Wazuh Installation and Configuration Manual

Prepared By: Moeez Javed

Wazuh Installation and Configuration Manual

Introduction to Wazuh

Wazuh is a free, open-source security platform that unifies **Extended Detection and Response (XDR)** and **Security Information and Event Management (SIEM)** capabilities. It's designed to provide comprehensive protection for a wide range of IT environments, including on-premises infrastructure, cloud workloads, virtual machines, and containerized systems.

In essence, Wazuh acts as a central hub for security monitoring, threat detection, incident response, and compliance management across your entire digital landscape.

How Wazuh Works

Wazuh operates through a distributed and scalable architecture, primarily consisting of three core components and an agent:

> ***Wazuh Agent*:** This is a lightweight software program installed on the endpoints you want to monitor (laptops, desktops, servers, cloud instances, virtual machines, etc.). The agent's primary role is to:
>
> > **Collect data:** It gathers various types of security-related data, including system logs (operating system, application logs), file integrity data, vulnerability scan results, configuration assessment data, and system inventory data.
> >
> > **Detect local security issues:** It can detect malware, rootkits, and suspicious anomalies by scanning for hidden files, cloaked processes, unregistered network listeners, and inconsistencies in system call responses.
> >
> > **Execute active responses:** When instructed by the Wazuh server, it can perform automated countermeasures like blocking network connections, stopping processes, or deleting malicious files.

***Wazuh Server*:** This is the core component where the security analysis and correlation take place. The Wazuh server:

Receives and processes data: It collects data from thousands of Wazuh agents.

Analyzes data: It uses decoders to identify the type of information being processed (e.g., Windows events, SSH logs, web server logs) and extracts relevant data elements (e.g., source IP, event ID, username).

Applies rules: It then uses a robust rule engine to identify specific patterns in the decoded events that could indicate a security incident, triggering alerts.

Manages agents: It provides centralized configuration management, allowing you to remotely configure, upgrade, and monitor agents.

API: It exposes a RESTful API for external applications and users to interact with the Wazuh infrastructure, manage settings, and query data.

Clustering: Can be deployed as a cluster for high availability and load balancing to handle large-scale environments.

***Wazuh Indexer (based on OpenSearch/Elasticsearch)*:** This component is responsible for indexing and storing the alerts and security events generated by the Wazuh server. It provides a highly scalable, full-text search and analytics engine, enabling efficient storage and retrieval of vast amounts of security data.

***Wazuh Dashboard (based on OpenSearch Dashboards/Kibana)*:** This is the web-based user interface that provides a powerful visualization and analysis platform. Through the dashboard, security analysts can:

Visualize data: See real-time security events, trends, and alerts in intuitive dashboards.

Perform threat hunting: Query and analyze historical data to identify potential threats that may have bypassed initial controls.

Generate reports: Create reports for regulatory compliance (e.g., PCI DSS, GDPR, HIPAA, NIST 800-53), vulnerability assessments, file integrity monitoring, and more.

Manage Wazuh: Monitor the status of the Wazuh environment and agents.

Data Flow Summary: Wazuh agents collect security data from endpoints and securely forward it to the Wazuh server. The server analyzes this data, applies rules, and generates alerts. These alerts are then sent to the Wazuh indexer for storage and can be visualized and analyzed through the Wazuh dashboard. Wazuh can also monitor agent-less devices (like firewalls or routers) by receiving data via syslog or through API integrations.

Importance of Wazuh in Cybersecurity

Wazuh plays a crucial role in modern cybersecurity for several reasons:

Comprehensive Threat Detection and Response: By combining SIEM (for log aggregation and analysis) and XDR (for endpoint visibility and response), Wazuh offers a holistic view of your security posture. It can detect a wide range of threats, including:

Intrusion Detection: Identifying suspicious activities, malware, and rootkits.

Malware Detection: Non-signature-based detection of anomalies, hidden files, processes, and network listeners.

Vulnerability Detection: Scanning for known software vulnerabilities by correlating inventory data with CVE databases.

File Integrity Monitoring (FIM): Tracking changes to critical system files and directories to detect unauthorized modifications.

Configuration Assessment: Ensuring systems comply with security policies and hardening guides, detecting misconfigurations.

Real-time Monitoring and Alerting: It provides instant notifications for potential security incidents, allowing security teams to respond quickly and minimize the impact of threats.

Centralized Visibility: It aggregates data from diverse sources (endpoints, cloud, containers, network devices) into a single platform, offering a unified view of your IT environment's security. This is especially vital in today's hybrid and distributed infrastructures.

Incident Response Automation: Wazuh's "Active Response" module can automatically take countermeasures when threats are detected, such as blocking IP addresses or isolating infected systems. This speeds up incident response and reduces manual effort.

Regulatory Compliance: It helps organizations meet various compliance standards (like PCI DSS, HIPAA, GDPR, NIST 800-53) by providing necessary security controls, logging, reporting, and auditing capabilities.

Cost-Effectiveness and Open Source: Being open source, Wazuh is free to download and deploy for on-premise environments, offering a cost-effective solution for organizations of all sizes, from small businesses to large enterprises. Its open-source nature also ensures transparency, flexibility, and a large community for support and continuous improvement.

Improved IT Hygiene: By providing capabilities like system inventory, security configuration assessment, and vulnerability management, Wazuh helps organizations maintain good IT hygiene, proactively identify weaknesses, and strengthen their overall security posture.

Importance of Wazuh in Cybersecurity

Threat Detection: *Detects malware, anomalies, intrusions*

File Integrity Monitoring (FIM): *Tracks changes in critical files*

Vulnerability Detection: *Matches software versions with CVE database*

Compliance: *PCI DSS, HIPAA, GDPR, NIST 800-53*

Automation: *Active Response module blocks or isolates threats*

Cost-Effective: *Open-source with a strong community*

Downloading Wazuh

Step 1: Download Wazuh Installation Script and Configuration File

curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh
curl -sO https://packages.wazuh.com/4.12/config.yml

```
┌──(kali㉿kali)-[~]
└─$ curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh
curl -sO https://packages.wazuh.com/4.12/config.yml
```

Step 2: Generate Configuration Files

bash wazuh-install.sh --generate-config-files

```
┌──(root㉿kali)-[/home/kali]
└─# bash wazuh-install.sh --generate-config-files

24/07/2025 07:35:46 INFO: Starting Wazuh installation assistant. Wazuh version: 4.12.0
24/07/2025 07:35:46 INFO: Verbose logging redirected to /var/log/wazuh-install.log
24/07/2025 07:35:46 INFO: The recommended systems are: Red Hat Enterprise Linux 7, 8, 9; CentOS 7, 8; Amazon Linux 2; Ubuntu 16.04, 18.04, 20.04, 22.04.
24/07/2025 07:35:46 WARNING: The current system does not match with the list of recommended systems. The installation may not work properly.
24/07/2025 07:36:37 INFO: Verifying that your system meets the recommended minimum hardware requirements.
24/07/2025 07:36:37 INFO: ––– Configuration files –––
24/07/2025 07:36:37 INFO: Generating configuration files.
24/07/2025 07:36:38 INFO: Generating the root certificate.
24/07/2025 07:36:38 INFO: Generating Admin certificates.
24/07/2025 07:36:38 INFO: Generating Wazuh indexer certificates.
24/07/2025 07:36:38 ERROR: Invalid IP or DNS <indexer-node-ip>
```

