Tổng quan về Wazuh

# 1. Giới thiệu về Wazuh

Wazuh là một nền tảng bảo mật toàn diện cung cấp khả năng bảo vệ XDR (Extended Detection and Response) và SIEM (Security Information and Event Management) thống nhất cho cả endpoints và cloud workloads. Với kiến trúc hiện đại và khả năng mở rộng linh hoạt, Wazuh đáp ứng nhu cầu bảo mật từ doanh nghiệp nhỏ đến tập đoàn lớn.

Kiến trúc Hệ thống

Giải pháp Wazuh được xây dựng từ một agent đa năng và ba thành phần trung tâm hoạt động đồng bộ:

- Wazuh Server: Bộ não xử lý của hệ thống, phân tích dữ liệu và tạo cảnh báo

- Wazuh Indexer: Công cụ lưu trữ và tìm kiếm dữ liệu hiệu suất cao

- Wazuh Dashboard: Giao diện quản lý trực quan và thân thiện

# 2. Các thành phần của Wazuh

## 2.1. Wazuh Indexer

### 2.1.1. Giới thiệu về Wazuh Indexer

Wazuh indexer là một công cụ phân tích và tìm kiếm toàn văn có khả năng mở rộng cao. Đây là thành phần trung tâm của Wazuh, có nhiệm vụ lập chỉ mục và lưu trữ các cảnh báo do máy chủ Wazuh tạo ra, đồng thời cung cấp khả năng phân tích và tìm kiếm dữ liệu gần thời gian thực.

Wazuh indexer được xây dựng dựa trên OpenSearch, một nền tảng tìm kiếm và phân tích mã nguồn mở, kế thừa các tính năng mạnh mẽ từ Elasticsearch. Điều này đảm bảo rằng Wazuh indexer không chỉ có hiệu suất cao mà còn có khả năng tương thích rộng rãi với các công cụ và thư viện phân tích dữ liệu hiện có trong cộng đồng.

### 2.1.2. Kiến trúc và Khả năng mở rộng

Wazuh indexer có thể được cấu hình dưới dạng một cụm một nút hoặc nhiều nút, mang lại khả năng mở rộng và tính sẵn sàng cao. Trong môi trường sản xuất, việc triển khai cụm nhiều nút được khuyến nghị để đảm bảo tính liên tục của dịch vụ và khả năng xử lý khối lượng dữ liệu lớn.

Cụm Wazuh indexer có thể được mở rộng theo chiều ngang bằng cách thêm các nút mới, cho phép hệ thống xử lý ngày càng nhiều dữ liệu mà không ảnh hưởng đến hiệu suất. Mỗi nút trong cụm có thể đảm nhận các vai trò khác nhau như master node, data node, hoặc coordinating node, tùy thuộc vào cấu hình và yêu cầu của hệ thống.

### 2.1.3. Cấu trúc dữ liệu và Lưu trữ

Wazuh indexer lưu trữ dữ liệu dưới dạng tài liệu JSON, trong đó mỗi tài liệu liên kết một tập hợp các khóa, tên trường hoặc thuộc tính với các giá trị tương ứng của chúng, có thể là chuỗi, số, boolean, ngày, mảng giá trị, vị trí địa lý hoặc các loại dữ liệu khác. Một chỉ mục là một tập hợp các tài liệu có liên quan với nhau.

Mỗi tài liệu trong Wazuh indexer được gán một ID duy nhất và được lưu trữ trong một loại chỉ mục cụ thể. Cấu trúc linh hoạt này cho phép lưu trữ các loại dữ liệu đa dạng từ logs hệ thống đơn giản đến các sự kiện bảo mật phức tạp với nhiều trường thông tin chi tiết.

### 2.1.4. Phân mảnh và Tính dự phòng

Các tài liệu được lưu trữ trong Wazuh Indexer được phân phối trên các vùng chứa khác nhau được gọi là phân mảnh (shards). Mỗi shard có thể có các bản sao (replica shards) để tăng cường độ tin cậy và hiệu suất truy vấn. Số lượng shards và replicas có thể được cấu hình tùy theo nhu cầu của hệ thống và khối lượng dữ liệu dự kiến.

Bằng cách phân phối các tài liệu trên nhiều phân mảnh và phân phối các phân mảnh đó trên nhiều nút, Wazuh indexer có thể đảm bảo tính dự phòng. Điều này bảo vệ hệ thống của bạn khỏi các lỗi phần cứng và tăng khả năng truy vấn khi các nút được thêm vào một cụm.

Khi một nút trong cụm gặp sự cố, các replica shards trên các nút khác sẽ tự động được thăng cấp thành primary shards, đảm bảo dữ liệu luôn sẵn sàng và có thể truy cập được. Quá trình này diễn ra tự động mà không cần can thiệp thủ công từ quản trị viên.

### 2.1.5. Các chỉ mục chính trong Wazuh

Wazuh sử dụng bốn chỉ mục khác nhau để lưu trữ các loại sự kiện khác nhau:

- wazuh-alerts:

Lưu trữ các cảnh báo được tạo bởi máy chủ Wazuh. Các cảnh báo này được tạo mỗi khi một sự kiện kích hoạt một quy tắc có mức độ ưu tiên đủ cao (ngưỡng này có thể cấu hình được). Chỉ mục này thường chứa thông tin chi tiết về các mối đe dọa bảo mật, hành vi bất thường và các vi phạm chính sách được phát hiện.

- wazuh-archives:

Lưu trữ tất cả các sự kiện (dữ liệu lưu trữ) nhận được bởi máy chủ Wazuh, cho dù chúng có kích hoạt quy tắc hay không. Điều này đảm bảo rằng toàn bộ lịch sử hoạt động của hệ thống được bảo tồn cho mục đích kiểm toán và phân tích sau này.

