Wazuh

What is Wazuh?
Wazuh integrates various security functionalities into a single platform, including:

- **Log Data Collection & Analysis**: Aggregates logs from diverse sources (e.g., Linux, Windows, network devices) for centralized analysis.
- **Host-Based Intrusion Detection System (HIDS)**: Monitors systems for suspicious activities, malware, rootkits, and unauthorized changes.
- **File Integrity Monitoring (FIM)**: Detects unauthorized modifications to critical system files.
- **Threat Intelligence**: Identifies and responds to known threats using threat intelligence feeds.
- **Incident Response**: Facilitates rapid response to security incidents through automated actions.
- **Regulatory Compliance**: Assists in meeting compliance requirements such as PCI DSS, GDPR, and HIPAA.
- The platform comprises a lightweight agent, a central server for data processing, and a dashboard for visualization and management.

Why Use Wazuh?

- **Cost-Effective**: Being open-source, it eliminates licensing fees, making it accessible for organizations of all sizes.
- **Scalability**: Designed to scale from small setups to large enterprise environments.
- **Flexibility**: Offers customizable rules and integrations to fit specific security needs.
- **Community Support**: Backed by an active community contributing to continuous improvement.
- **Comprehensive Coverage**: Provides visibility across on-premises, virtualized, containerized, and cloud-based environments.

Key Features of Wazuh

- **Intrusion Detection**: Wazuh agents scan monitored systems to detect malware, rootkits, and suspicious anomalies, providing real-time visibility into potential threats.
- **Log Data Analysis**: Aggregates and analyzes logs from diverse sources such as Linux, Windows, and network devices, facilitating centralized monitoring and threat detection.
- **File Integrity Monitoring (FIM)**: Monitors critical system files for unauthorized changes, helping to detect potential security breaches or policy violations.

- **Vulnerability Detection**: Identifies vulnerabilities in the operating system and installed applications by comparing them against known vulnerability databases, aiding in proactive risk management.
- **Configuration Assessment**: Evaluates system configurations against security policies and standards to ensure compliance and identify misconfigurations that could lead to security issues.
- **Incident Response**: Automates response actions to detected threats through the Active Response module, enabling timely and consistent mitigation of security incidents.
- **Regulatory Compliance**: Assists organizations in meeting regulatory requirements such as PCI DSS, GDPR, HIPAA, and NIST 800-53 by providing tools for log analysis, configuration assessment, and reporting.
- **Cloud Security**: Provides security monitoring for cloud environments, including integration with cloud provider APIs to detect changes and collect log data, ensuring visibility and protection in cloud infrastructures.

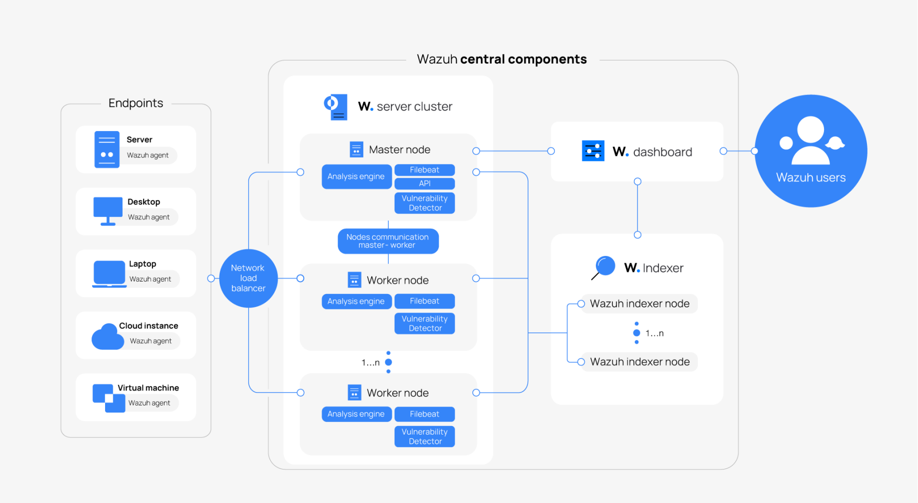
Central Components

- **Wazuh Indexer**
  The Wazuh Indexer is a real-time, full-text search and analytics engine for security data. It indexes and stores alerts generated by the Wazuh server, enabling efficient querying and analysis through the Wazuh Dashboard. The indexer can be configured as a single-node or multi-node cluster, providing scalability and high availability.
- **Wazuh Server**
  The Wazuh Server analyzes data received from agents, triggering alerts when threats or anomalies are detected. It manages agent configurations remotely, monitors their status, and enriches alert data using threat intelligence sources and frameworks like MITRE ATT&CK. The server can also integrate with external software, including ticketing systems and messaging platforms, to streamline security operations.
- **Wazuh Dashboard**
  The Wazuh Dashboard is a flexible and intuitive web user interface for mining, analyzing, and visualizing security events and alerts data. It provides features for role-based access control (RBAC), single sign-on (SSO), and includes out-of-the-box dashboards for regulatory compliance standards such as PCI DSS, GDPR, HIPAA, and NIST 800-53. Users can manage agent configurations, monitor system status, and interact with the Wazuh API directly through the dashboard.