Step 3: Run Installation Using Configuration File

sudo ./wazuh-install.sh --config-file config.yml

```
┌──(root㉿kali)-[/home/kali]
└─# sudo ./wazuh-install.sh --config-file config.yml

24/07/2025 07:42:45 INFO: Starting Wazuh installation assistant. Wazuh version: 4.12.0
24/07/2025 07:42:45 INFO: Verbose logging redirected to /var/log/wazuh-install.log
24/07/2025 07:42:45 INFO: The recommended systems are: Red Hat Enterprise Linux 7, 8, 9; CentOS 7, 8; Amazon Linux 2; Ubuntu 16.04, 18.04, 20.04, 22.04.
24/07/2025 07:42:45 WARNING: The current system does not match with the list of recommended systems. The installation may not work properly.
24/07/2025 07:42:51 ERROR: At least one of these arguments is necessary -a|──all-in-one, -g|──generate-config-files, -wi|──wazuh-indexer, -wd|──wazuh-dashboard, -s|──
start-cluster, -ws|──wazuh-server, -u|──uninstall, -dw|──download-wazuh.
```

Step 4: Run with Auto-Approve Option

sudo ./wazuh-install.sh -a --config-file config.yml

```
┌──(root㉿kali)-[/home/kali]
└─# sudo ./wazuh-install.sh -a --config-file config.yml

24/07/2025 07:44:18 INFO: Starting Wazuh installation assistant. Wazuh version: 4.12.0
24/07/2025 07:44:18 INFO: Verbose logging redirected to /var/log/wazuh-install.log
24/07/2025 07:44:18 INFO: The recommended systems are: Red Hat Enterprise Linux 7, 8, 9; CentOS 7, 8; Amazon Linux 2; Ubuntu 16.04, 18.04, 20.04, 22.04.
24/07/2025 07:44:18 WARNING: The current system does not match with the list of recommended systems. The installation may not work properly.
24/07/2025 07:44:25 INFO: Verifying that your system meets the recommended minimum hardware requirements.
24/07/2025 07:44:25 INFO: Wazuh web interface port will be 443.
24/07/2025 07:44:32 INFO: ─── Dependencies ───
24/07/2025 07:44:32 INFO: Installing apt-transport-https.
24/07/2025 07:44:57 INFO: Installing debhelper.
24/07/2025 07:45:23 INFO: Installing software-properties-common.
24/07/2025 07:45:49 INFO: Wazuh repository added.
24/07/2025 07:45:49 INFO: ─── Configuration files ───
24/07/2025 07:45:49 INFO: Generating configuration files.
24/07/2025 07:45:51 INFO: Generating the root certificate.
24/07/2025 07:45:51 INFO: Generating Admin certificates.
24/07/2025 07:45:51 INFO: Generating Wazuh indexer certificates.
24/07/2025 07:45:51 INFO: Generating Filebeat certificates.
24/07/2025 07:45:51 INFO: Generating Wazuh dashboard certificates.
24/07/2025 07:45:53 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
24/07/2025 07:45:53 INFO: ─── Wazuh indexer ───
24/07/2025 07:45:53 INFO: Starting Wazuh indexer installation.
24/07/2025 07:54:54 INFO: Wazuh indexer installation finished.
24/07/2025 07:54:55 INFO: Wazuh indexer post-install configuration finished.
24/07/2025 07:54:55 INFO: Starting service wazuh-indexer.
24/07/2025 07:55:29 INFO: wazuh-indexer service started.
24/07/2025 07:55:29 INFO: Initializing Wazuh indexer cluster security settings.
24/07/2025 07:55:39 INFO: Wazuh indexer cluster security configuration initialized.
24/07/2025 07:55:39 INFO: Wazuh indexer cluster initialized.
24/07/2025 07:55:39 INFO: ─── Wazuh server ───
24/07/2025 07:55:39 INFO: Starting the Wazuh manager installation.
24/07/2025 08:01:26 INFO: Wazuh manager installation finished.
```

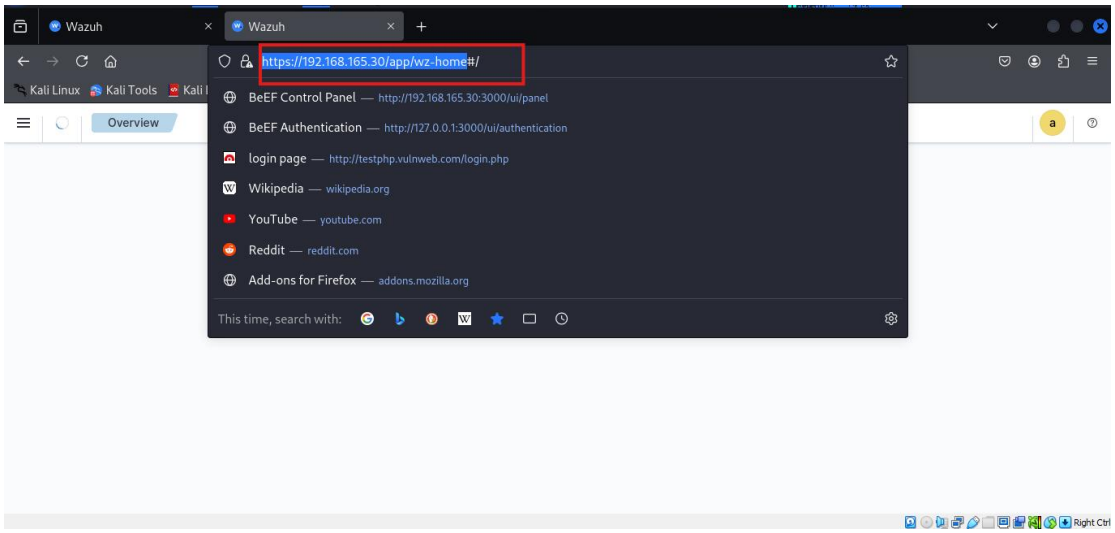
Step 5: Wazuh Dashboard Credentials

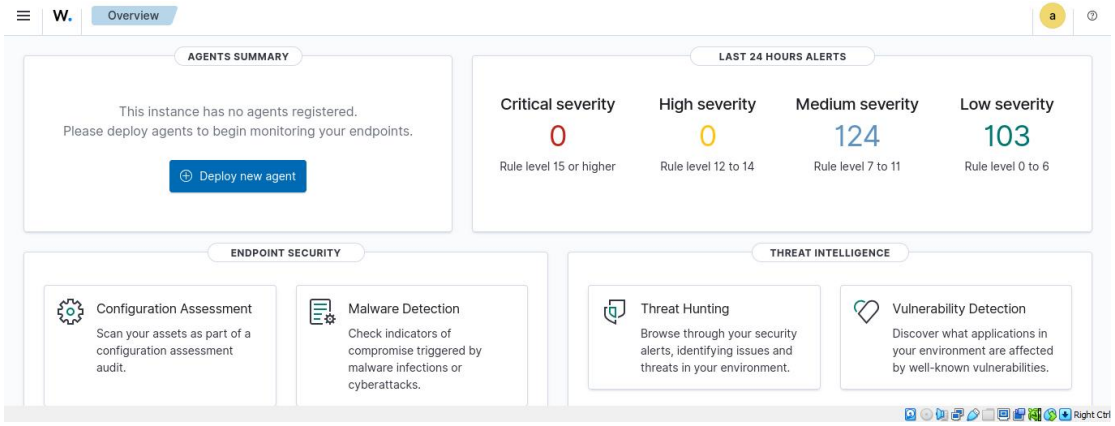
User: admin
Password: CpbPNUk6r4ZRyM.SXv1?nw9hywkaU+SV

```
24/07/2025 07:54:55 INFO: Starting service wazuh-indexer.
24/07/2025 07:55:29 INFO: wazuh-indexer service started.
24/07/2025 07:55:29 INFO: Initializing Wazuh indexer cluster security settings.
24/07/2025 07:55:39 INFO: Wazuh indexer cluster security configuration initialized.
24/07/2025 07:55:39 INFO: Wazuh indexer cluster initialized.
24/07/2025 07:55:39 INFO: ─── Wazuh server ───
24/07/2025 07:55:39 INFO: Starting the Wazuh manager installation.
24/07/2025 08:01:26 INFO: Wazuh manager installation finished.
24/07/2025 08:01:27 INFO: Wazuh manager vulnerability detection configuration finished.
24/07/2025 08:01:27 INFO: Starting service wazuh-manager.
24/07/2025 08:01:47 INFO: wazuh-manager service started.
24/07/2025 08:01:47 INFO: Starting Filebeat installation.
24/07/2025 08:02:12 INFO: Filebeat installation finished.
24/07/2025 08:02:27 INFO: Filebeat post-install configuration finished.
24/07/2025 08:02:27 INFO: Starting service filebeat.
24/07/2025 08:02:30 INFO: filebeat service started.
24/07/2025 08:02:30 INFO: ─── Wazuh dashboard ───
24/07/2025 08:02:30 INFO: Starting Wazuh dashboard installation.
24/07/2025 08:08:19 INFO: Wazuh dashboard installation finished.
24/07/2025 08:08:19 INFO: Wazuh dashboard post-install configuration finished.
24/07/2025 08:08:19 INFO: Starting service wazuh-dashboard.
24/07/2025 08:08:19 INFO: wazuh-dashboard service started.
24/07/2025 08:08:22 INFO: Updating the internal users.
24/07/2025 08:08:33 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/internalusers-backup folder.
24/07/2025 08:09:06 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and password.
24/07/2025 08:10:00 INFO: Initializing Wazuh dashboard web application.
24/07/2025 08:10:00 INFO: Wazuh dashboard web application not yet initialized. Waiting ...
24/07/2025 08:10:17 INFO: Wazuh dashboard web application not yet initialized. Waiting ...
24/07/2025 08:10:32 INFO: Wazuh dashboard web application initialized.
24/07/2025 08:10:32 INFO: ─── Summary ───
24/07/2025 08:10:32 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: CpbPNUk6r4ZRyM.SXv1?nw9hywkaU+SV
24/07/2025 08:10:32 INFO: Installation finished.
```

