
alliance libre
pôle d'expertise logiciels libres

# Présentation Wazuh

Alexis Leduc
*Chef de Projet*
Alexis.leduc@pci-conseil.net
**07 68 00 22 43**

Performance Conseil Informatique

# Sommaire

- Contexte
- Vue macro
- Vue détaillée
- Travaux Pratique/Démo

# Un peu d’histoire

2005 – Création de OSSEC par Daniel Cid

2013 – Santiago Basset rejoint le projet OSSEC

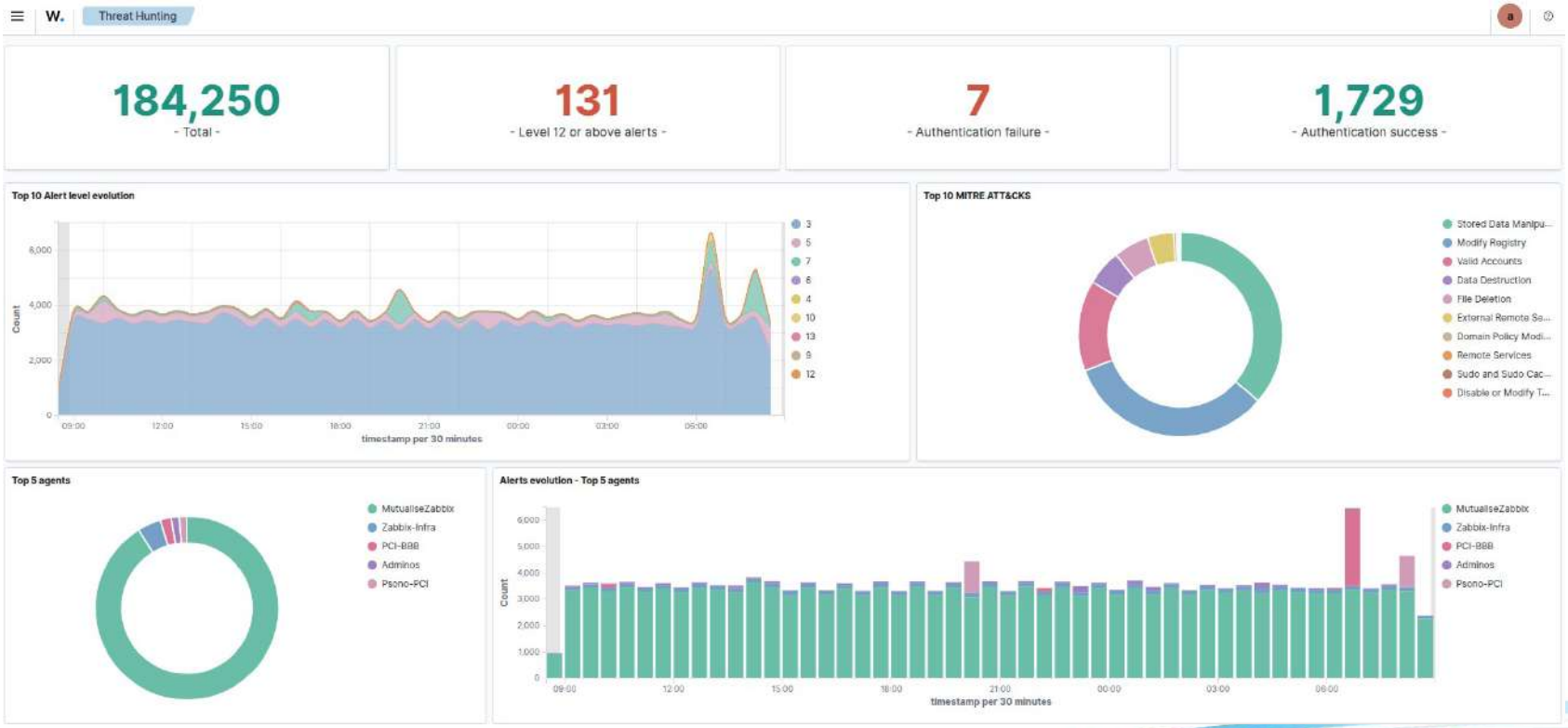
2015 – Création de Wazuh par Santiago Basset

