

SOLUTION PROPOSAL

Prepared for:
Company

company@gmail.com
www.company1.com
8386-8386-8386

Prepared by:
Nguyễn Tài Hiếu

taihieunguyen@gmail.com
www.taihieunguyen.com
123-1233-1231

MỤC LỤC

I. Bối cảnh an ninh mạng hiện tại.....	4
II. Các thách thức chính.....	4
III. Đề xuất giải pháp toàn diện.....	5
IV. Thành phần và tính năng của giải pháp.....	6
4.1. Thành phần của Wazuh	6
4.1.1. Wazuh indexer	7
4.1.2. Wazuh server	8
4.1.3. Wazuh dashboard.....	10
4.1.4. Wazuh agent	12
4.2. Tính năng của Wazuh	14
4.2.1. Đánh giá cấu hình (Configuration assessment)	14
4.2.2. Phát hiện mã độc (Malware detection)	15
4.2.3. Giám sát tính toàn vẹn của tệp (File Integrity Monitoring).....	16
4.2.4. Săn tìm mối đe dọa (Threat hunting)	18
4.2.5. Phát hiện lỗ hổng (Vulnerability detection)	22
4.2.6. Tuân thủ theo các quy định (Regulatory compliance)\.....	25
4.2.7. Bảo vệ công việc trên môi trường cloud (Cloud workload protection)	28
V. Giải pháp nâng cao: Trợ lý an ninh ảo (AI Assisstant).....	29
5.1. Thách thức trong phân tích bảo mật và điều tra log truyền thông	29
5.2. Giới thiệu trợ lý ảo	29
5.3. Tính năng và giá trị cốt lõi	30
5.4. Kiến trúc của trợ lý ảo	30
5.4.1. Luồng 1 - Xử lý log và xây dựng cơ sở tri thức.....	31

5.4.2. Luồng 2 - Truy vấn và phản hồi	31
VI. Lợi ích và lợi thế cạnh tranh của Wazuh	32
6.1. Tại sao chọn nền tảng Wazuh?	32
6.2. So sánh với các giải pháp thương mại khác	33
6.2.1. Các giải pháp Enterprise hàng đầu	33
6.2.2. So sánh ưu và nhược điểm (Wazuh và Enterprise)	34

I. BỐI CẢNH AN NINH MẠNG HIỆN TẠI

Chúng ta đang hoạt động trong một kỷ nguyên mà chuyển đổi số không còn là một lựa chọn, mà là yếu tố sống còn của doanh nghiệp. Hạ tầng Công nghệ thông tin, từ on-premise, cloud, hybrid-cloud đến các thiết bị người dùng cuối (endpoints) và IoT (Internet of thing), đã trở thành xương sống cho mọi hoạt động vận hành, giao dịch và lưu trữ tài sản trí tuệ.

Trong bối cảnh đó, an ninh mạng đã vượt ra khỏi phạm vi của một vấn đề kỹ thuật thuần túy để trở thành một yếu tố chiến lược cấp cao. Lý do rất rõ ràng: dữ liệu là tài sản vô giá, tội phạm mạng ngày càng chuyên nghiệp hóa với các hình thức tấn công tống tiền (Ransomware) và gián tiếp có chủ đích, trong khi xu hướng “làm việc từ mọi nơi” đã xóa mờ hoàn toàn ranh giới an ninh mạng, khiến bể mặt tấn công của doanh nghiệp mở rộng ra toàn cầu.

Do đó, tư duy an ninh mạng hiện đại đã buộc phải chuyển dịch. Thay vì chỉ tập trung vào phòng thủ (Prevention) với giả định có thể ngăn chặn 100% các cuộc tấn công, các tổ chức hàng đầu đang áp dụng mô hình “Giả định xâm nhập” (Assume Breach). Mô hình này thừa nhận việc bị xâm nhập chỉ là vấn đề thời gian. Vì vậy, ưu tiên chiến lược được chuyển sang: “Làm thế nào để phát hiện kẻ tấn công đã ở trong hệ thống nhanh nhất có thể, và vô hiệu hóa chúng trước khi chúng kịp gây ra thiệt hại?”. Điều này đặt ra yêu cầu cấp thiết về một khả năng giám sát liên tục, toàn diện và thông minh trên toàn bộ hệ thống.

II. CÁC THÁCH THỨC CHÍNH

Dù nhận thức về tầm quan trọng của việc giám sát đã rõ ràng, các doanh nghiệp đang phải đổi mới với những thách thức kỹ thuật và vận hành vô cùng lớn:

- **Bùng nổ dữ liệu log:** Mỗi ngày, các hệ thống (firewall, máy chủ, cloud, ứng dụng) tạo ra hàng triệu, thậm chí hàng tỷ bản ghi (logs). Dữ liệu này, nếu bị lưu trữ phân tán, sẽ trở thành “dữ liệu câm” – tồn tại nhưng không mang lại giá trị cảnh báo. Kẻ tấn công lợi dụng chính sự phân mảnh này. Mỗi cảnh báo “login thất bại” trên máy chủ A, một “cảnh báo Powershell” trên máy chủ B có thể bị bỏ qua riêng lẻ. Nhưng khi xâu chuỗi lại, chúng là một chuỗi tấn công rõ ràng. Nếu không có hệ thống tập trung, doanh nghiệp không thể thấy được “bức tranh toàn cảnh” của cuộc tấn công.
- **Các “Điểm mù” chết người (Critical Blind Spots):** Nhiều tổ chức chỉ giám sát vành đai (firewall) mà bỏ qua những gì đang xảy ra bên trong hệ thống của mình (máy chủ, máy

trạm). Kẻ tấn công hiện đại (APTs) thường xâm nhập qua một điểm yếu (ví dụ: email lừa đảo) và sau đó “di chuyển ngang” (lateral movement) trong nội bộ. Nếu không giám sát được các hoạt động đáng ngờ này, kẻ tấn công có thể “ẩn mình” nhiều ngày, nhiều tháng để leo thang đặc quyền và đánh cắp dữ liệu.

- **Sự tinh vi của kỹ thuật tấn công “Ẩn mình” (Stealth Tactics):** Kẻ tấn công không còn sử dụng virus dễ bị phát hiện. Chúng chuyển sang kỹ thuật “Sống bằng tài nguyên sẵn có” (Living-off-the-Land), tức là sử dụng chính các công cụ quản trị hợp lệ của hệ thống (như PowerShell, VMI, PsExec) để thực hiện hành vi độc hại. Các công cụ Antivirus truyền thống hoàn toàn không phản ứng với kỹ thuật này vì chúng không thể phân biệt đâu là hành vi quản trị hợp lệ và đâu là hành vi độc hại.
- **Tình trạng Alert Fatigue:** Nhiều giải pháp bảo mật tạo ra quá nhiều cảnh báo “nhiều” (false positives). Điều này khiến đội ngũ vận hành (IT/Security) bị quá tải, dẫn đến việc vô tình bỏ qua những cảnh báo quan trọng thực sự. Thiếu một hệ thống có khả năng lọc nhiễu, phân tích bối cảnh và ưu tiên hóa các mối đe dọa khiến đội ngũ luôn ở trong thế bị động.
- **Tuân thủ các chính sách (Compliance Pressure):** Các quy định pháp lý (như Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, hoặc các chuẩn quốc tế như PCI-DSS, ISO 27001) đều có yêu cầu nghiêm ngặt về việc phải ghi log, lưu trữ và bảo vệ log để phục vụ điều tra, kiểm toán. Việc không tuân thủ có thể dẫn đến các chế tài pháp lý nặng nề.

III. ĐỀ XUẤT GIẢI PHÁP TOÀN DIỆN

Để giải quyết triệt để các thách thức đã phân tích tại Mục II, chúng tôi đề xuất triển khai một giải pháp an ninh mạng toàn diện, bao gồm hai thành phần bổ trợ nhau:

- **Nền tảng SIEM/XDR Wazuh (nền tảng cốt lõi):** Đây là “trái tim” của hệ thống giám sát, cung cấp khả năng phòng thủ và hiển thị toàn diện. Wazuh đóng vai trò là nền tảng SIEM/XDR hợp nhất, chịu trách nhiệm thu thập và tập trung hóa log từ mọi nguồn (máy chủ, cloud, thiết bị mạng). Nó chủ động phát hiện mối đe dọa (sử dụng bộ luật MITRE ATT&CK), giám sát tính toàn vẹn tệp (FIM), đánh giá cấu hình (SCA) và đảm bảo tuân thủ các quy trình (PCI, ISO,...).



- Trợ lý ảo (giải pháp tăng tốc vận hành): Đây là “bộ não” AI thông minh do công ty chúng tôi phát triển, được tích hợp độc quyền vào Wazuh. Nếu Wazuh giải quyết bài toán “Thu thập và phát hiện”, thì trợ lý AI giải quyết bài toán “Phân tích và phản ứng”.
 - Giải quyết triệt để tình trạng “Alert Fatigue” bằng cách tóm tắt hàng trăm cảnh báo thành một chuỗi sự cố duy nhất.
 - Trao quyền cho đội ngũ của bạn bằng cách cho phép hỏi – đáp bằng ngôn ngữ tự nhiên, giúp rút ngắn thời gian điều tra từ hàng giờ xuống còn vài phút.

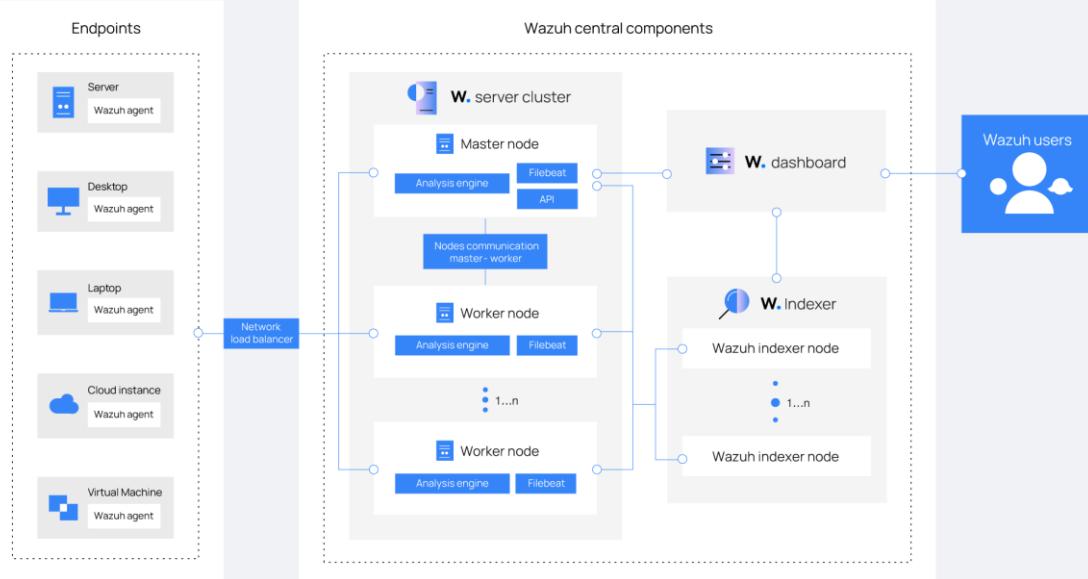
Chúng tôi không chỉ đề xuất một công cụ giám sát – Wazuh, mà là một Trung tâm vận hành An ninh (SOC) thông minh. Sự kết hợp giữa nền tảng Wazuh mạnh mẽ và Trợ lý AI độc quyền sẽ cung cấp cho bạn khả năng phát hiện sớm, hiểu sâu và phản ứng nhanh chóng trước mọi mối đe dọa.

IV. THÀNH PHẦN VÀ TÍNH NĂNG CỦA GIẢI PHÁP

4.1. Thành phần của Wazuh

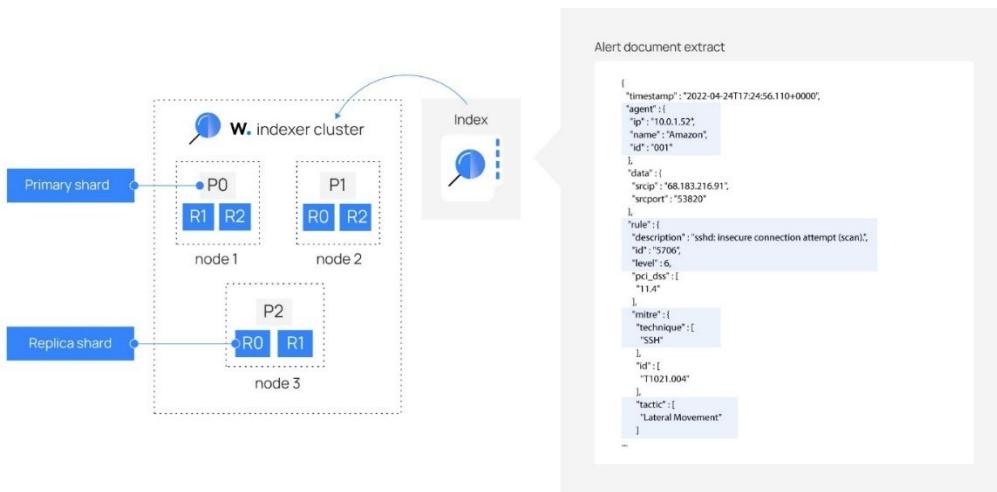
Kiến trúc Wazuh bao gồm một agent đa nền tảng và ba thành phần trung tâm: Wazuh server, Wazuh indexer, và Wazuh dashboard. Agent được triển khai trên các điểm cuối (endpoints) để thu thập và chuyển tiếp dữ liệu bảo mật đến Wazuh server để phân tích. Dữ liệu sau khi phân tích được chuyển tiếp đến Wazuh indexer để lập chỉ mục và lưu trữ, và tiếp theo đến Wazuh dashboard để hiển thị cảnh báo và trực quan hóa.

Wazuh cũng hỗ trợ giám sát không cần agent (agentless monitoring) cho các hệ thống và thiết bị không thể cài đặt Wazuh agent. Các thiết bị mạng như tường lửa, thiết bị chuyển mạch (switches), bộ định tuyến (routers) và điểm truy cập (access points) có thể chủ động chuyển tiếp dữ liệu log qua Syslog và SSH.