Step 6: Access the Wazuh Dashboard

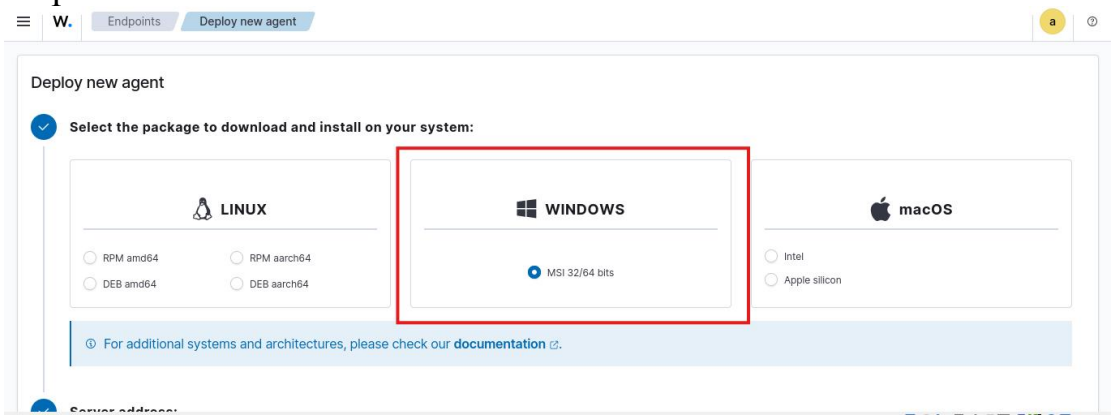
https://192.168.165.30/app/wz-home



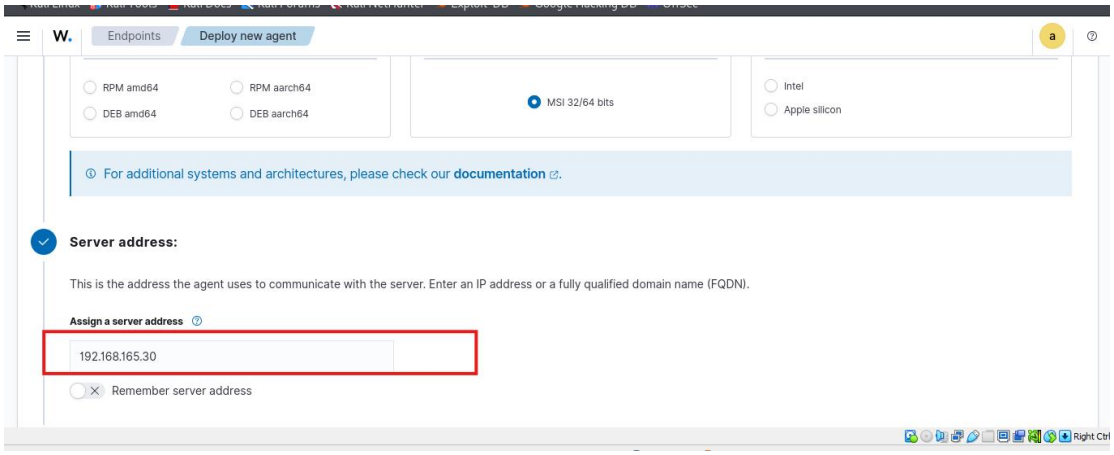


Windows Agent Installation

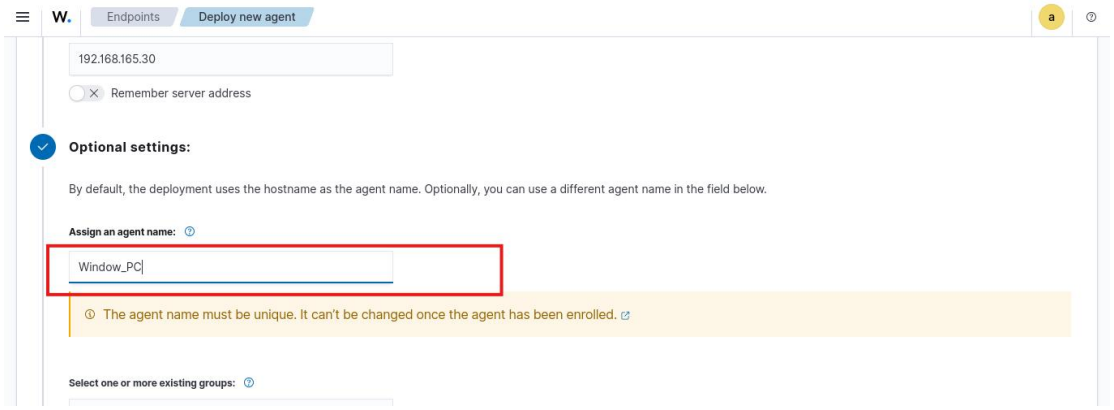
Step 1:



Step 2:



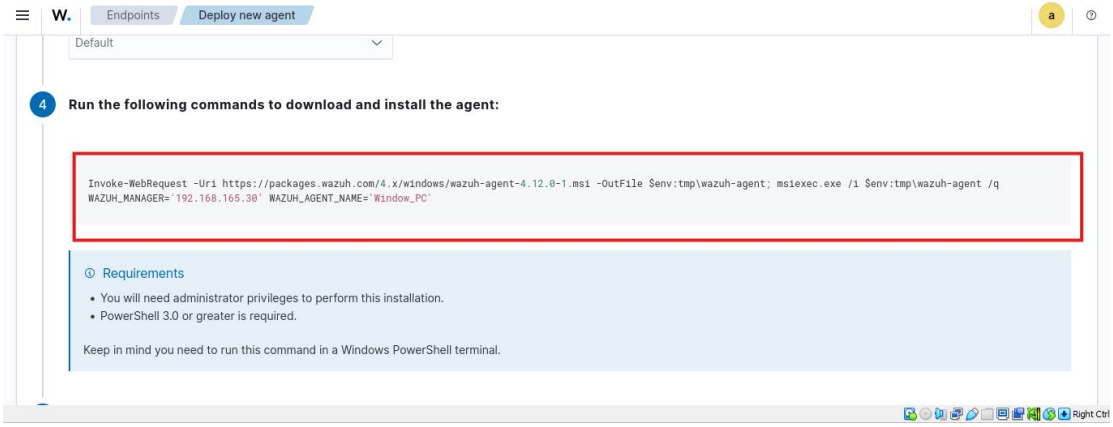
Step 3:



Step 4:

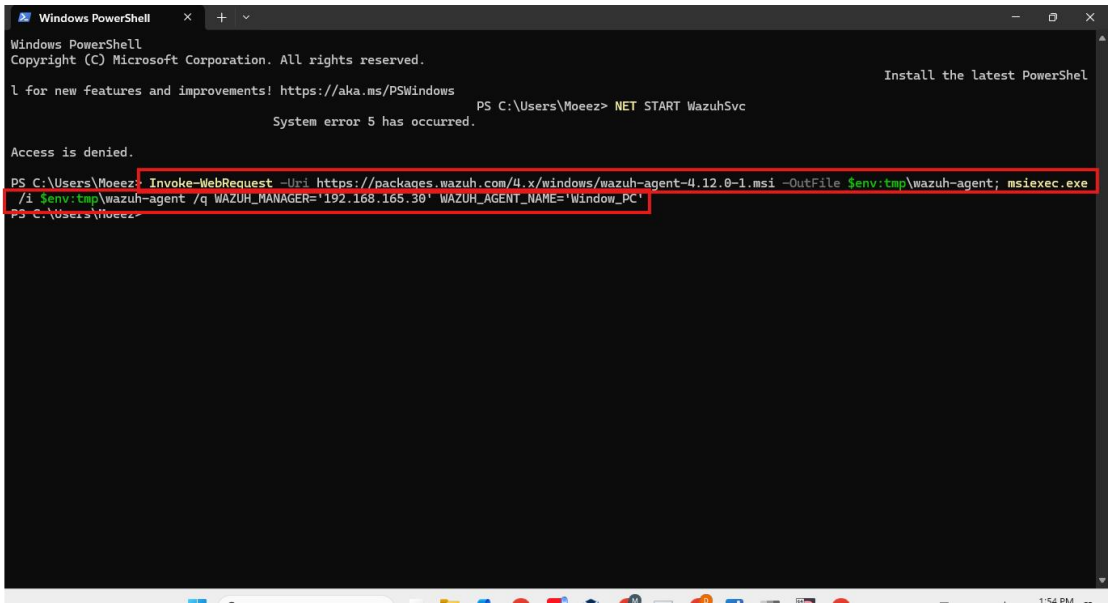
Copy this commend and run on window host

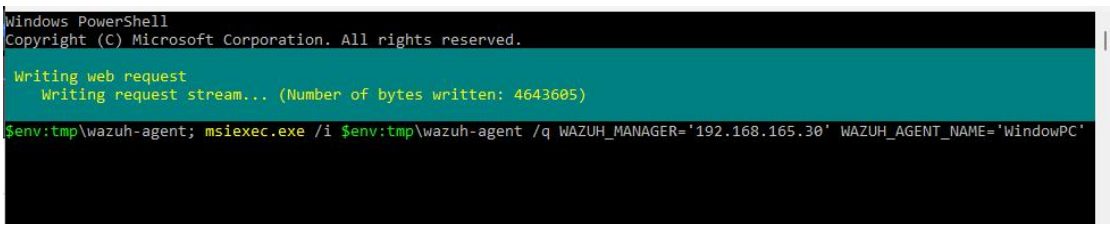
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.12.0-1.msi -OutFile $env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.165.30' WAZUH_AGENT_NAME='Window_PC'



Windows Agent Installation

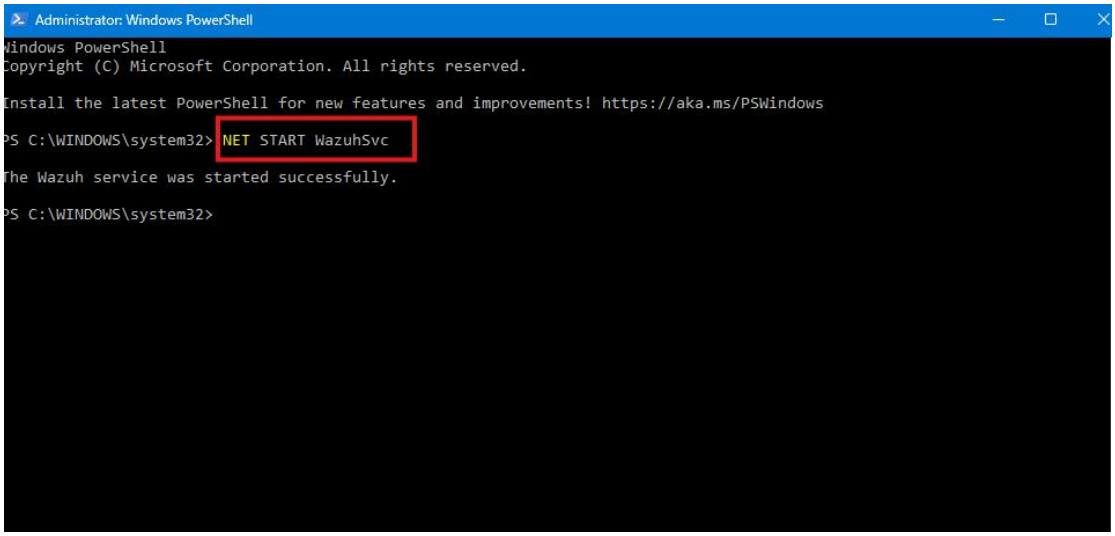
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.12.0-1.msi -OutFile $env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.165.30' WAZUH_AGENT_NAME='Window_PC'





Start the Wazuh Agent Service

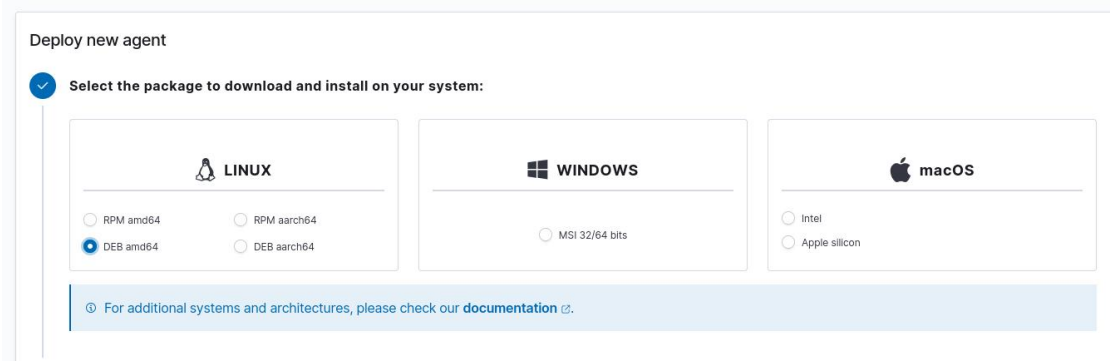
NET START WazuhSvc



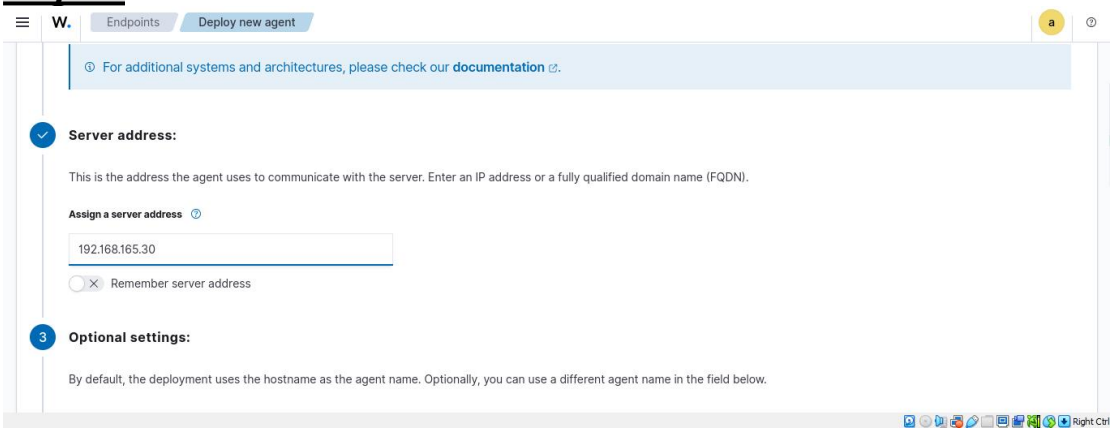
Ubuntu Agent Installation

*wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.12.0-1_amd64.deb && *
sudo WAZUH_MANAGER='192.168.165.30' WAZUH_AGENT_NAME='Ubuntu' dpkg -i ./wazuh-agent_4.12.0-1_amd64.deb