- wazuh-monitoring:

Lưu trữ dữ liệu liên quan đến trạng thái tác nhân Wazuh theo thời gian. Nó được giao diện web sử dụng để thể hiện khi các tác nhân đang hoặc đã ở trạng thái Hoạt động, Ngắt kết nối hoặc Không bao giờ kết nối. Thông tin này rất quan trọng để theo dõi tình trạng sức khỏe của toàn bộ hạ tầng được giám sát.

- wazuh-statistics:

Lưu trữ dữ liệu liên quan đến hiệu suất máy chủ Wazuh. Nó được giao diện web sử dụng để thể hiện các số liệu thống kê hiệu suất như tốc độ xử lý sự kiện, mức độ sử dụng tài nguyên, và các metrics khác giúp tối ưu hóa hiệu suất hệ thống.

### 2.1.6 Quản lý vòng đời chỉ mục

Các chỉ mục này được quản lý theo chính sách vòng đời (Index Lifecycle Management - ILM), cho phép tự động xoay vòng, nén và xóa dữ liệu cũ để tối ưu hóa hiệu suất và dung lượng lưu trữ. ILM giúp đảm bảo rằng dữ liệu mới nhất luôn có sẵn với tốc độ truy cập nhanh nhất, trong khi dữ liệu cũ hơn được chuyển sang các phương thức lưu trữ hiệu quả hơn về chi phí.

Các chính sách ILM có thể được cấu hình để:

- Tự động tạo chỉ mục mới theo chu kỳ thời gian hoặc kích thước

- Nén dữ liệu cũ để tiết kiệm không gian lưu trữ

- Di chuyển dữ liệu sang các tier lưu trữ khác nhau dựa trên tần suất truy cập

- Xóa tự động dữ liệu quá hạn theo chính sách bảo tồn

### 2.1.7. Tương tác với Wazuh Indexer

Có thể tương tác với cụm Wazuh indexer bằng cách sử dụng API REST của Wazuh indexer, cung cấp nhiều tính linh hoạt. Bạn có thể thực hiện tìm kiếm, thêm hoặc xóa tài liệu, sửa đổi chỉ mục và nhiều hơn nữa.

API REST cung cấp các endpoint để:

- Thực hiện các truy vấn tìm kiếm phức tạp với nhiều điều kiện lọc

- Tạo và quản lý chỉ mục, mapping và aliases

- Thực hiện các thao tác bulk để xử lý lượng lớn dữ liệu hiệu quả

- Giám sát tình trạng cụm và các metrics hiệu suất

- Cấu hình các settings và policies cho chỉ mục

## 2.2. Wazuh Server

### 2.2.1. Giới thiệu tổng quan

Máy chủ Wazuh (Wazuh Server) đóng vai trò là trung tâm điều khiển và xử lý trong hệ sinh thái bảo mật Wazuh, hoạt động như một nền tảng SIEM (Security Information and Event Management) và XDR (Extended Detection and Response) mã nguồn mở. Đây không chỉ là một công cụ thu thập log đơn thuần, mà là một hệ thống phân tích bảo mật toàn diện, có khả năng xử lý hàng triệu sự kiện mỗi ngày từ các nguồn khác nhau như endpoints, containers, cloud workloads, network devices và applications.

Máy chủ Wazuh được thiết kế để đáp ứng nhu cầu của các tổ chức từ quy mô nhỏ đến enterprise, với khả năng mở rộng linh hoạt và hỗ trợ triển khai trên nhiều môi trường khác nhau. Nó không chỉ phân tích dữ liệu mà còn cung cấp khả năng phản ứng tự động, quản lý tuân thủ quy định, và tích hợp sâu với hệ sinh thái bảo mật hiện có của tổ chức.

### 2.2.2. Chức năng và vai trò cốt lõi

Thu thập và xử lý dữ liệu đa nguồn

- Wazuh Server có khả năng thu thập và xử lý dữ liệu từ vô số nguồn khác nhau. Ngoài các Wazuh agents được cài đặt trên endpoints, server còn có thể nhận dữ liệu từ syslog servers, cloud services (AWS CloudTrail, Azure Activity Logs, Google Cloud Audit Logs), container platforms (Docker, Kubernetes), network devices (firewalls, routers, switches), và các ứng dụng web thông qua các API hoặc log forwarding mechanisms.

- Quá trình xử lý dữ liệu được thực hiện theo thời gian thực, với khả năng normalization và enrichment tự động. Server sử dụng các bộ parser và decoder để chuẩn hóa dữ liệu từ các format khác nhau thành một cấu trúc thống nhất, giúp việc phân tích và correlation trở nên hiệu quả hơn.

Phân tích và phát hiện mối đe dọa nâng cao

- Công cụ phân tích của Wazuh Server sử dụng nhiều kỹ thuật phát hiện khác nhau bao gồm signature-based detection, anomaly detection, behavioral analysis, và machine learning algorithms. Hệ thống rules engine cực kỳ linh hoạt, cho phép tạo ra các quy tắc phức tạp với multiple conditions, time-based correlations, và cross-event analysis.

- Server tích hợp sẵn hàng nghìn rules được xây dựng sẵn để phát hiện các mối đe dọa phổ biến như malware infections, brute force attacks, privilege escalation, data exfiltration, và insider threats. Đồng thời, nó cũng hỗ trợ custom rules development, cho phép security teams tạo ra các detection logic phù hợp với môi trường cụ thể của tổ chức.