2022 – PCI commence à utiliser Wazuh

# Un peu d’histoire


Performance Conseil Informatique

# Un peu d’histoire

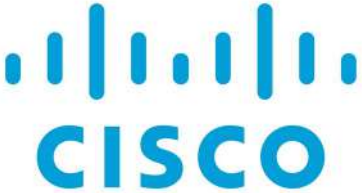


# Un peu de chiffre

15 millions d’appareils supervisés

100 000 Utilisateurs en entrepris







# Wazuh observe et agit

**SIEM (Security Information and Event Management)**

Gestion centralisée des logs et événements de sécurité. Permet de détecter de potentielles failles/attaques en temps réels

**EDR (Endpoint Detection en Response)**

Permet, lors de la détection d'événements anormaux, une réponse à l'anomalie par le Endpoint

**XDR (Extended Detection Response)**

En plus d'une réponse par le Endpoint, cette réponse va être communiquée à  tout le réseau et bloquer de manière générale

# Wazuh

## HIDS

Host-Based Intrusion Detection System. Identifie directement sur le client les activités suspecte, via un agent.

## Agentless

Permet une analyse sur des systèmes ne permettant pas l'installation d'un agent (Pare-feu, switch ..) via SSH ou Syslog notamment.

# Wazuh à vos services

**Wazuh-Agent**

Agent multiplateforme (Windows, Linux, MAC, Solaris, AIX, HP-UX) qui se déploie sur le client, de manière simple. C'est cet agent qui opère sur la partie client.

**Wazuh-Manager**

Elément central de l'ecosystème Wazuh. S'occupe de l'analyse des données, déclenchement des alertes, gestion des agents.