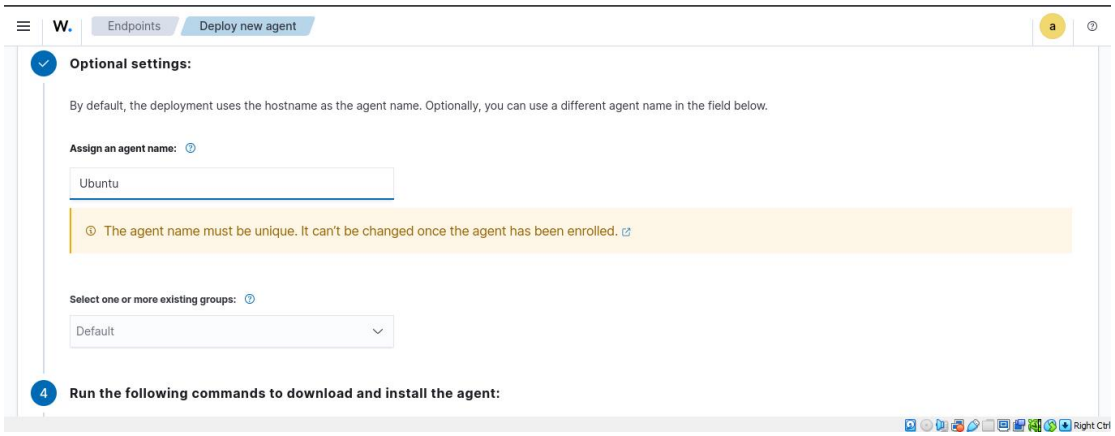
Step 1:



Step 2:

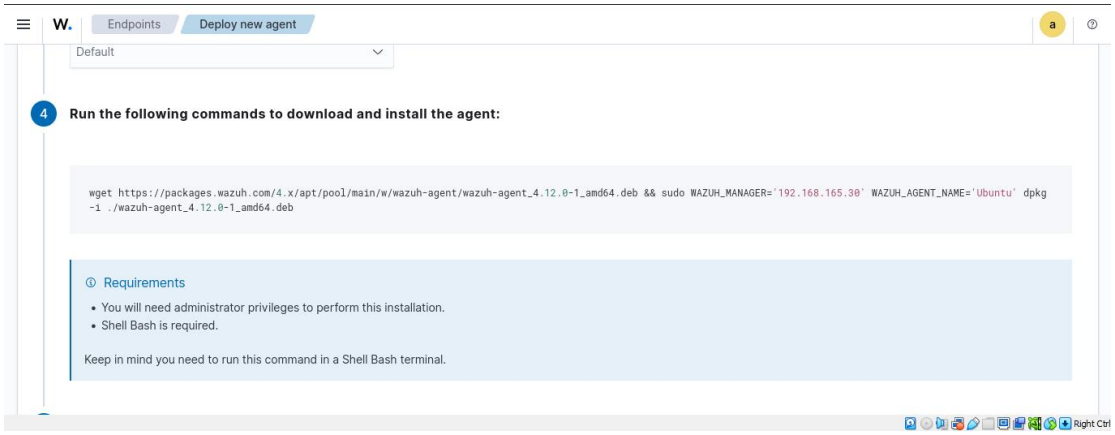


Step 3:



Step 4:

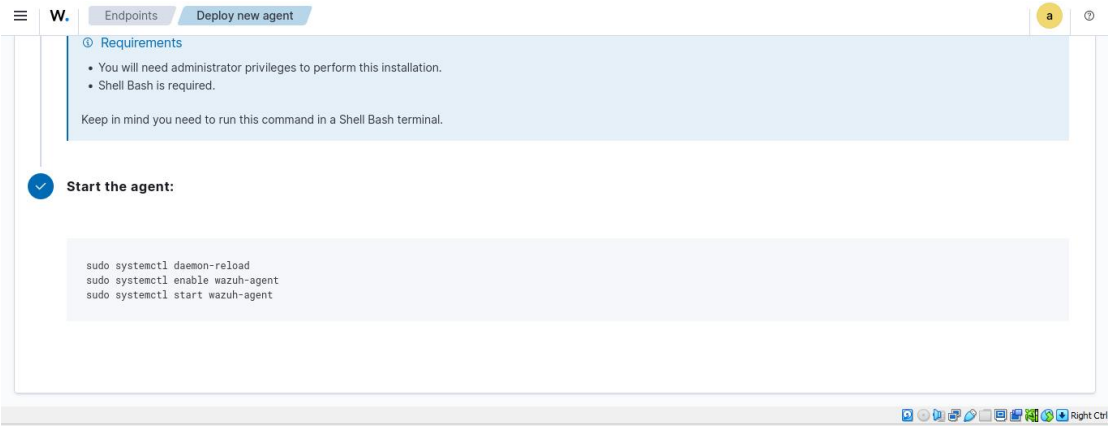
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.12.0-1_amd64.deb && sudo WAZUH_MANAGER='192.168.165.30' WAZUH_AGENT_NAME='Ubuntu' dpkg -i ./wazuh-agent_4.12.0-1_amd64.deb



```
ubuntu@ubuntu-VirtualBox:~$ wget https://packages.wazuh.com/4.x/apt/pool/main/w
/wazuh-agent/wazuh-agent_4.12.0-1_amd64.deb && sudo WAZUH_MANAGER='192.168.165.
30' WAZUH_AGENT_NAME='ubuntu' dpkg -i ./wazuh-agent_4.12.0-1_amd64.deb
--2025-07-25 09:35:57--  https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-a
gent/wazuh-agent_4.12.0-1_amd64.deb
Resolving packages.wazuh.com (packages.wazuh.com)... 3.161.104.23, 3.161.104.53
, 3.161.104.110, ...
Connecting to packages.wazuh.com (packages.wazuh.com)|3.161.104.23|:443... conn
ected.
HTTP request sent, awaiting response... 200 OK
Length: 11963008 (11M) [application/vnd.debian.binary-package]
Saving to: ‘wazuh-agent_4.12.0-1_amd64.deb.1’

wazuh-agent_4.12.0- 100%[===================>]  11.41M  4.33MB/s    in 2.6s

2025-07-25 09:36:00 (4.33 MB/s) - ‘wazuh-agent_4.12.0-1_amd64.deb.1’ saved [119
63008/11963008]

Selecting previously unselected package wazuh-agent.
(Reading database ... 191909 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.12.0-1_amd64.deb ...
Unpacking wazuh-agent (4.12.0-1) ...
Setting up wazuh-agent (4.12.0-1) ...
Processing triggers for systemd (245.4-4ubuntu3.20) ...
```

