: Installing gawk.
```

Hình 2.6: Bash cài đặt

```
18/06/2026 23:38:59 INFO: Generating configuration files.
18/06/2026 23:39:00 INFO: Generating the root certificate.
18/06/2026 23:39:01 INFO: Generating Admin certificates.
18/06/2026 23:39:01 INFO: Generating Wazuh indexer certificates.
18/06/2026 23:39:02 INFO: Generating Filebeat certificates.
18/06/2026 23:39:02 INFO: Generating Wazuh dashboard certificates.
18/06/2026 23:39:03 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key,
18/06/2026 23:39:04 INFO: --- Wazuh indexer ---
18/06/2026 23:39:04 INFO: Starting Wazuh indexer installation.
^[[2-18/06/2026 23:46:08 INFO: Wazuh indexer installation finished.
18/06/2026 23:46:08 INFO: Wazuh indexer post-install configuration finished.
18/06/2026 23:46:08 INFO: Starting service wazuh-indexer.
18/06/2026 23:46:43 INFO: wazuh-indexer service started.
18/06/2026 23:46:43 INFO: Initializing Wazuh indexer cluster security settings.
18/06/2026 23:46:51 INFO: Wazuh indexer cluster security configuration initialized.
18/06/2026 23:46:51 INFO: Wazuh indexer cluster initialized.
18/06/2026 23:46:51 INFO: --- Wazuh server ---
18/06/2026 23:46:51 INFO: Starting the Wazuh manager installation.
18/06/2026 23:51:19 INFO: Wazuh manager installation finished.
18/06/2026 23:51:19 INFO: Wazuh manager vulnerability detection configuration finished.
18/06/2026 23:51:19 INFO: Starting service wazuh-manager.
18/06/2026 23:51:40 INFO: wazuh-manager service started.
18/06/2026 23:51:40 INFO: Starting Filebeat installation.
18/06/2026 23:52:25 INFO: Filebeat installation finished.
18/06/2026 23:52:27 INFO: Filebeat post-install configuration finished.
18/06/2026 23:52:27 INFO: Starting service filebeat.
18/06/2026 23:52:34 INFO: filebeat service started.
18/06/2026 23:52:34 INFO: --- Wazuh dashboard ---
18/06/2026 23:52:34 INFO: Starting Wazuh dashboard installation.
18/06/2026 23:55:54 INFO: Wazuh dashboard installation finished.
```

Hình 2.7: Cài đặt các gói quan trọng

Sau khi cài đặt hoàn tất: Wazuh Server (Manager), Wazuh Indexer, Wazuh Dashboard sẽ được triển khai tự động trên cùng máy chủ.

Truy cập Dashboard

Truy cập:

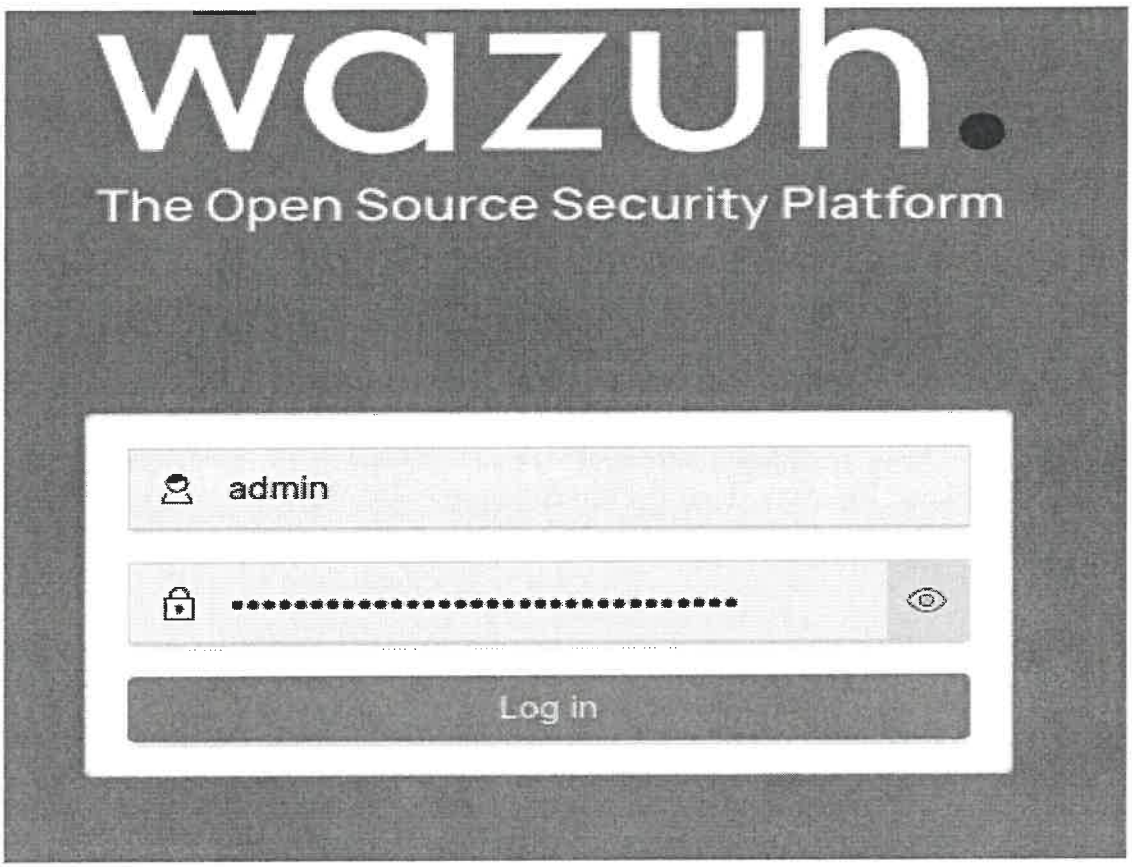
https://<IP-Wazuh-Server>



Đăng nhập bằng tài khoản được sinh ra trong quá trình cài đặt.

User: admin

Password: <ADMIN_PASSWORD>



Hình 2.8: Cài đặt các gói quan trọng

2.2.2. Cấu hình Wazuh Agent

Agent là thành phần thu thập dữ liệu trên các máy được giám sát.

Đối với Agent cài đặt trên Ubuntu

Terminal type:

curl -so wazuh-agent.deb \

https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.x.x-1_amd64.deb

sudo WAZUH_MANAGER="192.168.1.10" dpkg -i wazuh-agent.deb

Khởi động dịch vụ:

sudo systemctl daemon-reload

sudo systemctl enable wazuh-agent

sudo systemctl start wazuh-agent

Đối với Agent cài đặt trên Windows

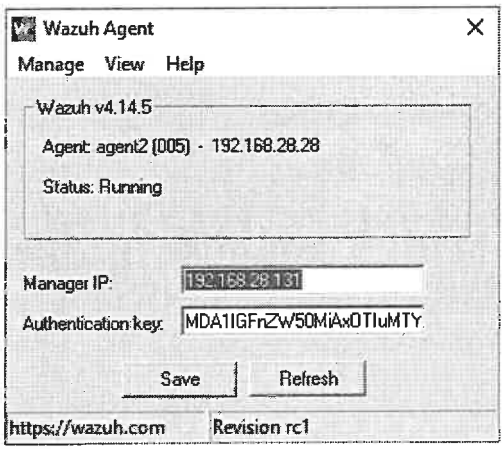
Bước 1: Tải Agent từ trang Wazuh.

Bước 2: Chạy file cài đặt.

Bước 3: Nhập địa chỉ IP Wazuh Server.

Ví dụ:

Manager Address: 192.168.28.131



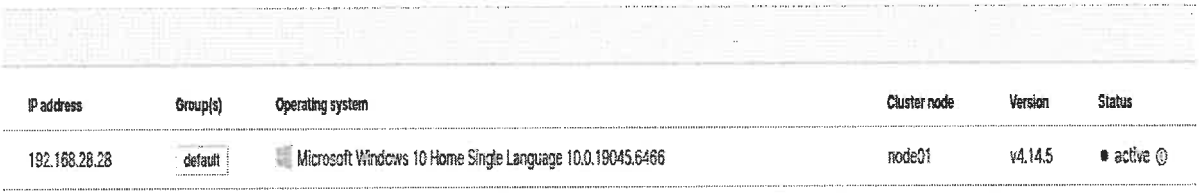
Hình 2.9: Cấu hình Wazuh Agent

Khởi động dịch vụ Agent.

Kiểm tra Agent đã kết nối bằng cách trên Wazuh Dashboard:

Agents → Summary

Trạng thái: Active → kết nối thành công.



Hình 2.10: Thông tin Agent

2.2.3. Thu thập dữ liệu

Sau khi Agent hoạt động, hệ thống bắt đầu thu thập nhiều loại dữ liệu bảo mật.

Nhật ký hệ điều hành

Linux:

/var/log/auth.log

/var/log/syslog

Windows:

Config: C:\Program Files (x86)\ossec-agent\ossec.conf

File log: C:\Program Files (x86)\ossec-agent\ossec.log

Các log thu thập bao gồm:

Security Event Log

System Event Log

Application Event Log

VD: Sử dụng chức năng giám sát tính toàn vẹn tập tin (File Integrity Monitoring – FIM) - Đâylà một trong những chức năng quan trọng của Wazuh, giúp theo dõi và phát hiện các thay đổi xảy ra đối với các tập tin và thư mục quan trọng trong hệ thống. Chức năng này góp phần phát hiện sớm các hành vi truy cập trái phép, chỉnh sửa cấu hình hoặc cài đặt mã độc.

Wazuh Agent thực hiện việc giám sát các tập tin và thư mục được cấu hình trước, chẳng hạn như:

/etc/passwd và **/etc/shadow** trên hệ điều hành Linux, là các tập tin chứa thông tin tài khoản và mật khẩu người dùng.

C:\Windows\System32 trên hệ điều hành Windows, là thư mục chứa các tệp hệ thống và thư viện quan trọng.

Trong quá trình giám sát, Wazuh có khả năng phát hiện các thay đổi như: Thêm mới tập tin hoặc thư mục, xóa tập tin, chỉnh sửa nội dung tập tin, hoặcthay đổi quyền truy cập, thuộc tính hoặc giá trị băm (Hash) của tập tin. Khi phát hiện các thay đổi ngoài mong đợi, Wazuh sẽ tạo cảnh báo để quản trị viên kiểm tra và xác minh nguyên nhân, từ đó kịp thời xử lý các nguy cơ ảnh hưởng đến tính toàn vẹn của hệ thống.

2.2.4 Cách kiểm tra, phân tích và phát hiện dữ liệu bất thường, lỗ hổng bảo mật bằng Wazuh [5]

1. Phân tích cảnh báo bảo mật

Wazuh Dashboard cung cấp giao diện **Security Events**, cho phép quản trị viên theo dõi và phân tích các sự kiện bảo mật được phát hiện trên toàn bộ hệ thống theo thời gian thực. Đây là chức năng quan trọng giúp giám sát trạng thái an toàn thông tin, thông qua giao diện này, người quản trị có thể theo dõi các cảnh báo bảo mật theo thời gian thực, tìm kiếm và truy xuất nhật ký (log) theo nhiều tiêu chí khác nhau, lọc cảnh báo theo mức độ nghiêm trọng, thời gian, thiết bị hoặc loại sự kiện. Ví dụ, khi

xảy ra sự kiện **SSH authentication failed**, Wazuh sẽ phân tích bản ghi nhật ký và hiển thị các thông tin quan trọng như: Tài khoản được sử dụng để đăng nhập, địa chỉ IP của thiết bị thực hiện đăng nhập, thời điểm xảy ra sự kiện, mức độ nghiêm trọng của cảnh báo. Các thông tin này giúp quản trị viên nhanh chóng đánh giá nguyên nhân và đưa ra biện pháp xử lý phù hợp.

2. Phát hiện tấn công Brute Force SSH

Wazuh có khả năng phát hiện các cuộc tấn công **Brute Force** nhằm dò quét mật khẩu dịch vụ SSH thông qua cơ chế phân tích và tương quan nhiều sự kiện đăng nhập thất bại trong một khoảng thời gian xác định. Ví dụ, kẻ tấn công sử dụng công cụ Hydra để thử nhiều mật khẩu đối với tài khoản *root*:

hydra -l root -P passwords.txt ssh://192.168.28.28

Trong trường hợp này, Wazuh sẽ ghi nhận nhiều lần xác thực SSH thất bại và tạo cảnh báo với nội dung **Multiple SSH authentication failures**. Cảnh báo thường được gán **Level 10**, phản ánh mức độ nghiêm trọng cao do có dấu hiệu của một cuộc tấn công dò quét mật khẩu.

Thông qua cảnh báo, quản trị viên có thể xác định: Địa chỉ IP nguồn thực hiện tấn công, số lần thử đăng nhập thất bại, thông tin tài khoản bị nhắm mục tiêu, thời gian diễn ra cuộc tấn công.

Những thông tin này hỗ trợ quá trình điều tra, đồng thời giúp triển khai các biện pháp ngăn chặn như chặn địa chỉ IP, cấu hình Firewall hoặc áp dụng các cơ chế bảo vệ như Fail2Ban.

3. Phát hiện thay đổi tập tin

Wazuh sử dụng chức năng **File Integrity Monitoring (FIM)** để giám sát tính toàn vẹn của các tập tin và thư mục quan trọng trong hệ thống. Khi một tập tin quan trọng, chẳng hạn như:

/etc/passwd bị chỉnh sửa, Wazuh sẽ tính toán lại giá trị băm (Hash) của tập tin và so sánh với giá trị đã lưu trước đó. Nếu phát hiện sự khác biệt, hệ thống sẽ sinh cảnh báo với nội dung như: **Integrity checksum changed** Cảnh báo này giúp quản trị viên nhanh chóng phát hiện các hành vi như: Cài đặt cửa hậu (Backdoor), leo thang đặc quyền (Privilege Escalation), chỉnh sửa trái phép các tập tin hệ thống hoặc thay

đổi cấu hình có thể ảnh hưởng đến an toàn thông tin. Nhờ đó, quản trị viên có thể kịp thời kiểm tra nguyên nhân và khôi phục tính toàn vẹn của hệ thống.

4. Phát hiện Malware và Rootkit

Wazuh tích hợp **Rootcheck Module**, cho phép kiểm tra và phát hiện một số dấu hiệu liên quan đến mã độc và Rootkit trên các thiết bị được giám sát. Module này thực hiện nhiều cơ chế kiểm tra khác nhau, bao gồm: Phát hiện các Rootkit phổ biến dựa trên cơ sở dữ liệu nhận diện, kiểm tra các tập tin hoặc thư mục bị ẩn bất thường, phát hiện các tiến trình đang hoạt động nhưng có dấu hiệu che giấu hoặc không hiển thị đầy đủ, kiểm tra các thay đổi bất thường đối với cấu hình hệ thống.

Ví dụ, khi phát hiện một tiến trình bị che giấu, Wazuh có thể sinh cảnh báo với nội dung: **Hidden process detected.** Những cảnh báo này hỗ trợ quản trị viên nhận diện sớm các dấu hiệu xâm nhập hoặc sự hiện diện của phần mềm độc hại trên hệ thống.

5. Phân tích lỗ hổng bảo mật

Wazuh hỗ trợ chức năng **Vulnerability Detection**, cho phép phát hiện các lỗ hổng bảo mật tồn tại trên hệ thống thông qua việc đối chiếu thông tin thiết bị với cơ sở dữ liệu CVE (Common Vulnerabilities and Exposures). Trên giao diện Dashboard, quản trị viên có thể truy cập: **Threat Intelligence → Vulnerability Detection** để theo dõi các lỗ hổng được phát hiện. Wazuh tiến hành đối chiếu các thông tin như: Phiên bản hệ điều hành, danh sách phần mềm đã cài đặt, phiên bản của từng phần mềm, tình trạng cập nhật các bản vá bảo mật với cơ sở dữ liệu CVE được cập nhật thường xuyên.

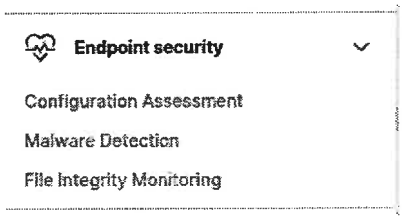
Ví dụ, hệ thống có thể phát hiện lỗ hổng **CVE-2023-4911** trên một thiết bị chưa được cập nhật bản vá tương ứng. Đối với mỗi lỗ hổng, Dashboard sẽ hiển thị các thông tin quan trọng như:

- Mã định danh CVE.