Các thành phần trung tâm của Wazuh có thể được triển khai theo nhiều cách khác nhau, tùy thuộc vào nhu cầu về khả năng mở rộng (scalability) và tính sẵn sàng cao (availability): All-in-one deployment, Single-node deployment, Multi-node deployment.

4.1.1. Wazuh indexer.



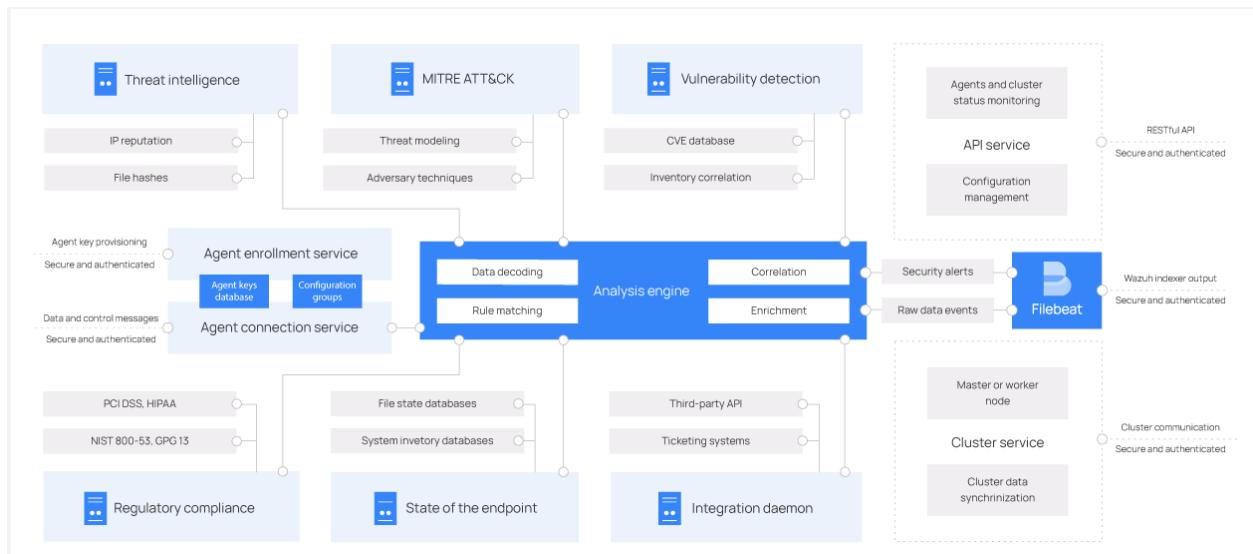
Wazuh indexer rất phù hợp cho các trường hợp sử dụng nhạy cảm về thời gian (time-sensitive) như phân tích bảo mật và giám sát cơ sở hạ tầng, vì nó là một nền tảng tìm kiếm gần như thời

gian thực. Độ trễ (latency) từ thời điểm một tài liệu được lập chỉ mục cho đến khi nó có thể tìm kiếm được là rất ngắn, thường là một giây.

Wazuh indexer lưu trữ dữ liệu dưới dạng tài liệu JSON (JSON documents). Mỗi tài liệu tương quan một tập hợp các khóa (keys), tên trường (field names) hoặc thuộc tính (properties) với các giá trị tương ứng của chúng, có thể là chuỗi, số, giá trị Boolean, ngày tháng, mảng giá trị, vị trí địa lý hoặc các kiểu dữ liệu khác.

4.1.2. Wazuh server

Wazuh server là thành phần trung tâm chịu trách nhiệm phân tích dữ liệu được thu thập từ **Wazuh agents** và các thiết bị không cài agent (agentless). Nó phát hiện các mối đe dọa, sự bất thường và các vi phạm tuân thủ quy định trong thời gian thực, tạo ra cảnh báo khi phát hiện hoạt động đáng ngờ. Ngoài việc phát hiện, Wazuh server còn cho phép quản lý tập trung bằng cách cấu hình các Wazuh agent từ xa và liên tục giám sát trạng thái hoạt động của chúng.



Wazuh server bao gồm một số thành phần có các chức năng khác nhau, chẳng hạn như đăng ký các agent mới, xác thực danh tính của từng agent và mã hóa các giao tiếp giữa Wazuh agent và Wazuh server.

- Dịch vụ Đăng ký Agent (Agent enrollment service):** Đăng ký các Wazuh agent mới, đồng thời tạo và phân phối các khóa xác thực duy nhất cho mỗi agent. Nó chạy như một

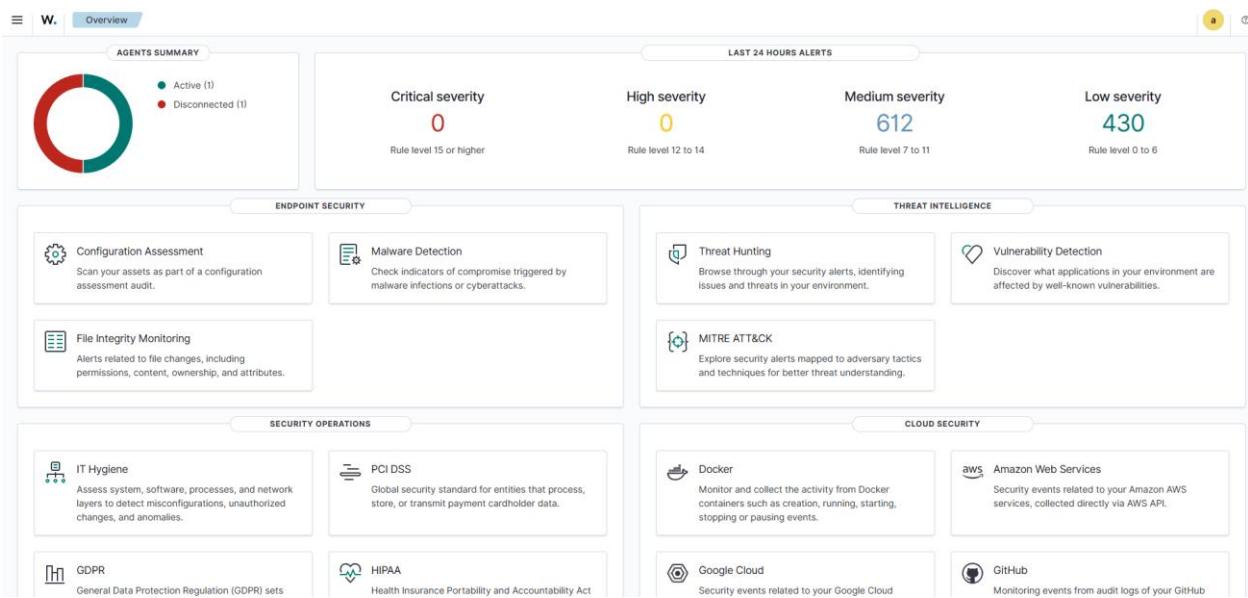
dịch vụ mạng và hỗ trợ xác thực dựa trên chứng chỉ TLS và SSL, hoặc đăng ký bằng mật khẩu cố định.

- **Dịch vụ Kết nối Agent (Agent connection service):** Quản lý giao tiếp giữa Wazuh agent và Wazuh server. Nó xác thực danh tính của Wazuh agent bằng các khóa đăng ký, thực thi mã hóa để truyền dữ liệu an toàn và cho phép quản lý cấu hình tập trung để đầy các cài đặt agent cập nhật từ xa.
- **Công cụ Phân tích (Analysis engine):** Là cốt lõi của khả năng phát hiện mối đe dọa của Wazuh, Công cụ Phân tích xử lý dữ liệu bảo mật nhận được bằng cách sử dụng các bộ giải mã (decoders) và bộ luật (rules):
 - **Bộ giải mã (Decoders)** phân loại các loại log (ví dụ: sự kiện Windows, log SSH, log máy chủ web) và trích xuất các trường liên quan như địa chỉ IP, tên người dùng và ID sự kiện.
 - **Bộ luật (Rules)** so khớp các sự kiện đã được giải mã với các mẫu (patterns) đã biết để phát hiện các mối đe dọa và sự bất thường. Khi được kích hoạt, các bộ luật sẽ tạo ra cảnh báo và gọi các hành động phản ứng sự cố (incident response) như chặn địa chỉ IP, chấm dứt các tiến trình độc hại hoặc loại bỏ các thành phần của phần mềm độc hại.
- **Wazuh server API:** Cung cấp một giao diện lập trình (programmatic interface) để tương tác với Wazuh server. Nó cho phép quản trị viên sử dụng Wazuh dashboard hoặc dòng lệnh để thực hiện các việc sau:
 - Cấu hình và quản lý agent hoặc server
 - Giám sát tình trạng hệ thống và trạng thái cơ sở hạ tầng
 - Truy vấn cảnh báo và dữ liệu điểm cuối
 - Tạo hoặc cập nhật các bộ giải mã và bộ luật
- **Trình điều khiển Cụm Wazuh (Wazuh cluster daemon):** Cho phép mở rộng theo chiều ngang (horizontal scaling) bằng cách kết nối nhiều Wazuh server thành một cụm (cluster). Việc sử dụng bộ cân bằng tải (load balancer) cung cấp tính sẵn sàng cao (high availability), khả năng chịu lỗi (fault tolerance) và phân phối tải (load distribution).
- **Filebeat:** Chuyển tiếp các sự kiện và cảnh báo từ công cụ phân tích của Wazuh đến Wazuh indexer.

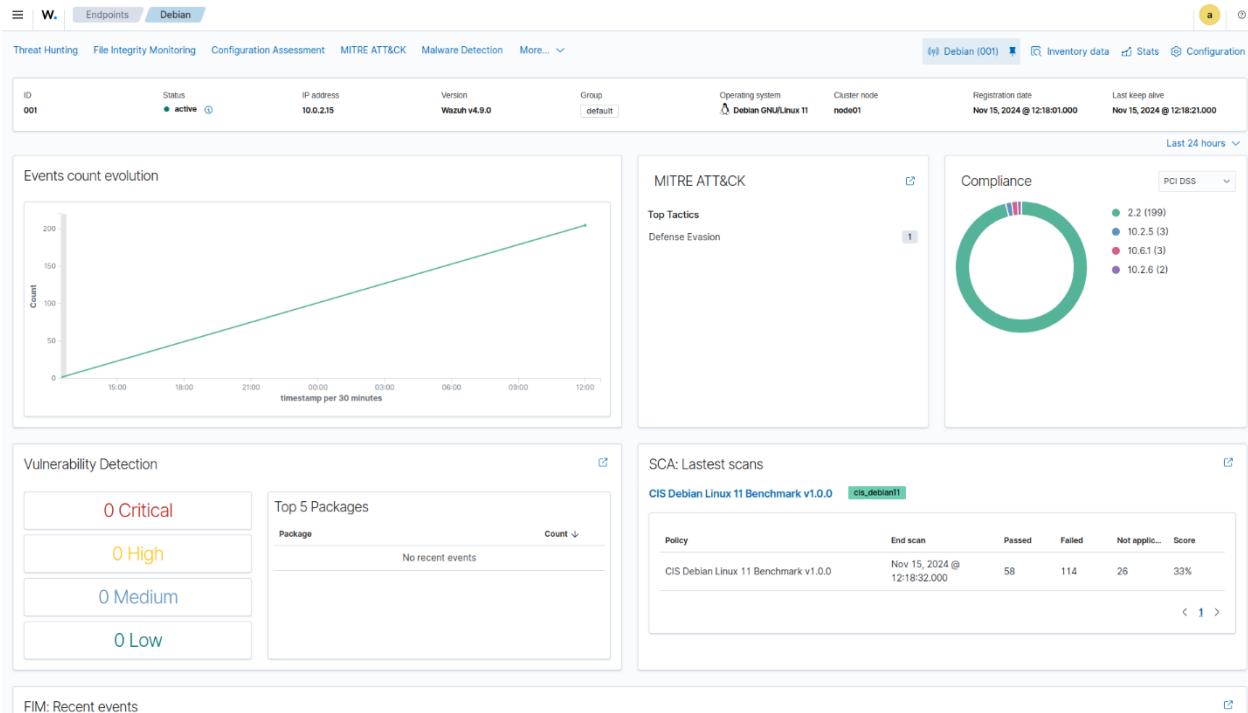
4.1.3. Wazuh dashboard

Wazuh dashboard là một giao diện web linh hoạt và trực quan để trực quan hóa, phân tích và quản lý dữ liệu bảo mật. Nó cho phép người dùng điều tra các sự kiện và cảnh báo, giám sát nền tảng Wazuh, và thực thi các chính sách kiểm soát truy cập dựa trên vai trò (RBAC) và đăng nhập một lần (SSO).

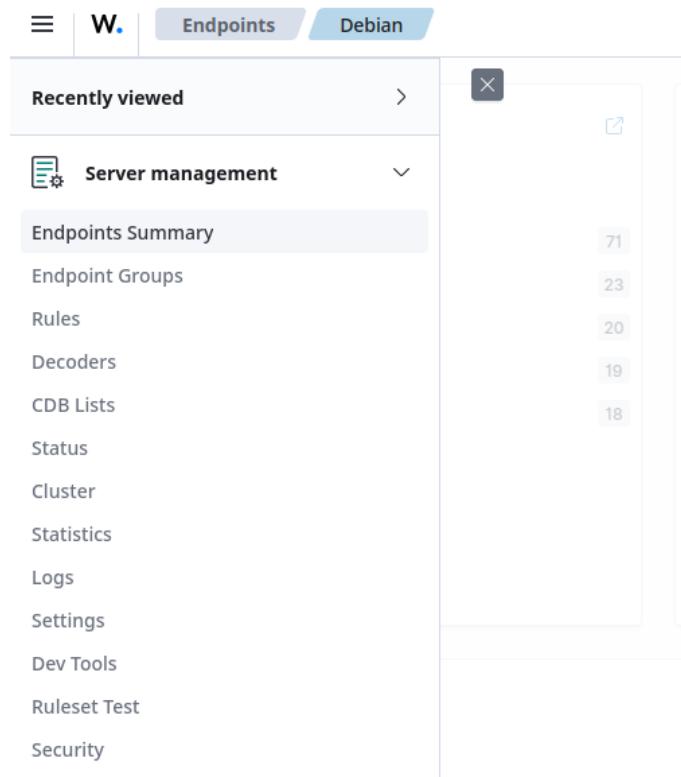
Trực quan hóa và phân tích dữ liệu Wazuh dashboard cho phép người dùng điều hướng (navigate) dữ liệu bảo mật được thu thập từ Wazuh agent và các thiết bị không cài agent (agentless), cũng như các cảnh báo do Wazuh server tạo ra. Nó bao gồm các bảng điều khiển (dashboards) để săn lùng mối đe dọa (threat hunting), phát hiện phần mềm độc hại, giám sát tính toàn vẹn tệp, kiểm kê hệ thống (system inventory) và tuân thủ quy định (ví dụ: PCI DSS, GDPR, HIPAA và NIST 800-53). Chúng ta có thể tạo báo cáo và tạo các hình ảnh trực quan và bảng điều khiển tùy chỉnh.