Quản lý tuân thủ quy định toàn diện

- Wazuh Server được thiết kế để hỗ trợ các tổ chức đáp ứng các yêu cầu tuân thủ quy định khắt khe. Với PCI DSS, server cung cấp monitoring cho file integrity, log management, vulnerability assessment, và access control monitoring. Đối với GDPR, nó giúp theo dõi data access patterns, privacy breaches, và data processing activities.

- Đối với HIPAA trong ngành healthcare, server có thể monitor PHI (Protected Health Information) access, audit trails, và compliance với các administrative, physical, và technical safeguards. Với SOX compliance, nó cung cấp financial data monitoring, change management tracking, và audit trail maintenance. Các framework khác như ISO 27001, NIST Cybersecurity Framework, và CIS Controls cũng được hỗ trợ đầy đủ.

### 2.2.3. Kiến trúc và thành phần kỹ thuật

Wazuh Server có thể được triển khai theo nhiều mô hình khác nhau để phù hợp với các yêu cầu khác nhau về performance, availability, và security. Single-node deployment phù hợp cho các tổ chức nhỏ hoặc testing environments, trong khi multi-node cluster deployment được khuyến nghị cho production environments với high availability requirements.

Đối với các tổ chức lớn, distributed architecture với multiple Wazuh servers trong các regions khác nhau có thể được triển khai, với central management server để coordination và policy distribution. Cloud-native deployments trên AWS, Azure, hoặc Google Cloud Platform cũng được hỗ trợ đầy đủ với auto-scaling capabilities và cloud-specific integrations.

Chi tiết các thành phần cốt lõi

- Agent Enrollment Service - Dịch vụ đăng ký nâng cao

Dịch vụ đăng ký agent của Wazuh không chỉ đơn giản là việc cấp phát keys mà là một hệ thống quản lý identity và access management hoàn chỉnh. Nó hỗ trợ multiple enrollment methods bao gồm password-based enrollment, certificate-based enrollment với PKI integration, và automatic enrollment thông qua configuration management tools như Ansible, Puppet, hoặc Chef.

Hệ thống này cũng hỗ trợ agent grouping và policy assignment tự động dựa trên các attributes như operating system, location, function, hoặc security level. Advanced features bao gồm agent registration approval workflows, bulk enrollment capabilities, và integration với enterprise directory services như Active Directory hoặc LDAP.

- Agent Connection Service - Kết nối và truyền thông bảo mật

Dịch vụ kết nối agent sử dụng các giao thức bảo mật tiên tiến để đảm bảo tính toàn vẹn và bảo mật của dữ liệu truyền tải. Ngoài AES encryption, nó còn hỗ trợ perfect forward secrecy, message authentication codes, và anti-replay mechanisms.

Service này cũng cung cấp intelligent load balancing cho các agent connections, automatic failover trong trường hợp server outages, và bandwidth optimization để giảm thiểu impact lên network infrastructure. Advanced monitoring capabilities cho phép real-time tracking của connection status, data transfer rates, và network latency.

- Analysis Engine - Công cụ phân tích thế hệ mới

Analysis Engine của Wazuh là một hệ thống xử lý event streaming phức tạp với khả năng horizontal scaling. Nó sử dụng multi-threaded architecture để xử lý song song hàng nghìn events per second, với intelligent queuing mechanisms để đảm bảo no data loss ngay cả trong peak load conditions.

Engine hỗ trợ complex event processing (CEP) với time-window based analysis, statistical anomaly detection, và machine learning-based behavioral analysis. Nó có thể thực hiện correlation analysis across multiple data sources và time periods, enabling detection of sophisticated attack campaigns và advanced persistent threats (APTs).

Decoder system được thiết kế modular, với support cho custom decoder development using XML-based configuration hoặc scripting languages như Python. Rules engine hỗ trợ hierarchical rule structures, rule inheritance, và dynamic rule loading without service restart.

- Wazuh RESTful API - Giao diện quản lý toàn diện

Wazuh API không chỉ là một interface đơn giản mà là một comprehensive management platform với GraphQL support, real-time WebSocket connections, và extensive authentication mechanisms bao gồm API keys, JWT tokens, và OAuth2 integration.

API cung cấp fine-grained access control với role-based permissions, allowing different levels of access cho different user groups. Nó hỗ trợ bulk operations, asynchronous processing cho long-running tasks, và comprehensive audit logging cho tất cả API activities.

Advanced features bao gồm API rate limiting, request throttling, và comprehensive monitoring với metrics exposure cho prometheus-compatible monitoring systems. API documentation được tự động generate và maintain, với interactive testing interfaces và SDK generation cho multiple programming languages.

- Cluster Daemon - Quản lý cụm nâng cao

Wazuh Cluster Daemon implement một distributed consensus algorithm để đảm bảo data consistency across cluster nodes. Nó sử dụng advanced leader election mechanisms, automatic split-brain prevention, và intelligent data replication strategies.

Daemon hỗ trợ rolling updates without downtime, automatic node health monitoring với intelligent failure detection, và dynamic load redistribution khi có nodes join hoặc leave cluster. Advanced networking features bao gồm multi-network support, network partition tolerance, và encrypted inter-node communications.

- Filebeat Integration - Shipping và indexing tối ưu

Filebeat integration trong Wazuh được customize extensively để optimize performance và reliability. Nó hỗ trợ advanced parsing với multiple processors, data transformation pipelines, và intelligent retry mechanisms with exponential backoff.

System cung cấp advanced monitoring với detailed metrics về shipping performance, indexing rates, và error tracking. Load balancing capabilities cho phép efficient distribution của data across multiple Indexer nodes, với automatic failover và health checking.