- Điểm đánh giá mức độ nghiêm trọng theo thang **CVSS**.
- Mô tả chi tiết về lỗ hổng.
- Các hệ điều hành hoặc phần mềm bị ảnh hưởng.
- Khuyến nghị cập nhật bản vá hoặc các biện pháp giảm thiểu rủi ro.

Thông qua chức năng này, Wazuh giúp quản trị viên nhanh chóng xác định các điểm yếu trong hệ thống, ưu tiên xử lý các lỗ hổng có mức độ nghiêm trọng cao và nâng cao hiệu quả quản lý an toàn thông tin.

2.2.5. Một số tính năng cơ bản khác

1. Endpoint security



Hình 2.11: Endpoint security

Configuration Assesment (Đánh giá cấu hình bảo mật):

- Thực hiện kiểm tra cấu hình hệ thống so với các tiêu chuẩn bảo mật.
- Phát hiện các cấu hình sai lệch có thể làm giảm mức độ an toàn của hệ thống.

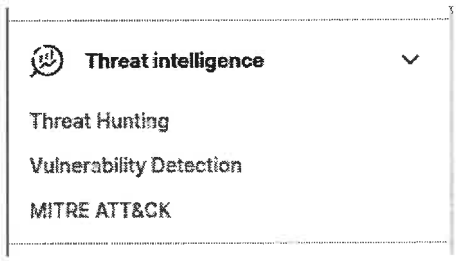
Malware Detection (Phát hiện phần mềm độc hại):

- Phân tích hành vi và dấu hiệu của các tệp tin hoặc quá trình để phát hiện mã độc.
- Có thể tích hợp với công cụ như VirusTotal để xác minh các tệp đáng ngờ.

File Integrity Monitoring (Giám sát toàn vẹn tệp tin):

- Theo dõi các thay đổi đối với tệp hệ thống quan trọng (thêm, sửa, xóa).
- Ghi lại thông tin khi nào đã thay đổi tệp, giúp phát hiện truy cập hoặc chỉnh sửa trái phép.

2. Threat Intelligence



Hình 2.12: Threat Intelligence

Threat Hunting (Săn tìm mối đe dọa):

- Hỗ trợ phân tích sâu và tìm kiếm các dấu hiệu tấn công trong hệ thống.

- Dựa trên log, hành vi và các chỉ số xâm nhập để truy vết các mối đe dọa đang ẩn nấp.

Vulnerability Detection (Phát hiện lỗ hổng bảo mật):

- Tự động quét và phát hiện phần mềm dễ bị tổn thương trên các endpoint.
- Sử dụng dữ liệu từ các nguồn như NVD, OVAL, và thông tin từ nền tảng CTI của Wazuh.

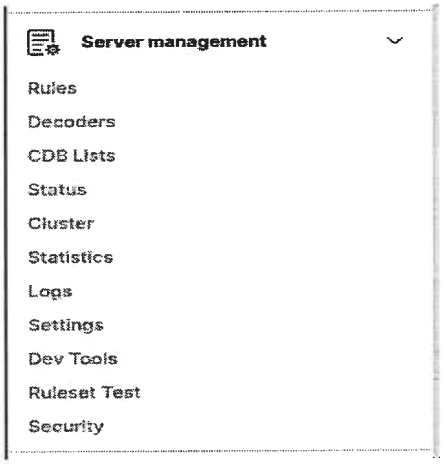
MTRE ATT&CK:

- Hệ thống hóa và phân loại hành vi tấn công theo ma trận MITRE ATT&CK.
- Giúp hiểu rõ kỹ thuật của kẻ tấn công và xây dựng biện pháp phòng vệ hiệu quả hơn.

VirusTotal:

- Tích hợp với dịch vụ VirusTotal để phân tích tệp tin và URL nghi ngờ.
- Gửi hash để so sánh với cơ sở dữ liệu virus từ nhiều antivirus khác nhau.

3. Server management

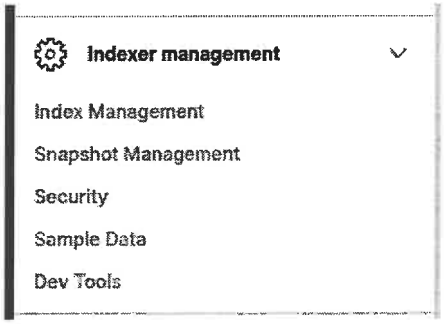


Hình 2.13: Server management

- Endpoints Summary và Endpoints Groups tổng quát và phân nhóm các máy giám sát.
- Rules, Decoders và CDB Lists quản lý các quy tắc phát hiện, bộ giải mã log, và cơ sở dữ liệu tùy chỉnh.
- Status, Cluster, Statistics, và Logs là tính năng giám sát trạng thái hệ thống, cụm node, thống kê và log.

- Settings, Dev Tools, Ruleset Test và Security cho phép cấu hình, công cụ phát triển, kiểm thử quy tắc, và cài đặt bảo mật.

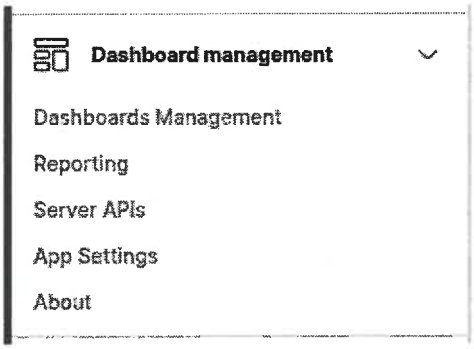
4. **Indexer management**



Hình 2.14: Indexer management

- Index Management và Snapshot Management là chức năng quản lý chỉ mục dữ liệu và sao lưu.
- Security, Sample Data và Dev Tools quản lý bảo mật dữ liệu chỉ mục, dữ liệu mẫu và công cụ phát triển.

5. **Dashboard management**



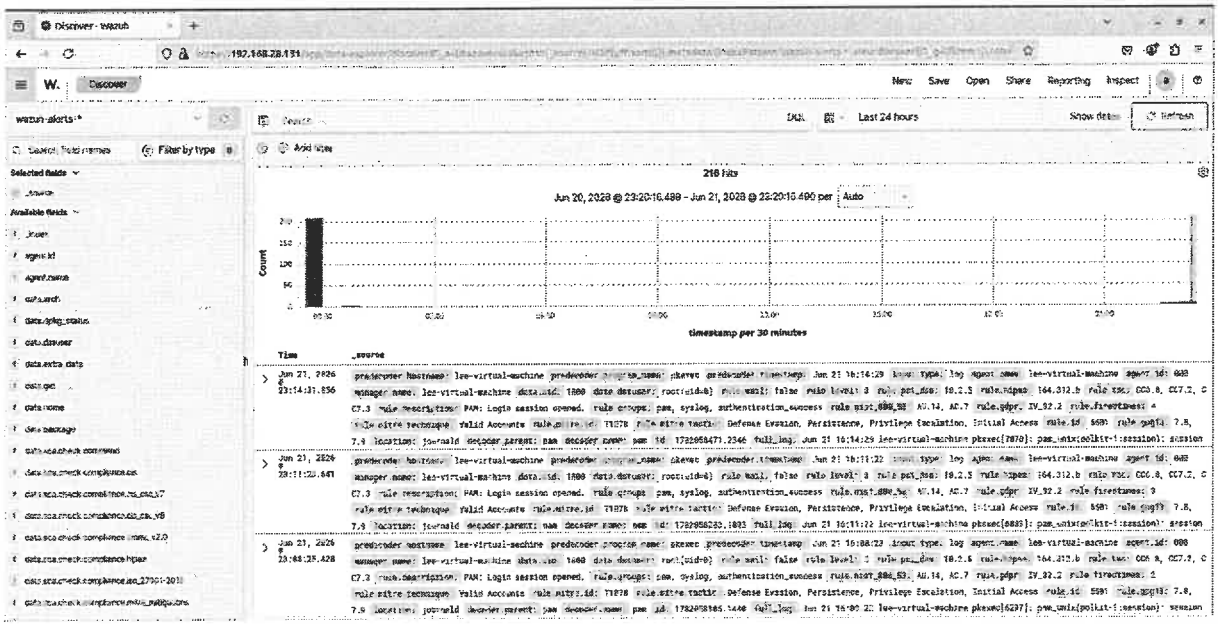
Hình 2.15: Dashboard management

- Dashboards Management và Reporting có chức năng quản lý các bảng điều khiển trực quan, xuất báo cáo.
- Server APIs, App Settings và App Logs cho phép xem API máy chủ, cài đặt ứng dụng, nhật ký ứng dụng và thông tin phần mềm.

6. **Giám sát log trên Dashboard**

Sau khi đăng nhập hệ thống thành công, click vào menu và chọn menu Explore và chọn Discover để đi đến phần giám sát log. Tại đây, người dùng sẽ có cái nhìn tổng

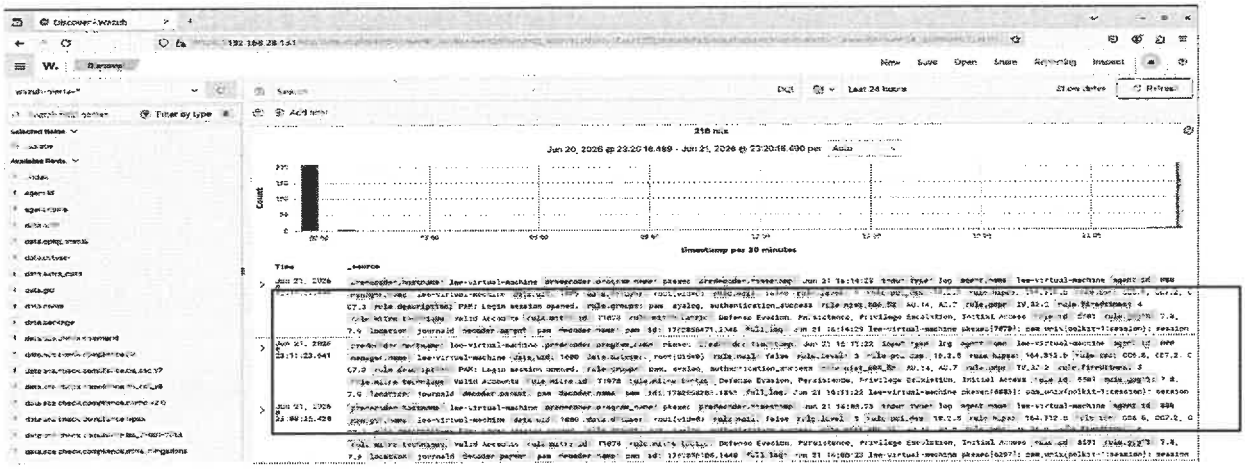
quan đến chi tiết về các sự kiện liên quan đến các lỗ hổng bảo mật được hệ thống rò quét phát hiện.



Hình 2.16: Giám sát log

7. Thống kê

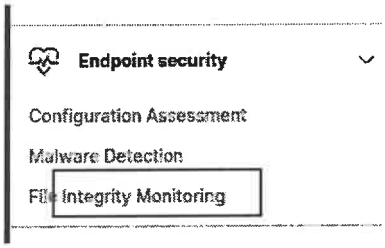
Hệ thống hiển thị biểu đồ số lượng sự kiện và danh sách các sự kiện theo thời gian liên quan đến thay đổi file với thông tin được hiển thị theo các trường mong muốn. Có thể xem chi tiết một sự kiện bằng cách nhấn vào nút được tô đỏ tại sự kiện mong muốn.



Hình 2.17: Thống kê log

8. Giám sát toàn vẹn tệp

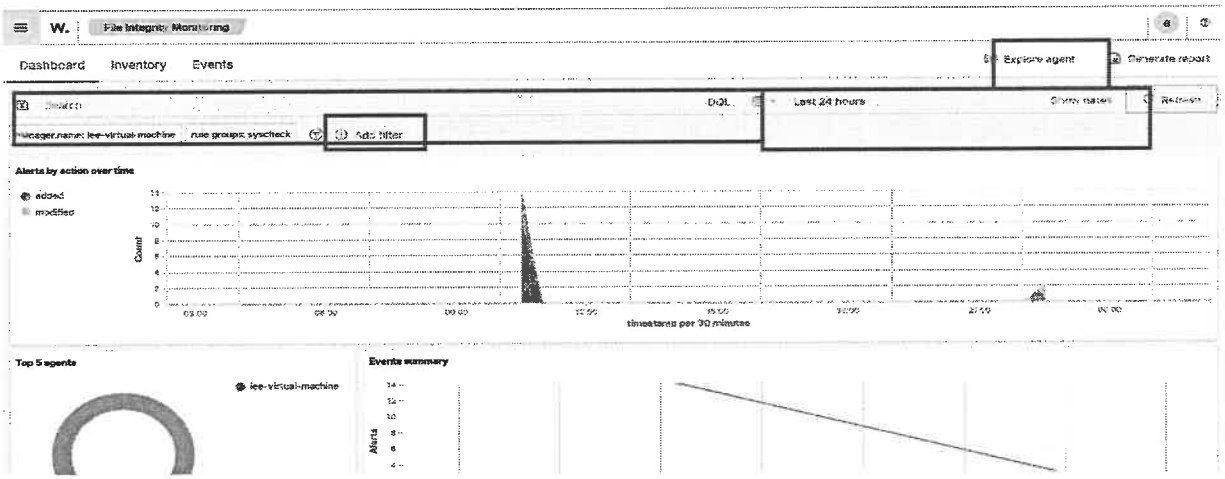
Sau khi đăng nhập vào hệ thống, tại Wazuh, click chọn menu Endpoint Security và chọn File Intergrity Monitoring để quản lý cảnh báo liên quan đến thay đổi tệp, bao gồm quyền, nội dung, quyền sở hữu và thuộc tính.



Hình 2.18: Menu FIM

Màn hình giao diện bảng điều khiển File Intergrity monitoring được hiển thị.

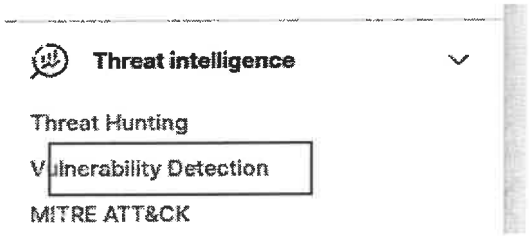
Có thể tìm kiếm linh hoạt theo ý muốn, bộ lọc bao gồm nhiều trường dữ liệu hỗ trợ tìm kiếm một cách nhanh chóng và chính xác nhất gồm: Search, Date time, Add filter.



Hình 2.19: Lọc FIM log

- **Quản lý lỗ hổng bảo mật CVE**

Sau khi đăng nhập vào hệ thống, tại Wazuh, click chọn menu Threat Intelligence và chọn Vulnerabilities để sử dụng chức năng quản lý, khám phá những ứng dụng, thiết bị, hệ điều hành trong hệ thống mạng của bạn bị ảnh hưởng bởi các lỗ hổng an toàn thông tin.