Giám sát và cấu hình Agent: Wazuh dashboard cho phép người dùng quản lý cấu hình agent và giám sát trạng thái agent. Đối với mỗi điểm cuối (endpoint) được giám sát, người dùng có thể xác định mô-đun agent nào được bật, tệp log nào được đọc, tệp nào được giám sát về các thay đổi tính toàn vẹn, và các kiểm tra cấu hình nào được thực hiện.



Quản lý nền tảng: Wazuh dashboard cung cấp một giao diện người dùng để quản lý một hệ thống Wazuh đã triển khai (Wazuh deployment). Điều này bao gồm giám sát trạng thái, log và số liệu thống kê của các thành phần Wazuh, cấu hình Wazuh server, và tạo các bộ luật (rules) và bộ giải mã (decoders) tùy chỉnh để phân tích log và phát hiện mối đe dọa.



Công cụ cho nhà phát triển (Developer tools): Wazuh dashboard bao gồm một công cụ kiểm tra bộ luật (ruleset test tool) xử lý các thông báo log để hiển thị cách chúng được giải mã và liệu chúng có khớp với một bộ luật phát hiện hay không. Điều này hữu ích khi kiểm tra các bộ giải mã và bộ luật tùy chỉnh.



The screenshot shows the 'Ruleset Test' interface. At the top, there's a header with tabs for 'W.' and 'Ruleset Test'. Below the header, the title 'Ruleset Test' is displayed. A log entry is shown: 'Jul 7 10:51:24 ubuntu-agent sshd[19537]: Invalid user blimy from 1.3.1.3 port 48223'. Below the log, there's a 'Test' button and a 'Clear sess...' button. The main area contains three sections of text: '**Messages:', '**Phase 1: Completed pre-decoding.', and '**Phase 2: Completed decoding.'. The '**Phase 2' section includes detailed information about the event, such as the name ('sshd'), program ('/usr/sbin/sshd'), source IP ('1.3.1.3'), source port ('48223'), and user ('blimy'). The '**Phase 3' section shows the final output of the rule matching process.

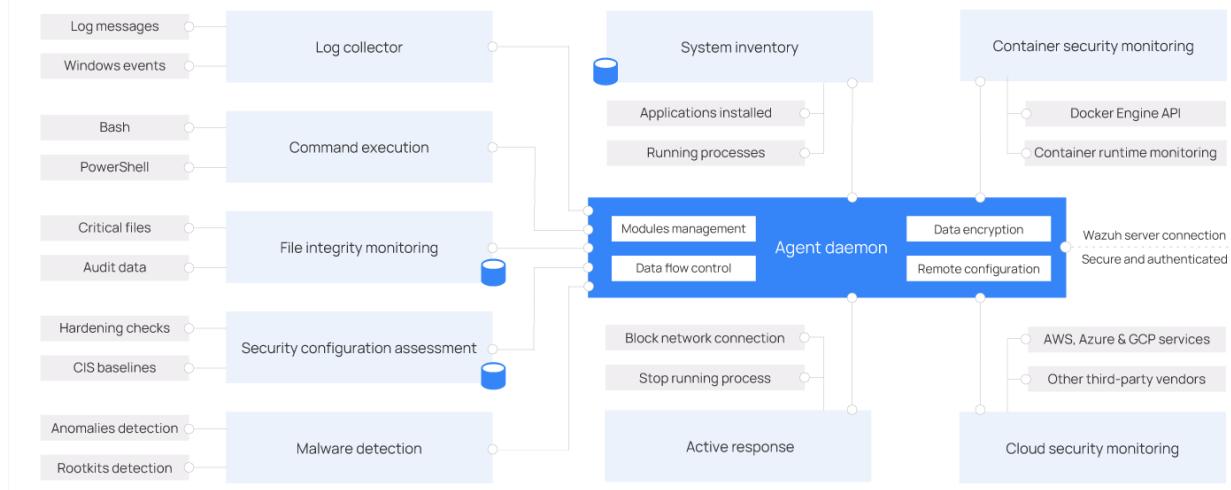
```
**Messages:  
INFO: (7202): Session initialized with token 'c0b5c0ec'  
  
**Phase 1: Completed pre-decoding.  
full_event: 'Jul 7 10:51:24 ubuntu-agent sshd[19537]: Invalid user blimy from 1.3.1.3 port 48223'  
timestamp: 'Jul 7 10:51:24'  
hostname: 'ubuntu-agent'  
program_name: 'sshd'  
  
**Phase 2: Completed decoding.  
name: 'sshd'  
program: '/usr/sbin/sshd'  
srcip: '1.3.1.3'  
srcport: '48223'  
srcuser: 'blimy'  
  
**Phase 3: Completed filtering (rules).  
id: 'syno'  
level: 'S'  
description: 'sshd: Attempt to login using a non-existent user'  
groups: ['syslog', 'sshd', 'authentication_failed', 'invalid_login']  
firedtimes: '1'  
gdpr: ['TIV_38.7.d', 'TIV_32.2']  
geopl: ['7.7.1.1']  
https: ['1.3.1.3:48223']  
mail: 'False'  
mitre_id: ['T1110.001', 'T1021.004']'
```

Wazuh server tích hợp với các nền tảng bên ngoài để hỗ trợ các quy trình công việc được tinh giản. Ví dụ bao gồm các hệ thống ticketing như ServiceNow, Jira và PagerDuty, cũng như các công cụ giao tiếp như Slack. Các tích hợp này giúp tự động hóa việc theo dõi sự cố, tăng tốc thời gian phản hồi và cải thiện sự hợp tác trong các nhóm vận hành an ninh.

4.1.4. Wazuh agent

Wazuh agent chạy trên Linux, Windows, macOS, Solaris, AIX và các hệ điều hành khác. Nó có thể được triển khai trên máy tính xách tay, máy tính để bàn, máy chủ, các phiên bản cloud (cloud instances), container hoặc máy ảo. Wazuh agent giúp bảo vệ hệ thống bằng cách cung cấp các khả năng ngăn chặn, phát hiện và phản hồi mới đe dọa. Nó cũng được sử dụng để thu thập các loại dữ liệu hệ thống và ứng dụng khác nhau mà nó chuyển tiếp đến **Wazuh server** thông qua một kênh được mã hóa và xác thực.

Kiến trúc Agent:



Các mô-đun của Wazuh agent:

Tất cả các mô-đun của agent đều có thể cấu hình và thực hiện các nhiệm vụ bảo mật khác nhau. Kiến trúc mô-đun này cho phép cấu hình từng mô-đun theo nhu cầu bảo mật của mình: Thu thập log (log collector), Thực thi lệnh (Command execution), Giám sát Tính toàn vẹn tệp (File integrity Monitoring – FIM), Đánh giá cấu hình an ninh (Security Configuration Assessment – SCA), Kiểm kê hệ thống (System inventory), Phát hiện phần mềm độc hại (Malware detection), Phản ứng chủ động (Active Response), Giám sát an ninh Container (Container security monitoring), Giám sát an ninh đám mây (Cloud security monitoring).

Giao tiếp với Wazuh server:

Wazuh agent giao tiếp với **Wazuh server** để chuyển tiếp dữ liệu đã thu thập và các sự kiện liên quan đến bảo mật. Wazuh agent cũng gửi dữ liệu hoạt động, báo cáo về cấu hình và trạng thái của nó. Sau khi kết nối, agent có thể được nâng cấp, giám sát và cấu hình từ xa từ Wazuh server.

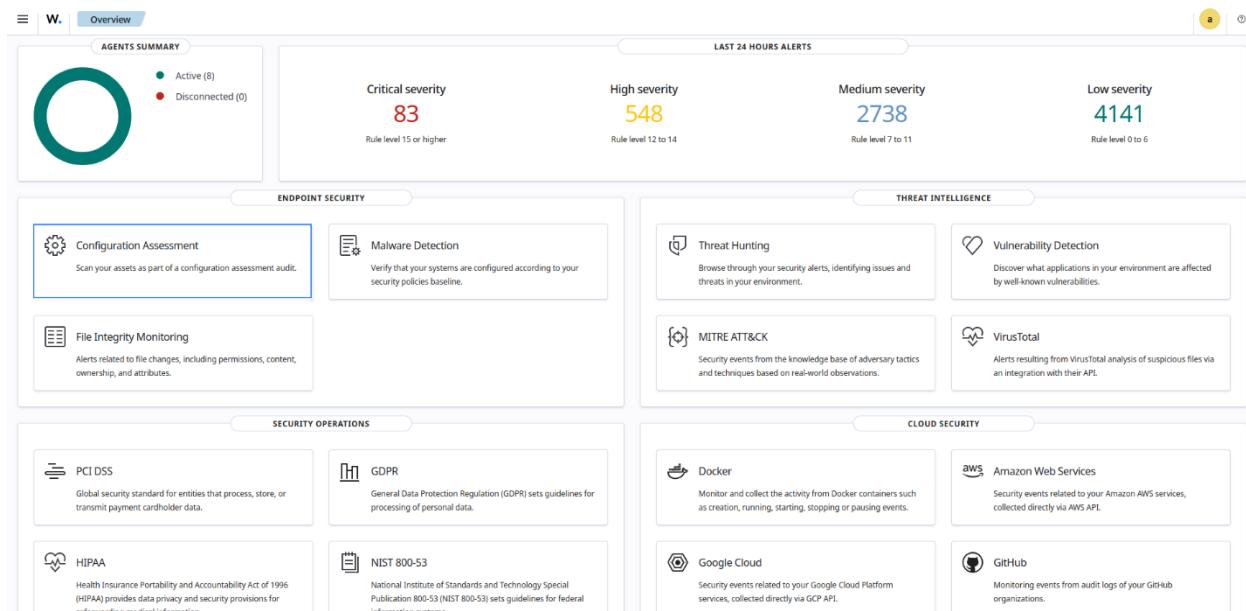
Việc giao tiếp giữa Wazuh agent và Wazuh server diễn ra thông qua một kênh bảo mật (TCP hoặc UDP), cung cấp mã hóa và nén dữ liệu trong thời gian thực. Ngoài ra, nó bao gồm các cơ chế kiểm soát luồng (flow control) để tránh tình trạng quá tải (flooding), xếp hàng các sự kiện khi cần thiết và bảo vệ băng thông mạng.

4.2. Tính năng của Wazuh

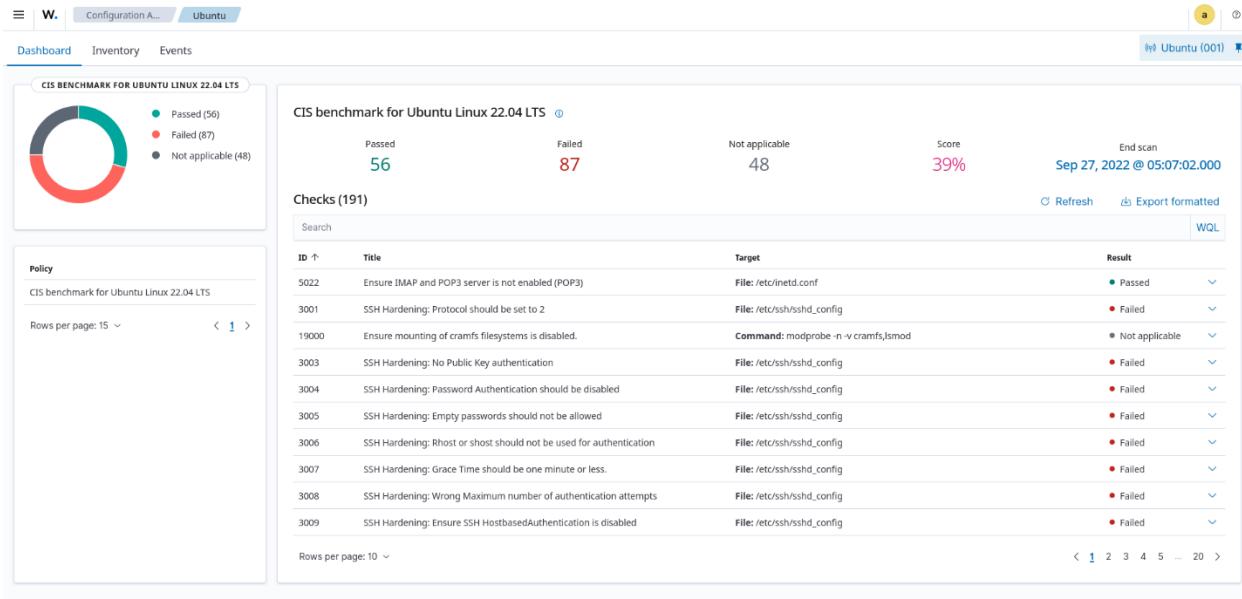
4.2.1. Đánh giá cấu hình (Configuration assessment)

Wazuh cung cấp một mô-đun Đánh giá Cấu hình an ninh (Security Configuration Assessment – SCA) để hỗ trợ đội ngũ bảo mật quét và phát hiện các cấu hình sai trong môi trường của họ. Wazuh agent sử dụng các tệp chính sách (policy files) để quét các điểm cuối mà nó giám sát. Các tệp này chứa các kiểm tra được xác định trước để thực hiện trên mỗi điểm cuối được giám sát.