## 2.3. Wazuh Agent

### 2.3.1. Giới thiệu và tổng quan

Wazuh Agent đại diện cho thành phần điểm cuối quan trọng nhất trong hệ sinh thái bảo mật Wazuh, hoạt động như một cảm biến thông minh được triển khai trực tiếp trên các hệ thống cần bảo vệ. Không chỉ đơn giản là một công cụ thu thập dữ liệu, Wazuh Agent là một agent phát hiện và phản hồi điểm cuối đầy đủ tính năng, có khả năng thực hiện các hoạt động giám sát, phát hiện, ngăn chặn và phản hồi ngay tại điểm cuối.

Agent được thiết kế theo triết lý "bảo vệ theo chiều sâu", cung cấp nhiều lớp bảo vệ bao gồm giám sát thời gian thực, phân tích hành vi, phát hiện dựa trên chữ ký và phát hiện bất thường. Với dung lượng nhỏ gọn và hiệu suất cao, agent có thể hoạt động hiệu quả trên các hệ thống từ thiết bị nhúng đến máy chủ hiệu suất cao mà không ảnh hưởng đáng kể đến hiệu suất của hệ thống chủ.

### 2.3.2. Khả năng đa nền tảng và triển khai linh hoạt

Wazuh Agent hỗ trợ một loạt rộng các nền tảng và kiến trúc, bao gồm các bản phân phối Linux (Ubuntu, CentOS, RHEL, SUSE, Debian, Amazon Linux), Windows (từ Windows 7/Server 2008 đến các phiên bản mới nhất), macOS (từ 10.15 trở lên), và các biến thể Unix như Solaris, AIX, và HP-UX. Đối với mỗi nền tảng, agent được tối ưu hóa để tận dụng tối đa các tính năng và API gốc của hệ điều hành.

Trong môi trường điện toán đám mây, agent hỗ trợ triển khai trên tất cả các nhà cung cấp đám mây chính bao gồm AWS EC2, Azure Virtual Machines, Google Compute Engine, và các nền tảng đám mây khác. Triển khai container được hỗ trợ đầy đủ với Docker containers, Kubernetes pods, và các nền tảng điều phối container khác. Agent cũng có thể được triển khai trong máy ảo với hỗ trợ đầy đủ cho VMware vSphere, Microsoft Hyper-V, KVM, và các hypervisor khác.

### 2.3.3. Kiến trúc và thiết kế hệ thống

Kiến trúc mô-đun và có thể mở rộng

Kiến trúc mô-đun của Wazuh Agent được thiết kế theo nguyên tắc của kiến trúc dịch vụ nhỏ, trong đó mỗi mô-đun hoạt động như một dịch vụ độc lập với các giao diện và trách nhiệm được xác định rõ ràng. Kiến trúc cốt lõi bao gồm tiến trình daemon chính (wazuh-agentd) quản lý vòng đời của tất cả các mô-đun, hệ thống con truyền thông xử lý tương tác với máy chủ, và hệ thống quản lý cấu hình cho phép cấu hình lại động mà không cần khởi động lại.

Agent sử dụng các cơ chế bộ nhớ chia sẻ để chia sẻ dữ liệu hiệu quả giữa các mô-đun, kiến trúc hướng sự kiện để xử lý thời gian thực, và quản lý tài nguyên thông minh để tối ưu hóa hiệu suất và giảm thiểu tác động hệ thống. Các tính năng nâng cao bao gồm quản lý phụ thuộc mô-đun, khôi phục lỗi tự động, và giám sát sức khỏe toàn diện của từng thành phần.

Kiến trúc bảo mật và mô hình mối đe dọa

Agent được thiết kế với cách tiếp cận bảo mật trước tiên, triển khai nhiều lớp bảo mật để bảo vệ chống lại cả các cuộc tấn công bên ngoài và khả năng thỏa hiệp của chính agent. Xác minh tính toàn vẹn mã đảm bảo các tệp nhị phân agent không bị giả mạo, các cơ chế bảo vệ bộ nhớ ngăn chặn tràn bộ đệm và các cuộc tấn công tiêm mã, và phân tách đặc quyền đảm bảo các mô-đun khác nhau chạy với các đặc quyền tối thiểu cần thiết.

Bảo mật truyền thông bao gồm xác thực lẫn nhau với máy chủ, mã hóa đầu cuối của tất cả việc truyền dữ liệu, và các cơ chế chống phát lại để ngăn chặn các cuộc tấn công phát lại tin nhắn. Agent cũng triển khai các cơ chế tự bảo vệ để phát hiện và phản hồi các nỗ lực vô hiệu hóa hoặc thao túng chức năng agent.

### 2.3.4. Chi tiết các mô-đun và chức năng

Mô-đun Thu thập Nhật ký - Thu thập và xử lý nhật ký nâng cao

- Mô-đun Thu thập Nhật ký của Wazuh Agent không chỉ đơn giản đọc các tệp nhật ký mà là một công cụ xử lý nhật ký tinh vi với khả năng phân tích cú pháp nâng cao. Mô-đun hỗ trợ giám sát nhật ký thời gian thực với inotify (Linux) hoặc ReadDirectoryChangesW (Windows) để phát hiện ngay lập tức các thay đổi nhật ký, xử lý xoay vòng nhật ký thông minh để duy trì tính liên tục trong việc thu thập nhật ký, và các cơ chế lọc nâng cao để giảm nhiễu và tập trung vào các sự kiện liên quan đến bảo mật.

- Đối với môi trường Windows, mô-đun hỗ trợ thu thập Nhật ký Sự kiện Windows toàn diện với khả năng lọc XPath, cho phép lựa chọn chi tiết các loại sự kiện, nguồn hoặc tiêu chí cụ thể. Hỗ trợ nhật ký nhiều dòng cho phép xử lý đúng các định dạng nhật ký phức tạp như theo dõi ngăn xếp Java, nhật ký cơ sở dữ liệu hoặc nhật ký lỗi ứng dụng. Khả năng làm phong phú nhật ký JSON cho phép thêm siêu dữ liệu ngữ cảnh như thông tin vị trí địa lý, gắn thẻ tài sản hoặc ngữ cảnh kinh doanh.