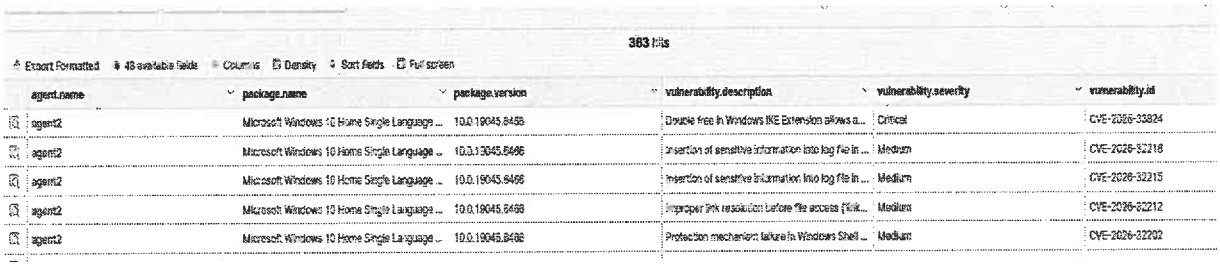


Hình 2.20: Chức năng quản lý lỗ hổng bảo mật

- **Giám sát lỗ hổng**

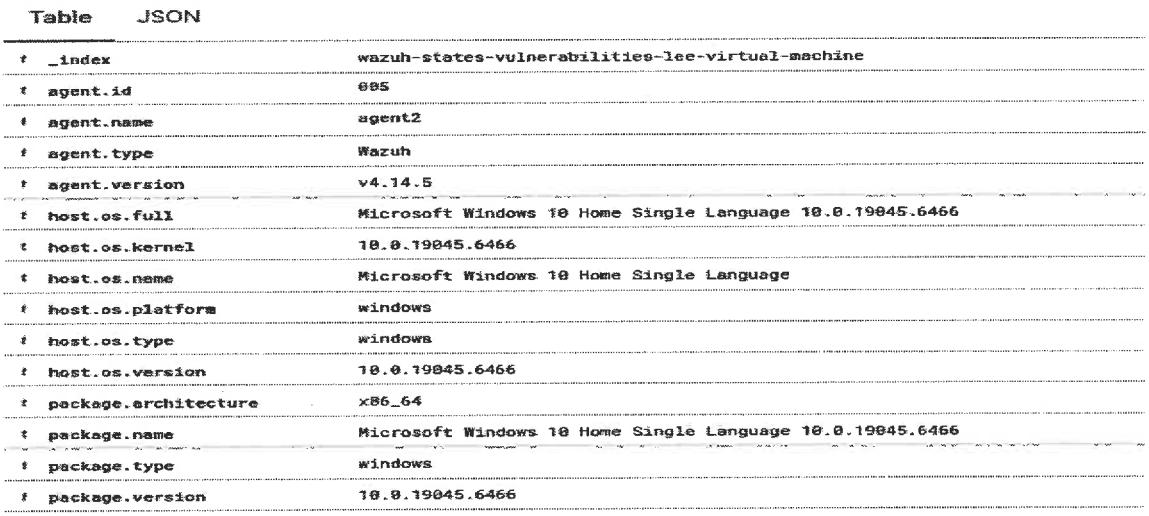
Thông thường các EDR sẽ được trang bị một máy quét lỗ hổng vunerability detector, dữ liệu của máy quét được lấy từ các nguồn uy tín nên đảm bảo tính chính xác. Máy quét lỗ hổng sẽ định kì quét 1 tháng 2 lần cho mỗi máy. Các lỗ hổng có thể quét được chủ yếu là lỗ hổng trên hệ điều hành. Không phải tất cả ứng dụng chạy trên hệ thống đều quét được lỗ hổng.

Chọn tab Inventory



Hình 2.21: Chọn log

Có thể chọn nút "kính lúp" để xem chi tiết thông tin.



Hnh 2.22: Thông tin log

- **Phản hồi chủ động**

Tạo rule mới trong /var/ossecc/etc/rules/local_rules.xml



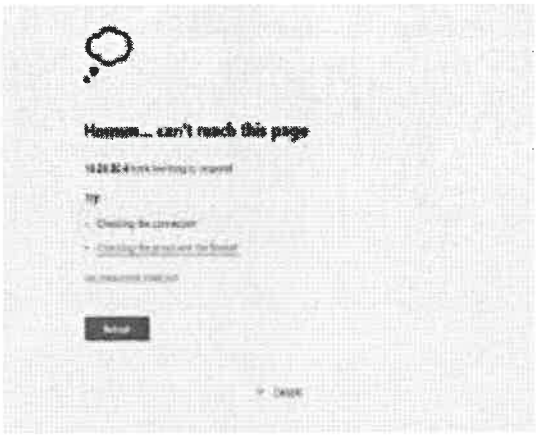
Hình 2.23: local_rules

Tạo cảnh báo cho rule này tại /var/ossecc/etc/ossecc.conf

```
#Ubuntu
<ossec_config>
  <active-response>
    <command>firewall-drop</command>
    <location>local</location>
    <rules_id>100100</rules_id>
    <timeout>60</timeout>
  </active-response>
</ossec_config>
```

Hình 2.24: Tạo cảnh báo

Sau khi có một máy cố tình truy cập vào trang web sẽ bị chặn



Hình 2.25: Truy cập web và bị ngắt truy cập

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

2.3.1. Tùy chỉnh Decoder và Rules

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.

1. Decoder

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.

Ví dụ, Decoder cho log Apache có thể được cấu hình như sau:

```
<decoder name="apache-access">
  <prematch>apache</prematch>
  <regex>
    (\S+) - - \[(.*?)\]
      </regex>
</decoder>
```

Decoder này giúp nhận diện các log truy cập Apache và trích xuất các thông tin liên quan từ nội dung log.

2. Rule

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. Ví dụ, một Rule có thể được xây dựng để phát hiện các truy cập web đáng ngờ như sau:

```
<rule id="100100" level="10">
 <decoded_as>apache-access</decoded_as>
 <description>
   Suspicious web access
 </description>
</rule>
```

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.

Việc tùy chỉnh Decoder và Rules mang lại nhiều lợi ích quan trọng, bao gồm: tăng khả năng phát hiện các loại tấn công đặc thù theo từng môi trường hệ thống, cho phép tùy biến linh hoạt theo nhu cầu và đặc thù hoạt động của từng doanh nghiệp và nâng cao độ chính xác trong việc phát hiện sự kiện bảo mật, giảm thiểu cảnh báo không cần thiết.

2.3.2. Tích hợp Active Response

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 mạng khi phát hiện cảnh báo có mức độ nghiêm trọng từ level 10 trở lên. Ví dụ: Trong trường hợp một địa chỉ IP thực hiện nhiều lần đăng nhập SSH thất bại (ví dụ hơn 5 lần), hệ thống sẽ tự động xác định đây là hành vi bất thường và tiến hành: Ghi nhận địa chỉ IP tấn công, ví dụ: 192.168.1.100 và tự động chặn địa chỉ IP này thông qua Firewall. Cơ chế này giúp ngăn chặn kịp thời các cuộc tấn công Brute Force và giảm thiểu nguy cơ xâm nhập hệ thống.

2.3.3. Tích hợp Threat Intelligence

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. Wazuh có thể tích hợp với nhiều nền tảng và dịch vụ, bao gồm: VirusTotal., AbuseIPDB.AlienVault OTX nhằm tăng khả năng tra cứu mức độ tin cậy và độc hại của địa chỉ IP, kiểm tra mã hash của tệp tin để phát hiện mã độc và đối chiếu các chỉ báo tấn công (Indicators of Compromise – IOC) với cơ sở dữ liệu bên ngoài. Ví dụ hoạt động: Khi hệ thống phát hiện một địa chỉ IP, ví dụ 185.x.x.x, Wazuh

sẽ tự động gửi truy vấn đến các nguồn Threat Intelligence để kiểm tra danh tiếng của IP này. Nếu địa chỉ IP nằm trong danh sách đen hoặc được xác định là độc hại, hệ thống sẽ tạo cảnh báo và hiển thị thông tin chi tiết trên Dashboard. Nhờ cơ chế này, Wazuh nâng cao đáng kể khả năng phát hiện sớm các mối đe dọa, đặc biệt là các cuộc tấn công đã được ghi nhận trong cộng đồng an ninh mạng toàn cầu.

CHƯƠNG 3. XÂY DỰNG HỆ THỐNG GIÁM SÁT

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

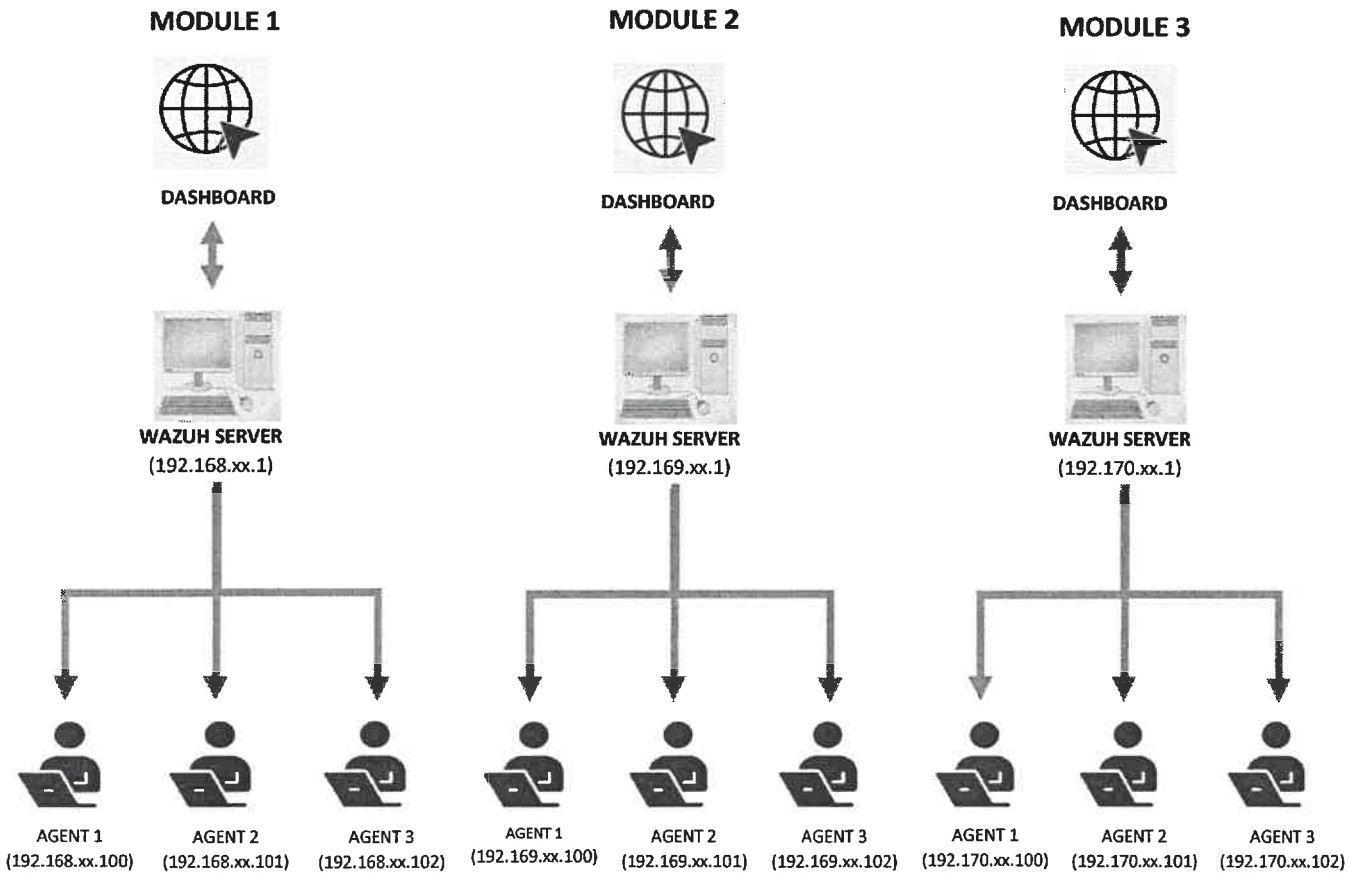
3.1.1. Phân loại đối tượng cần giám sát và bảo vệ

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.

1. 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. Đây là hạ tầng cốt lõi đảm bảo việc trao đổi thông tin và vận hành các dịch vụ CNTT. Các nguy cơ mất an toàn thông tin dễ gặp phải nhất bao gồm: tấn công mạng, truy cập trái phép, khai thác lỗ hổng dịch vụ, lây nhiễm mã độc, mã hóa thông tin dữ liệu và đánh cắp dữ liệu.

2. Hệ thống máy tính nhân sự



Hình 3.1: Hệ thống máy tính văn phòng

Hệ thống máy tính nhân sự bao gồm máy tính của nhân viên sử dụng trên văn phòng thực hiện các hoạt động phục vụ công việc khác nhau như: 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. Mỗi node mạng (agent) được gán IP riêng liên kết với nhau bằng phương thức truyền thông ethernet. Hệ thống mạng và server được chia làm nhiều module tùy thuộc vào mặt hàng sản xuất. Mỗi module sẽ được cài đặt khác nhau và không liên kết để tránh rò rỉ thông tin do đảm nhận vai trò khác nhau, vì vậy yêu cầu bảo mật thông tin và mức độ bảo mật của mỗi module cũng khác nhau. VD: Module A sản xuất mặt hàng theo yêu cầu của khách hàng sẽ cần nhiều lớp cơ chế bảo mật hơn. Đây là thành phần quan trọng trong hạ tầng công nghệ thông tin của tổ chức, đồng thời cũng là mục tiêu thường xuyên của các cuộc tấn công mạng.

Do người dùng thường xuyên truy cập Internet, sử dụng thư điện tử và kết nối với nhiều thiết bị ngoại vi, máy trạm là một trong những thành phần có nguy cơ cao bị tấn công. Một số rủi ro an toàn thông tin thường gặp bao gồm:

Nhiễm mã độc (Malware): Máy trạm có thể bị lây nhiễm mã độc thông qua các tệp đính kèm trong email, các liên kết độc hại, thiết bị lưu trữ USB hoặc phần mềm tải xuống từ các nguồn không tin cậy.

Đánh cắp tài khoản và thông tin cá nhân: Kẻ tấn công có thể sử dụng các hình thức lừa đảo hoặc kỹ thuật đánh cắp thông tin xác thực để đăng nhập trái phép tài khoản người dùng.

Cài đặt phần mềm trái phép: Người dùng có thể tự ý cài đặt các phần mềm không được cấp phép hoặc không rõ nguồn gốc, làm gia tăng nguy cơ xuất hiện lỗ hổng bảo mật hoặc mã độc trong hệ thống.

Rò rỉ hoặc đánh cắp dữ liệu nội bộ: Các tài liệu, dữ liệu quan trọng của tổ chức có thể bị sao chép, truyền ra ngoài hoặc truy cập trái phép thông qua thiết bị lưu trữ, dịch vụ lưu trữ đám mây hoặc các cuộc tấn công mạng.

Sử dụng trái phép các thiết bị thông tin: Nhằm mục đích sao lưu và đánh cắp dữ liệu thông tin như USB, ổ cứng để đánh cắp dữ liệu.

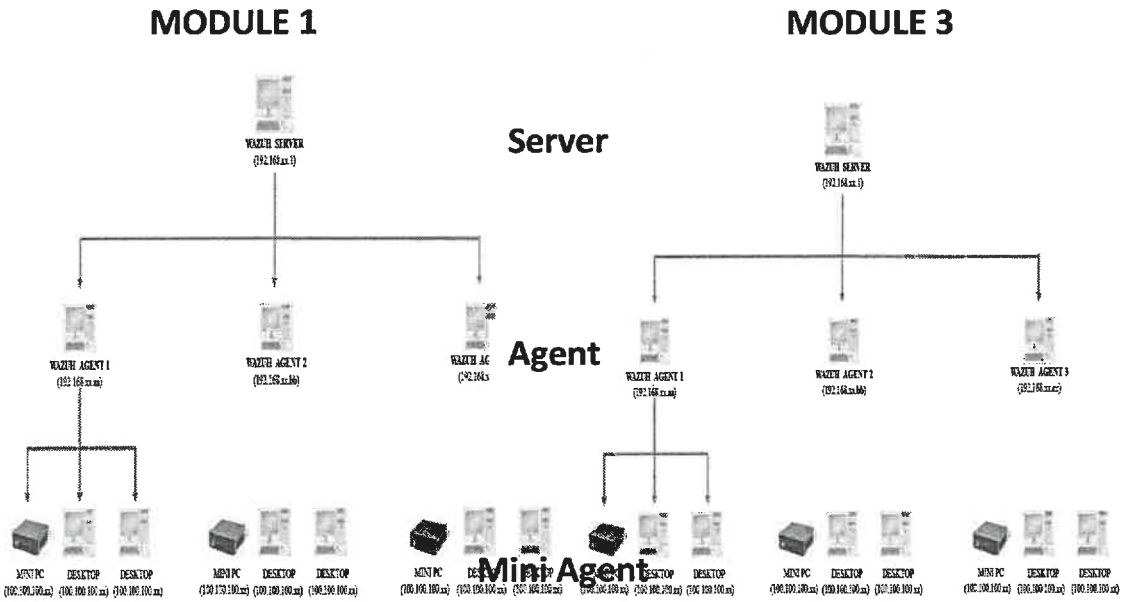
☞ Giải pháp bảo mật ATTT đề xuất:

- Phát hiện xâm nhập/ đăng nhập trái phép hệ thống trên máy agent.