Wazuh bao gồm các chính sách SCA có sẵn (out-of-the-box) dựa trên các tiêu chuẩn bảo mật (benchmarks) của Trung tâm An ninh Internet (CIS). Các tiêu chuẩn này đóng vai trò là hướng dẫn thiết yếu về các hành động tốt nhất để bảo vệ hệ thống CNTT và dữ liệu khỏi các cuộc tấn công mạng. Wazuh cung cấp hướng dẫn rõ ràng để thiết lập một cấu hình cơ sở (baseline) an toàn và đưa ra chỉ dẫn để đảm bảo người dùng thực hiện các biện pháp hiệu quả nhằm bảo vệ tài sản quan trọng và giảm thiểu các lỗ hổng tiềm ẩn.



Hình bên dưới hiển thị chính sách dựa trên tiêu chuẩn CIS cho Ubuntu Linux 22.04 LTS. Có thể thấy 191 lượt kiểm tra đã được chạy dựa trên điểm cuối Ubunt 22.04. Trong số này, 56 đạt, 87 không đạt và 48 không áp dụng được cho điểm cuối. Nó cũng cho thấy số điểm 39% được tính dựa trên số lượng bài kiểm tra đã vượt qua.



4.2.2. Phát hiện mã độc (Malware detection)

Các phương pháp truyền thống, chỉ dựa vào việc phát hiện dựa trên chữ ký (signature-based), có những hạn chế và không thể phát hiện các mối đe dọa mới. Các phương pháp dựa trên chữ ký gấp khó khăn trong việc phát hiện các cuộc tấn công zero-day, phần mềm độc hại đa hình (polymorphic malware) và các kỹ thuật lẩn tránh khác mà các tác nhân đe dọa sử dụng. Do đó, các tổ chức có nguy cơ bị vi phạm và đánh cắp dữ liệu mà không bị phát hiện.

Wazuh phát hiện các hoạt động độc hại bằng các bộ rules phát hiện mối đe dọa. Wazuh có các bộ luật (rules) phát hiện mối đe dọa cho phép phát hiện phần mềm độc hại dựa trên hành vi. Thay vì chỉ dựa vào các chữ ký (signatures) được xác định trước, Wazuh tập trung vào việc giám sát và phân tích hành vi bất thường do phần mềm độc hại thể hiện. Điều này cho phép Wazuh phát hiện các mối đe dọa đã biết và cả các mối đe dọa chưa từng được biết đến trước đây. Bằng cách này, Wazuh cung cấp một cơ chế phòng thủ chủ động và dễ thích ứng để chống lại các mối đe dọa mạng.

Hình ảnh bên dưới hiển thị một cảnh báo với ID bộ luật (rule ID) 92213 được kích hoạt khi một tệp thực thi (executable) được thả (dropped) vào một thư mục thường được phần mềm độc hại sử dụng.

The screenshot shows a Wazuh Threat Hunting interface. On the left, there's a sidebar with various log fields like agent.id, agent.ip, agent.name, etc. The main area has tabs for 'Time' and 'rule.description'. A specific log entry is highlighted: 'rule.description' is 'Executable file dropped in folder commonly used by malware', 'rule.level' is 15, and 'rule.id' is 92213. Below this, an 'Expanded document' section shows a JSON table with fields such as '_Index', 'agent.id' (001), 'agent.ip' (192.168.0.154), 'agent.name' (Windoswell), 'data.win.eventdata.creationUtcTime' (2024-05-03 15:00:50.257), 'data.win.eventdata.image' (C:\Program Files (x86)\Microsoft\EdgeWebView\Application\114.0.1823.82\msedgewebview2.exe), 'data.win.eventdata.processGuid' (450d4aff-0fa2-84c9-3601-00000000600), 'data.win.eventdata.processId' (1668), 'data.win.eventdata.ruleName' (technique_id=T1047,technique_name=File System Permissions Weakness), and 'data.win.eventdata.targetFileName' (C:\Users\Thecotiking\AppData\Local\Temp\chrome_ComponentUnpacker_BeginUnzipping1668_1275834351\manifest.json). Buttons for 'View surrounding documents' and 'View single document' are at the bottom.

Wazuh cho phép người dùng tạo ra các **bộ luật tùy chỉnh (custom rules)** để linh hoạt hơn trong việc phát hiện, trao quyền cho họ tập trung vào các hoạt động có liên quan và tối ưu hóa việc phát hiện phần mềm độc hại. Wazuh giải mã (decodes) và sắp xếp (organizes) các bản log từ các điểm cuối được giám sát thành các trường (fields), sau đó có thể được sử dụng để tạo các bộ luật tùy chỉnh nhằm đưa ra cảnh báo khi phát hiện hoạt động độc hại.

Các quy tắc được tạo cảnh báo hiển thị trong mô-đun Threat Hunting trên Wazuh dashboard

The screenshot shows a Wazuh Threat Hunting interface with a 'Security Alerts' section. It lists several alerts from May 4, 2024, at 21:31:34.468 to 21:31:31.585, all originating from agent 001 (Windows11). The alerts describe LimeRAT activity, specifically suspicious DNS queries, registry modifications, and DLL injection. Each alert includes its timestamp, agent ID, agent name, technique(s), tactic(s), description, level, and rule ID. For example, the first alert (May 4, 2024 @ 21:31:34.468) is at level 12 and rule ID 100026, describing a suspicious DNS query made by C:\Users\...\User\AppData\Roaming\checker.netflix.exe.

4.2.3. Giám sát tính toàn vẹn của tệp (File Integrity Monitoring)

Mô-đun **Giám sát Tính toàn vẹn Tệp (File Integrity Monitoring)** mã nguồn mở của Wazuh theo dõi các hoạt động được thực hiện trong các thư mục hoặc tệp được giám sát để thu thập thông tin sâu rộng về việc tạo, sửa đổi và xóa tệp. Khi một tệp bị thay đổi, Wazuh sẽ so sánh giá trị tổng kiểm (checksum) của nó với một giá trị cơ sở (baseline) đã được tính toán trước và kích hoạt cảnh báo nếu phát hiện thấy sự không trùng khớp.

Mô-đun FIM mã nguồn mở thực hiện giám sát theo thời gian thực và quét theo lịch trình (scheduled scans) tùy thuộc vào mức độ nhạy cảm của các tệp được giám sát.

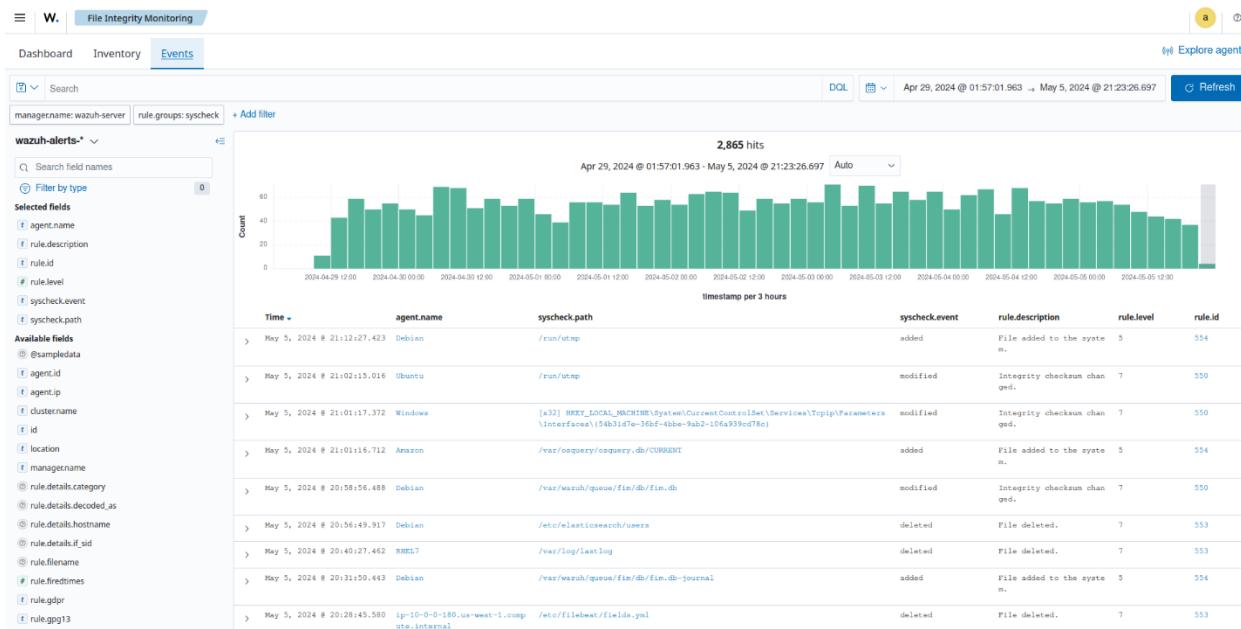
The screenshot shows a table titled "Files (847)" listing 847 monitored files. The columns include File, Last Modified, User, User ID, Group, Group ID, and Size. The table shows various system files like /bin, /etc/pwd.lock, and /etc/adduser.conf, all modified on April 15, 2024, by root with User ID 0 and Group ID 0, sizes ranging from 0 to 3028 bytes. A "WQL" button is visible at the top right. Below the table, a "Rows per page: 15" dropdown and a navigation bar with page numbers 1 through 57 are shown.

Phần Dashboard hiển thị tổng quan về các sự kiện được mô-đun FIM kích hoạt cho tất cả các điểm cuối được giám sát.

The screenshot displays several monitoring dashboards:

- Alerts by action over time:** A stacked area chart showing the count of deleted (blue), added (red), and modified (green) files over time from April 29 to May 5, 2024, with a peak around 60 events per hour.
- Top 5 agents:** A donut chart showing the distribution of agents: Ubuntu (yellow), Windows (orange), CentOS (grey), ip-10-0-0-180.us-west (dark red), and Debian (red).
- Events summary:** A line chart showing the number of alerts per hour from April 29 to May 5, 2024, fluctuating between 40 and 80 alerts.
- Rule distribution:** A donut chart showing the distribution of rules: File deleted (blue), Integrity checksum c... (pink), File added to the syst... (green), Registry Entry Deleted (light green), and Registry Integrity Ch... (yellow).
- Actions:** A pie chart showing the distribution of actions: deleted (blue), added (red), and modified (green).
- Top 5 users:** A table listing top users with their counts: Administrators (003), ip-10-0-0-180.us-west (60), Administrators (002), Amazon (57), Administrators (001), RHEL7 (53), Administrators (005), Centos (53), Administrators (007), Debian (50).

Phần Event hiển thị các cảnh báo do mô-đun FIM kích hoạt. Nó hiển thị các chi tiết như tên agent, đường dẫn tệp của tệp được giám sát, loại sự kiện FIM, mô tả cảnh báo và cấp độ quy tắc của từng cảnh báo.



Việc sửa đổi các tệp cấu hình và thuộc tính tệp là những sự kiện thường xuyên xảy ra trên các điểm cuối (endpoints) trong cơ sở hạ tầng CNTT. Nếu không được xác thực, có thể có những thay đổi trái phép và vô ý ảnh hưởng đến hành vi của các điểm cuối hoặc các ứng dụng chạy trên chúng.

4.2.4. Săn tìm mối đe dọa (Threat hunting)

Wazuh cung cấp một số khả năng hỗ trợ các đội ngũ bảo mật trong việc săn lùng các mối đe dọa trong môi trường của họ, trao quyền cho họ thực hiện các hành động nhanh chóng để ngăn chặn mối đe dọa và ngăn ngừa thiệt hại thêm.

Phân tích dữ liệu log (Log data analysis):

Wazuh, với tư cách là một nền tảng XDR và SIEM hợp nhất, cung cấp khả năng **thu thập dữ liệu log tập trung**, cho phép thu thập dữ liệu từ các nguồn đa dạng như điểm cuối, thiết bị mạng và ứng dụng. Phương pháp tiếp cận tập trung này giúp đơn giản hóa việc phân tích và giảm nỗ lực cần thiết để giám sát nhiều nguồn.

Hình ảnh bên dưới hiển thị các cài đặt cấu hình trên Wazuh dashboard để thu thập log kiểm toán (audit logs) từ một điểm cuối được giám sát.

Wazuh sử dụng các **bộ giải mã (decoders)** để trích xuất thông tin có ý nghĩa từ dữ liệu log thu được từ nhiều nguồn khác nhau. Nó chia nhỏ (breaks down) dữ liệu log thành các trường (fields) hoặc thuộc tính (attributes) riêng lẻ, chẳng hạn như dấu thời gian (timestamp), địa chỉ IP nguồn, địa chỉ IP đích, loại sự kiện, và các loại khác.