Enable and Start Agent

sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent



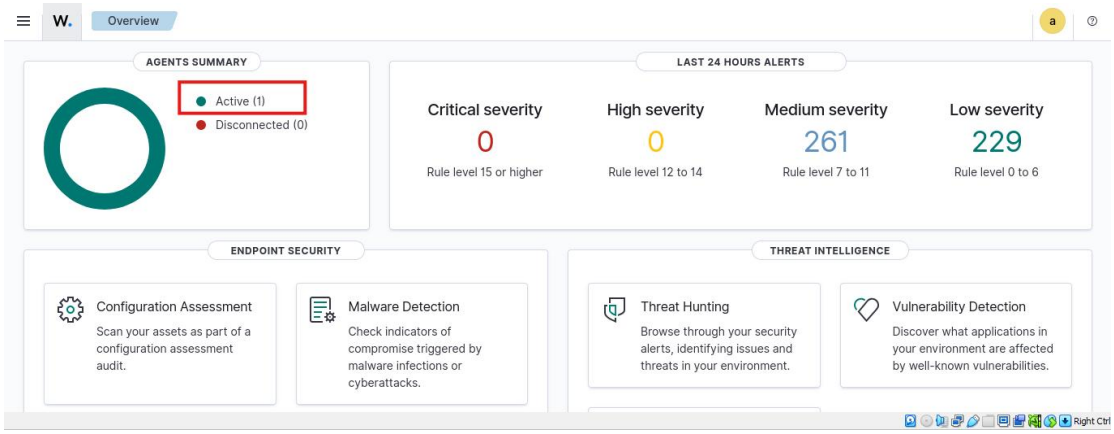

```
ubuntu@ubuntu-VirtualBox:~$ sudo systemctl daemon-reload
ubuntu@ubuntu-VirtualBox:~$ sudo systemctl enable wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service
 → /lib/systemd/system/wazuh-agent.service.
ubuntu@ubuntu-VirtualBox:~$ sudo systemctl start wazuh-agent
```

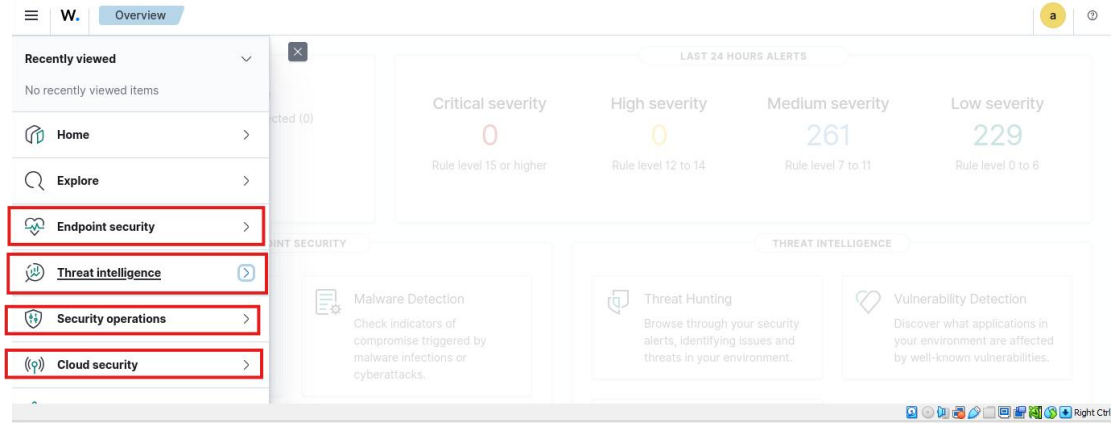
Start Wazuh Server (if needed)

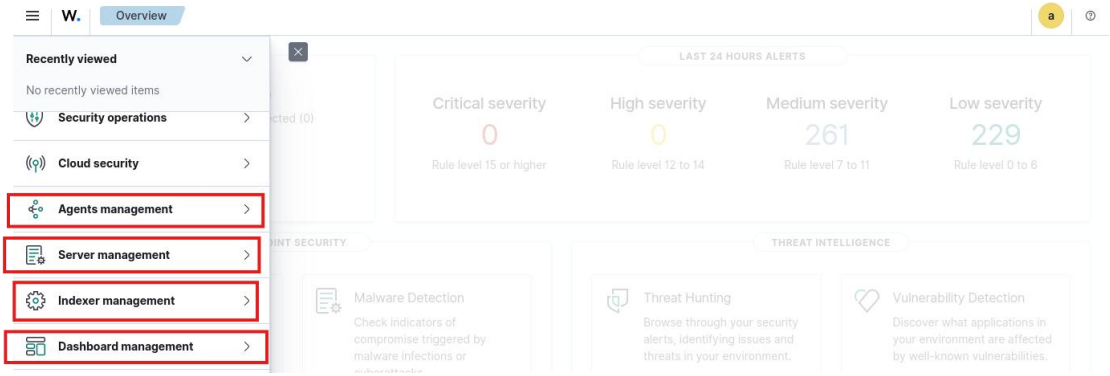
sudo systemctl enable wazuh-manager
sudo systemctl start wazuh-manager

```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start wazuh-manager
[sudo] password for kali:
┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable wazuh-manager

┌──(kali㉿kali)-[~]
└─$
```

Key Features (Explained)

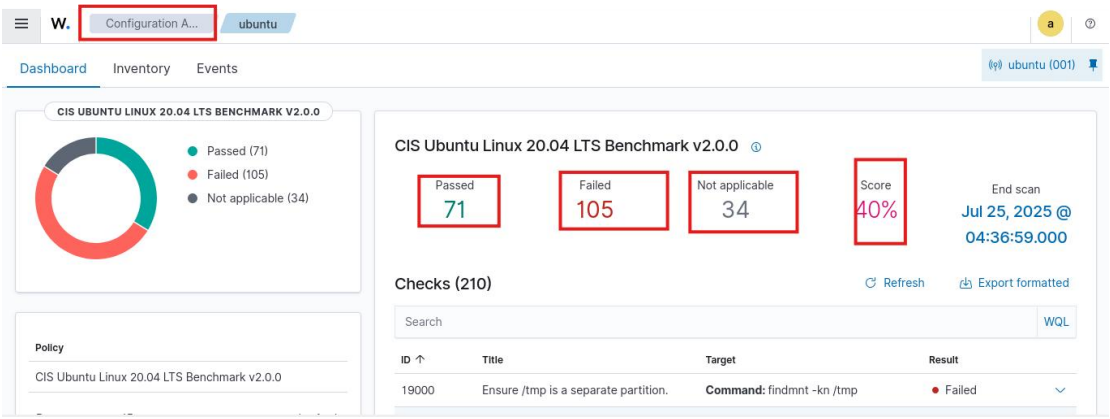






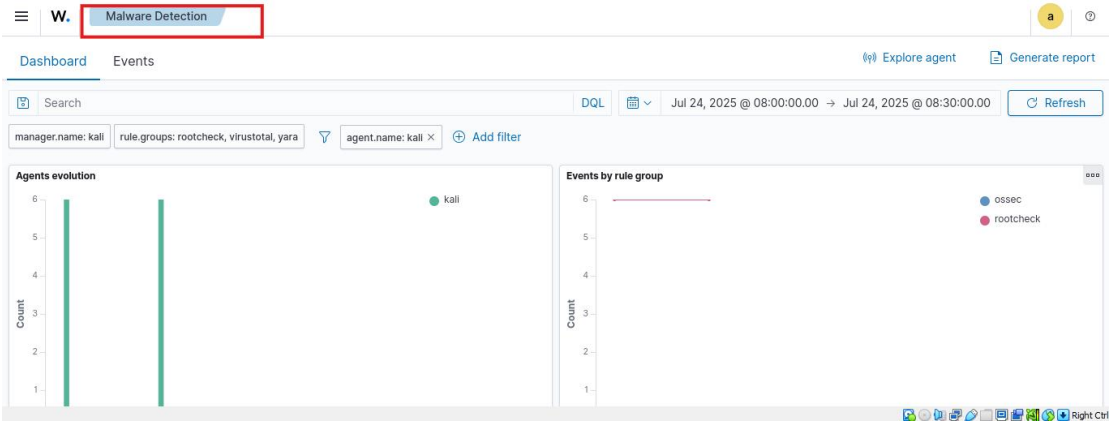
Configuration Assessment

Checks system configurations for compliance and security best practices.