- Quản lý lưu trữ tài liệu trong thư mục, giám sát tính toàn vẹn tập.

- Phát hiện kết nối thiết bị ngoại vi và phần mềm bất thường.

3. Hệ thống vận hành sản xuất

Cấu trúc của hệ thống mạng 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 CIM – máy CIM này đóng vai trò như một Wazuh Agent giao tiếp và truyền tải dữ liệu giữa hệ thống sản xuất và hệ thống quản lý dữ liệu của công ty Samsung. Mỗi thiết bị mini agent giao tiếp với agent bằng phương thức truyền thông ethernet (VD: Dải IP : 100.100.100.xx). Mỗi Wazuh Agent cũng sẽ được quản lý IP riêng liên kết với nhau, đồng thời cũng liên kết với Wazuh Server bằng dải IP riêng. VD: 192.168.100.xx . Cũng như hệ thống quản lý đối với hệ thống máy tính văn phòng, mỗi module sẽ đảm nhận vai trò khác nhau, do vậy yêu cầu bảo mật thông tin và mức độ bảo mật của mỗi module cũng khác nhau. VD: Module A sản xuất mặt hàng theo yêu cầu của khách hàng sẽ cần nhiều lớp cơ chế bảo mật hơn.



Hình 3.2: Hệ thống máy tính nhà xưởng

Một số nguy cơ phổ biến bao gồm:

Lây nhiễm mã độc gây ảnh hưởng đến hệ thống vận hành: Các thiết bị trong môi trường sản xuất có thể bị tấn công bởi mã độc từ các phần mềm không rõ ràng, dẫn đến gián đoạn hoạt động, làm chậm hoặc ngừng dây chuyền sản xuất, gây thiệt hại về kinh tế và ảnh hưởng đến tiến độ sản xuất.

Thay đổi trái phép thông số kỹ thuật thiết bị: Kẻ tấn công hoặc người dùng nội bộ có thể can thiệp vào các file dữ liệu cấu hình kỹ thuật của thiết bị như thông số vận hành, ngưỡng an toàn hoặc chế độ hoạt động. Điều này có thể dẫn đến sai lệch trong quy trình sản xuất, giảm chất lượng sản phẩm hoặc gây hư hỏng thiết bị.

Đánh cắp dữ liệu sản xuất: Dữ liệu trong môi trường sản xuất như hình ảnh sản phẩm, thông số kỹ thuật hàng hóa, cấu hình thiết bị và dữ liệu vận hành có thể bị truy cập trái phép và đánh cắp.

☞ Giải pháp bảo mật ATTT đề xuất:

- Phát hiện cài đặt phần mềm trái phép.
- Phát hiện kết nối thiết bị ngoại vi bất thường.
- Quản lý lưu trữ tài liệu trong thư mục, giám sát tính toàn vẹn tập tin

4. Dữ liệu và tài liệu kinh doanh

Tài liệu và dữ liệu là một trong những tài sản quan trọng nhất của tổ chức, 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, cụ thể như:

- Hồ sơ khách hàng, bao gồm thông tin cá nhân, lịch sử giao dịch và dữ liệu liên quan đến dịch vụ.
- Dữ liệu sản xuất, phản ánh quy trình vận hành, thông số kỹ thuật và kết quả sản xuất.
- Tài liệu kỹ thuật, bao gồm thiết kế hệ thống, cấu hình thiết bị và hướng dẫn vận hành.
- Công nghệ cốt lõi, liên quan đến bí quyết kỹ thuật, quy trình độc quyền và tài sản trí tuệ của tổ chức.
- Báo cáo tài chính, cung cấp thông tin về tình hình kinh doanh, doanh thu, chi phí và hiệu quả hoạt động.

Do tính chất quan trọng và giá trị cao, nhóm tài sản này thường là mục tiêu tấn công của nhiều hình thức xâm phạm an ninh mạng. Các nguy cơ chính có thể bao gồm:

Rò rỉ hoặc đánh cắp dữ liệu: Dữ liệu có thể bị truy cập trái phép và bị khai thác bởi các đối tượng bên ngoài hoặc nội bộ nhằm phục vụ mục đích xấu, gây ảnh hưởng nghiêm trọng đến uy tín và hoạt động của tổ chức.

Mã hóa dữ liệu bởi ransomware: Các cuộc tấn công mã độc tống tiền (ransomware) có thể mã hóa toàn bộ hoặc một phần dữ liệu quan trọng, khiến hệ thống không thể truy cập dữ liệu cho đến khi tiền chuộc được thanh toán.

Mất dữ liệu do lỗi hoặc tấn công mạng: Dữ liệu có thể bị mất do lỗi hệ thống, cấu hình sai, sự cố phần cứng hoặc do các cuộc tấn công phá hoại từ bên ngoài, gây gián đoạn hoạt động và ảnh hưởng đến quá trình ra quyết định của tổ chức.

☞ Giải pháp bảo mật ATTT đề xuất:

- Quản lý lưu trữ tài liệu.
- Mã hóa dữ liệu.

5. Thiết bị và công cụ lưu trữ thông tin

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 có tính linh hoạt cao, tuy nhiên cũng tiềm ẩn nhiều rủi ro về an toàn thông tin nếu không được kiểm soát chặt chẽ. Các thiết bị phổ biến bao gồm:

USB (Universal Serial Bus): Thiết bị lưu trữ di động nhỏ gọn, dễ dàng sử dụng để sao chép và truyền tải dữ liệu giữa các máy tính.

Ổ cứng di động (External Hard Drive): Thiết bị lưu trữ có dung lượng lớn, thường được sử dụng để sao lưu hoặc di chuyển dữ liệu.

Thiết bị sao lưu (Backup devices): Bao gồm các hệ thống hoặc phương tiện dùng để sao lưu dữ liệu nhằm đảm bảo khả năng khôi phục khi xảy ra sự cố.

Mặc dù mang lại sự tiện lợi trong việc quản lý và di chuyển dữ liệu, các thiết bị này cũng là nguồn tiềm ẩn nhiều nguy cơ an ninh thông tin, cụ thể như có thể mang mã độc lây nhiễm vào hệ thống hoặc sao chép trái phép dữ liệu.

☞ Giải pháp bảo mật ATTT đề xuất:

- Phát hiện kết nối thiết bị ngoại vi bất thường.
- Phát hiện cài đặt phần mềm trái phép.

3.1.2. Phân tích các dạng tấn công an toàn thông tin

1. Tấn công Brute Force

Tấn công Brute Force là hình thức tấn công trong đó kẻ tấn công cố gắng truy cập trái phép vào hệ thống bằng cách thử liên tục nhiều tổ hợp tên người dùng và mật khẩu khác nhau cho đến khi tìm ra thông tin xác thực hợp lệ. Đây là một trong những phương pháp tấn công phổ biến nhằm chiếm quyền truy cập vào hệ thống.

Đặc điểm của tấn công:

Xuất hiện nhiều lần đăng nhập thất bại liên tiếp trong một khoảng thời gian ngắn.

Thường nhắm vào các dịch vụ truy cập từ xa như SSH, RDP hoặc VPN.

Giải pháp phòng chống:

Giới hạn số lần đăng nhập thất bại nhằm giảm khả năng thử mật khẩu liên tục.

Sử dụng cơ chế phát hiện và phản ứng tự động của Wazuh Active Response để cảnh báo và chặn địa chỉ IP có hành vi tấn công.

2. Tấn công Malware/Ransomware

Tấn công mã độc (Malware) và mã độc tống tiền (Ransomware) là các hình thức tấn công nhằm xâm nhập và kiểm soát hệ thống thông qua việc cài đặt phần mềm độc hại. Các mã độc này thường được phát tán qua email, thiết bị lưu trữ USB hoặc tải xuống từ các nguồn không an toàn trên Internet.

Mục tiêu của tấn công:

Đánh cắp thông tin và dữ liệu quan trọng của hệ thống.

Mã hóa dữ liệu và yêu cầu tiền chuộc để khôi phục truy cập.

Chiếm quyền điều khiển thiết bị hoặc hệ thống bị nhiễm.

Giải pháp phòng chống:

Sử dụng cơ chế giám sát tính toàn vẹn tập tin (File Integrity Monitoring – FIM) để phát hiện các thay đổi bất thường.

Theo dõi các hoạt động hệ thống nhằm phát hiện hành vi đáng ngờ liên quan đến mã độc.

Kết hợp hệ thống giám sát an ninh như Wazuh để phát hiện sớm dấu hiệu tấn công.

3. Tấn công khai thác lỗ hổng (Vulnerability Exploitation)

Tấn công khai thác lỗ hổng xảy ra khi kẻ tấn công lợi dụng các điểm yếu trong phần mềm, hệ điều hành hoặc dịch vụ chưa được cập nhật bản vá bảo mật để xâm nhập vào hệ thống.

Mục tiêu của tấn công:

Thực hiện leo thang đặc quyền (Privilege Escalation).

Thực thi mã độc trên hệ thống mục tiêu.

Truy cập trái phép vào tài nguyên và dữ liệu quan trọng.

Giải pháp phòng chống:

Sử dụng chức năng Vulnerability Detection của Wazuh để quản lý và phát hiện các lỗ hổng bảo mật.

Thực hiện cập nhật bản vá hệ thống và phần mềm định kỳ nhằm giảm thiểu nguy cơ bị khai thác.

4. Tấn công nội bộ (Insider Threat)

Tấn công nội bộ là các hành vi gây mất an toàn thông tin xuất phát từ chính người dùng trong tổ chức, bao gồm nhân viên hoặc người có quyền truy cập hợp lệ vào hệ thống. Các hành vi này có thể mang tính cố ý hoặc vô ý, nhưng đều có khả năng gây ảnh hưởng nghiêm trọng đến an toàn dữ liệu.

Giải pháp phòng chống:

Giám sát và phân tích hoạt động người dùng trên hệ thống.

Áp dụng cơ chế kiểm soát truy cập dựa trên nguyên tắc phân quyền tối thiểu (Least Privilege).

Ghi nhận và lưu trữ đầy đủ nhật ký truy cập để phục vụ điều tra và truy vết khi cần thiết.

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

3.2.1. Mô hình đề xuất cho hệ thống

1. Xây dựng hệ thống quản lý cho khối sản xuất

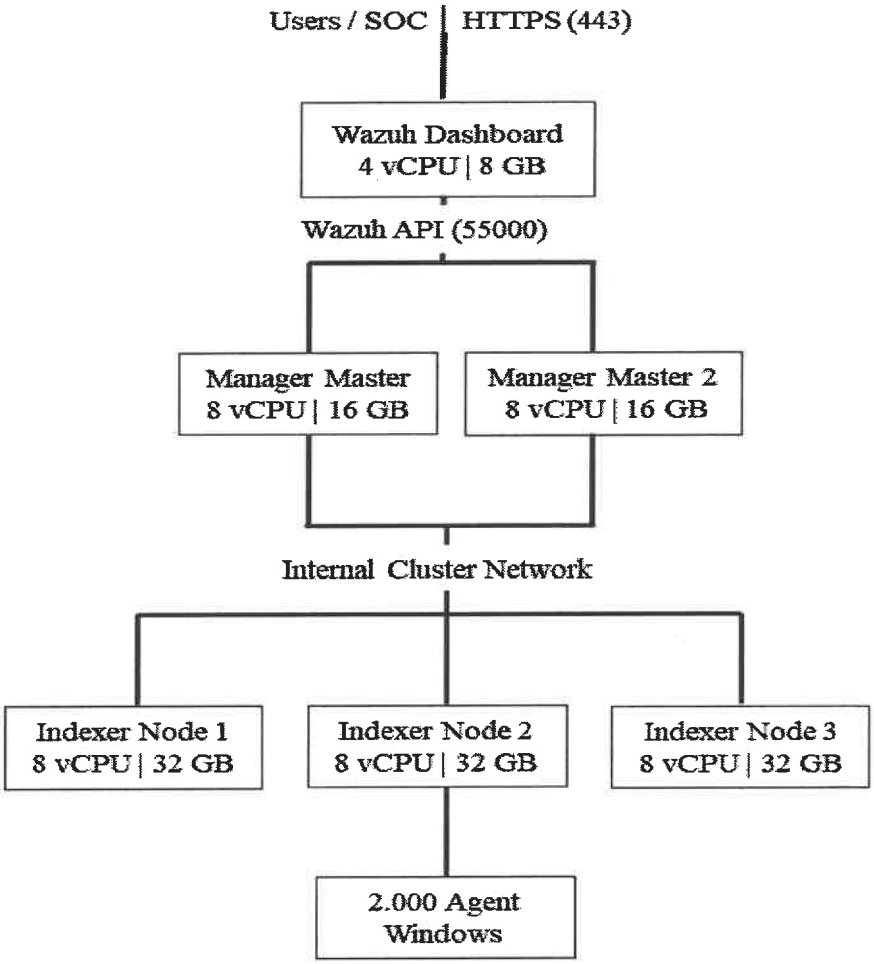
Xây dựng hệ thống quản lý cho khối sản xuất 2000 Agent

Cấu hình phần cứng đề xuất				
Thành phần	**Số lượng**	**CPU**	**RAM**	**Ổ cứng**
Wazuh Dashboard	1	4 vCPU	8 GB	100 GB SSD
Wazuh Manager Master	2	8 vCPU	16 GB	300 GB SSD
Wazuh Manager Worker	1	8 vCPU	16 GB	300 GB SSD
Wazuh Indexer	3	8 vCPU	32 GB	1 TB NVMe
Load Balancer (HAProxy/Nginx) *(tùy chọn)*	1	2 vCPU	4 GB	40 GB

Bảng 3.1: Cấu hình đề xuất cho các máy trên hệ thống

Ưu điểm của mô hình

- Khả năng mở rộng: dễ tăng lên 5.000–10.000 Agent bằng cách bổ sung Worker.
- Hiệu năng: chia tải xử lý giữa các Manager.
- Tính sẵn sàng: nếu một Worker gặp sự cố, các Worker khác vẫn có thể tiếp nhận tải (kết hợp với Load Balancer).
- Lưu trữ ổn định: cụm 3 Indexer đảm bảo khả năng chịu lỗi và duy trì dữ liệu khi một nút gặp sự cố.



Hình 3.3: Sơ đồ mô phỏng cấu hình cho 2000 máy Agent

2. Xây dựng hệ thống quản lý cho khối nhân sự

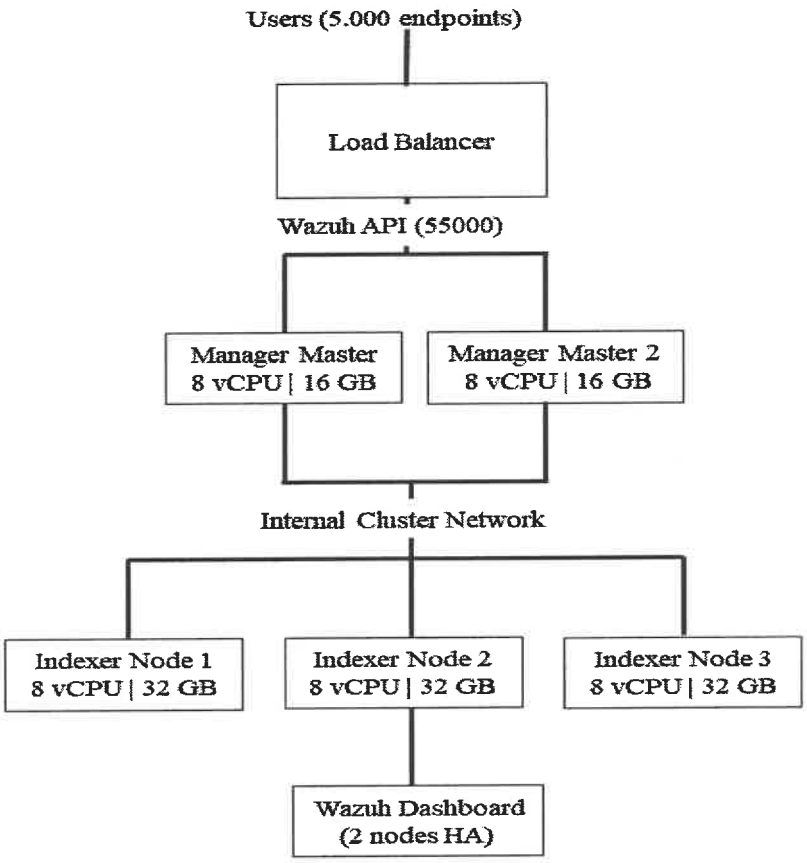
Xây dựng hệ thống quản lý cho khối nhân sự 5000 Agent

ZZ				
Thành phần	**Số lượng**	**CPU**	**RAM**	**Ổ cứng**
Wazuh Dashboard	2	4 vCPU	8 GB	100 GB SSD
Wazuh Manager Master	1	8 vCPU	16 GB	300 GB SSD
Wazuh Indexer	3	8 vCPU	32 GB	1 TB NVMe
Load Balancer (HAProxy/Nginx) *(tùy chọn)*	1	2 vCPU	4 GB	40 GB

Bảng 3.2: Cấu hình đề xuất cho các máy trên hệ thống sản xuất

Ưu điểm của mô hình

- Khả năng mở rộng: dễ tăng lên 5.000–10.000 Agent bằng cách bổ sung Worker.