Endpoint Component

Wazuh Agent

The Wazuh Agent is a multi-platform component that runs on monitored systems, providing threat prevention, detection, and response capabilities. It collects various types of system and application data, forwarding it securely to the Wazuh Server. The agent's modular architecture allows for tasks such as file integrity monitoring, log data collection, vulnerability detection, and configuration assessment.



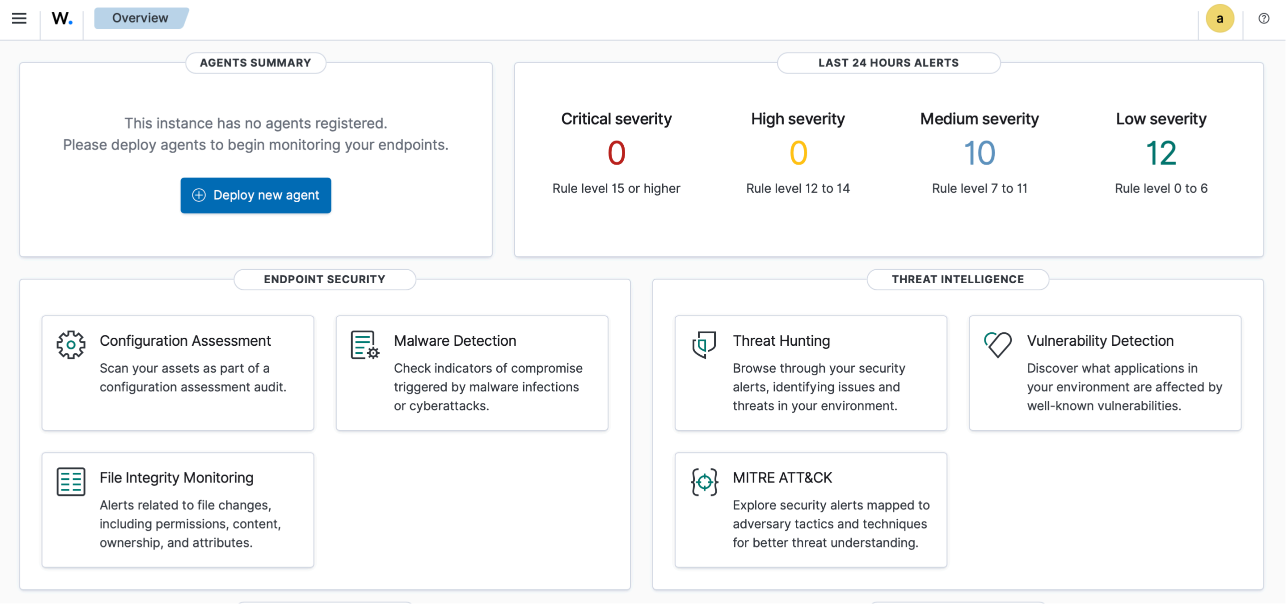
Alternatives & Comparisons

When evaluating alternatives to Wazuh, consider the following options:

- **CrowdStrike Falcon**: A cloud-native endpoint protection platform offering advanced threat detection and response capabilities.
- **SentinelOne Singularity**: Provides autonomous endpoint protection with AI-driven threat detection.
- **Datadog**: Offers infrastructure monitoring and security features, including log management and anomaly detection.
- **Carbon Black EDR**: Delivers endpoint detection and response with real-time threat hunting capabilities.

Cortex XDR: Integrates network, endpoint, and cloud data to prevent sophisticated attacks.

Dash board



AGENTS SUMMARY

This instance has no agents registered.
Please deploy agents to begin monitoring your endpoints.

Deploy new agent

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	10	12
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Check indicators of compromise triggered by malware infections or cyberattacks.