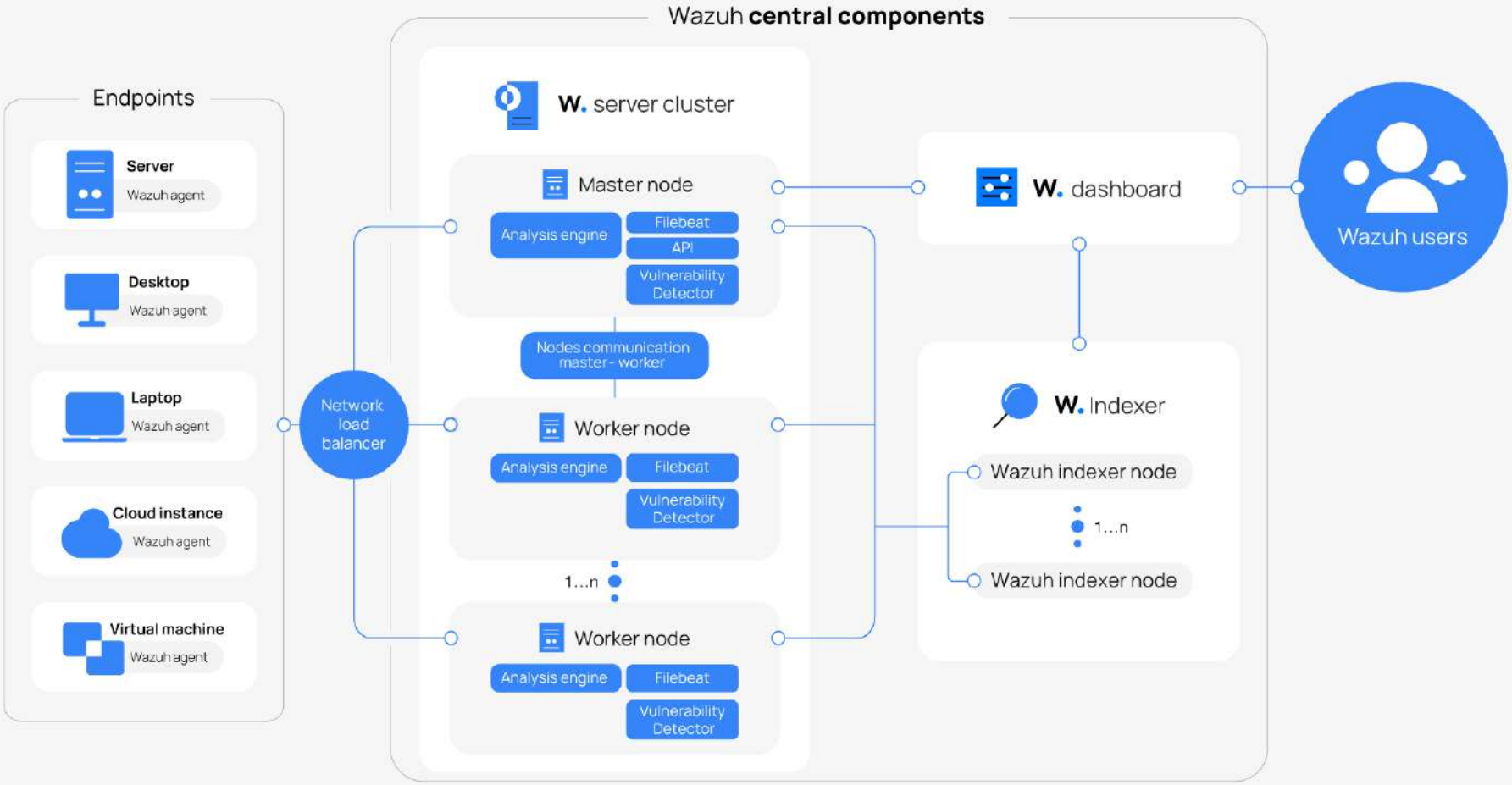
# Wazuh à vos services

**Wazuh-Indexer**

Basé sur Opensearch, stock l'ensemble des données de l'écosystème (Vulnérabilités, incidents, agents …)

**Wazuh-Dashboard**

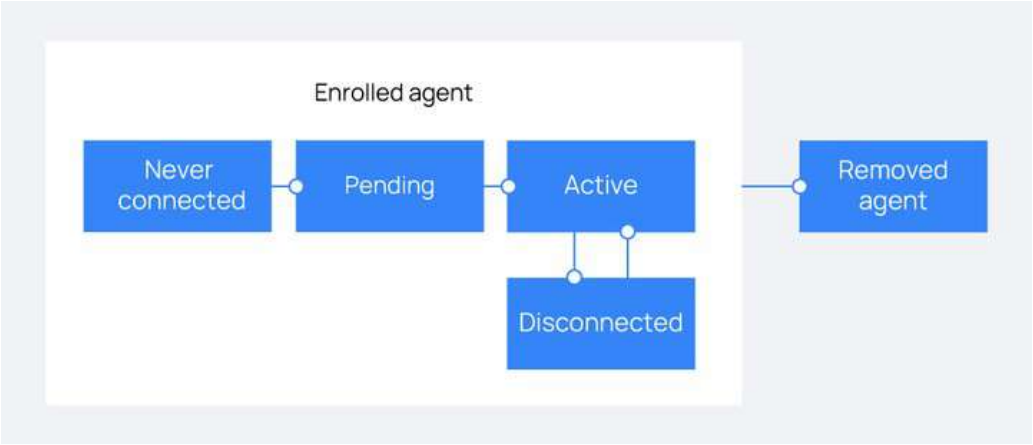
Interface graphique d'analyse et de visualisation des informations


Wazuh central components
Endpoints
Server
Wazuh agent
Desktop
Wazuh agent
Laptop
Wazuh agent
Cloud instance
Wazuh agent
Virtual machine
Wazuh agent
Network load balancer
W. server cluster
Master node
Analysis engine
Filebeat
API
Vulnerability Detector
Nodes communication master - worker
Worker node
Analysis engine
Filebeat
Vulnerability Detector
1...n
Worker node
Analysis engine
Filebeat
Vulnerability Detector
W. dashboard
W. Indexer
Wazuh indexer node
1...n
Wazuh indexer node
Wazuh users

# Wazuh-Agent – La petite souris


- Flux chiffré
- Collection de données
- Intégrité des fichiers
- Détection d'attaque
- Vérification de configuration
- Détection de vulnérabilité
- Réponse à incident

# Wazuh-Agent – La petite souris




| Port | Protocol | Purpose |
|---|---|---|
| 1514 | TCP (default) | Agent connection service |
| 1514 | UDP (optional) | Agent connection service (disabled by default) |
| 1515 | TCP | Agent enrollment service |