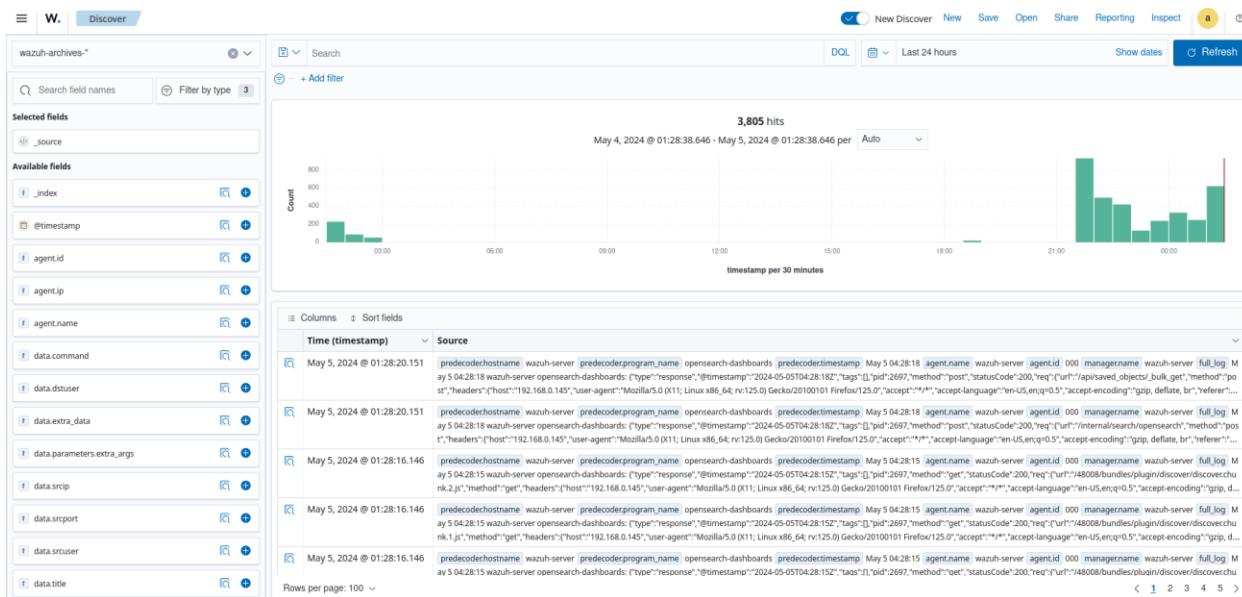
Name	Type	Format	Searchable	Aggregatable	Excluded
@sampledata	boolean		●	●	
@timestamp	date		●	●	●
@version	string		●		
GeoLocation.area_code	number		●	●	
GeoLocation.city_name	string		●	●	
GeoLocation.continent_code	string		●		
GeoLocation.coordinates	number		●	●	
GeoLocation.country_code2	string		●		
GeoLocation.country_code3	string		●		
GeoLocation.country_name	string		●	●	

Wazuh cung cấp khả năng **giám sát không cần agent (agentless monitoring)** và **thu thập log qua syslog** để xử lý dữ liệu log hiệu quả. Nó đảm bảo tính nhất quán và tương thích giữa các định dạng log khác nhau. Khả năng lập chỉ mục và truy vấn của Wazuh tạo điều kiện thuận lợi cho việc tìm kiếm nhanh và truy cập vào dữ liệu log cụ thể, giúp tinh giản quá trình phân tích và điều tra. Wazuh sử dụng khả năng phân tích cú pháp (parsing) tiên tiến và phân tích

thời gian thực để tăng cường săn lùng mối đe dọa bằng cách chủ động xác định và giảm thiểu rủi ro, qua đó nâng cao tính bảo mật.

Wazuh archives

Wazuh cung cấp một vị trí lưu trữ tập trung để lưu trữ (archiving) tất cả các log được thu thập từ các điểm cuối được giám sát. Các bản log lưu trữ của Wazuh (Wazuh archives logs) bao gồm cả những log không kích hoạt cảnh báo trên Wazuh dashboard. Sự sẵn có của các bản log chi tiết là rất quan trọng để săn lùng mối đe dọa hiệu quả, cung cấp khả năng hiển thị toàn diện (comprehensive visibility) về môi trường của bạn.



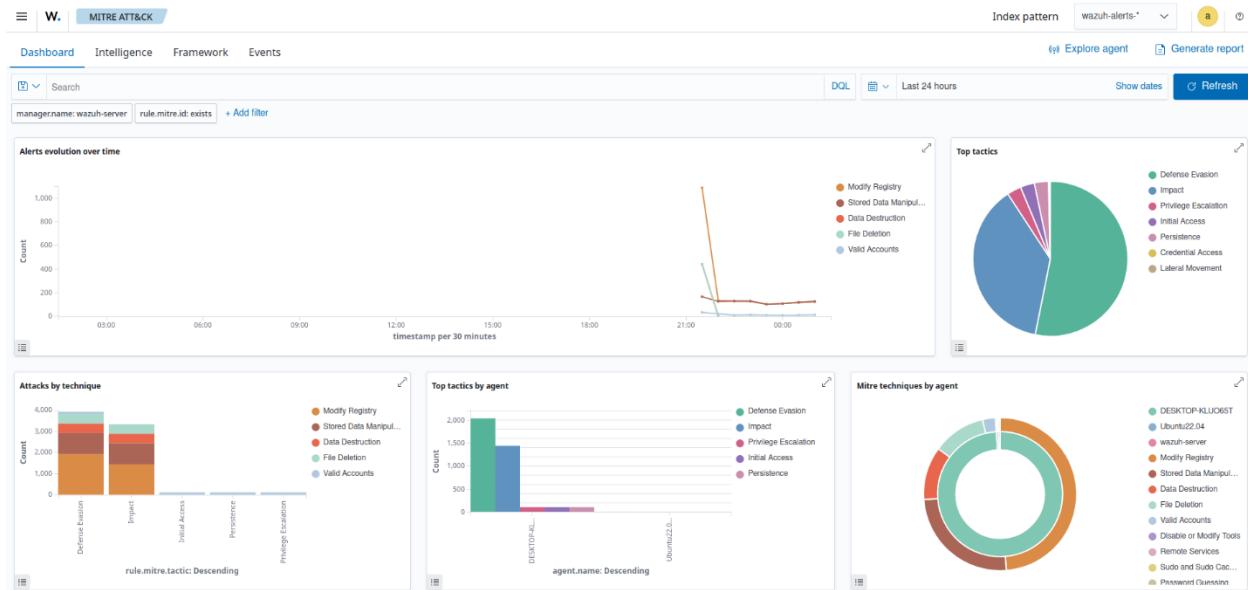
MITRE ATT&CK mapping

Framework MITRE ATT&CK cung cấp một phương pháp tiếp cận được tiêu chuẩn hóa để ánh xạ và hiểu các chiến thuật (tactics), kỹ thuật (techniques) và quy trình (procedures) tấn công mạng (TTPs). Bằng cách sử dụng **mô-đun MITRE ATT&CK của Wazuh**, chúng ta có thể nâng cao hiểu biết của mình về các TTP mà các tác nhân đe dọa sử dụng và chủ động phòng thủ chống lại chúng.

Mô-đun MITRE ATT&CK của Wazuh ánh xạ các TTP với các sự kiện được tạo ra, tạo điều kiện thuận lợi cho việc săn lùng mối đe dọa hiệu quả bằng cách nhanh chóng xác định các mẫu (patterns) trong hành vi của kẻ tấn công.

The screenshot shows the Wazuh dashboard interface for the MITRE ATT&CK framework. The top navigation bar includes 'Index pattern' (wazuh-alerts-*), 'Explore agent', and a search bar ('managername: wazuh-server rule.mitre.id: exists'). Below the search bar are buttons for 'DQL', 'Last 24 hours', 'Show dates', and 'Refresh'. The main content area is divided into two sections: 'Tactics' on the left and 'Techniques' on the right. The 'Tactics' section lists various attack tactics with their respective counts: Defense Evasion (2043), Impact (1446), Privilege Escalation (114), Persistence (112), Initial Access (111), Credential Access (9), Lateral Movement (8), Execution (6), Exfiltration (5), Discovery (4), Collection (3), Resource Development (2), Reconnaissance (1), and Command and Control (1). The 'Techniques' section displays a grid of techniques, each with an ID, name, and count. Some techniques have a small icon next to them.

Mô-đun này tạo ra các báo cáo và hình ảnh trực quan trên Wazuh dashboard, hiển thị tần suất và mức độ nghiêm trọng của các cuộc tấn công sử dụng các TTP cụ thể. Các báo cáo này giúp theo dõi việc tuân thủ các tiêu chuẩn và quy định bảo mật, đồng thời nhấn mạnh các lĩnh vực mà các biện pháp bảo mật có thể cần được tăng cường. Mô-đun **MITRE ATT&CK** của Wazuh trên Wazuh dashboard có một bảng điều khiển tùy biến (customizable dashboard) hiển thị tổng quan về các TTP được tìm thấy trong một môi trường được giám sát như hình bên dưới.

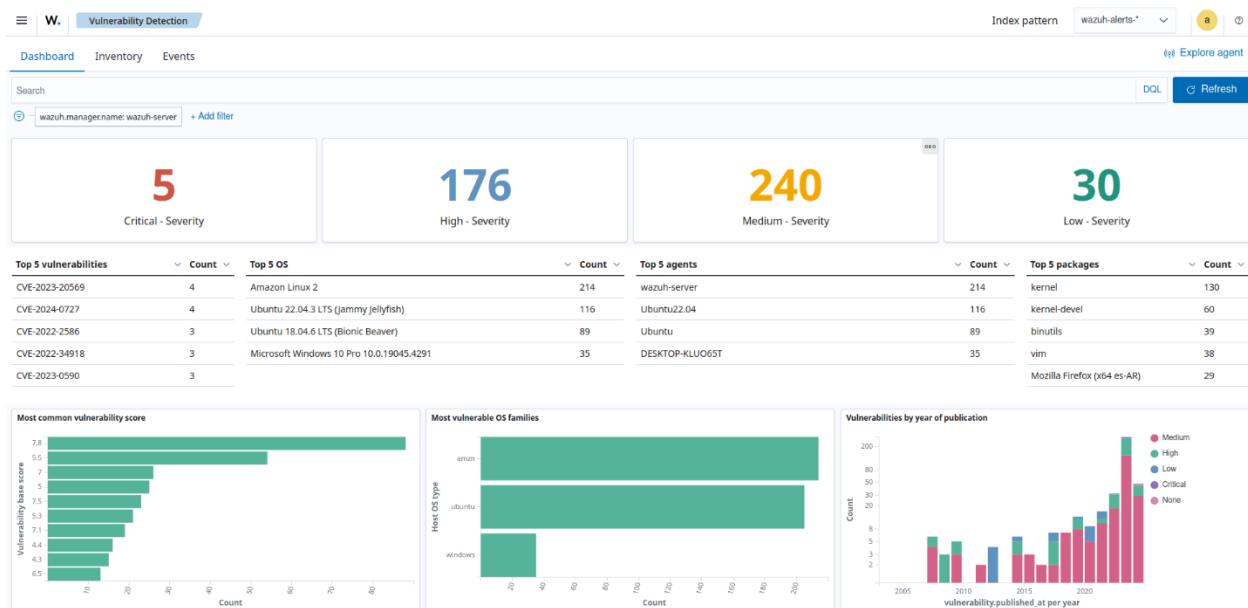


4.2.5. Phát hiện lỗ hổng (Vulnerability detection)

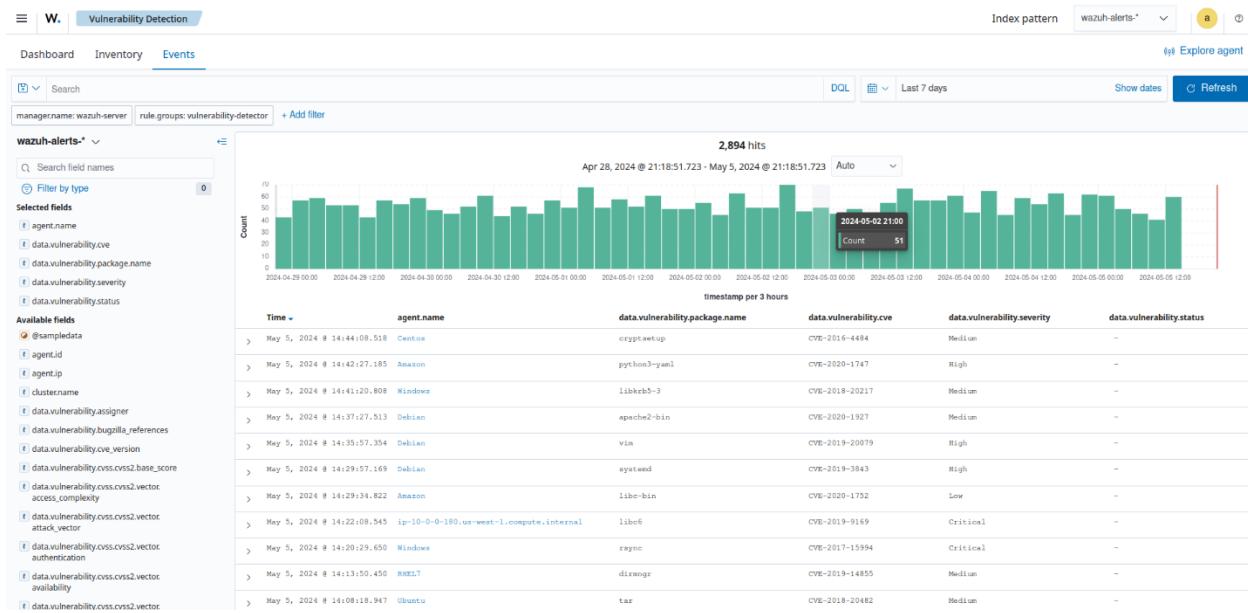
Wazuh agent sử dụng mô-đun **Syscollector** để thu thập thông tin kiểm kê (inventory details) từ điểm cuối được giám sát. Nó gửi dữ liệu đã thu thập đến Wazuh server. Bên trong Wazuh server, mô-đun **Phát hiện Lỗ hổng (Vulnerability Detection)** sẽ đối chiếu (correlates) dữ liệu kiểm kê phần mềm với các tài liệu nội dung về lỗ hổng (vulnerability content documents) để phát hiện phần mềm có lỗ hổng trên điểm cuối được giám sát.