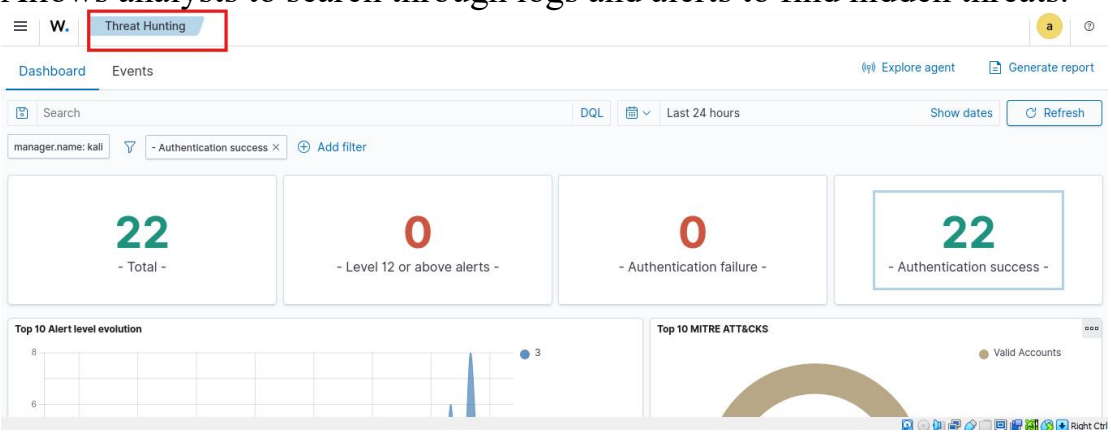
Malware Detection

Detects malware using anomaly detection, rootkit scanning, and file analysis



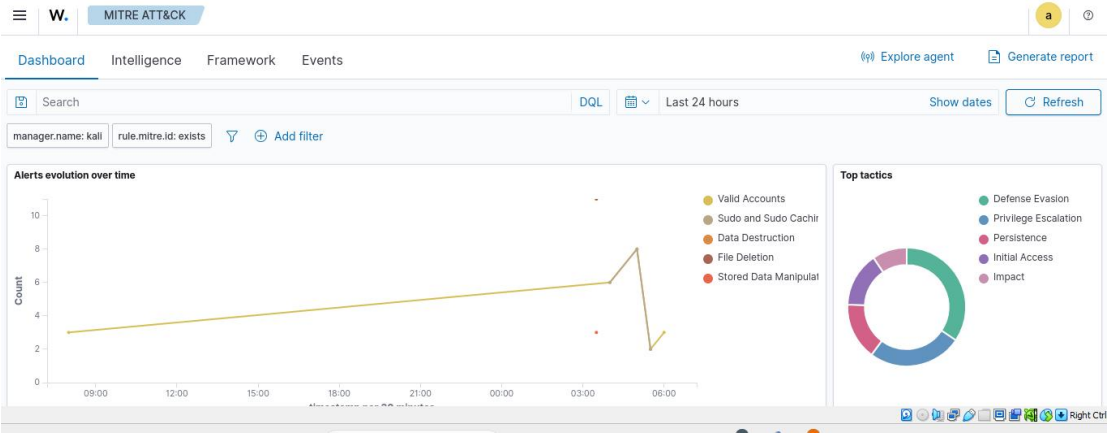
Threat Hunting

Allows analysts to search through logs and alerts to find hidden threats.



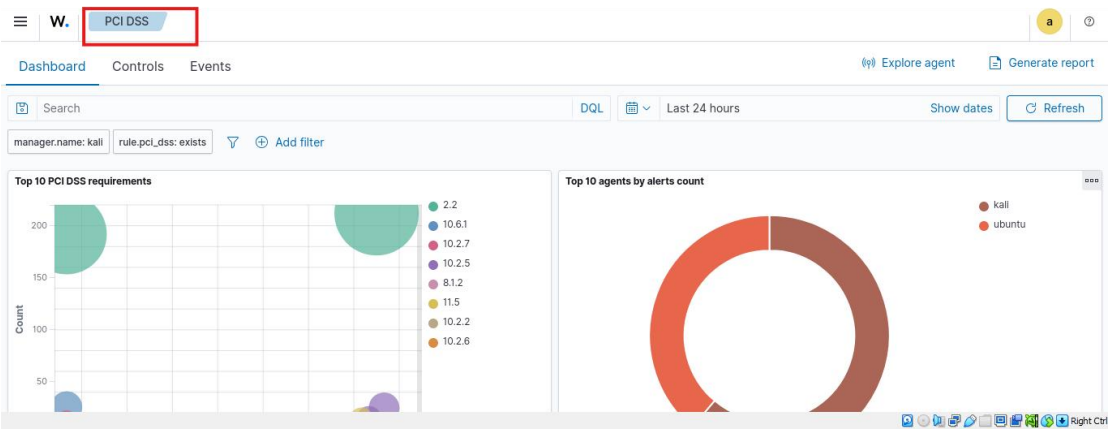
MITM Attack Detection

Detects man-in-the-middle attacks by monitoring traffic and system behavior.



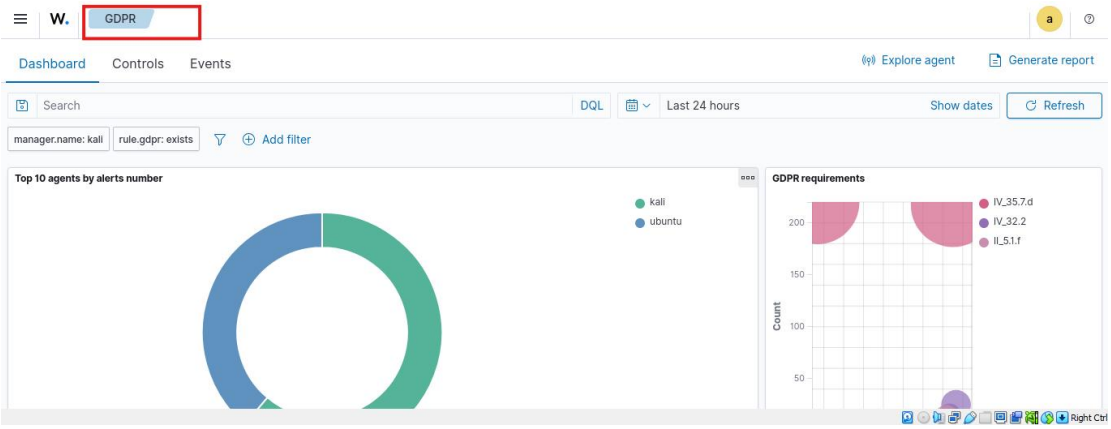
PCI DSS

Helps meet Payment Card Industry compliance by monitoring and reporting required controls.