# Wazuh-Agent – La petite souris

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.10.1-1_amd64.deb && sudo WAZUH_MANAGER='wazuhagent.pci-conseil.net' WAZUH_AGENT_GROUP='PCI' dpkg -i ./wazuh-agent_4.10.1-1_amd64.deb
```

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.10.1-1_amd64.deb
```

```
sudo WAZUH_MANAGER='wazuhagent.pci-conseil.net' WAZUH_AGENT_GROUP='PCI'
```

```
dpkg -i ./wazuh-agent_4.10.1-1_amd64.deb
```

# Wazuh-Agent – La petite souris

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.10.1-1.msi -OutFile $env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='wazuhagent.pci-conseil.net' WAZUH_AGENT_GROUP='PCI'
```

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.10.1-1.msi -OutFile $env:tmp\wazuh-agent;
```

```
msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='wazuhagent.pci-conseil.net' WAZUH_AGENT_GROUP='PCI'
```

# Wazuh-Agent – Rester Groupir

Groups > AllianceLibre

agent.conf of AllianceLibre group

```
<agent_config>
  <labels>
    <label key="group">alliancelibre</label>
  </labels>
  <!-- Shared agent configuration here -->
  <wodle name="syscollector">
    <disabled>no</disabled>
    <interval>1h</interval>
    <os>yes</os>
    <packages>yes</packages>
    <hotfixes>yes</hotfixes>
  </wodle>
  <rootcheck>
    <rootkit_files>etc/shared/rootkit_files.txt</rootkit_files>
    <rootkit_trojans>etc/shared/rootkit_trojans.txt</rootkit_trojans>
  </rootcheck>
  <syscheck>
    <directories check_all="yes" repo
    <directories check_all="yes" repo
    <ignore>c:\program files (x86)\os
    <frequency>720</frequency>
    <directories realtime="yes">/etc<
  </syscheck>
</agent_config>
```

```
<wodle name="syscollector">
  <disabled>no</disabled>
  <interval>1h</interval>
  <os>yes</os>
  <packages>yes</packages>
  <hotfixes>yes</hotfixes>
</wodle>
```

```
<rootcheck>
  <rootkit_files>etc/shared/rootkit_files.txt</rootkit_files>
  <rootkit_trojans>etc/shared/rootkit_trojans.txt</rootkit_trojans>
</rootcheck>
```

```
<syscheck>
  <directories check_all="yes" report_changes="yes">/usr/bin,/usr/sbin</directories>
  <directories check_all="yes" report_changes="yes">C:\Program Files (x86),C:\Program Files</directories>
  <ignore>c:\program files (x86)\ossec-agent</ignore>
  <frequency>720</frequency>
  <directories realtime="yes">/etc</directories>
</syscheck>
```

# Wazuh-Manager – Le Cerveau

- Inscription des agents
- Connection avec la base de données
- Analyse les données
- Gestion des alertes
- Lien avec CTI Wazuh pour liste CVE

# Wazuh-Manager & ses démons

Wazuh-agentlessd -> Pour les checks d’intégrité système sur les périphériques sans agents

Wazuh-analysisd -> Reçoit les logs et les compares aux règles de détections

Wazuh-authd-> Ajoute les agents au Wazuh manager

Wazuh-csyslogd -> Si configuré, envoi les alertes Wazuh via syslog

Wazuh-dbd -> Ajoute les journaux d’alerte dans la base de données

# Wazuh-Manager & ses démons

Wazuh-maild -> Envoi les alertes mail


Wazuh-monitord -> Gère la disponibilité  des agents

Wazuh-remoted-> Pour la communication avec les agents

Wazuh-reportd -> Génère les rapports à partir des alertes

# Wazuh-Manager & ses démons

Wazuh-clusterd -> Si Wazuh en cluster, manage les différents éléments de celui-ci

Wazuh-db -> Gère les bases de données Wazuh


Wazuh-integratord -> Permet à Wazuh de se connecter à des API externe

# Wazuh-Manager & ses démons

Sur Manager et Agents :

Wazuh-execd -> Pour la partie réponse à incident

Wazuh-logcollector -> Supervise les fichiers et commande défini

Wazuh-syscheckd-> Supervise le checksum et les permissions des fichiers définis

Wazuh-modulesd -> Manage les différents modules de sécurité qu'utilise Wazuh (SCA, Vulnérabilité ...)