- Các tính năng nâng cao bao gồm ẩn danh hóa nhật ký để tuân thủ các quy định bảo mật, các cơ chế đệm thông minh để xử lý các sự cố mạng tạm thời, và các thuật toán nén để tối ưu hóa việc sử dụng băng thông mạng. Mô-đun cũng hỗ trợ phân tích cú pháp nhật ký tùy chỉnh với biểu thức chính quy, cho phép thích ứng với các định dạng nhật ký độc quyền.

Mô-đun Thực thi Lệnh - Giám sát hệ thống và thu thập thông tin tình báo

- Mô-đun Thực thi Lệnh cung cấp khả năng mạnh mẽ để thu thập thông tin tình báo hệ thống thông qua việc thực thi lệnh theo lịch trình. Mô-đun không chỉ chạy các lệnh mà còn cung cấp ngữ cảnh thực thi toàn diện, bao gồm đầu ra lệnh, mã thoát, thời gian thực thi và các chỉ số sử dụng tài nguyên.

- Các trường hợp sử dụng tập trung vào bảo mật bao gồm giám sát các tiến trình không được ủy quyền, kiểm tra các kết nối mạng đáng ngờ, xác thực cấu hình hệ thống so với đường cơ sở, và thu thập thông tin pháp y sau các sự cố bảo mật. Mô-đun hỗ trợ thực thi lệnh đa nền tảng với phát hiện nền tảng tự động và thích ứng lệnh thích hợp.

- Khả năng lập lịch nâng cao cho phép các mẫu thực thi phức tạp với cú pháp giống cron, thực thi có điều kiện dựa trên trạng thái hệ thống, và xử lý lỗi thông minh với các cơ chế thử lại. Các tính năng xử lý đầu ra bao gồm trích xuất dữ liệu có cấu trúc, phát hiện bất thường trong đầu ra lệnh, và tương quan với các sự kiện bảo mật khác.

Giám sát Tính toàn vẹn Tệp (FIM) - Bảo vệ tính toàn vẹn toàn diện

- Mô-đun FIM của Wazuh Agent triển khai một giải pháp giám sát hệ thống tệp toàn diện với phát hiện thay đổi thời gian thực, phân tích thay đổi chi tiết, và quản lý đường cơ sở thông minh. Mô-đun sử dụng các API giám sát hệ thống tệp nâng cao như fanotify (Linux) hoặc ReadDirectoryChangesW (Windows) để thông báo ngay lập tức về các thay đổi hệ thống tệp.

- Khả năng giám sát bao gồm không chỉ các thay đổi nội dung tệp mà còn các thay đổi thuộc tính (quyền, quyền sở hữu, dấu thời gian), thay đổi siêu dữ liệu, và các hoạt động hệ thống tệp như tạo, xóa, di chuyển hoặc đổi tên. Các thuật toán băm nâng cao (MD5, SHA-1, SHA-256) cung cấp xác minh mật mã của tính toàn vẹn tệp, với các chiến lược băm thông minh để tối ưu hóa hiệu suất cho các tệp lớn.

- Tích hợp cơ sở dữ liệu duy trì thông tin trạng thái hệ thống tệp toàn diện trong các cơ sở dữ liệu SQLite cục bộ, cho phép các truy vấn phức tạp và phân tích lịch sử. Khả năng cảnh báo thời gian thực cung cấp thông báo ngay lập tức về các thay đổi quan trọng, với các ngưỡng cảnh báo có thể cấu hình dựa trên tính quan trọng của tệp, mẫu thay đổi hoặc tác động kinh doanh.

- Các tính năng nâng cao bao gồm các mẫu bỏ qua để loại trừ các thay đổi không liên quan, xem trước nội dung tệp trong cảnh báo, và tích hợp với các nguồn cấp dữ liệu tình báo mối đe dọa để tự động gắn cờ các tệp độc hại đã biết. Mô-đun cũng hỗ trợ giám sát hệ thống tệp mạng và theo dõi hệ thống tệp phân tán.

Đánh giá Cấu hình Bảo mật (SCA) - Tuân thủ và tự động hóa củng cố

- Mô-đun SCA triển khai khả năng giám sát và đánh giá cấu hình bảo mật toàn diện, sử dụng bộ quy tắc mở rộng dựa trên các tiêu chuẩn ngành và thực tiễn tốt nhất. Mô-đun không chỉ kiểm tra cấu hình tĩnh mà còn thực hiện giám sát tuân thủ động với đánh giá chính sách thời gian thực.

- Các bộ quy tắc tích hợp sẵn bao gồm các khung tuân thủ chính bao gồm CIS Benchmarks cho các hệ điều hành khác nhau, yêu cầu PCI DSS, hướng dẫn NIST, quy tắc bảo mật HIPAA, và các biện pháp kỹ thuật GDPR. Mỗi bộ quy tắc chứa hàng trăm kiểm tra cụ thể bao gồm củng cố hệ thống, kiểm soát truy cập, bảo mật mạng, cấu hình ghi nhật ký, và cài đặt bảo mật ứng dụng.

- Khả năng phát triển chính sách tùy chỉnh cho phép các tổ chức tạo ra các kiểm tra tuân thủ chuyên biệt cho các ứng dụng độc quyền, chính sách bảo mật tùy chỉnh hoặc yêu cầu quy định cụ thể. Ngôn ngữ chính sách hỗ trợ logic có điều kiện phức tạp, tương quan kiểm tra chéo, và tích hợp với các nguồn dữ liệu bên ngoài.