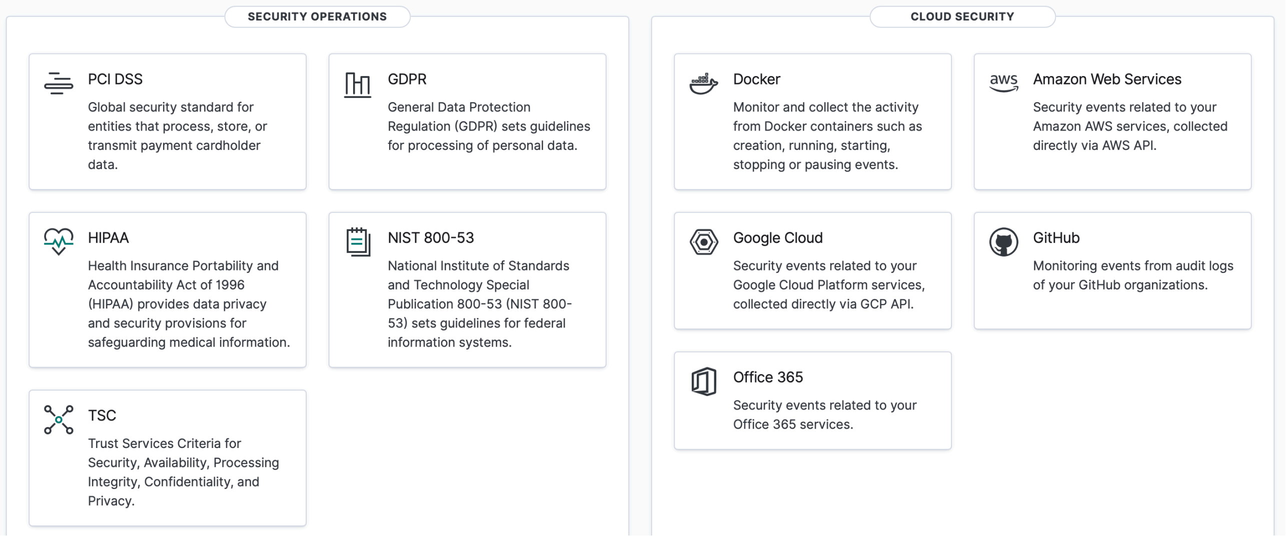
File Integrity Monitoring
Alerts related to file changes, including permissions, content, ownership, and attributes.

THREAT INTELLIGENCE

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK
Explore security alerts mapped to adversary tactics and techniques for better threat understanding.



SECURITY OPERATIONS

PCI DSS
Global security standard for entities that process, store, or transmit payment cardholder data.

GDPR
General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.

HIPAA
Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides data privacy and security provisions for safeguarding medical information.

NIST 800-53
National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

TSC
Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

CLOUD SECURITY

Docker
Monitor and collect the activity from Docker containers such as creation, running, starting, stopping or pausing events.

Amazon Web Services
Security events related to your Amazon AWS services, collected directly via AWS API.

Google Cloud
Security events related to your Google Cloud Platform services, collected directly via GCP API.

GitHub
Monitoring events from audit logs of your GitHub organizations.

Office 365
Security events related to your Office 365 services.

Overview of Wazuh Dashboard Components

Agents Summary

This section provides a snapshot of all connected and disconnected agents, offering insights into their status and health. It allows administrators to monitor agent activity and ensure that all endpoints are adequately covered.

Last 24 Hours Alerts

Displays a real-time feed of security alerts generated in the past 24 hours. Alerts are categorized by severity levels, enabling quick identification and response to critical issues.

Endpoint Security Features

Focuses on the security status of individual endpoints.

It includes dashboards for:

- **Configuration Assessment**: Evaluates system configurations against security benchmarks.
- **Malware Detection**: Identifies malicious software and potential threats.
- **File Integrity Monitoring**: Tracks changes to critical files, detecting unauthorized modifications.

Threat Intelligence

Provides tools for proactive threat hunting and vulnerability assessment.

Key features include:

- **Threat Hunting**: Analyzes patterns to detect potential threats.
- **Vulnerability Detection**: Identifies known vulnerabilities within the system.
- **MITRE ATT&CK Integration**: Maps detected threats to the MITRE framework for better understanding of adversary tactics.
- **VirusTotal Integration**: Cross-references files and URLs against VirusTotal's database for threat analysis.

Security Operations Frameworks

Supports compliance with various regulatory standards by providing dedicated dashboards for:

- PCI DSS
- GDPR
- HIPAA
- NIST 800-53
- TSC

These dashboards help organizations monitor and maintain compliance with industry-specific security requirements.

Cloud Security Integration

Monitors security events and configurations across various cloud platforms, including:

- Docker
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- GitHub
- Office 365

Note:
You can find the passwords for all the Wazuh indexer and Wazuh API users in the wazuh-passwords.txt file inside wazuh-install-files.tar.