Khả năng hiển thị toàn diện:

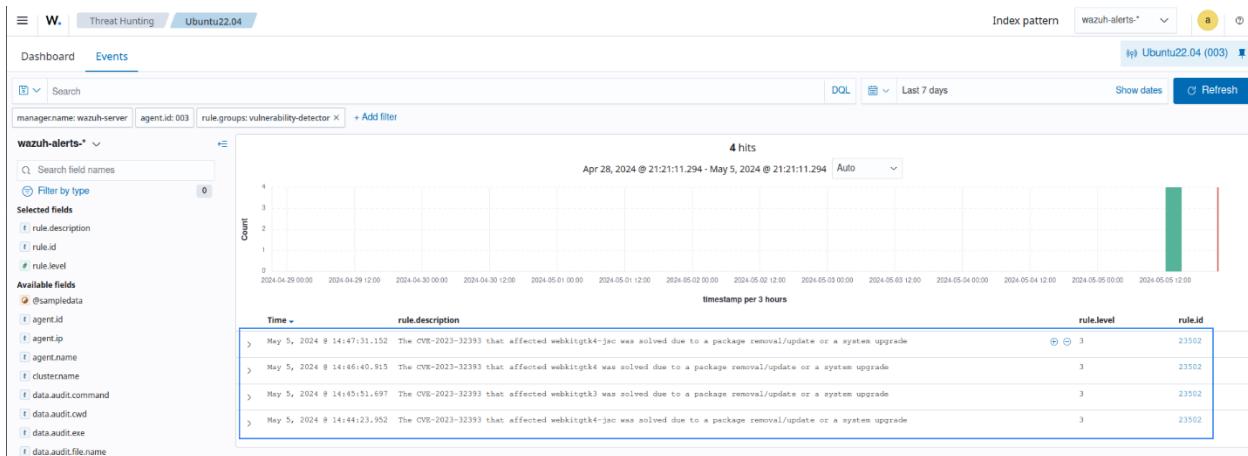
Mô-đun Phát hiện Lỗ hổng (Vulnerability Detection) tạo ra cảnh báo cho các lỗ hổng được phát hiện trên hệ điều hành và các ứng dụng được cài đặt trên điểm cuối được giám sát. Nó đối chiếu (correlates) dữ liệu kiểm kê phần mềm (software inventory) do Wazuh agent thu thập với các tài liệu nội dung về lỗ hổng và hiển thị cảnh báo được tạo ra trên Wazuh dashboard. Điều này cung cấp một cái nhìn rõ ràng và toàn diện về các lỗ hổng được xác định trên tất cả các điểm cuối được giám sát, cho phép xem, phân tích và khắc phục các lỗ hổng.



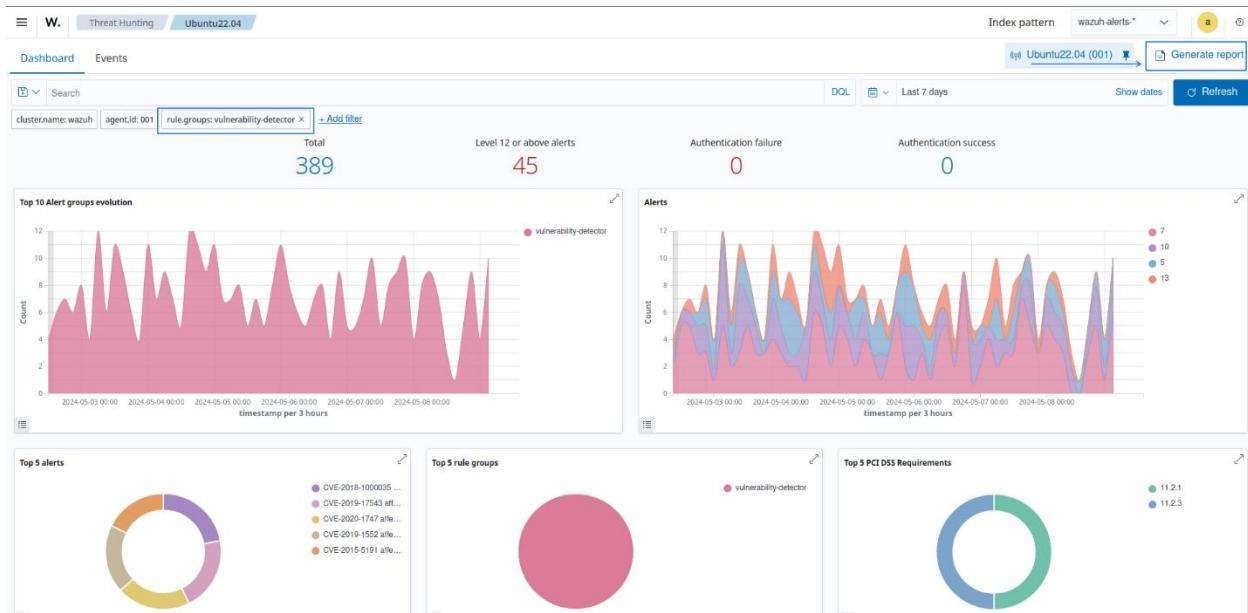
Có thể xem các cảnh báo được tạo trên dashboard khi phát hiện lỗ hổng mới.



Cảnh báo được tạo trên dashboard cũng có thể là kết quả của các hành động khắc phục sự cố. Hình ảnh dưới đây hiển thị các cảnh báo được tạo sau khi nâng cấp hoặc gỡ cài đặt gói đã giải quyết lỗ hổng.



Wazuh cung cấp cho người dùng khả năng tải xuống báo cáo chứa các sự kiện bảo mật liên quan đến các lỗ hổng được phát hiện và giải quyết. Tính năng này cho phép người dùng xác định các điểm cuối có lỗ hổng chưa được giải quyết và theo dõi các hoạt động được khắc phục.



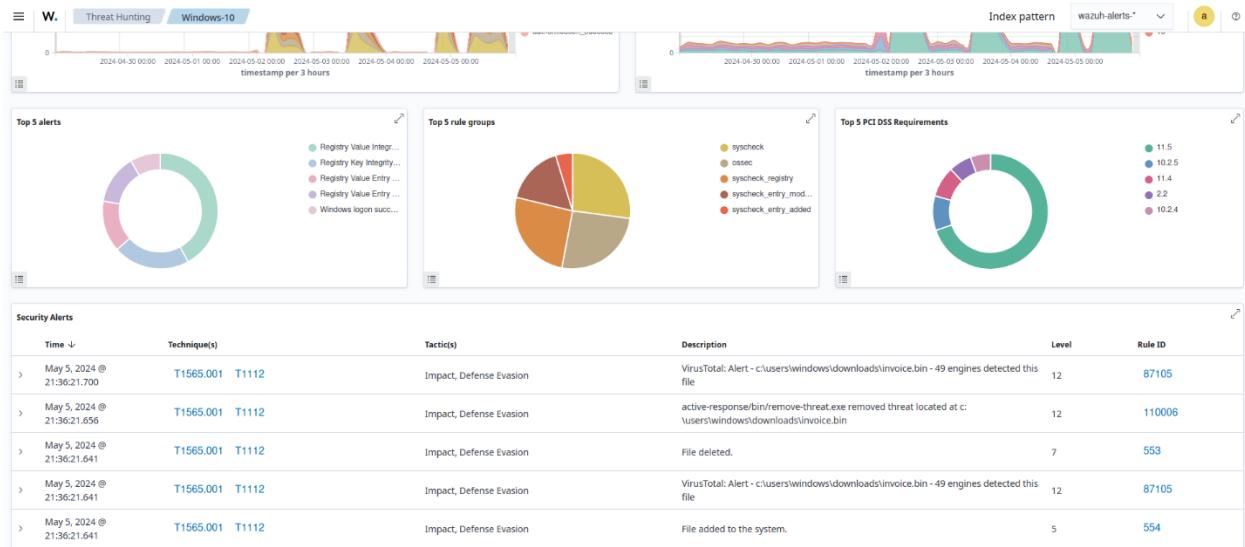
Ứng phó sự cố tự động (Automated incident response) bao gồm các hành động tự động được thực hiện khi ứng phó với các sự cố an ninh. Các hành động này có thể bao gồm cách ly các điểm cuối (endpoints) bị xâm nhập, chặn các địa chỉ IP độc hại, đưa các thiết bị bị lây nhiễm vào vùng cách ly (quarantining) hoặc vô hiệu hóa các tài khoản người dùng bị xâm nhập. Bằng cách tự động hóa ứng phó sự cố, các đội ngũ an ninh mạng giảm thời gian phản hồi đối với các mối đe dọa được phát hiện, ngăn chặn hoặc giảm thiểu tác động của sự cố, và xử lý hiệu quả một khối lượng lớn các sự kiện an ninh.

Wazuh Active Response module

Mô-đun Phản ứng Chủ động (Active Response) của Wazuh cho phép người dùng chạy các hành động tự động khi các sự cố được phát hiện trên các điểm cuối. Điều này cải thiện các quy trình ứng phó sự cố của tổ chức, cho phép các đội ngũ bảo mật thực hiện các hành động tự động và ngay lập tức để chống lại các mối đe dọa được phát hiện.

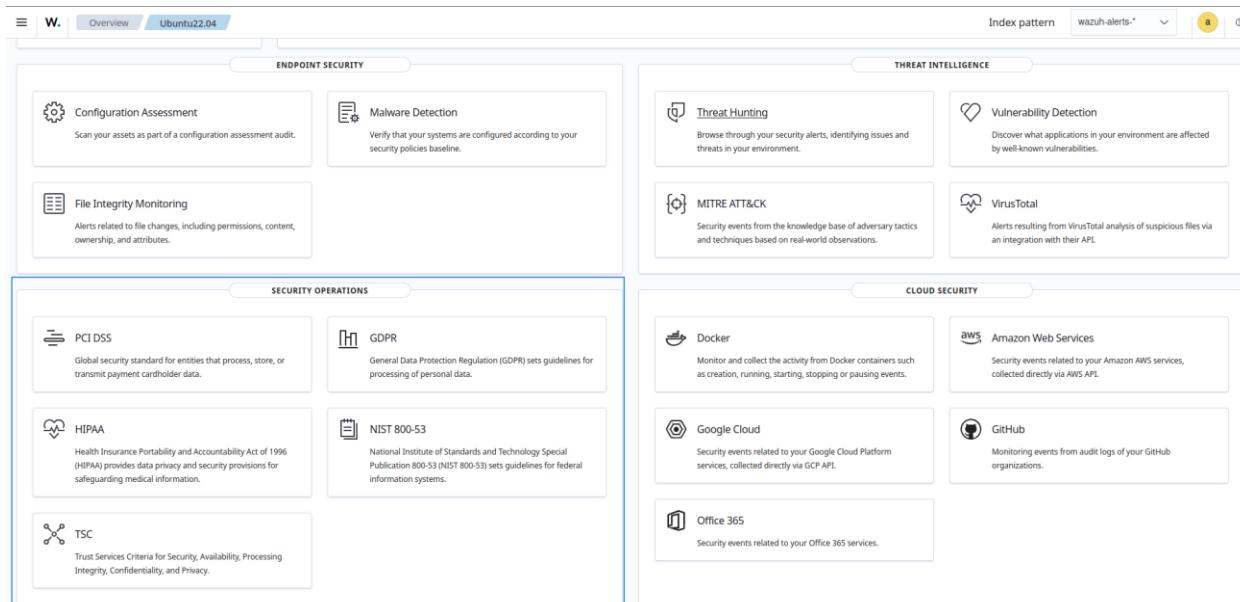
Các hành động phản ứng chủ động mặc định: Các kịch bản (scripts) có sẵn (out-of-the-box) có trên mọi hệ điều hành chạy Wazuh agents. Một số kịch bản phản ứng chủ động mặc định bao gồm.

Các hành động phản ứng chủ động tùy chỉnh: Wazuh cho phép các đội ngũ bảo mật tạo các hành động phản ứng chủ động được tùy chỉnh (custom active response) bằng bất cứ ngôn ngữ lập trình nào, điều chỉnh theo nhu cầu cụ thể. Điều này đảm bảo rằng khi một mối đe dọa được phát hiện, phản ứng có thể được tùy chỉnh để phù hợp với các yêu cầu của tổ chức.



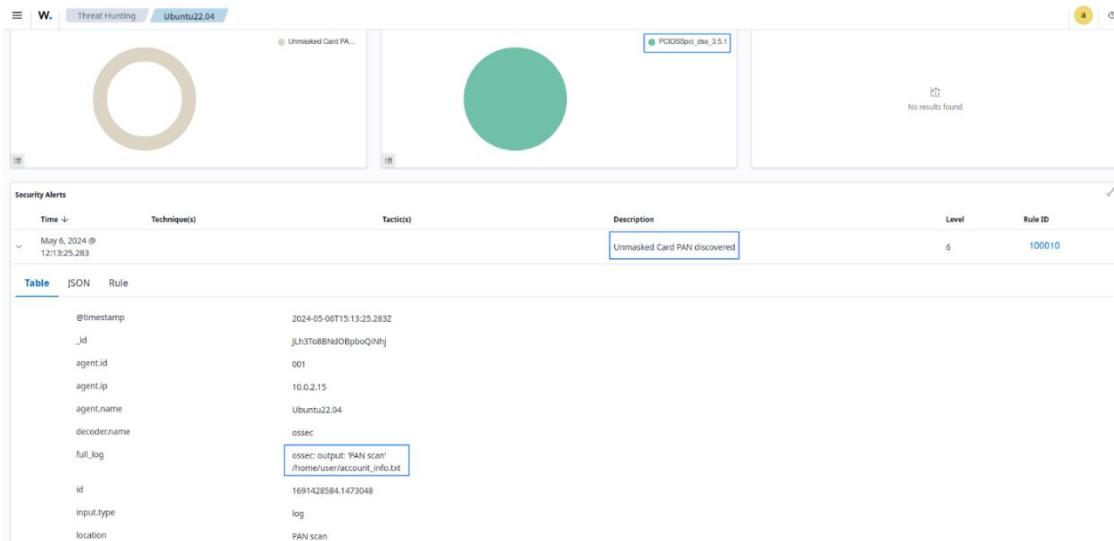
4.2.6. Tuân thủ theo các quy định (Regulatory compliance)\

Việc tuân thủ các yêu cầu quy định là một thành phần quan trọng trong khuôn khổ (framework) an ninh mạng của một tổ chức. Thông qua việc tuân thủ các luật, quy tắc và tiêu chuẩn (benchmarks) liên quan, các tổ chức có thể bảo vệ tài nguyên thông tin của mình và giảm thiểu khả năng xảy ra vi phạm an ninh. Wazuh cung cấp các bộ luật (rulesets) có sẵn (out-of-the-box) được ánh xạ với các thẻ (tags) tuân thủ cho các khuôn khổ và tiêu chuẩn PCI DSS, HIPAA, NIST 800-53, TSC và GDPR.