- Hiệu năng: chia tải xử lý giữa các Dashboard.
- Tính sẵn sàng: nếu một Worker gặp sự cố, các Worker khác vẫn có thể tiếp nhận tải (kết hợp với Load Balancer).
- Lưu trữ ổn định: cụm 3 Indexer đảm bảo khả năng chịu lỗi và duy trì dữ liệu khi một nút gặp sự cố.



Hình 3.4: Sơ đồ mô phỏng cấu hình cho 5000 máy Agent

3. Triển khai hệ thống

Các bước thực hiện:

Bước 1: Cài đặt Wazuh Server.

Bước 2: Cài đặt Wazuh Agent trên Ubuntu và cài đặt Wazuh Agent trên Windows.

Bước 3: Kết nối Agent tới Wazuh Manager.

Bước 4: Kiểm tra trạng thái Agent trên Dashboard.

4. Kết quả thu thập dữ liệu

Sau khi hệ thống Wazuh Agent được triển khai và kết nối thành công với Wazuh Server, quá trình thu thập dữ liệu từ các thiết bị giám sát được thực hiện một cách liên tục và tự động. Dữ liệu thu thập được bao gồm nhiều loại thông tin quan trọng phục vụ cho công tác giám sát và phân tích an toàn thông tin, cụ thể như:

Nhật ký đăng nhập hệ thống, bao gồm các sự kiện đăng nhập thành công và thất bại của người dùng.

Nhật ký dịch vụ SSH, ghi nhận các hoạt động truy cập và xác thực từ xa qua giao thức SSH.

Windows Event Log, bao gồm các sự kiện hệ thống, bảo mật và ứng dụng trên nền tảng Windows.

Thông tin về thay đổi tập tin thông qua cơ chế File Integrity Monitoring (FIM), giúp phát hiện các hành vi chỉnh sửa, tạo mới hoặc xóa dữ liệu.

Thông tin về phần mềm đã cài đặt trên thiết bị, phục vụ cho công tác quản lý tài sản và đánh giá an toàn hệ thống.

Toàn bộ dữ liệu sau khi được thu thập sẽ được truyền về Wazuh Server, xử lý và lưu trữ tập trung trên hệ thống Wazuh Indexer. Đồng thời, dữ liệu được hiển thị trực quan trên Wazuh Dashboard, giúp quản trị viên dễ dàng theo dõi, truy vấn và phân tích theo thời gian thực.

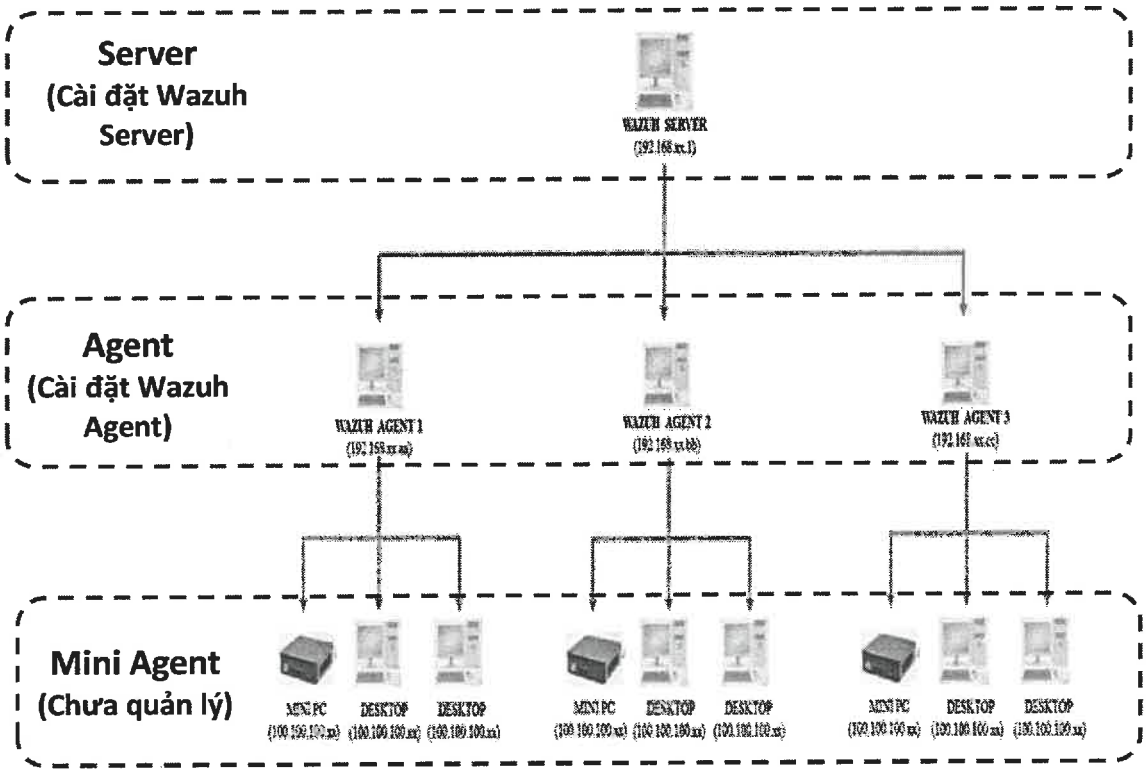
3.2.2 Xây dựng các kịch bản tấn công và phòng chống

1. Mô hình triển khai thử nghiệm

Hệ thống công nghệ thông tin của Samsung được triển khai với quy mô lớn, trong đó hệ thống vận hành sản xuất đóng vai trò chủ đạo và được tổ chức thành nhiều công đoạn khác nhau.

Trong mỗi công đoạn sản xuất, hệ thống lại được chia thành nhiều line (khu vực) nhằm tối ưu hóa quy trình vận hành và quản lý. Hiện tại, các máy chủ CIM tại các line đã được cài đặt agent và kết nối về hệ thống quản lý tập trung Wazuh để thu thập và giám sát dữ liệu. Tuy nhiên, phạm vi quản lý hiện tại mới chỉ tập trung vàocác

máy CIM 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.



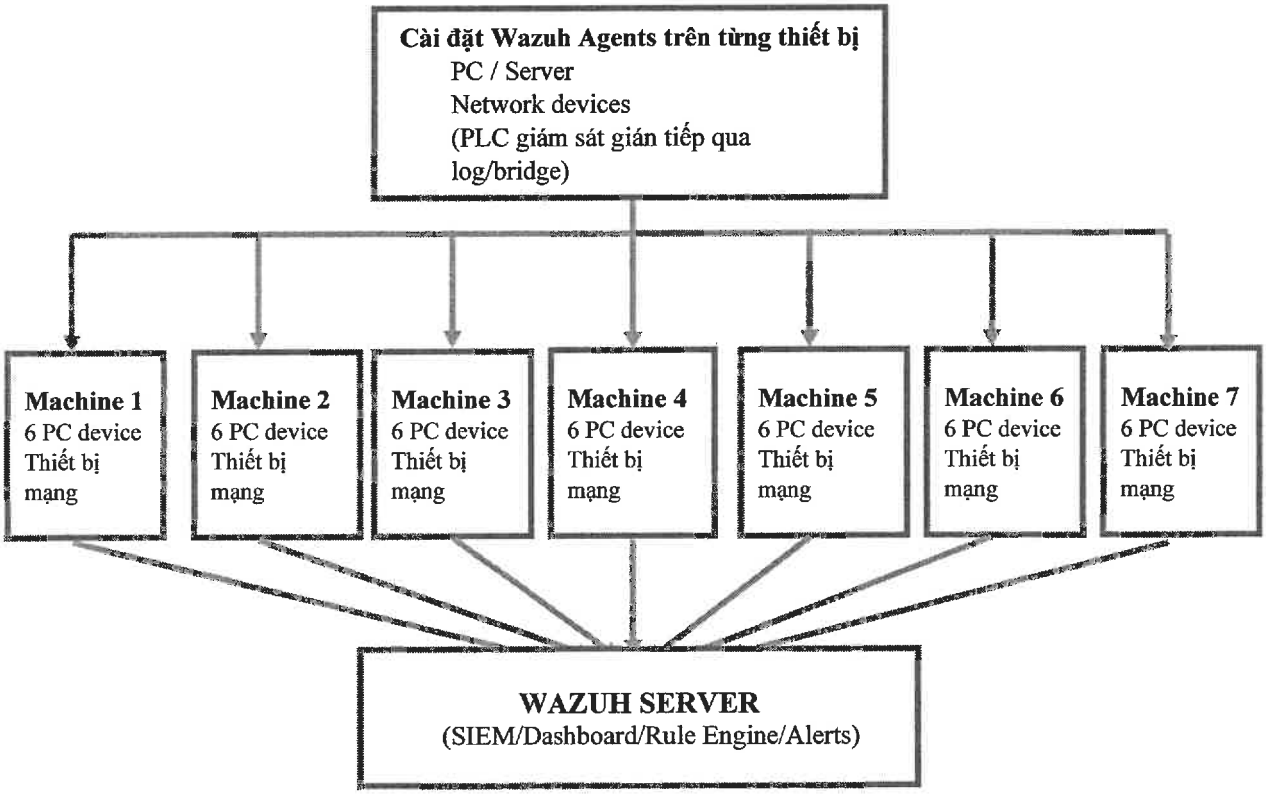
Hình 3.5: Hiện trạng quản lý bảo mật hệ thống tại công ty Samsung Display.

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. 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: Trên các máy tính thiết bị thường chứa các thông tin thông số kỹ thuật thiết bị quan

trọng, khi tác nhân bên ngoài chỉnh sửa dữ liệu có thể gửi dữ liệu sai cho thiết bị -> Gây ra lỗi sản xuất.

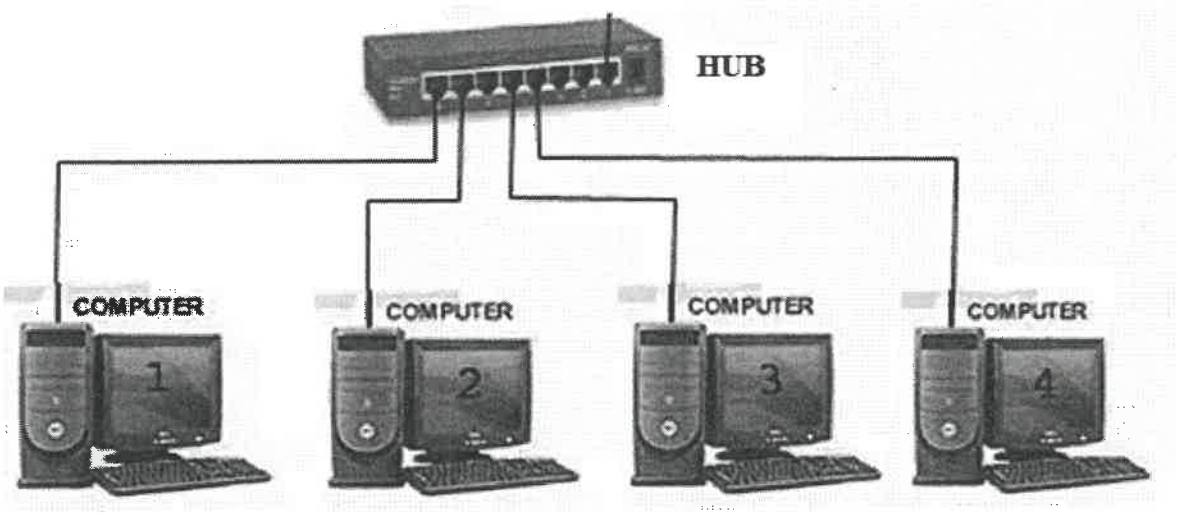
Do vậy, trong thời gian tới, đề án đang tiến hành xây dựng và triển khai quy trình bảo mật nhằm nâng cấp phạm vi quản lý, mở rộng từ các máy CIM hiện tại sang toàn bộ hệ thống máy tính trong công đoạn. Việc mở rộng này hướng tới mục tiêu quản lý các thiết bị đầu cuối, máy trạm và các thành phần liên quan, qua đó tăng cường khả năng giám sát, phát hiện sớm các rủi ro an ninh và nâng cao mức độ an toàn tổng thể của hệ thống. 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



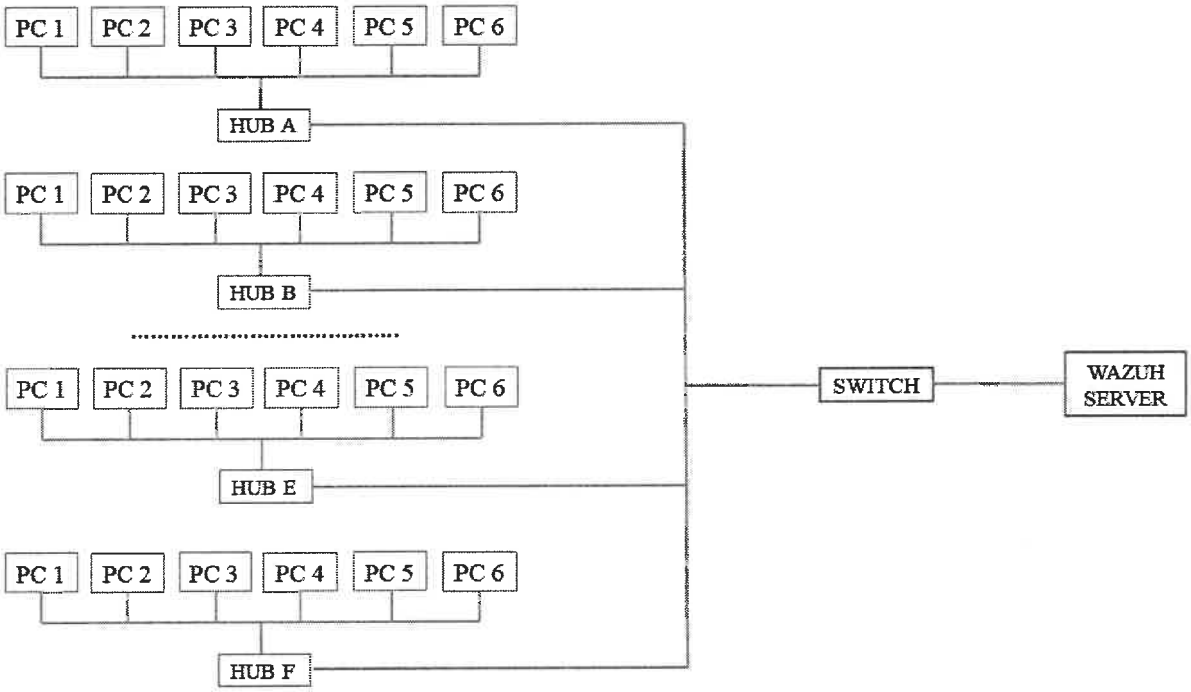
Hình 3.6: Mô phỏng hệ thống setup cho từng line.