To print them, run the following command:

```
sudo tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt
```

Component	Description
sudo	Runs the command with superuser (root) privileges. Useful when the archive or file requires elevated permissions to read.
tar	Command to manipulate `.tar` archive files (create, extract, list, etc.).
-O	Sends the extracted file to **standard output** (i.e., prints it to the terminal instead of extracting to disk).
-x	Extract files from the archive.
-v	Verbose mode — lists the files being extracted to the terminal.
-f	Tells `tar` the next argument is the archive file name.
wazuh-install-files.tar	Name of the archive file to operate on.
wazuh-install-files/wazuh-passwords.txt	The specific file path **inside** the archive to extract and print. Must match the internal structure of the `.tar` file.

Wazuh Directories:

/etc/wazuh-indexer/

Contains configuration files for the Wazuh Indexer, which is responsible for indexing and storing security data.

```
tiago-paquete@Linux:~$ sudo ls -l /etc/wazuh-indexer/
==========================================================================
total 84
dr-x------   2 wazuh-indexer wazuh-indexer  4096 May  7 12:39 certs
drwxr-x---   2 wazuh-indexer wazuh-indexer  4096 May  7 12:41 internalusers-backup
-rw-rw----   1 wazuh-indexer wazuh-indexer  3068 May  7 12:39 jvm.options
drwxr-x---   2 wazuh-indexer wazuh-indexer  4096 Mar 26 20:15 jvm.options.d
-rw-rw----   1 wazuh-indexer wazuh-indexer 17919 Mar 26 20:14 log4j2.properties
drwxr-x---   2 wazuh-indexer wazuh-indexer  4096 May  7 12:39 opensearch-notifications
drwxr-x---   2 wazuh-indexer wazuh-indexer  4096 May  7 12:39 opensearch-notifications-core
drwxr-x---   2 wazuh-indexer wazuh-indexer  4096 May  7 12:39 opensearch-observability
drwxr-x---   2 wazuh-indexer wazuh-indexer  4096 May  7 12:39 opensearch-performance-analyzer
drwxr-x---   2 wazuh-indexer wazuh-indexer  4096 May  7 12:39 opensearch-reports-scheduler
drwxr-x---   2 wazuh-indexer wazuh-indexer  4096 May  7 12:39 opensearch-security
-rw-rw----   1 wazuh-indexer wazuh-indexer   196 May  7 12:39 opensearch.keystore
-rw-rw----   1 wazuh-indexer wazuh-indexer  2152 May  7 12:39 opensearch.yml
==========================================================================
```

/etc/filebeat/

Holds Filebeat configuration files. Filebeat is used to forward logs and alerts from the Wazuh Manager to the Wazuh Indexer.

```
tiago-paquete@Linux:~$ sudo ls -l /etc/filebeat/
==========================================================================
total 480
dr-x------ 2 root root   4096 May  7 12:40 certs
-rw-r--r-- 1 root root 297349 Jan 12  2021 fields.yml
-rw-r--r-- 1 root root  91838 Jan 12  2021 filebeat.reference.yml
-rw------- 1 root root    985 May  7 12:41 filebeat.yml
drwxr-xr-x 2 root root   4096 May  7 12:40 modules.d
-rw-r--r-- 1 root root  84218 May  7 12:40 wazuh-template.json
==========================================================================
```

/etc/wazuh-dashboard/

Stores configuration files for the Wazuh Dashboard, the web interface for visualizing and managing security events.

```
tiago-paquete@Linux:~$ sudo ls -l /etc/wazuh-dashboard/
==========================================================================
total 16
dr-x------ 2 wazuh-dashboard wazuh-dashboard 4096 May  7 12:41 certs
-rw-r----- 1 wazuh-dashboard wazuh-dashboard  312 May  5  2023 node.options
-rw-r--r-- 1 wazuh-dashboard wazuh-dashboard  254 May  7 12:41 opensearch_dashboards.keystore
-rw-r----- 1 wazuh-dashboard wazuh-dashboard  714 May  7 12:41 opensearch_dashboards.yml
==========================================================================
```

/usr/share/wazuh-dashboard/data/wazuh/config/

Contains the wazuh.yml file, which defines settings for the Wazuh Dashboard's communication with the Wazuh API.

```
tiago-paquete@Linux:~$ sudo ls -l /usr/share/wazuh-dashboard/data/wazuh/config/
================================================================================
total 12
-rw------- 1 wazuh-dashboard wazuh-dashboard 8349 May  7 12:41 wazuh.yml
================================================================================
```

/var/ossec/logs/

Holds various log files generated by Wazuh, including alerts and archives. For example:

- alerts.log and alerts.json: Store security alerts generated by Wazuh.
- archives.log and archives.json: Store all events received from agents.

```
tiago-paquete@Linux:~$ sudo ls -l /var/ossec/logs/
================================================================================
total 56
-rw-rw---- 1 wazuh wazuh     0 May  7 12:39 active-responses.log
drwxr-x--- 3 wazuh wazuh  4096 May  7 12:41 alerts
drwxr-x--- 2 wazuh wazuh  4096 Mar 26 20:15 api
-rw-rw---- 1 wazuh wazuh 11846 May  7 13:20 api.log
drwxr-x--- 3 wazuh wazuh  4096 May  7 12:41 archives
drwxr-x--- 2 wazuh wazuh  4096 Mar 26 20:15 cluster
-rw-rw---- 1 wazuh wazuh     0 May  7 12:40 cluster.log
drwxr-x--- 3 wazuh wazuh  4096 May  7 12:41 firewall
-rw-r----- 1 wazuh wazuh     0 May  7 12:39 integrations.log
-rw-rw---- 1 root  wazuh 17453 May  7 13:08 ossec.log
drwxr-x--- 2 wazuh wazuh  4096 Mar 26 20:15 wazuh
================================================================================
```

/var/ossec/etc/

Contains configuration files for the Wazuh Manager and agents, including:

- ossec.conf: Main configuration file for Wazuh.
- internal_options.conf: Contains internal settings for Wazuh components.

```
tiago-paquete@Linux:~$ sudo ls -l /var/ossec/etc/
================================================================================
total 64
-rw-r----- 1 root wazuh     0 May  7 12:41 client.keys
drwxrwx--- 2 root wazuh  4096 May  7 12:39 decoders
-rw-r----- 1 root wazuh 14480 Mar 26 20:15 internal_options.conf
drwxrwx--- 3 root wazuh  4096 May  7 12:40 lists
-rw-r----- 1 root wazuh   320 Mar 26 20:15 local_internal_options.conf
-rw-r----- 1 root wazuh  2298 Mar 26 18:28 localtime
-rw-rw---- 1 root wazuh  9090 May  7 12:40 ossec.conf
drwxrwx--- 2 root wazuh  4096 May  7 12:39 rootcheck
drwxrwx--- 2 root wazuh  4096 May  7 12:39 rules
drwxrwx--- 3 root wazuh  4096 May  7 12:40 shared
-rw-r----- 1 root root   1164 May  7 12:39 sslmanager.cert
-rw-r----- 1 root root   1704 May  7 12:39 sslmanager.key
================================================================================
```

/var/ossec/active-response/bin

Stores scripts used for active responses to security events, such as blocking IP addresses or disabling user accounts.

```
tiago-paquete@Linux:~$ sudo ls -l /var/ossec/active-response/bin
================================================================================
total 284
-rwxr-x--- 1 root wazuh 21032 Mar 26 20:15 default-firewall-drop
-rwxr-x--- 1 root wazuh 17712 Mar 26 20:15 disable-account
-rwxr-x--- 1 root wazuh 21032 Mar 26 20:15 firewall-drop
-rwxr-x--- 1 root wazuh 18096 Mar 26 20:15 firewalld-drop
-rwxr-x--- 1 root wazuh 19336 Mar 26 20:15 host-deny
-rwxr-x--- 1 root wazuh 17280 Mar 26 20:15 ip-customblock
-rwxr-x--- 1 root wazuh 17872 Mar 26 20:15 ipfw
-rwxr-x--- 1 root wazuh 16528 Mar 26 20:15 kaspersky
-rwxr-x--- 1 root wazuh 14491 Mar 26 20:15 kaspersky.py
-rwxr-x--- 1 root wazuh 17624 Mar 26 20:15 npf
-rwxr-x--- 1 root wazuh 19344 Mar 26 20:15 pf
-rwxr-x--- 1 root wazuh 16288 Mar 26 20:15 restart-wazuh
-rwxr-x--- 1 root wazuh   695 Mar 26 20:15 restart.sh
-rwxr-x--- 1 root wazuh 17312 Mar 26 20:15 route-null
-rwxr-x--- 1 root wazuh 19288 Mar 26 20:15 wazuh-slack
================================================================================
```