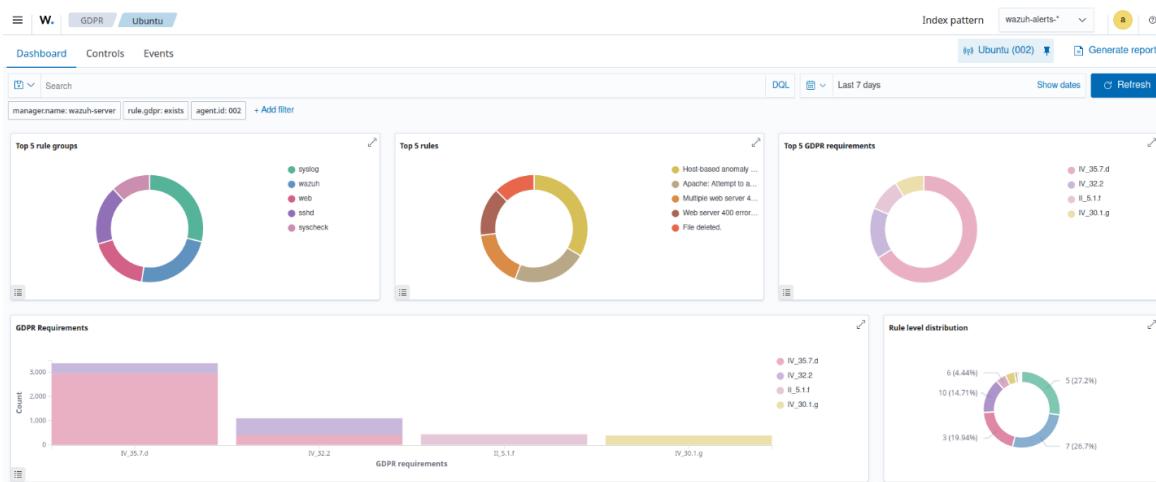
PCI DSS

PCI DSS (Payment Card Industry Data Security Standard) cung cấp các tiêu chí bảo mật mà các doanh nghiệp xử lý, lưu trữ và truyền tải dữ liệu thẻ phải tuân thủ. Tiêu chuẩn này được thiết kế để thắt chặt các biện pháp bảo mật xung quanh dữ liệu chủ thẻ và giảm thiểu gian lận trong ngành thẻ thanh toán.



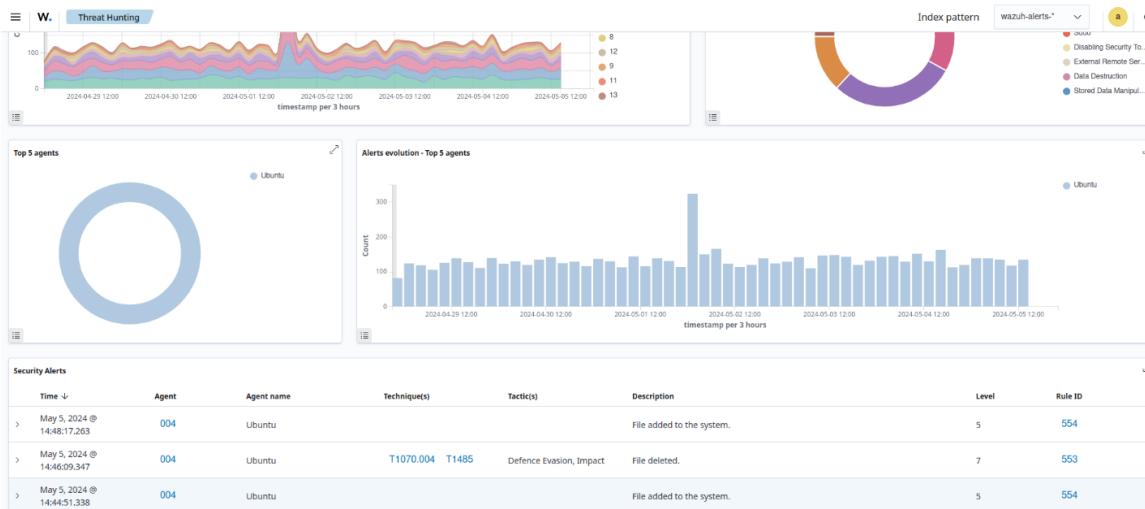
GDPR

GDPR (The General Data Protection Regulation) nhằm tăng cường quyền riêng tư dữ liệu của người dùng và thay đổi cách thức mà Liên minh Châu Âu, và các tổ chức xử lý dữ liệu của công dân EU, xử lý quyền riêng tư dữ liệu. Wazuh đi kèm với các bộ luật và bộ giải mã mặc định để xác định các loại tấn công mạng, hệ thống cấu hình sai, lỗ hổng bảo mật và vi phạm chính sách khác nhau.



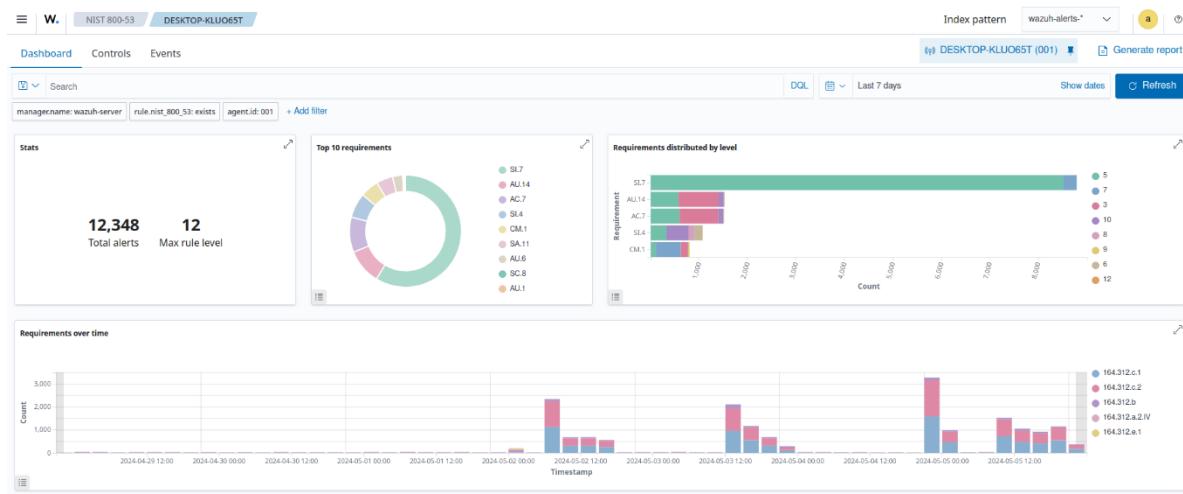
HIPAA

HIPAA (The Health Insurance Portability and Accountability Act) đặt ra các hướng dẫn và quy trình xử lý thông tin sức khỏe để tăng hiệu quả của các dịch vụ chăm sóc sức khỏe. Nó bao gồm các hướng dẫn cho các giao dịch chăm sóc sức khỏe điện tử và các tiêu chuẩn về bảo mật và nhận dạng sức khỏe đặc thù. Các tổ chức có thể giám sát việc truy cập và các thay đổi được thực hiện đối với PII (thông tin nhận dạng cá nhân) và các tài liệu bí mật khác bằng cách sử dụng mô-đun Wazuh FIM.



NIST 800-53

NIST (The National Institute of Standards and Technology) cung cấp các khuyến nghị về quản lý an ninh thông tin và quyền riêng tư cho các tổ chức và cơ quan liên bang. Nó giúp các tổ chức bảo vệ dữ liệu nhạy cảm đồng thời bảo vệ hệ thống thông tin và dữ liệu của họ khỏi các mối đe dọa khác nhau.



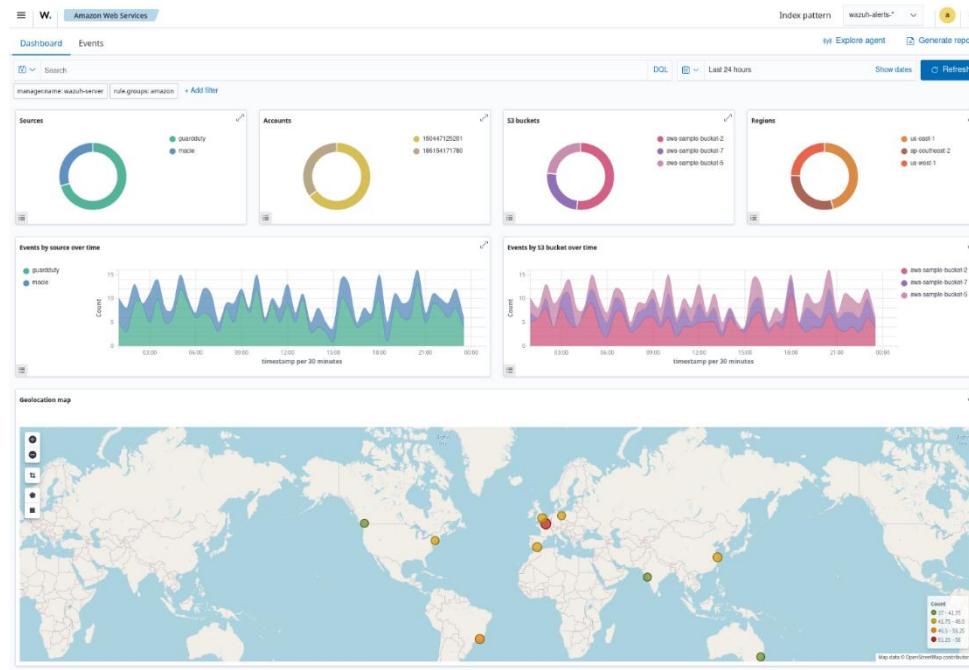
4.2.7. Bảo vệ công việc trên môi trường cloud (Cloud workload protection)

Nền tảng an ninh Wazuh cung cấp khả năng phát hiện mối đe dọa, tuân thủ cấu hình và giám sát liên tục cho các môi trường on-premise (tại chỗ), cloud (đám mây) và hybrid (lai). Nó bảo vệ các tải công việc (workloads) trên đám mây bằng cách giám sát cơ sở hạ tầng ở hai cấp độ:

- Endpoint level: giám sát các phiên bản cloud (cloud instances) hoặc máy ảo bằng cách sử dụng **Wazuh agent**.
- Cloud infrastructure level: giám sát hoạt động của dịch vụ đám mây bằng cách thu thập và phân tích dữ liệu từ API của nhà cung cấp. Wazuh hỗ trợ Amazon AWS, Microsoft Azure và Google Cloud.

Cloud log data analysis and retention

Các môi trường đám mây tạo ra lượng lớn dữ liệu log, rất quan trọng để xác định các sự cố an ninh. Các bộ luật (rules) và bộ giải mã (decoders) của Wazuh chịu trách nhiệm phân tích cú pháp (parsing) và phân tích dữ liệu log để phát hiện các sự kiện bất thường. Wazuh thu thập và phân tích dữ liệu log từ các nền tảng và dịch vụ đám mây khác nhau, chẳng hạn như AWS, Azure, Google Cloud, Office 365 và GitHub.



V. GIẢI PHÁP NÂNG CAO: TRỢ LÝ AN NINH ẢO (AI ASSISTANT)

5.1. Thách thức trong phân tích bảo mật và điều tra log truyền thông

Việc triển khai một nền tảng SIEM giải quyết được thách thức thu thập log tập trung, nhưng đây mới chỉ là 50% của cuộc chiến. Thách thức thực sự nằm ở việc phân tích. Các hệ thống hiện đại tạo ra hàng tỷ bản ghi, ngay cả khi đã được lọc thành hàng ngàn cảnh báo, vẫn dẫn đến tình trạng “quá tải thông tin” (Alert Fatigue). Đội ngũ vận hành nhanh chóng bị quá tải bởi false positive và các cảnh báo ưu tiên thấp, khiến họ vô tình bỏ qua các dấu hiệu quan trọng của một cuộc tấn công thực sự. Phần lớn dữ liệu log trở thành “dữ liệu câm” – được lưu trữ nhưng hiếm khi được con người xem xét, khiến các mối đe dọa dễ dàng ẩn mình.

Hơn nữa, quá trình điều tra thủ công đòi hỏi kỹ thuật cao, đặc biệt là phải thành thạo các ngôn ngữ truy vấn (query language) phức tạp để xâu chuỗi sự kiện. Quá trình tìm kiếm thủ công (từ cảnh báo – truy vấn IP – truy vấn người dùng) cực kỳ tốn thời gian, đẩy Thời gian rung bình để phản ứng (MTTR) lên mức hàng giờ, thậm chí hàng ngày. Trong khoảng thời gian quý giá đó, kẻ tấn công đã có đủ thời để di chuyển ngang, đánh cắp dữ liệu và xóa dấu vết.

5.2. Giới thiệu trợ lý ảo

Để giải quyết trực tiếp các thách thức về quá tải cảnh báo (Alert Fatigue) và độ phức tạp trong điều tra, chúng tôi giới thiệu Trợ lý An ninh ảo – một giải pháp đột phá được tích hợp sâu vào nền tảng giám sát Wazuh.

Bằng cách tận dụng sức mạnh của các mô hình Ngôn ngữ lớn (LLM) Ollama chạy hoàn toàn tại chỗ (on-premise) và kiến trúc Truy xuất – Bô sung Thông tin (RAG), Trợ lý an ninh ảo biến hàng tỷ bản log thành các cuộc hội thoại trực quan. Giải pháp này cho phép đội ngũ vận hành của bạn – từ chuyên gia IT đến các nhà phân tích an ninh (SOC) có thể đặt câu hỏi bằng ngôn ngữ tự nhiên và nhận về các câu trả lời chính xác, tóm tắt thông minh và các bằng chứng cụ thể, giúp phát hiện và điều tra sự cố với tốc độ chưa từng có.