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 3.7: Kết nối mạng Lan trên từng thiết bị



Hình 3.8. Kết nối mạng giữa các thiết bị trên cùng hệ thống

Mô hình cài đặt cho hệ thống này

WAZUH SERVER

Số lượng PC Wazuh Server :1

Cấu hình:

CPU: 2–4 vCPU

RAM: 4–8 GB

Disk: 50–100 GB SSD

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)

Giải pháp an toàn áp dụng cho hệ thống này:

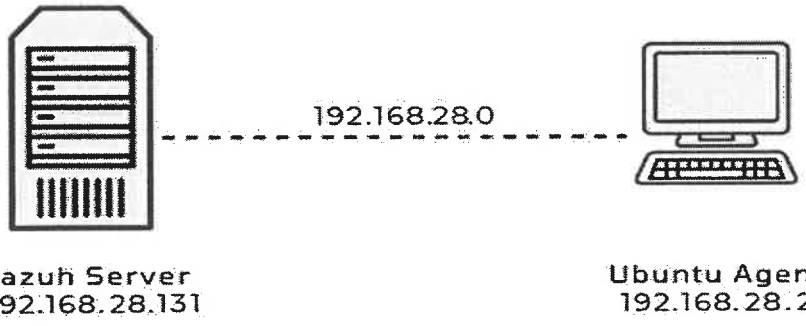
- Phát hiện đăng nhập trái phép trên thiết bị.
- Phát hiện kết nối thiết bị ngoại vi bất thường.
- Phát hiện cài đặt phần mềm trái phép.
- Quản lý lưu trữ tài liệu trong thư mục, giám sát tính toàn vẹn tập tin
- Phát hiện tấn công mạng từ thiết bị bên ngoài

Cảnh báo & hiển thị: Hiển thị trên Dashboard hoặc gửi cảnh báo theo thời gian thực cho SOC

2. Kịch bản và phương thức kiểm thảo

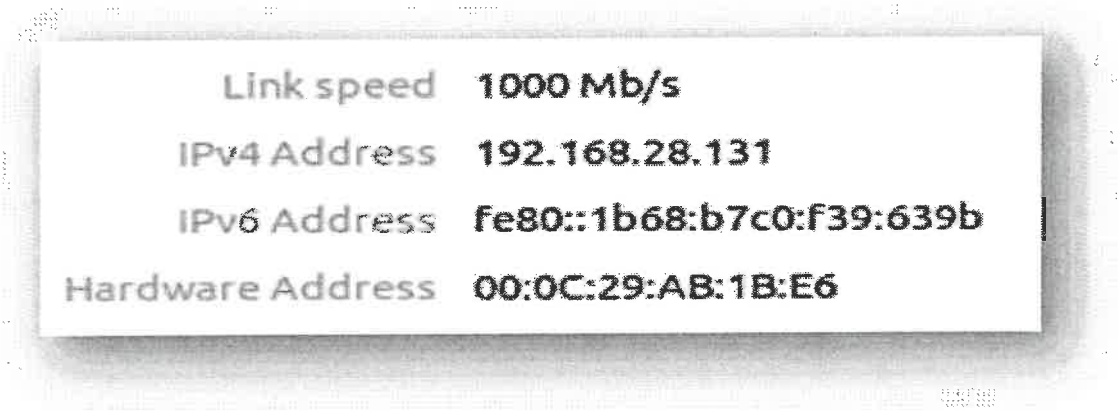
Phương thức kiểm thảo:

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 dựa vào các giải pháp an toàn đã được đưa ra như sau



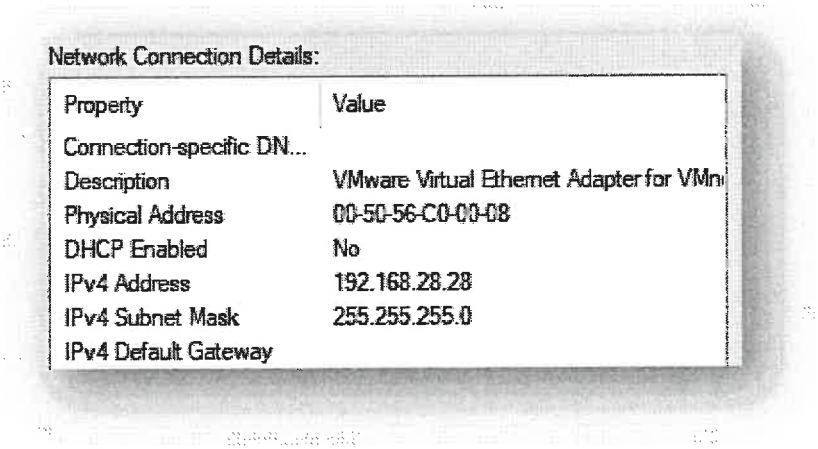
Hình 3.9. Mô phỏng kết nối từ Agent đến Server

VD: trên máy Server được trên máy tính hệ điều hành Ubuntu sẽ được cải IP: 192.168.28.131



Hình 3.10. Cấu hình trên máy WAZUH SERVER

Agent sẽ được cải trên PC Win10 và cấu hình Ipv4 Address: 192.168.28.28



Hình 3.11. Cấu hình trên máy WAZUH AGENT

Kịch bản kiểm thảo:

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. Thực hiện bằng cách tiến hành đăng nhập sai mật khẩu nhiều lần hoặc sử dụng tài khoản không tồn tại để truy cập vào thiết bị. Hệ thống Wazuh sẽ thu thập log từ các sự kiện đăng nhập thất bại (như Event ID 4625 trên Windows hoặc authentication failure trên Linux) và tạo cảnh báo khi phát hiện số lần đăng nhập sai bất thường hoặc dấu hiệu tấn công dò mật khẩu. Kết quả mong

đợi là hệ thống ghi nhận được nguồn truy cập, tài khoản thử đăng nhập và đưa ra cảnh báo mức độ phù hợp.

Kịch bản 2: Giám sát tính toàn vẹn tập tin (File Integrity Monitoring - FIM)

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 số thư mục quan trọng trên hệ thống hoặc thư mục chứa dữ liệu quan trọng, sau đó thực hiện các hành động như tạo mới, chỉnh sửa hoặc xóa tập tin. Wazuh sử dụng module FIM để ghi nhận trạng thái trước và sau khi thay đổi, bao gồm nội dung file, thời gian và người thực hiện thay đổi. Khi có bất kỳ sự thay đổi nào xảy ra, hệ thống sẽ sinh cảnh báo. Kết quả mong đợi là hệ thống phát hiện chính xác các thay đổi và hiển thị đầy đủ thông tin liên quan.

Kịch bản 3: Phát hiện phần mềm có lỗ hổng bảo mật

Kịch bản này nhằm đánh giá khả năng phát hiện các phần mềm tồn tại lỗ hổng bảo mật do sử dụng phiên bản cũ. Thực hiện bằng cách cài đặt hoặc hạ cấp một số phần mềm như trình duyệt, dịch vụ hệ thống hoặc ứng dụng có phiên bản đã được công bố có lỗ hổng. Wazuh Vulnerability Detector sẽ tự động đối chiếu phiên bản phần mềm với cơ sở dữ liệu CVE và đưa ra cảnh báo nếu phát hiện lỗ hổng. Kết quả mong đợi là hệ thống hiển thị danh sách lỗ hổng kèm mức độ nghiêm trọng và thông tin phần mềm bị ảnh hưởng.

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

Kịch bản này kiểm tra khả năng giám sát các thiết bị ngoại vi được kết nối vào hệ thống. Thực hiện bằng cách cắm các thiết bị như USB hoặc thiết bị ngoại vi khác vào máy tính đang cài Wazuh agent. Hệ thống sẽ thu thập log từ hệ điều hành liên quan đến sự kiện thiết bị được kết nối và phát hiện các thiết bị mới không nằm trong danh sách cho phép. Khi phát hiện thiết bị ngoại vi, Wazuh sẽ tạo cảnh báo kèm thông tin về thiết bị như tên, mã định danh và thời gian kết nối. Kết quả mong đợi là hệ thống phát hiện chính xác các thiết bị lạ được gắn vào hệ thống.

3.3. Thực hiện mô phỏng tấn công và kết quả

Kịch bản 1: Phát hiện tấn công Brute Force SSH/ Đăng nhập trái phép trên thiết bị.

Bước 1: Cấu hình trên file /var/ossec/etc/rules/local_rules.xml.

Trên Terminal Wazuh Server bash:

sudo nano /var/ossec/etc/rules/local_rules.xml

Tạo rule cảnh báo đăng nhập bằng cách thêm nội dung như sau:

```
<group name="local,windows,bruteforce,">
  <rule id="100100" level="12" frequency="3" timeframe="60">
    <if_matched_sid>60122</if_matched_sid>
    <same_field>win.eventdata.ipAddress</same_field>
    <description>Windows: 3 lần đăng nhập thất bại trên agent</description>
    <mitre>
      <id>T1110</id>
    </mitre>
  </rule>
</group>
```

Hình 3.12: Thêm rule để Wzuh phát hiện đăng nhập thất bại

Đoạn rule này có nghĩa như sau: Nếu trong vòng 60s, tại cùng một máy tính xảy ra hiện tượng đăng nhập thất bại 3 lần (3 event) thì sẽ phát sinh cảnh báo đăng nhập thất bại nhiều lần trên agent. VD:

IP	Event
192.168.28.28	login fail
192.168.28.28	login fail
192.168.28.28	login fail

Trong đó

<group name="local, windows, bruteforce,">

☞ Đây là nhóm rule (classification)

Ý nghĩa:

local → rule tự viết (custom)

windows → liên quan Windows log

bruteforce → dùng để tìm attack brute force

id=100100: mã định danh rule (phải duy nhất trong Wazuh)

level=12: mức độ nghiêm trọng (severity)

frequency=3 → cần 3 event

timeframe=60 → trong 60 giây

Rule ID = 60122: Evemt đăng nhập thất bại trong Wazuh có mã định danh là 60122

60122 = "Logon Failure - bad password"

<same_field> win.eventdata.ipAddress</same_field>

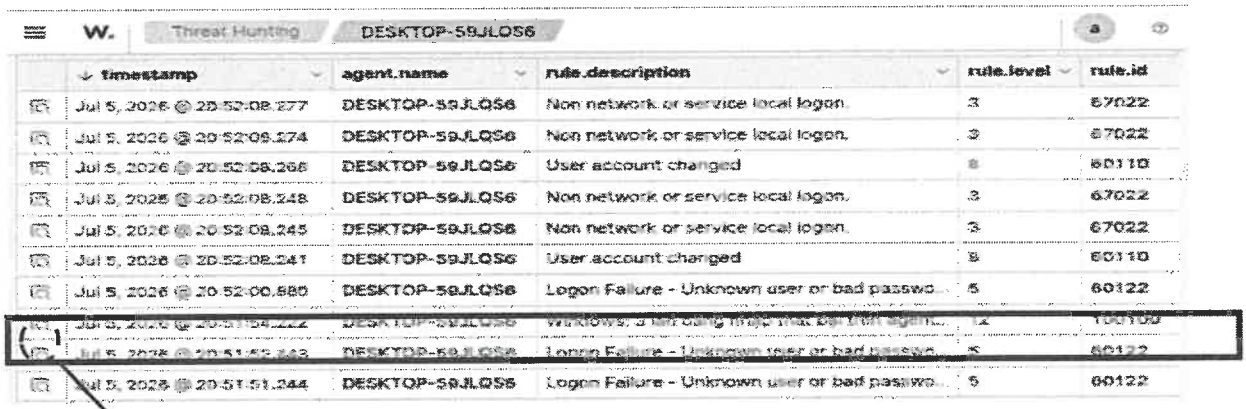
Điều kiện: Trùng địa chỉ ipAddress

<description>Windows: 3 lần đăng nhập thất bại trên agent </description> - > Nội dung sẽ cảnh bảo

Bước 2: Thực hiện đăng nhập Window và nhập sai mật khẩu liên tiếp 3 lần

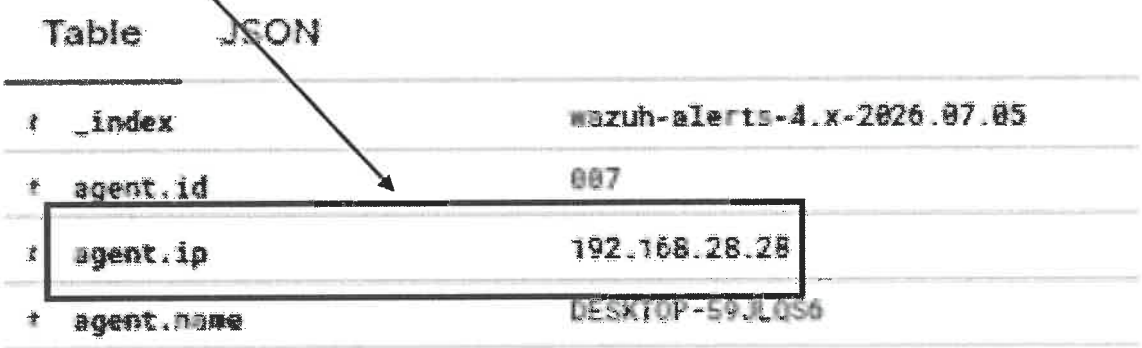
Bước 3: Tra cứu kết quả trên Wazuh

Tra cứu thông báo trên Dashboard tại thư mục: **Endpoint Security -> Threat Hunting -> Events**



Hình 3.13: Cảnh báo đăng nhập thất bại sau 3 lần

Click vào biểu tượng kính lúp để xem thông tin IP của máy bị đăng nhập



Hình 3.14: Thông tin đăng nhập

Biện pháp phòng chống:

- Kích hoạt cơ chế Active Response chặn kết nối IP

Bước 1: Mở file ossec.config trên Manager để sửa rule

Terminal bash: sudo nano /var/ossec/etc/ossec.conf

Thêm 2 thẻ:

<command>

<name>block-ip</name>

<executable>block-ip.cmd</executable>

<timeout_allowed>yes</timeout_allowed>

</command>

Và

<active-response>

<disabled>no</disabled>

<command>block-ip</command>

<location>local</location>

<rules_id>100100</rules_id>

<timeout>600</timeout>

</active-response>

Rule này có ý nghĩa như sau:

Khi rule 100100 (đăng nhập 3 lần thất bại liên tiếp) được kích hoạt sẽ kích hoạt cơ chế tại <command>block-ip</command>. Khi đó Wazuh sẽ tiến hành khởi chạy file block-ip.cmd block IP của máy bị đăng nhập thất bại

Bước 2: Mở notepad trên máy Wazuh Agent dưới quyền Administrator sau đó thêm nội dung:

@echo off

set IP=%1

netsh advfirewall firewall add rule ^

name="Wazuh Block %IP%" ^

dir=in action=block remoteip=%IP%

exit /b 0

Sau đó lưu file dưới tên C:\Program Files (x86)\ossec-agent\active-response\bin\block-ip.cmd

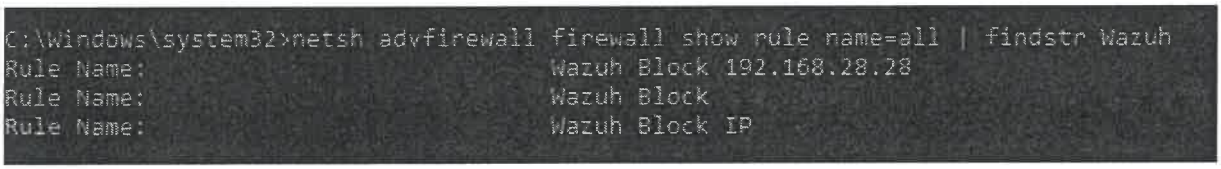
Bước 3: Tiến hành đăng nhập sai 3 lần liên tiếp trên máy Window Agent

Bước 4: Kiểm tra kết quả

Kiểm tra Dashboard sẽ thấy sự kiện Netsh thêm một rule firewall mới



Chạy CMD trên máy Agent dưới quyền Adminstrator và nhập: netsh advfirewall firewall show rule name=all | findstr Wazuh để tìm log mới nhất từ Wazuh



Hình 3.15: Thông tin IP đăng nhập bị block

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

Mục tiêu: Thêm, sửa, xóa file tại thư mục C:\wazuhtest\fim-test.txt và kiểm tra cảnh báo WAZUH.

Bước 1: Mở file C:\Program Files(x86)\ossec-agent\ossec.conf để cấu hình thư mục quản lý.