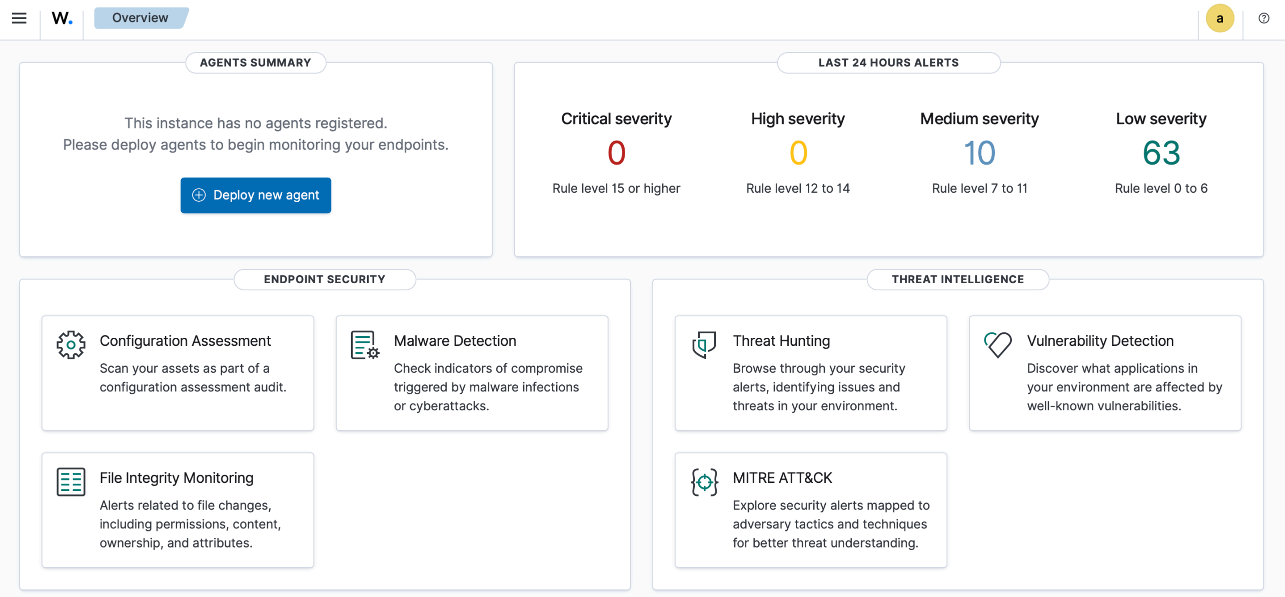
/var/ossec/ruleset/rules

Contains default rules used by Wazuh to analyze events and generate alerts. It's recommended to place custom rules in /var/ossec/etc/rules/ to avoid overwriting during updates.

```
tiago-paquete@Linux:~$ sudo ls -l /var/ossec/ruleset/rules
================================================================================
total 1920
-rw-r----- 1 root wazuh   1540 Mar 26 20:15 0010-rules_config.xml
-rw-r----- 1 root wazuh  20961 Mar 26 20:15 0015-ossec_rules.xml
..
-rw-r----- 1 root wazuh   1385 Mar 26 20:15 0997-maltiverse_rules.xml
-rw-r----- 1 root wazuh  21753 Mar 26 20:15 0998-aws-security-hub-rules.xml
================================================================================
```

Deploy new agent

Follow the steps:



AGENTS SUMMARY

This instance has no agents registered.
Please deploy agents to begin monitoring your endpoints.

⊕ Deploy new agent

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	10	63
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Check indicators of compromise triggered by malware infections or cyberattacks.