- Khả năng khắc phục tự động có thể tự động sửa chữa một số vấn đề cấu hình nhất định khi được kích hoạt, với việc ghi nhật ký toàn diện tất cả các hành động khắc phục. Các tính năng báo cáo tuân thủ cung cấp bảng điều khiển tuân thủ chi tiết, phân tích xu hướng và tóm tắt cấp điều hành.

Mô-đun Kiểm kê Hệ thống - Khám phá và quản lý tài sản

- Mô-đun Kiểm kê Hệ thống cung cấp khả năng khám phá tài sản và quản lý kiểm kê toàn diện, thực hiện lập hồ sơ hệ thống chi tiết và duy trì thông tin tài sản cập nhật. Mô-đun thực hiện quét hệ thống thường xuyên để thu thập thông tin về cấu hình phần cứng, cài đặt phần mềm, cấu hình mạng, dịch vụ đang chạy, và cài đặt bảo mật.

- Kiểm kê phần cứng bao gồm thông tin chi tiết về thông số kỹ thuật CPU, cấu hình bộ nhớ, thiết bị lưu trữ, giao diện mạng, và thiết bị ngoại vi. Kiểm kê phần mềm theo dõi các ứng dụng đã cài đặt, bản vá, cập nhật, thư viện chia sẻ, và các tiến trình đang chạy với thông tin phiên bản chi tiết và tương quan lỗ hổng.

- Kiểm kê mạng cung cấp thông tin cấu hình mạng toàn diện bao gồm địa chỉ IP, bảng định tuyến, quy tắc tường lửa, cổng mở, kết nối hoạt động, và cấu hình dịch vụ mạng. Kiểm kê bảo mật bao gồm tài khoản người dùng, thành viên nhóm, phân công đặc quyền, chính sách bảo mật, và cấu hình kiểm soát truy cập.

- Khả năng tương quan nâng cao cho phép theo dõi các thay đổi theo thời gian, xác định các cài đặt phần mềm không được ủy quyền, phát hiện sự trôi dạt cấu hình, và cung cấp quản lý vòng đời tài sản toàn diện. Tích hợp với các hệ thống quản lý lỗ hổng cung cấp tương quan lỗ hổng tự động và đánh giá rủi ro.

Mô-đun Phát hiện Phần mềm Độc hại - Phát hiện mối đe dọa nâng cao

- Mô-đun Phát hiện Phần mềm Độc hại triển khai khả năng phát hiện phần mềm độc hại tinh vi sử dụng nhiều kỹ thuật phát hiện vượt ra ngoài các cách tiếp cận dựa trên chữ ký truyền thống. Mô-đun sử dụng phân tích hành vi để phát hiện các hoạt động tiến trình đáng ngờ, bất thường hệ thống tệp, mẫu hành vi mạng, và bất thường sử dụng tài nguyên hệ thống.

- Khả năng phát hiện rootkit bao gồm quét hệ thống toàn diện để tìm các tiến trình ẩn, tệp ẩn, kết nối mạng ẩn, và các sửa đổi cấp kernel. Mô-đun thực hiện kiểm tra tính toàn vẹn của các tệp hệ thống quan trọng, phát hiện hijacking thư viện, và giám sát cuộc gọi hệ thống đáng ngờ.

- Phân tích heuristic nâng cao đánh giá các mẫu hành vi tiến trình, mẫu truy cập tệp, mẫu giao tiếp mạng, và mẫu sửa đổi hệ thống để xác định các hoạt động phần mềm độc hại tiềm năng. Khả năng học máy cho phép phát hiện thích ứng các biến thể phần mềm độc hại mới và chưa biết.

- Các tính năng bảo vệ thời gian thực bao gồm giám sát thực thi tiến trình, giám sát truy cập tệp, giám sát kết nối mạng, và giám sát sửa đổi registry (Windows). Khả năng cách ly cho phép tự động cô lập các tệp độc hại nghi ngờ với bảo tồn pháp y toàn diện.

Mô-đun Phản hồi Chủ động - Phản hồi mối đe dọa tự động

- Mô-đun Phản hồi Chủ động cung cấp khả năng phản hồi tự động toàn diện để ngăn chặn và giảm thiểu mối đe dọa ngay lập tức. Mô-đun không chỉ thực thi các phản hồi được xác định trước mà còn hỗ trợ các quy trình phản hồi phức tạp với logic có điều kiện và chuỗi phản hồi nhiều bước.

- Các hành động phản hồi tích hợp sẵn bao gồm chặn kết nối mạng (tích hợp tường lửa), chấm dứt tiến trình, cách ly tệp, vô hiệu hóa tài khoản người dùng, và cô lập hệ thống. Khả năng phản hồi nâng cao bao gồm thu thập kết xuất bộ nhớ, bắt lưu lượng mạng, thu thập artifact pháp y, và bảo tồn bằng chứng.

- Phát triển phản hồi tùy chỉnh cho phép các tổ chức tạo ra các hành động phản hồi chuyên biệt cho các mối đe dọa cụ thể hoặc yêu cầu tuân thủ. Scripting phản hồi hỗ trợ nhiều ngôn ngữ lập trình và tích hợp với các công cụ bảo mật bên ngoài, nền tảng SOAR, và hệ thống điều phối.

- Các cơ chế xác thực phản hồi đảm bảo các hành động phản hồi được thực thi thành công với việc ghi nhật ký và đường kiểm toán toàn diện. Khả năng rollback cho phép hoàn nguyên các phản hồi tự động nếu cần thiết, với theo dõi thay đổi chi tiết và đánh giá tác động.