Bước 2: Thêm thẻ sau vào file ossec.conf

<syscheck>

<disabled>no</disabled>

<directories realtime="yes">C:\wazuhtest</directories>

<frequency>43200</frequency>

</syscheck>

Để quản lý các file trong thư mục C:\wazuhtest. Trong đó:

<frequency>43200</frequency>

Wazuh sẽ kiểm tra trong vòng 43200s (12 giờ) để gom các event liên quan

realtime="yes" – Quản lý theo thời gian thực

Bước 3: Tiến hành thêm/ sửa đổi file và test cảnh báo

Case1: Tạo file C:\wazuhtest\fim-test.txt.

Trên PowerShell bash:

New-Item C:\wazuhtest\fim-test.txt

```
PS C:\Windows\system32> New-Item C:\wazuhtest\fim-test.txt


    Directory: C:\wazuhtest


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         6/25/2026   9:28 PM              0 fim-test.txt
```

Hình 3.16: Tạo file trên Window Agent

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

c:\wazuhtest\fim-test.txt	added	File added to the system.

Hình 3.15: Sự kiện phát hiện thêm file trên Dashboard

Case2: Sửa file C:\wazuhtest\fim-test.txt.

Trên PowerShell bash:

Add-Content C:\wazuhtest\fim-test.txt

```
PS C:\Windows\system32> Add-Content C:\wazuhtest\fim-test.txt
PS C:\Windows\system32>
```

Hình 3.17: Thêm dữ liệu vào file.

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

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

Hình 3.18: Sự kiện thay đổi file trên Dashboard.

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

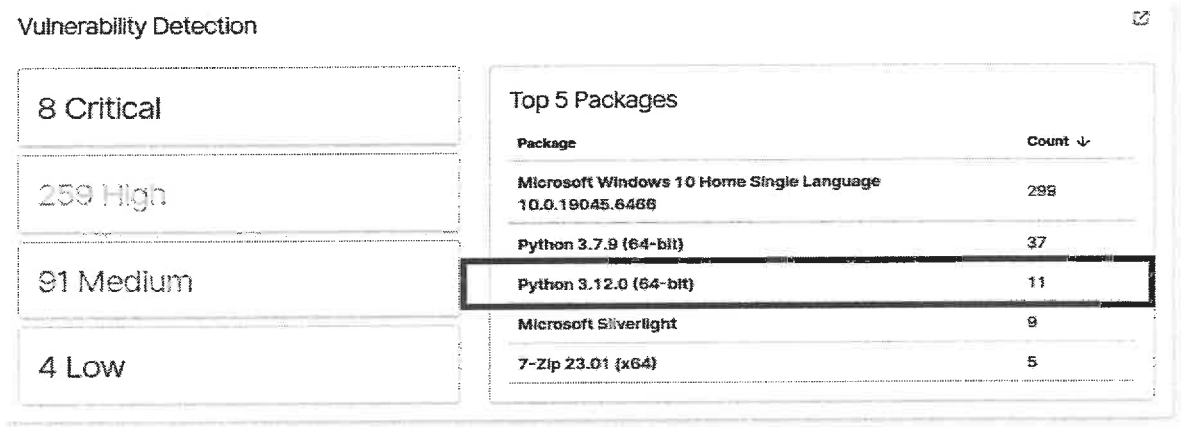
Thực hiện: Cài đặt phiên bản phần mềm cũ chứa lỗ hổng đã biết.

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



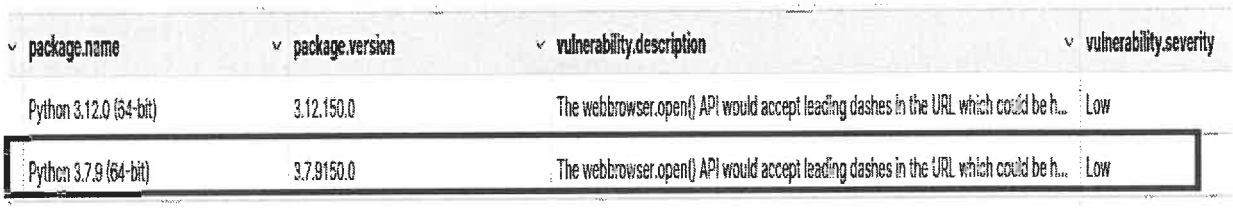
Hình 3.19: Cài đặt phần mềm phiên bản cũ.

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. Wazuh tiến hành đối chiếu các thông tin như: Phiên bản hệ điều hành, danh sách phần mềm đã cài đặt, phiên bản của từng phần mềm và số nguy cơ bảo mật của phần mềm này.



Hình 3.20: Phát sinh cảnh báo.

Hiển thị mức độ nghiêm trọng và khuyến nghị khắc phục.



Hình 3.21: Hiển thị mức độ nghiêm trọng và nguy cơ

Biện pháp phòng chống:

- Cập nhật phiên bản phần mềm.
- Áp dụng bản vá bảo mật.

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

```
<group name="custom_usb">

  <rule id="110002" level="12">
    <if_group>windows</if_group>
    <match>USBSTOR</match>
    <description>USB device connected</description>
  </rule>

</group>
```

Hình 3.22: Cấu hình để phát hiện kết nối USB trên thiết bị

Ý nghĩa:

<if_group>windows</if_group> - Kiểm tra từ log Window

<match>USBSTOR</match> - Nội dung sẽ tạo ra cảnh báo

Tra cứu thông báo tại: **Threat Hunting -> Events** sẽ thấy thông báo

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

Inspect document details	agent.name	rule.description
Jun 28, 2026 @ 02:40:01.7...	DESKTOP-59JLQS6	USB device connected
Jun 28, 2026 @ 02:40:01.7...	DESKTOP-59JLQS6	USB device connected

Hình 3.23: Cảnh báo kết nối USB

Table JSON

t	_index	wazuh-alerts-4.x-2026.06.27
t	agent.id	007
t	agent.ip	192.168.28.28
t	agent.name	DESKTOP-59JLQS6
◎	data.win.eventdata.commandLine	reg query HKLM\\SYSTEM\\CurrentControlSet\\Enum\\USBSTOR /s
◎	data.win.eventdata.company	Microsoft Corporation
◎	data.win.eventdata.currentDirectory	C:\\Program Files (x86)\\ossec-agent\\

Hình 3.24: Thông tin truy cập

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. Đồng thời, hệ thống giúp nâng cao khả năng giám sát liên tục, rút ngắn thời gian phát hiện và xử lý sự cố, góp phần tăng cường tính bảo mật và đảm bảo hoạt động ổn định của hạ tầng công nghệ thông tin. Tuy nhiên, để đạt hiệu quả tối ưu, Wazuh cần được cấu hình phù hợp với đặc thù của từng hệ thống và kết hợp với các giải pháp bảo mật khác nhằm xây dựng một cơ chế phòng thủ nhiều lớp.

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

1. Kết luận

Mặc dù trong quá trình nghiên cứu và triển khai đề tài đề án vẫn gặp không ít khó khăn, nhưng nhờ sự hướng dẫn tận tình của thầy ĐINH TRƯỜNG DUY cùng với tinh thần nỗ lực, chủ động, đề án đã đạt được nhiều kết quả vượt mong đợi so với đề cương ban đầu. Cụ thể, 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.

Đề án cũng đã nắm vững quy trình cài đặt, cấu hình và tùy chỉnh hệ thống Wazuh, từ việc nhỏ nhất là cài đặt agent cho đến tích hợp các chức năng khác và đưa lên trang chủ giám sát. Qua đó, 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.

Thông qua quá trình thực hiện đồ án, đề án đã cải thiện đáng kể nhiều kỹ năng quan trọng như: làm việc nhóm, trình bày báo cáo, tổng hợp và tóm tắt tài liệu chuyên ngành. Đặc biệt, việc thực hành thực tế giúp rèn luyện tư duy phản biện, khả năng liên kết các vấn đề, nhìn nhận tình huống một cách đa chiều và linh hoạt hơn. Nhờ vậy, đề án đã từng bước khắc phục được những hạn chế về chuyên môn và kỹ năng, chuẩn bị nền tảng tốt hơn cho các công việc trong tương lai

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. Cụ thể, việc ứng dụng các mô hình học máy có thể giúp hệ thống học từ các mẫu dữ liệu lịch sử để 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.

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.

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. Trong bối cảnh các cuộc tấn công mạng ngày càng gia tăng và phức tạp, việc ứng dụng Wazuh 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.

TÀI LIỆU THAM KHẢO

[1] Akobe-Ajibolu, E. (2024, January 15). Step-by-step setup of Wazuh SIEM on Ubuntu 22.04.3 LTS. Medium. https://medium.com/@akobeajiboluemmanuel/step-by-step-setup-of-wazuh-siem-on-ubuntu-22-04-3-lts-4663104fe69b truy cập ngày 29/06/2026.

[2] SECUREMINDACADEMY. (n.d.). Youtube. Retrieved April 28, 2025, from https://www.youtube.com/@SECUREMINDACADEMY, truy cập ngày 29/06/2026.

[3] DFIR-IRIS and integrate with WAZUH: step-by-step guide. (n.d.). Certbar.com. Retrieved April 28, 2025, from https://certbar.com/technical-blogs/install-dfir-iris-and-integration-with-wazuh truy cập ngày 05/07/2026.

[4] Gupta, R. (2024). Security Monitoring with Wazuh: A hands-on guide to effective enterprise security using real-life use cases in Wazuh. Packt Publishing. truy cập ngày 05/07/2026.

[5] Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures" Gustavo González-Granadillo. (n.d.).

[6] Wazuh. (n.d.). Wazuh documentation. Wazuh.com. Retrieved April 28, 2025, from https://documentation.wazuh.com/current/index.html truy cập ngày 02/07/2026.

[7] Wazuh - Nền tảng bảo mật mã nguồn mở. (2023, August 30). VNPT Cyber Immunity, truy cập ngày 05/07/2026.
https://sec.vnpt.vn/2023/08/wazuh-nen-tang-bao-mat-ma-nguon-mo/

[8] Hướng dẫn sử dụng hệ thống Snort
https://viblo.asia/p/phan-1-snort-opensource-theo-doi-he-thong-phat-hien-va-canh-bao-xam-nhap-MG24BkGdJz3 truy cập ngày 04/07/2026.

[9] Giới thiệu về hệ thống Suricata
https://wiki.nhanhoa.com/kb/suricata-kien-truc-va-co-che-hoat-dong-cua-he-thong-giam-sat-an-ninh-mang/, truy cập ngày 04/07/2026.

[10] Giới thiệu về hệ thống OSSEC

https://viblo.asia/p/tim-hieu-ve-he-thong-phat-hien-xam-nhap-ossec-phan-ii-ByEZkwd2ZQ0 truy cập ngày 04/07/2026.

[11] Phân tích về hệ thống Splunk

https://ngheandost.gov.vn/nghien-cuu-kh/he-thong-phan-tich-vet-truy-cap-dich-vu-cho-phep-phat-hien-canh-bao-hanh-vi-bat-thuong-va-nguy-co-mat-an-toan-thong-tin-trong-chinh-phu-dien-tu-2126.html truy cập ngày 04/07/2026.

[12] Tìm hiểu về hệ thống ELK

https://viettelidc.com.vn/tin-tuc/elk-stack-la-gi-tim-hieu-nen-tang-quan-ly-va-phan-tich-log-pho-bien-hien-nay-5495 truy cập ngày 04/07/2026.

[13] Tìm hiểu sơ đồ hoạt dộng của Zeek

https://blog.desdelinux.net/vi/zeek/ truy cập ngày 04/07/2026.

[14] Nghiên cứu hệ thống phân tích truy vết

https://ngheandost.gov.vn/nghien-cuu-kh/he-thong-phan-tich-vet-truy-cap-dich-vu-cho-phep-phat-hien-canh-bao-hanh-vi-bat-thuong-va-nguy-co-mat-an-toan-thong-tin-trong-chinh-phu-dien-tu-2126.html truy cập ngày 04/07/2026

BẢN CAM ĐOAN

Tôi cam đoan đã thực hiện việc kiểm tra mức độ tương đồng nội dung đề án qua phần mềm *Tailieu.vn* một cách trung thực và đạt kết quả mức độ tương đồng 11% toàn bộ nội dung đề án. Bản đề án kiểm tra qua phần mềm là bản cứng đề án đã nộp để bảo vệ trước hội đồng. Nếu sai tôi xin chịu các hình thức kỷ luật theo quy định hiện hành của Học viện.

Hà Nội, ngày 30 tháng 03 năm 2026

HỌC VIÊN CAO HỌC



Lê Thị Lý

KiểmTraTàiLiệu

BÁO CÁO KIỂM TRA TRÙNG LẶP

Thông tin tài liệu

Tên tài liệu:	Đề án_LÊ Thị Lý_B23CHIS018 demo (Autosaved)
Tác giả:	Le Thi Ly
Điểm trùng lặp:	11
Thời gian tải lên:	16:12 07/07/2026
Thời gian sinh báo cáo:	16:14 30/07/2026
Các trang kiểm tra:	92/92 trang

Kết quả kiểm tra trùng lặp



Có 11% nội dung trùng lặp



Có 89% nội dung không trùng lặp



Có 0% nội dung người dùng loại trừ



Có 0% nội dung hệ thống bỏ qua

Nguồn trùng lặp tiêu biểu

123docz.net gwdu.ptit.edu.vn tailieu.vn

BỘ KHOA HỌC VÀ CÔNG NGHỆ
HỌC VIỆN CÔNG NGHỆ
BƯU CHÍNH VIỄN THÔNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

BÁO CÁO GIẢI TRÌNH
SỬA CHỮA, HOÀN THIỆN ĐỀ ÁN TỐT NGHIỆP

Họ và tên học viên: Lê Thị Lý

Chuyên ngành: Hệ Thống Thông Tin

Khóa: 2023 đợt 1

Tên đề tài: Xây dựng hệ thống giám sát và phát hiện tấn công tại công ty Samsung Display Việt Nam

Người hướng dẫn khoa học: TS. Đinh Trường Duy

Ngày bảo vệ: 21/07/2026

Các nội dung học viên đã sửa chữa, bổ sung trong đề án tốt nghiệp theo ý kiến đóng góp của Hội đồng chấm đề án tốt nghiệp:

TT	Ý kiến hội đồng	Sửa chữa của học viên
1	Rà soát, chỉnh sửa nội dung của Đề án	Học viên đã rà soát, chỉnh sửa các lỗi soạn thảo, các lỗi ngữ pháp. Đã chỉnh sửa nội dung để trình bày lại lý do vì sao cần phát triển hệ thống hệ thống giám sát và phát hiện tấn công
2	Chuẩn hóa danh mục tài liệu tham khảo	Tiếp thu góp ý của Hội đồng, tác giả đã chuẩn hóa danh mục tài liệu tham khảo theo đúng nội dung tham khảo

Hà Nội, ngày 29 tháng 07 năm 2026

Ký xác nhận của

CHỦ TỊCH HỘI ĐỒNG CHẤM ĐỀ ÁN	THƯ KÝ HỘI ĐỒNG	NGƯỜI HƯỚNG DẪN KHOA HỌC	HỌC VIÊN
TS. Nguyễn Duy Phương	TS. Đào Thị Thúy Quỳnh	TS. Đinh Trường Duy	Lê Thị Lý

BỘ KHOA HỌC VÀ CÔNG NGHỆ
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

BIÊN BẢN
HỌP HỘI ĐỒNG CHẤM ĐỀ ÁN TỐT NGHIỆP THẠC SĨ

Căn cứ quyết định số Quyết định số 1949/QĐ-HV ngày 07 tháng 07 năm 2026 của Giám đốc Học viện Công nghệ Bưu chính Viễn thông về việc thành lập Hội đồng chấm đề án tốt nghiệp thạc sĩ. Hội đồng đã họp vào hồi 10 giờ 15 phút, ngày 21 tháng 07 năm 2026 tại Học viện Công nghệ Bưu chính Viễn thông để chấm đề án tốt nghiệp thạc sĩ cho:

Học viên: **Lê Thị Lý**

Tên đề án tốt nghiệp: **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: **8480104**

Các thành viên của Hội đồng chấm đề án tốt nghiệp có mặt: 5 / 05

TT	HỌ VÀ TÊN	TRÁCH NHIỆM TRONG HĐ	GHI CHÚ
1	**TS. Nguyễn Duy Phương**	Chủ tịch	
2	**TS. Đào Thị Thúy Quỳnh**	Thư ký	
3	**PGS.TS. Đặng Văn Đức**	Phản biện 1	
4	**TS. Trần Minh Tân**	Phản biện 2	
5	**TS. Đào Ngọc Phong**	Uỷ viên	

Các nội dung thực hiện:

1. Chủ tịch Hội đồng điều khiển buổi họp. Công bố quyết định của Giám đốc Học viện Công nghệ Bưu chính Viễn thông về việc thành lập Hội đồng chấm đề án tốt nghiệp thạc sĩ.