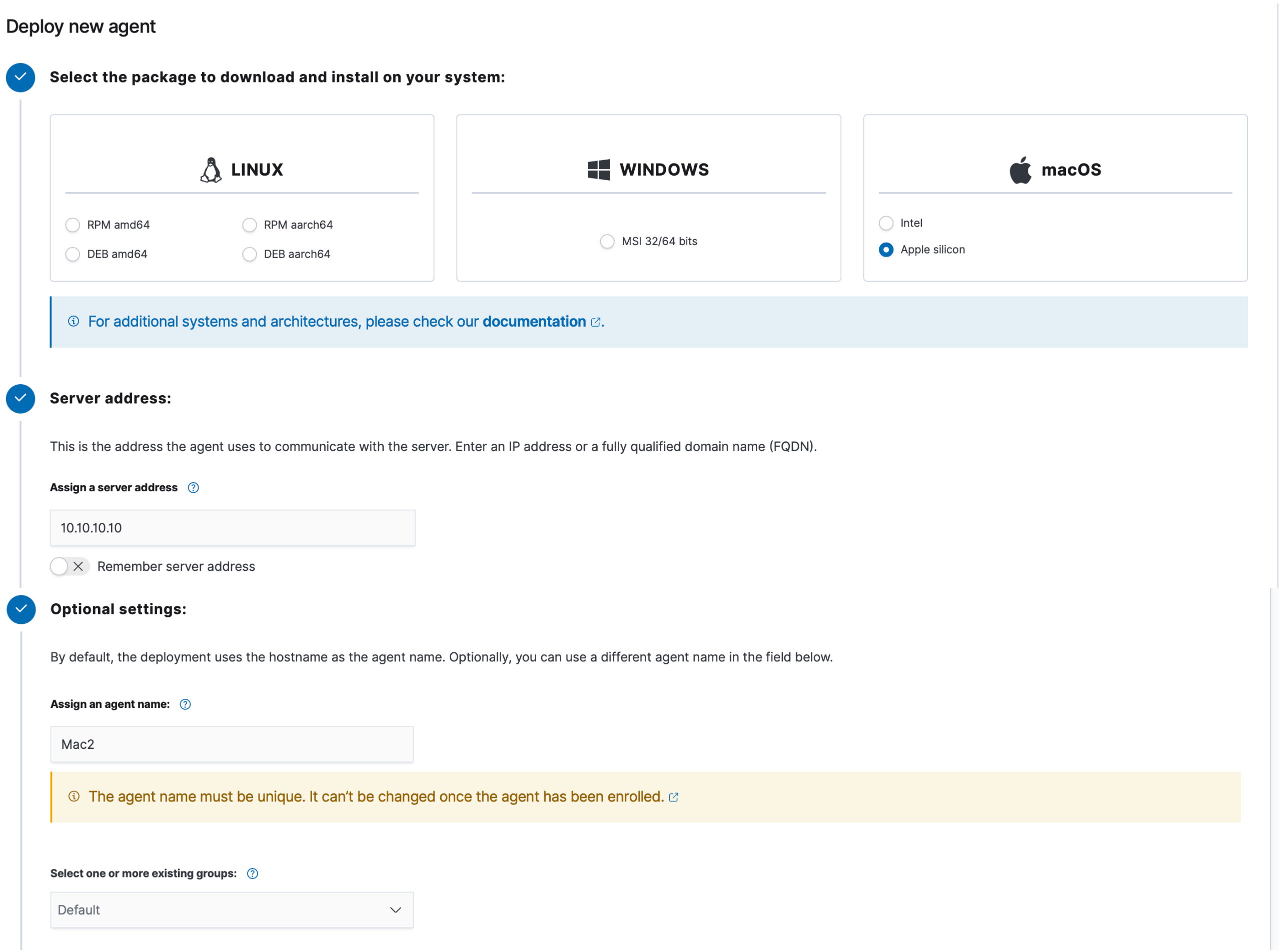
File Integrity Monitoring
Alerts related to file changes, including permissions, content, ownership, and attributes.

THREAT INTELLIGENCE

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK
Explore security alerts mapped to adversary tactics and techniques for better threat understanding.



Deploy new agent

✓ **Select the package to download and install on your system:**

LINUX
○ RPM amd64 ○ RPM aarch64
○ DEB amd64 ○ DEB aarch64

WINDOWS
○ MSI 32/64 bits

macOS
○ Intel
● Apple silicon

ⓘ For additional systems and architectures, please check our **documentation**.

✓ **Server address:**

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign a server address

10.10.10.10

Remember server address

✓ **Optional settings:**

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

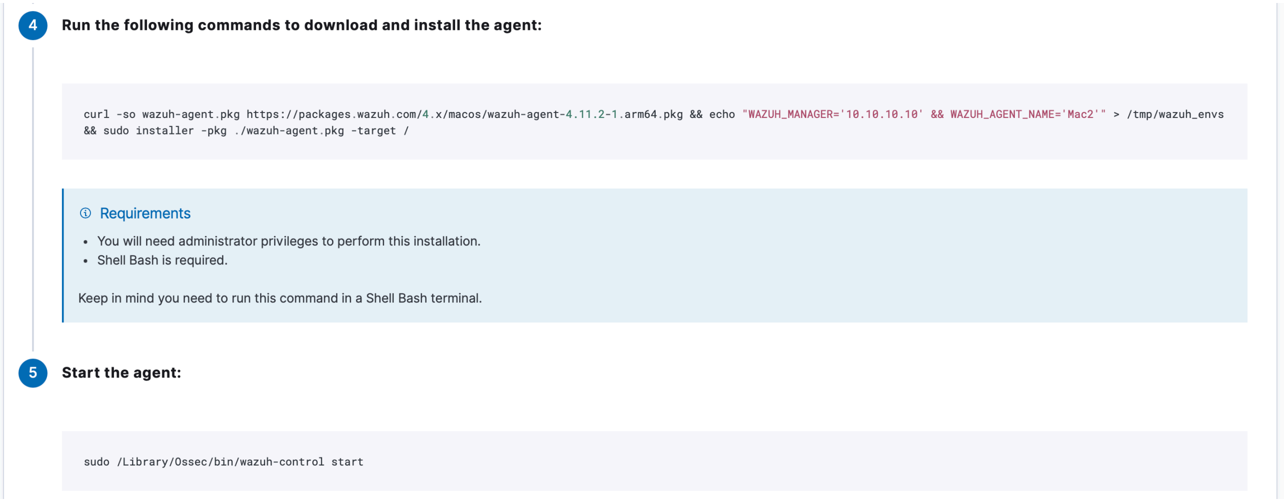
Assign an agent name:

Mac2

ⓘ The agent name must be unique. It can't be changed once the agent has been enrolled.

Select one or more existing groups:

Default



4 **Run the following commands to download and install the agent:**

```
curl -so wazuh-agent.pkg https://packages.wazuh.com/4.x/macos/wazuh-agent-4.11.2-1.arm64.pkg && echo "WAZUH_MANAGER='10.10.10.10' && WAZUH_AGENT_NAME='Mac2'" > /tmp/wazuh_envs
&& sudo installer -pkg ./wazuh-agent.pkg -target /
```

ⓘ Requirements

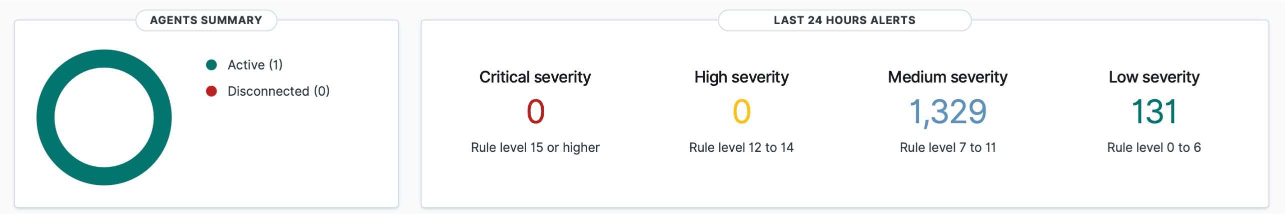
- You will need administrator privileges to perform this installation.
- Shell Bash is required.

Keep in mind you need to run this command in a Shell Bash terminal.

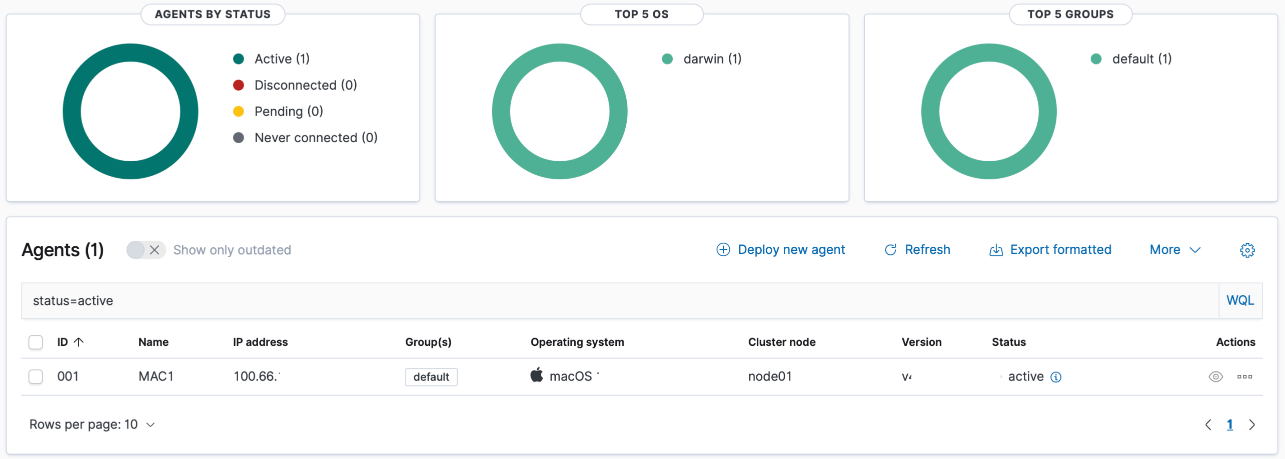
5 **Start the agent:**

```
sudo /Library/Ossec/bin/wazuh-control start
```

New agent



Critical severity	High severity	Medium severity	Low severity
0	0	1,329	131
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6



status=active

□	ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
□	001	MAC1	100.66.	default	macOS	node01	v	active ⓘ	