Giám sát Bảo mật Container - Bảo mật cloud-native

- Mô-đun Bảo mật Container cung cấp giám sát toàn diện cho các môi trường container hóa, tích hợp trực tiếp với Docker Engine API, Kubernetes API, và các API runtime container khác. Mô-đun giám sát các sự kiện vòng đời container, bảo mật image, bảo mật mạng, và hành vi runtime.

- Phân tích image container bao gồm quét lỗ hổng, đánh giá cấu hình, phát hiện bí mật, và kiểm tra tuân thủ theo các benchmark bảo mật container. Giám sát runtime theo dõi hành vi container, kết nối mạng, thay đổi hệ thống tệp, thực thi tiến trình, và mẫu sử dụng tài nguyên.

- Giám sát cụ thể Kubernetes bao gồm giám sát bảo mật pod, giám sát tài khoản dịch vụ, giám sát chính sách RBAC, giám sát thực thi chính sách mạng, và tích hợp admission controller. Phát hiện thoát container giám sát các nỗ lực phá vỡ cô lập container.

- Tích hợp với các nền tảng bảo mật container cung cấp quản lý vòng đời bảo mật container toàn diện từ quét bảo mật thời gian xây dựng đến phát hiện và phản hồi mối đe dọa runtime.

Giám sát Bảo mật Đám mây - Bảo mật đa đám mây

- Mô-đun Bảo mật Đám mây cung cấp giám sát toàn diện cho các nền tảng đám mây chính, triển khai tích hợp gốc với AWS, Azure, Google Cloud Platform, và các nhà cung cấp đám mây khác. Mô-đun giám sát các thay đổi cơ sở hạ tầng đám mây, mẫu truy cập, thay đổi cấu hình, và các sự kiện bảo mật.

- Tích hợp AWS bao gồm giám sát toàn diện các sự kiện CloudTrail, VPC Flow Logs, phát hiện GuardDuty, thay đổi Config, và hoạt động IAM. Tích hợp Azure bao gồm Activity Logs, cảnh báo Security Center, truy cập Key Vault, và sự kiện Azure AD. Tích hợp Google Cloud giám sát Cloud Audit Logs, VPC Flow Logs, phát hiện Security Command Center, và thay đổi chính sách IAM.

- Khả năng tương quan đa đám mây cung cấp giám sát bảo mật thống nhất trên nhiều môi trường đám mây, với cảnh báo tập trung, giám sát tuân thủ, và phát hiện mối đe dọa. Phát hiện mối đe dọa cụ thể đám mây bao gồm phát hiện thỏa hiệp tài khoản, giám sát leo thang đặc quyền, phát hiện rò rỉ dữ liệu, và giám sát mối đe dọa nội bộ.

- Các tính năng bảo mật đám mây nâng cao bao gồm phát hiện cấu hình sai đám mây, giám sát tuân thủ theo các khung bảo mật đám mây, khả năng khắc phục tự động, và tích hợp với các dịch vụ bảo mật gốc đám mây.

### 2.3.5. Giao tiếp và bảo mật

Wazuh Agent triển khai giao tiếp bảo mật cấp doanh nghiệp với Wazuh Server sử dụng nhiều lớp kiểm soát bảo mật. Giao thức giao tiếp hỗ trợ cả giao thức TCP và UDP với lựa chọn giao thức thông minh dựa trên điều kiện mạng và yêu cầu bảo mật.

Triển khai mã hóa sử dụng AES-256 với bảo mật chuyển tiếp hoàn hảo, đảm bảo rằng ngay cả khi các khóa dài hạn bị thỏa hiệp, các giao tiếp trong quá khứ vẫn được bảo mật. Các cơ chế trao đổi khóa bao gồm cả khóa chia sẻ trước và xác thực dựa trên chứng chỉ, với hỗ trợ tích hợp PKI doanh nghiệp.

Bảo vệ tính toàn vẹn tin nhắn sử dụng HMAC để phát hiện giả mạo hoặc hỏng dữ liệu truyền tải. Các cơ chế chống phát lại ngăn chặn các cuộc tấn công phát lại sử dụng số thứ tự và xác thực dựa trên thời gian. Các thuật toán nén tối ưu hóa việc sử dụng băng thông trong khi duy trì bảo mật.

### 2.4. Wazuh Dashboard

### 2.4.1. Tổng quan về Wazuh Dashboard

Wazuh Dashboard là một giao diện người dùng web linh hoạt và trực quan được thiết kế để khám phá, phân tích và trực quan hóa các sự kiện bảo mật và dữ liệu cảnh báo một cách toàn diện. Đây không chỉ là một công cụ hiển thị đơn thuần mà còn là một nền tảng quản lý và giám sát hoàn chỉnh cho toàn bộ hệ sinh thái Wazuh. Dashboard được xây dựng trên nền tảng OpenSearch Dashboards (trước đây là Kibana), cung cấp khả năng xử lý và hiển thị dữ liệu mạnh mẽ với hiệu suất cao.

Giao diện này đóng vai trò như trung tâm điều khiển chính cho các hoạt động bảo mật, cho phép các nhà phân tích bảo mật, quản trị viên hệ thống và các chuyên gia trung tâm vận hành bảo mật có thể theo dõi, phân tích và phản ứng với các mối đe dọa bảo mật một cách hiệu quả. Ngoài ra, Wazuh Dashboard tích hợp sâu các tính năng kiểm soát truy cập dựa trên vai trò và đăng nhập một lần, đảm bảo tính bảo mật và thuận tiện trong việc quản lý người dùng.