2. Người hướng dẫn khoa học hoặc thư ký đọc lý lịch khoa học và các điều kiện bảo vệ đề án tốt nghiệp của học viên. (có bản lý lịch khoa học và kết quả các môn học cao học của học viên kèm theo).
3. Học viên trình bày tóm tắt đề án tốt nghiệp.
4. Phản biện 1 đọc nhận xét (có văn bản kèm theo)
5. Phản biện 2 đọc nhận xét (có văn bản kèm theo)
6. Các câu hỏi của thành viên Hội đồng:

1) Cái luật mà em xây dựng có tác dụng gì để cảnh báo được tấn công giả?

2.) Đánh giá được không về cảnh báo sai?

3.) Xây dựng mở rộng của doanh nghiệp?

7. Trả lời của học viên:

1) Đây cũng chính là hướng phát triển tiếp theo mà Đề án sẽ tiếp tục phát triển và nghiên cứu kỹ hơn.

2) Đây cũng chính là hạn chế mà học viên mong muốn phát triển thêm trong tương lai em xi phát triển tiếp, nâng cấp liên

3) Trong 20 line có khoảng 5000 agent, em cũng mong muốn sẽ kết nối thành một khối bởi phương thức kết nối mạng

8. Thư ký đọc nhận xét về quá trình thực hiện đề án tốt nghiệp của học viên *(có văn bản kèm theo)*.

9. Hội đồng họp riêng:

- Bầu Ban kiểm phiếu:
  1. Trưởng Ban kiểm phiếu: TS. Nguyễn Duy Phương
  2. Uỷ viên Ban kiểm phiếu: TS. Đào Ngọc Phong
  3. Uỷ viên Ban kiểm phiếu: TS. Đào Thị Thúy Quỳnh
- Hội đồng chấm đề án tốt nghiệp bằng bỏ phiếu kín.
- Ban kiểm phiếu làm việc:
- Trưởng Ban kiểm phiếu báo cáo kết quả kiểm phiếu *(có Biên bản họp Ban kiểm phiếu kèm theo)*
- **Điểm trung bình của đề án tốt nghiệp:** 8,5

Kết luận:

1. Các nội dung cần chỉnh sửa, hoàn thiện sau bảo vệ đề án tốt nghiệp:

- Rà soát, chỉnh sửa nội dung của đề án
- Chuẩn bị danh mục tài liệu tham khảo

2. Đề nghị Học viện công nhận (hoặc không) và cấp bằng (hoặc không) thạc sĩ cho học viên: Có đề nghị công nhận

3. Đề án tốt nghiệp có thể phát triển thành đề tài nghiên cứu cho NCS: Không

Buổi làm việc kết thúc vào..... cùng ngày.

Chủ tịch	Thư ký
Nguyễn Duy Phương	Đào Thị Thúy Quỳnh

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

BẢN NHẬN XÉT ĐỀ ÁN TỐT NGHIỆP THẠC SĨ

(*Dùng cho người phản biện*)

Tên đề tài đề án tốt nghiệp: 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 chuyên ngành: 8.48.01.04.

Họ và tên học viên: Lê Thị Lý.

Họ và tên người nhận xét: Trần Minh Tân.

Học hàm, học vị: Tiến sỹ.

Chuyên ngành: Công nghệ thông tin.

Cơ quan công tác: Học viện Chiến lược Khoa học và Công nghệ.

Số điện thoại: 0913275577; E-mail: tantm@mst.gov.vn

NỘI DUNG NHẬN XÉT

I/ Cơ sở khoa học và thực tiễn, tính cấp thiết của đề tài:

Đề tài lựa chọn nghiên cứu xây dựng hệ thống giám sát và phát hiện tấn công mạng cho môi trường doanh nghiệp sản xuất quy mô lớn. Trong bối cảnh các cuộc tấn công mạng ngày càng gia tăng về quy mô và mức độ tinh vi, đặc biệt đối với các doanh nghiệp sở hữu hạ tầng CNTT lớn như Samsung Display Việt Nam, việc xây dựng hệ thống giám sát tập trung, phát hiện sớm các nguy cơ mất an toàn thông tin có ý nghĩa thực tiễn cao.

II/ Nội dung của đề án tốt nghiệp, các kết quả đã đạt được:

Đề án được tổ chức hợp lý gồm ba chương: Cơ sở lý luận; Nghiên cứu và triển khai nền tảng Wazuh; Xây dựng hệ thống giám sát và thực nghiệm trên môi trường mô phỏng. Bố cục các chương tương đối logic, phù hợp với mục tiêu nghiên cứu.

Học viên đã thực hiện các nội dung chính:

- Nghiên cứu kiến trúc và cơ chế hoạt động của Wazuh;

- Triển khai cài đặt Wazuh Server và Agent;

- Xây dựng mô hình giám sát phù hợp với môi trường doanh nghiệp và thực hiện mô phỏng một số tình huống tấn công, ghi nhận cảnh báo để đánh giá khả năng phát hiện và giám sát của hệ thống.

Đề tài có giá trị ứng dụng cao, đặc biệt đối với các doanh nghiệp có nhu cầu triển khai hệ thống giám sát an toàn thông tin sử dụng nền tảng mã nguồn mở. Tuy nhiên, dưới góc độ nghiên cứu khoa học, đề án vẫn còn một số hạn chế:

1. Đóng góp nghiên cứu chưa thật sự nổi bật. Phần lớn nội dung tập trung vào triển khai và cấu hình nền tảng Wazuh. Cần làm rõ hơn những nội dung học viên tự thiết kế hoặc tùy biến (Decoder, Rule, Active Response,...) để khẳng định giá trị của đề án.
2. Đánh giá thực nghiệm còn hạn chế. Các kịch bản mô phỏng mới tập trung vào một số tình huống điển hình; chưa có đánh giá định lượng về tỷ lệ phát hiện, tỷ lệ cảnh báo sai (false positive), thời gian phản hồi hoặc khả năng chịu tải của hệ thống.
3. Khả năng mở rộng của giải pháp đối với các môi trường doanh nghiệp khác hoặc hệ thống có quy mô lớn hơn chưa được phân tích đầy đủ.
4. Thiếu so sánh với các giải pháp khác. Đề án có giới thiệu nhiều công cụ (Snort, Suricata, Zeek, QRadar...) nhưng chưa có phân tích so sánh sâu để làm rõ lý do lựa chọn Wazuh ngoài yếu tố mã nguồn mở.
5. Đánh giá vận hành trong môi trường thực tế cần được bổ sung, nhất là các yêu cầu về bảo trì, cập nhật luật phát hiện và khả năng tích hợp với hệ thống SOC hiện có.

Nhìn chung, học viên đã hoàn thành mục tiêu nghiên cứu theo định hướng ứng dụng và xây dựng được mô hình thử nghiệm có khả năng triển khai trong thực tế.

III/ Những vấn đề cần giải thích thêm:

1. Nếu triển khai cho hệ thống có hàng chục nghìn Agent, học viên dự đoán những điểm nghẽn nào sẽ xuất hiện và đã có phương án đề xuất giải pháp khắc phục?

2. Đề án đã đánh giá tỷ lệ cảnh báo sai (False Positive) hoặc khả năng bỏ sót tấn công (False Negative) hay chưa?

3. Trong trường hợp xuất hiện một kỹ thuật tấn công hoàn toàn mới chưa có luật phát hiện, hệ thống Wazuh sẽ xử lý như thế nào? Học viên đề xuất giải pháp bổ sung nào để nâng cao khả năng phát hiện?

IV/ Kết luận:

Đề án có ý nghĩa thực tiễn, lựa chọn bài toán đang được quan tâm trong lĩnh vực an toàn thông tin doanh nghiệp. Học viên đã nghiên cứu, triển khai và thử nghiệm hệ thống giám sát dựa trên nền tảng Wazuh; kết quả bước đầu cho thấy giải pháp có khả năng hỗ trợ giám sát và phát hiện một số dạng tấn công phổ biến.

Mặc dù phần đóng góp khoa học và đánh giá thực nghiệm còn cần phải tiếp tục hoàn thiện thêm, tuy nhiên Học viên đã cơ bản hoàn thành các nội dung đặt ra trong đề cương và báo cáo đề án đáp ứng yêu cầu của một đề án tốt nghiệp thạc sĩ theo định hướng ứng dụng.

Đồng ý cho phép học viên bảo vệ đề án tốt nghiệp./.

Ngày 20 tháng 7 năm 2026
NGƯỜI NHẬN XÉT

Trần Minh Tân

TẬP ĐOÀN BƯU CHÍNH VIỄN THÔNG VN
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH-VIỄN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

BẢN NHẬN XÉT ĐỀ ÁN TỐT NGHIỆP THẠC SỸ
(Dùng cho cán bộ phản biện)

Tên đề tài đề án: ***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
Tên học viên: **Lê Thị Lý**
Cán bộ hướng dẫn: TS. Đinh Trường Duy
Họ và tên người nhận xét: PGS.TS Đặng Văn Đức, PB1
Chuyên ngành: Công nghệ thông tin
Cơ quan công tác: Viện Công nghệ thông tin, Viện Hàn lâm KH&CN Việt Nam

NỘI DUNG NHẬN XÉT

I. Cơ sở khoa học và thực tiễn, tính cấp thiết của đề án

Đề án của học viên *Lê Thị Lý* lựa chọn nghiên cứu xây dựng hệ thống giám sát và phát hiện tấn công mạng trên nền tảng Wazuh cho Công ty Samsung Display Việt Nam. Đây là vấn đề có ý nghĩa thực tiễn, phù hợp với xu hướng tăng cường bảo đảm an toàn thông tin tại các doanh nghiệp có hạ tầng CNTT lớn. Học viên đã xuất phát từ nhu cầu thực tế của doanh nghiệp, trong đó nêu được một số khó khăn như chi phí duy trì các giải pháp thương mại cao, hạ tầng có nhiều máy chủ và máy trạm, yêu cầu giám sát tập trung cũng như phát hiện sớm các nguy cơ mất an toàn thông tin. Vì vậy, đề tài có tính cấp thiết và phù hợp với định hướng ứng dụng của chương trình đào tạo.

Phần cơ sở lý luận trình bày các nội dung về giám sát an toàn mạng, IDS/IPS, SIEM và giới thiệu một số nền tảng phổ biến như Wazuh, Snort, Suricata, OSSEC, ELK Stack, Splunk và IBM QRadar. Nội dung tương đối đầy đủ, giúp làm rõ cơ sở để triển khai hệ thống. Tuy nhiên, phần tổng quan chủ yếu dừng ở việc giới thiệu các công nghệ và công cụ, chưa phân tích các nghiên cứu liên quan cũng như chưa chỉ ra khoảng trống mà đề án cần giải quyết. Việc lựa chọn Wazuh cũng mới được giải thích chủ yếu từ góc độ chi phí và khả năng triển khai, chưa có sự so sánh cụ thể với các giải pháp khác theo các tiêu chí như hiệu năng, khả năng mở rộng, chi phí vận hành hoặc yêu cầu quản trị. Các số liệu của Samsung Display trong đề án đều không có trích dẫn nguồn cụ thể, cần bổ sung.

II. Về nội dung, chất lượng của đề án, các kết quả đã đạt được

Đề án được trình bày theo bố cục hợp lý, các chương bám sát mục tiêu nghiên cứu. Kết quả nổi bật của đề án là học viên đã triển khai được hệ thống Wazuh gồm các thành phần Server, Indexer, Dashboard và Agent trên cả Windows và Linux. Học viên đã xây dựng một số kịch bản thử nghiệm như phát hiện tấn công Brute Force, giám sát thay đổi tập tin, phát hiện phần mềm tồn tại lỗ hổng bảo mật, phát hiện kết nối thiết bị USB và cấu hình

Active Response để tự động chặn địa chỉ IP. Ngoài ra, đề án cũng xây dựng thêm các Decoder, Rule phục vụ cảnh báo và bước đầu đề xuất cấu hình cho hệ thống có quy mô lớn hơn. Những kết quả này cho thấy học viên đã nắm được quy trình cài đặt, cấu hình và khai thác nền tảng Wazuh, đồng thời có khả năng vận dụng vào bài toán giám sát an toàn thông tin trong doanh nghiệp.

Tuy nhiên, phần đánh giá kết quả còn thiếu thuyết phục. Các thử nghiệm mới dừng ở việc chỉ ra hệ thống phát hiện được các sự kiện bất thường mà chưa đánh giá bằng các số liệu định lượng như tỷ lệ phát hiện, tỷ lệ cảnh báo giả, thời gian xử lý hoặc mức sử dụng tài nguyên của hệ thống. Đề án mang tên triển khai tại Công ty Samsung Display Việt Nam nhưng các kết quả trình bày chỉ được thực hiện trên môi trường mô phỏng. Về mặt nội dung, đề án chủ yếu dựa trên các chức năng sẵn có của nền tảng Wazuh để xây dựng hệ thống giám sát và cảnh báo. Tuy đây là hướng tiếp cận phù hợp với đề án định hướng ứng dụng, nhưng việc có thêm các đề xuất cải tiến phương pháp phát hiện hoặc giảm cảnh báo giả sẽ làm tăng giá trị của đề án. Về hình thức trình bày, đề án cơ bản đáp ứng yêu cầu. Tuy nhiên vẫn còn một số lỗi cần chỉnh sửa như đánh số chương, mục, bảng và hình chưa thống nhất; một số bảng, hình chưa được tham chiếu đầy đủ trong nội dung; cách trình bày tài liệu tham khảo và trích dẫn chưa theo qui định. Ngoài ra, đề án chưa đề cập đến các vấn đề như bảo vệ kênh truyền dữ liệu giữa Agent và Server, cơ chế xác thực Agent, cũng như phương án dự phòng khi Wazuh Server gặp sự cố trong môi trường sản xuất thực tế.

Câu hỏi dành cho học viên:

a. Học viên lựa chọn Wazuh thay vì Splunk hoặc IBM QRadar dựa trên những tiêu chí nào? Nếu chỉ xét trong môi trường của Samsung Display thì Wazuh có những ưu điểm và hạn chế gì?
b. Khi triển khai cho hệ thống có hàng nghìn máy trạm, học viên đánh giá như thế nào về khả năng mở rộng, hiệu năng và yêu cầu tài nguyên của hệ thống?
c. Các luật cảnh báo do học viên xây dựng đã được kiểm tra như thế nào để hạn chế cảnh báo giả? Có tiêu chí nào để đánh giá hiệu quả của các luật này không?
d. Nếu cần nâng cao khả năng phát hiện các cuộc tấn công chưa có mẫu nhận dạng (zero-day attack), học viên sẽ lựa chọn hướng phát triển nào? Việc tích hợp *Machine Learning* hoặc *Threat Intelligence* có khả thi trên nền tảng Wazuh hay không?

III. Kết luận

Bản đề án tốt nghiệp thạc sỹ này đã trình bày được các nội dung cơ bản để đạt được mục tiêu đề ra. Tuy vẫn còn một số điểm cần bổ sung và hoàn thiện như đã nêu trên, đề án nhìn chung đáp ứng yêu cầu của đề án thạc sĩ kỹ thuật định hướng ứng dụng. Tôi đồng ý để học viên *Lê Thị Lý* được bảo vệ tại Hội đồng chấm đề án thạc sỹ của Học viện CNBCVT.

Hà Nội, ngày tháng 7 năm 2026

NGƯỜI NHẬN XÉT

PGS.TS Đặng Văn Đức