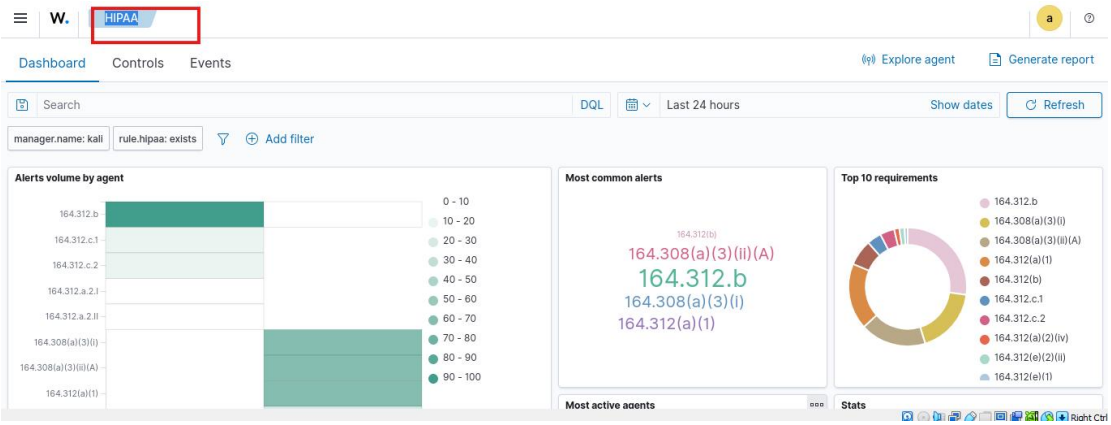
GDPR

Ensures data handling practices comply with the General Data Protection Regulation



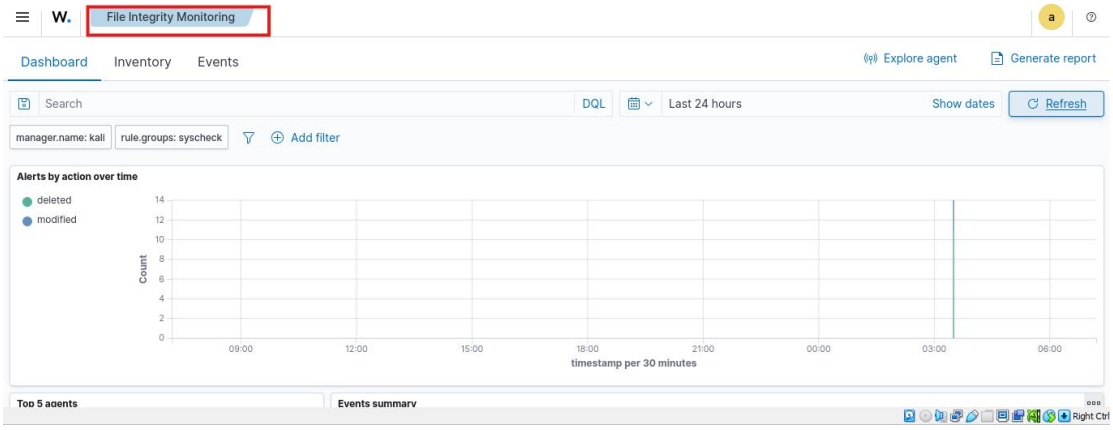
HIPAA

Supports healthcare compliance by securing Protected Health Information (PHI).



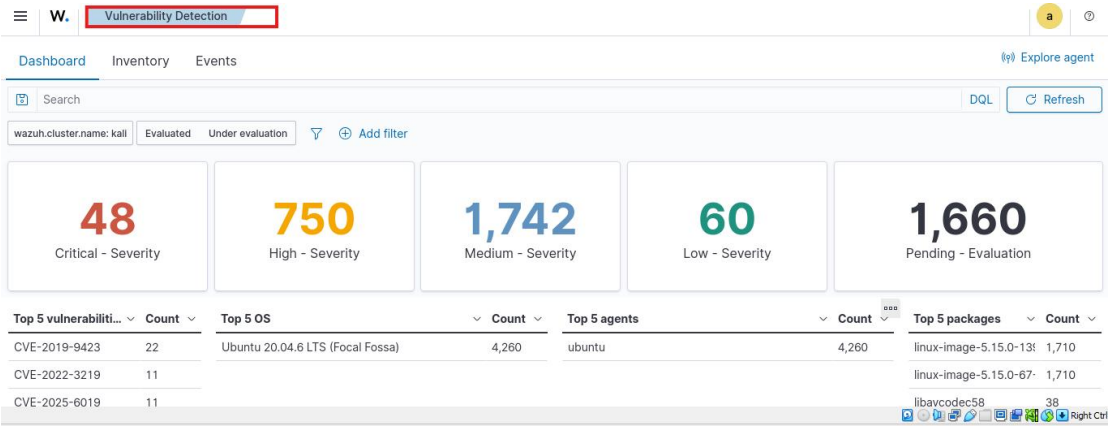
File Integrity Monitoring

Monitors changes in critical files to detect tampering or unauthorized access.



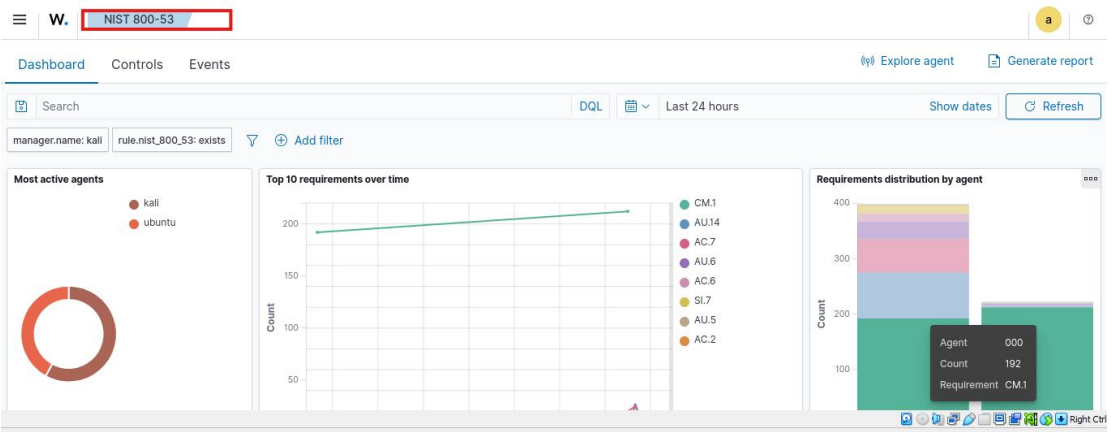
Vulnerability Detection

Identifies known software vulnerabilities using inventory data and CVE matching.



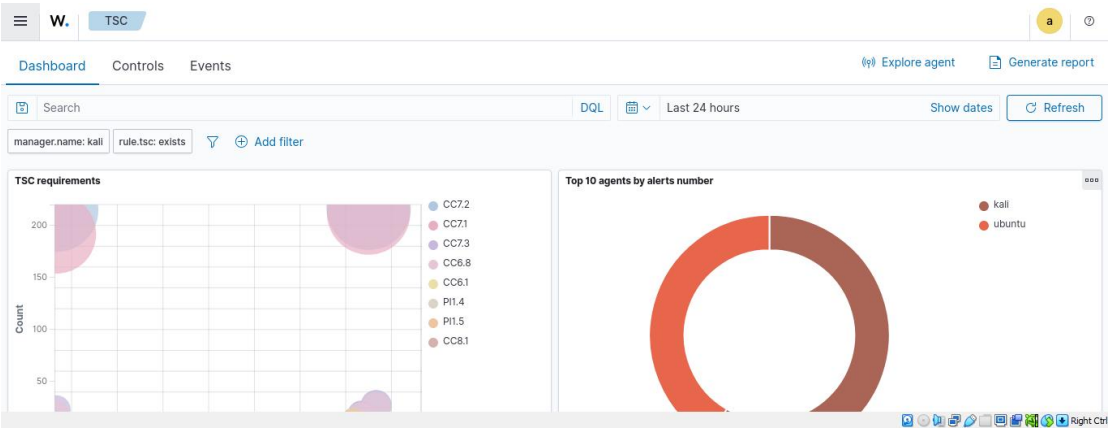
NIST 800-53

Supports NIST guidelines by providing auditing, access control, and incident response.



TCS (Total Cyber Security)

Covers comprehensive cybersecurity objectives including detection, response, compliance, and visibility.



Final Notes

Wazuh provides a scalable, open-source, and highly capable cybersecurity monitoring and management system. Proper installation and configuration of agents and the server ensure full visibility and strong security posture for any environment.