### 2.4.2. Trực quan hóa và phân tích dữ liệu nâng cao

Giao diện web này cung cấp khả năng điều hướng mạnh mẽ qua các loại dữ liệu phong phú được thu thập bởi các agent Wazuh từ nhiều nguồn khác nhau. Các nguồn dữ liệu này bao gồm nhật ký hệ thống, nhật ký ứng dụng, lưu lượng mạng, dữ liệu giám sát tính toàn vẹn tệp tin, đánh giá lỗ hổng bảo mật, kiểm tra tuân thủ, và nhiều loại dữ liệu bảo mật khác. Người dùng có thể dễ dàng chuyển đổi giữa các giao diện khác nhau, từ tổng quan tổng thể đến phân tích chi tiết của từng sự kiện cụ thể.

Dashboard hỗ trợ nhiều định dạng dữ liệu và có khả năng xử lý khối lượng lớn thông tin trong thời gian thực. Hệ thống tìm kiếm và lọc tiên tiến cho phép người dùng nhanh chóng định vị các sự kiện quan trọng thông qua các truy vấn phức tạp, sử dụng cú pháp tương tự như ngôn ngữ truy vấn của Elasticsearch.

Wazuh Dashboard cho phép người dùng tạo ra các báo cáo chi tiết và các trực quan hóa tùy chỉnh phù hợp với nhu cầu cụ thể của tổ chức. Hệ thống cung cấp nhiều loại biểu đồ khác nhau như biểu đồ đường, biểu đồ cột, biểu đồ tròn, bản đồ nhiệt, bảng dữ liệu, và các trực quan hóa phức tạp khác. Người dùng có thể kết hợp nhiều trực quan hóa thành các bảng điều khiển tổng hợp, cho phép giám sát đồng thời nhiều khía cạnh bảo mật khác nhau.

Tính năng lập lịch cho phép tự động tạo và gửi báo cáo theo lịch trình định sẵn, hỗ trợ nhiều định dạng xuất như PDF, CSV, và PNG. Điều này đặc biệt hữu ích cho việc báo cáo định kỳ cho ban lãnh đạo hoặc các bên liên quan khác.

Wazuh cung cấp các bảng điều khiển và mẫu sẵn có được thiết kế đặc biệt để hỗ trợ tuân thủ các quy định và tiêu chuẩn bảo mật quan trọng. Các bảng điều khiển cho PCI DSS giúp theo dõi các yêu cầu bảo mật cho dữ liệu thẻ tín dụng, bảng điều khiển GDPR hỗ trợ giám sát quyền riêng tư dữ liệu, bảng điều khiển HIPAA cho ngành y tế, và NIST 800-53 cho các tổ chức chính phủ và doanh nghiệp lớn.

Đặc biệt, Wazuh tích hợp sâu với khung MITRE ATT&CK, cung cấp giao diện trực quan để điều hướng qua các chiến thuật, kỹ thuật, và quy trình của kẻ tấn công. Mỗi cảnh báo bảo mật được ánh xạ tự động với các kỹ thuật tương ứng trong MITRE ATT&CK, giúp nhà phân tích hiểu rõ hơn về bản chất của cuộc tấn công và phản ứng phù hợp.

### 2.4.3. Giám sát và cấu hình Agent toàn diện

Wazuh Dashboard cung cấp giao diện trực quan và mạnh mẽ để quản lý cấu hình của toàn bộ nhóm agent được triển khai trên môi trường. Người dùng có thể dễ dàng xác định và điều chỉnh các module agent sẽ được kích hoạt cho từng điểm cuối hoặc nhóm điểm cuối cụ thể. Các module này bao gồm phân tích nhật ký, giám sát tính toàn vẹn tệp tin, phát hiện rootkit, phát hiện lỗ hổng, giám sát chính sách, và nhiều module chuyên biệt khác.

Giao diện cho phép cấu hình chi tiết các tệp nhật ký sẽ được giám sát, bao gồm việc chỉ định định dạng nhật ký, tần suất đọc, và các quy tắc xử lý đặc biệt. Người dùng cũng có thể định nghĩa các tệp và thư mục cần được giám sát về tính toàn vẹn, thiết lập các đường cơ sở và ngưỡng cho việc phát hiện thay đổi bất thường.

Dashboard cung cấp khả năng giám sát trạng thái thời gian thực của toàn bộ nhóm agent, bao gồm thông tin về trạng thái kết nối, thời điểm hoạt động cuối cùng, thông tin hệ điều hành, phiên bản agent, và các số liệu hiệu suất khác nhau. Hệ thống cảnh báo tự động thông báo khi có agent mất kết nối, gặp lỗi, hoặc hoạt động bất thường.

Các số liệu hiệu suất được thu thập và hiển thị bao gồm sử dụng CPU, tiêu thụ bộ nhớ, sử dụng băng thông mạng, tốc độ xử lý sự kiện, và kích thước hàng đợi. Thông tin này giúp quản trị viên tối ưu hóa hiệu suất và xác định các nút cổ chai tiềm năng trong hệ thống.

Một trong những tính năng mạnh mẽ của Wazuh là khả năng thực hiện đánh giá cấu hình và kiểm tra tuân thủ bảo mật. Dashboard cho phép người dùng định nghĩa và thực hiện các kiểm tra chính sách tự động, đánh giá cấu hình hệ thống so với các đường cơ sở bảo mật đã được thiết lập.

Các đánh giá cấu hình bảo mật được thực hiện định kỳ và báo cáo chi tiết về trạng thái tuân thủ, làm nổi bật các cấu hình sai và cung cấp hướng dẫn khắc phục. Hệ thống hỗ trợ các tiêu chuẩn ngành như CIS Benchmarks, hướng dẫn NIST, và các chính sách tổ chức tùy chỉnh.