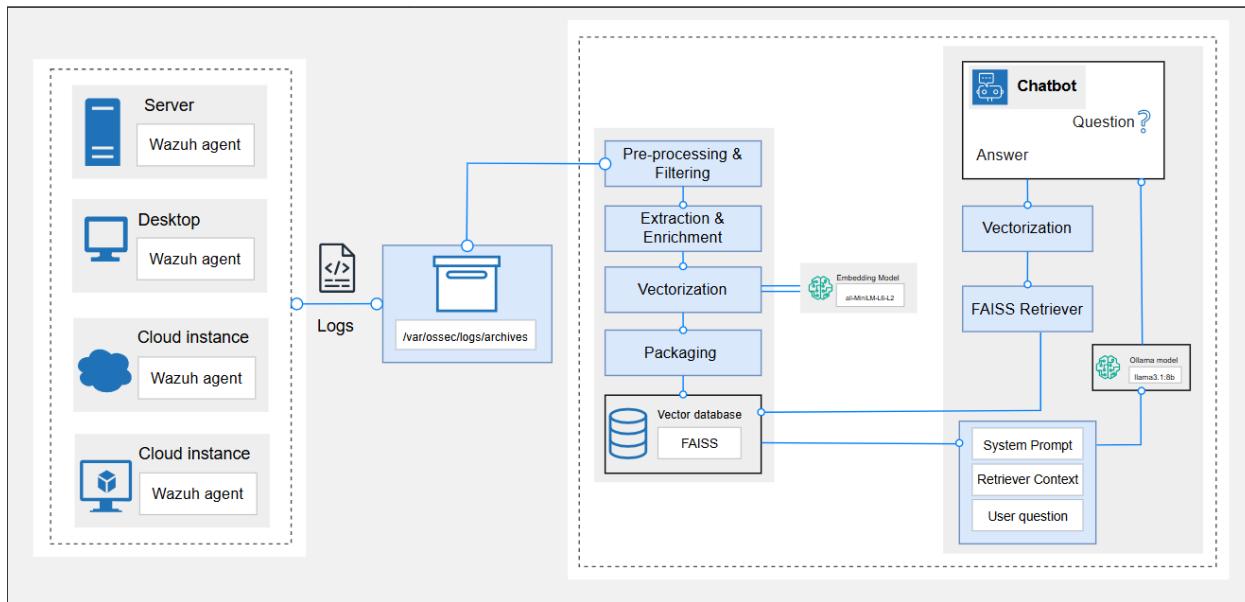
5.3. Tính năng và giá trị cốt lõi

Trợ lý an ninh ảo của chúng tôi chuyển đổi cách thức tương tác với dữ liệu SIEM, mang lại những giá trị then chốt sau:

- Hỏi – đáp (query) bằng ngôn ngữ tự nhiên:
 - Tính năng: Thay vì phải học và viết các cú pháp truy vấn phức tạp của SIEM, đội ngũ của bạn chỉ cần đặt câu hỏi đơn giản.
 - Ví dụ: Thay vì viết `rule.id:5712 AND data.win.system.eventID:4625`, bạn chỉ cần hỏi: “*Tìm các cảnh báo đăng nhập thất bại (rule 5712) nhưng sau đó đã đăng nhập thành công (event 4625) trong 24 giờ qua*”.
- Tóm tắt sự cố thông minh:
 - Tính năng: Khi nhận một cảnh báo, bạn có thể yêu cầu AI tóm tắt ngay lập tức.
 - Ví dụ: “*Giải thích cảnh báo rule 92213 có ý nghĩa gì?*”. AI sẽ đọc toàn bộ log (từ trường metadata được lưu trữ) và trả lời.
- Tăng tốc điều tra (giảm MTTR):
 - Tính năng: AI tự động xâu chuỗi các sự kiện. Khi bạn hỏi về một IP, nó không chỉ trả về log của IP đó mà còn phân tích các hoạt động liên quan (tiến trình đã chạy, người dùng đã đăng nhập, các IP khác đã kết nối đến).
 - Giá trị: Giảm thời gian điều tra trung bình (MTTR) từ hàng giờ xuống còn vài phút.
- Điều tra dựa trên bằng chứng (Evidence-Based):
 - Tính năng: Mọi câu trả lời của AI đều được hỗ trợ bởi các bản log gốc. Hệ thống (retriever) được cấu hình để tìm kiếm k bản log liên quan nhất và cung cấp chúng làm source documents cho câu trả lời.
 - Giá trị: Đảm bảo tính minh bạch, cho phép nhà phân tích xác thực ngay lập tức thông tin AI cung cấp.
- An toàn và bảo mật dữ liệu tuyệt đối:
 - Tính năng: Giải pháp sử dụng Ollama và các mô hình nhúng (Embedding) chạy hoàn toàn tại chỗ (on-premise).

5.4. Kiến trúc của trợ lý ảo

Kiến trúc của trợ lý an ninh ảo được xây dựng dựa trên mô hình RAG (Retrieval – Augmented Generation) tiên tiến. Kiến trúc này được thiết kế để đảm bảo an toàn dữ liệu tuyệt đối và cung cấp các câu trả lời thông minh, chính xác dựa trên chính dữ liệu log của tổ chức.



Mô hình hoạt động được chia thành hai luồng (pipeline) chính: (1) Luồng xử lý và nạp dữ liệu , (2) Luồng truy vấn và trả lời

5.4.1. Luồng 1 - Xử lý log và xây dựng cơ sở tri thức

- Tiền xử lý & Lọc (Pre-processing & Filtering): Dữ liệu log thô từ archives được đọc và lọc để loại bỏ các log “nhiều”, không quan trọng (ví dụ: log *sca* hoặc log có *rule_level* thấp).
- Trích xuất & làm giàu (Extraction & Enrichment): Hệ thống phân tích các log quan trọng còn lại, trích xuất các trường thông tin cốt lõi (IP nguồn, tên người dùng, ID cảnh báo) và làm giàu thêm các thông tin bối cảnh (như Event ID của Windows, câu lệnh của Linux).
- Vector hóa (Vectorization): Nội dung log đã được xử lý được đưa qua Mô hình Embedding (*all-MiniLM-L6-v2*). Mô hình này chuyển đổi ý nghĩa của mỗi log thành một vector số học.
- Đóng gói & lưu trữ (Packaging & Storage): Các vector này, cùng với log gốc (dưới dạng metadata), được đóng gói và nạp vào Cơ sở dữ liệu Vector (FAISS).

5.4.2. Luồng 2 - Truy vấn và phản hồi

- Người dùng đặt câu hỏi (Question): Nhà phân tích gõ một câu hỏi bằng ngôn ngữ tự nhiên.
- Vector hóa câu hỏi: Câu hỏi của người dùng ngay lập tức được đưa qua Embedding Model (cùng mô hình ở Luồng 1) để tạo ra một “vector câu hỏi”.

- Truy xuất bối cảnh (FAISS Retriever): “vector câu hỏi” được sử dụng để tìm kiếm trong CSDL FAISS. Hệ thống sẽ tìm và lấy ra các vector (cùng log gốc đính kèm) có ý nghĩa tương đồng nhất với câu hỏi. Kết quả này được gọi là “Retriever Context”.
- Sinh câu trả lời (LLM Generation): Đây là lúc mô hình Ollama (llama3.1:8b) hoạt động. Nó nhận một “Prompt lớn” bao gồm 3 phần:
 - System Prompt (chỉ thị hệ thống: “Bạn là một trợ lý an ninh,...”).
 - Retriever Context (bối cảnh: Các log gốc liên quan nhất mà FAISS vừa tìm thấy).
 - User Question (câu hỏi gốc của người dùng).
- Trả lời (Answer): Mô hình Ollama sẽ đọc và phân tích toàn bộ bối cảnh được cung cấp để tạo ra một câu trả lời tóm tắt, chính xác và dễ hiểu bằng ngôn ngữ tự nhiên, sau đó gửi lại cho giao diện Chatbot.

VI. LỢI ÍCH VÀ LỢI THẾ CẠNH TRANH CỦA WAZUH

6.1. Tại sao chọn nền tảng Wazuh?

Việc lựa chọn Wazuh làm nền tảng SIEM/XDR cốt lõi mang lại nhiều lợi thế chiến lược, vượt xa các giải pháp truyền thống:

- Tối ưu chi phí vận hành:
 - Wazuh là nền tảng mã nguồn mở (open-source), đồng nghĩa với việc khách hàng không phải trả chi phí bản quyền (license).
 - Không giống các giải pháp tính phí theo dung lượng log mỗi ngày (GB/ngày) hoặc theo số lượng agent, Wazuh cho phép thu thập và lưu trữ log mà không phải lo lắng về việc “vượt ngân sách” khi mở rộng hệ thống. Chi phí duy nhất là cho hạ tầng lưu trữ và dịch vụ hỗ trợ (nếu cần).
- Giải pháp hợp nhất toàn diện (All-in-one):
 - Wazuh không chỉ là một SIEM. Nó tích hợp sẵn các khả năng mà nhiều nhà cung cấp khác phải bán dưới dạng các mô-đun riêng lẻ, bao gồm: SIEM (Phân tích log), XDR (Phát hiện & Phản hồi), FIM (Giám sát Tính toàn vẹn tệp), SCA (Đánh giá Cấu hình) và Vulnerability Detection (Phát hiện Lỗ hổng).
- Linh hoạt, tùy biến cao và không bị “Vendor Lock-in”:

- Là mã nguồn mở, Wazuh cho phép tùy chỉnh không giới hạn. Doanh nghiệp có thể tự do phát triển các bộ luật (rules), bộ giải mã (decoders) và tích hợp (integrations) riêng để phù hợp hoàn hảo với các hệ thống đặc thù của mình.
- Bạn không bị "khóa" vào một nhà cung cấp duy nhất và có toàn quyền kiểm soát dữ liệu của mình.

6.2. So sánh với các giải pháp thương mại khác

6.2.1. Các giải pháp Enterprise hàng đầu

a. Splunk

- **Mô tả:** Splunk là "tiêu chuẩn vàng" lâu năm, cực kỳ mạnh mẽ trong việc tìm kiếm và phân tích (với ngôn ngữ SPL). Nó có một hệ sinh thái (Splunkbase) khổng lồ.
- **Nhược điểm lớn nhất:** Chi phí cực kỳ cao, được tính dựa trên dung lượng log nạp vào mỗi ngày (GB/day). Mô hình này "phạt" doanh nghiệp khi họ muốn thu thập nhiều log hơn, đi ngược lại nguyên tắc an ninh.

b. Microsoft Sentinel

- **Mô tả:** Đây là giải pháp SIEM/SOAR "cloud-native" (thuần đám mây) của Microsoft. Sức mạnh tuyệt đối của nó là khả năng **tích hợp sâu** với toàn bộ hệ sinh thái Microsoft (Azure, Microsoft 365, Defender).
- **Nhược điểm lớn nhất:** **"Vendor Lock-in"** (**Khóa nhà cung cấp**). Giải pháp này gần như chỉ hoạt động trên Azure và chi phí có thể tăng vọt nếu bạn cần nạp log từ các nguồn khác (như AWS, GCP, hoặc on-premise).

c. IBM QRadar

- **Mô tả:** Một giải pháp SIEM truyền thống rất mạnh, đặc biệt trong các môi trường on-premise lớn và các ngành (như tài chính, ngân hàng) yêu cầu tuân thủ (compliance) khắt khe.
- **Nhược điểm:** Thường bị xem là phức tạp, kiến trúc hơi "cũ" và không linh hoạt bằng các giải pháp mới.

6.2.2. So sánh ưu và nhược điểm (Wazuh và Enterprise)

Tiêu chí	Giải pháp Wazuh	Giải pháp Enterprise
Chi phí	Miễn phí (mã nguồn mở). Chỉ trả phí cho dịch vụ triển khai và hỗ trợ.	Chi phí bản quyền đắt đỏ, thường tính theo dung lượng log (GB/ngày) hoặc số lượng agent.
Phạm vi tính năng	Tích hợp sẵn SIEM, XDR, FIM, SCA, ...	Thường phải mua nhiều mô-đun riêng lẻ cho FIM, XDR... với chi phí bổ sung.
Khả năng tùy biến	Cho phép tùy chỉnh sâu trong bộ rule, tích hợp không giới hạn. Không bị “vendor lock-in”.	Bị giới hạn trong các tính năng và tích hợp do nhà cung cấp hỗ trợ. Phụ thuộc hoàn toàn vào nhà cung cấp.
Hệ tầng triển khai	Có thể triển khai tại chỗ (On-premise), Private Cloud, hoặc Public Cloud (AWS, Azure, GCP). Khách hàng toàn quyền kiểm soát dữ liệu.	Sentinel: Bắt buộc dùng Azure Cloud. Splunk/QRadar: Có thể on-premise nhưng rất phức tạp và tốn kém tài nguyên.
Tích hợp AI & Phân tích	Giải pháp của chúng tôi tích hợp AI (Ollama) on-premise. Dữ liệu log không bao giờ rời khỏi hệ thống.	Các mô-đun AI/ML/SOAR là các gói “add-on” đắt đỏ. Có thể yêu cầu gửi dữ liệu lên cloud của hang để phân tích.
Bảo trì & Vận hành	Cần có chuyên môn kỹ thuật để cài đặt, tinh chỉnh và tối ưu hóa hệ thống	Có hỗ trợ kỹ thuật chính hang (với chi phí hỗ trợ bắt buộc hàng năm cao).

Qua so sánh, có thể thấy rõ Wazuh không còn là một "giải pháp thay thế giá rẻ" mà đã trở thành một **lựa chọn chiến lược, thông minh và hiệu quả về chi phí** cho các doanh nghiệp hiện đại. Nó cung cấp một nền tảng **All-in-One** (SIEM, XDR, FIM, SCA) với đầy đủ tính năng mạnh mẽ, cho phép bạn thu thập log không giới hạn mà **không tốn một đồng chi phí**.

bản quyền nào. Nó mang lại cho bạn sự **linh hoạt tuyệt đối**—tùy quyền kiểm soát dữ liệu của mình, triển khai tại chỗ (on-premise) hay bất kỳ đám mây nào bạn muốn.

Thách thức lớn nhất của Wazuh là đòi hỏi chuyên môn kỹ thuật cao để triển khai và vận hành. **Và đây chính là giá trị mà công ty tôi mang lại.**

Khi lựa chọn giải pháp của chúng tôi, bạn không chỉ nhận được một hệ thống Wazuh được tinh chỉnh tối ưu bởi các chuyên gia, mà còn sở hữu **Trợ lý An ninh Ảo (AI) độc quyền**—một khả năng phân tích thông minh, an toàn mà các đối thủ thương mại không thể cung cấp với một chi phí hợp lý.