# Wazuh-Indexer – La bibliothèque

- Basé sur OpenSearch
- Simple nœud et multi-nœud
- Rotation des indices à la journée/semaine
- 5 indices principaux

# Wazuh-Indexer – La bibliothèque

- Wazuh-alerts-* -> Journalier -> Stocke toutes les alertes
- Wazuh-archives-* -> Optionnel -> Logs tous les évènements reçus par le serveur, à des fins d'archivage
- Wazuh-monitoring-* -> hebdomadaire -> Garde les états de connections des agents
- Wazuh-statistics-* -> hebdomadaire -> Stocke des statistiques à propos serveur Wazuh
- Wazuh-states-vulnerabilities-* -> Fait le lien entre les vulnérabilités et l'hôte monitoré

# Wazuh-Indexer – La bibliothèque


| Index | Health | Managed by policy | Status | Total size | Size of primaries | Total documents | Deleted documents | Primaries | Replicas |
|---|---|---|---|---|---|---|---|---|---|
| wazuh-alerts-4.x-2025.02.26 | Green | No | Open | 675.8mb | 675.8mb | 902850 | 0 | 1 | 0 |
| wazuh-alerts-4.x-2025.02.25 | Green | No | Open | 2.1gb | 2.1gb | 2723244 | 0 | 1 | 0 |
| wazuh-alerts-4.x-2025.02.24 | Green | No | Open | 2.3gb | 2.3gb | 2754078 | 0 | 1 | 0 |
| wazuh-alerts-4.x-2025.02.23 | Green | No | Open | 1gb | 1gb | 1350809 | 0 | 1 | 0 |
| wazuh-alerts-4.x-2025.02.22 | Green | No | Open | 1gb | 1gb | 1366906 | 0 | 1 | 0 |
| wazuh-alerts-4.x-2025.02.21 | Green | No | Open | 2.6gb | 2.6gb | 3118551 | 0 | 1 | 0 |
| wazuh-alerts-4.x-2025.02.20 | Green | No | Open | 2.5gb | 2.5gb | 3021020 | 17 | 1 | 0 |
| wazuh-alerts-4.x-2025.02.19 | Green | No | Open | 2.4gb | 2.4gb | 2835198 | 0 | 1 | 0 |
| wazuh-alerts-4.x-2025.02.18 | Green | No | Open | 2.3gb | 2.3gb | 2794566 | 0 | 1 | 0 |
| wazuh-alerts-4.x-2025.02.17 | Green | No | Open | 3.6gb | 3.6gb | 4439430 | 0 | 1 | 0 |
| wazuh-alerts-4.x-2025.02.16 | Green | No | Open | 982.9mb | 982.9mb | 1268952 | 0 | 1 | 0 |
| wazuh-alerts-4.x-2025.02.15 | Green | No | Open | 1.3gb | 1.3gb | 1656808 | 0 | 1 | 0 |
| wazuh-alerts-4.x-2025.02.14 | Green | No | Open | 2.9gb | 2.9gb | 3461639 | 0 | 1 | 0 |

# Wazuh-Indexer – La bibliothèque


| Index | Health | Managed by policy | Status | Total size | Size of primaries | Total documents | Deleted documents | Primaries | Replicas |
|---|---|---|---|---|---|---|---|---|---|
| wazuh-statistics-2025.9w | Green | No | Open | 2.1mb | 2.1mb | 1358 | 0 | 1 | 0 |
| wazuh-statistics-2025.8w | Green | No | Open | 1.8mb | 1.8mb | 3989 | 0 | 1 | 0 |
| wazuh-statistics-2025.7w | Green | No | Open | 1.8mb | 1.8mb | 3997 | 0 | 1 | 0 |
| wazuh-statistics-2025.6w | Green | No | Open | 1.7mb | 1.7mb | 3898 | 0 | 1 | 0 |
| wazuh-statistics-2025.5w | Green | No | Open | 1.9mb | 1.9mb | 3365 | 0 | 1 | 0 |
| wazuh-statistics-2025.4w | Green | No | Open | 1.9mb | 1.9mb | 3850 | 0 | 1 | 0 |
| wazuh-statistics-2025.3w | Green | No | Open | 1.3mb | 1.3mb | 2597 | 0 | 1 | 0 |
| wazuh-statistics-2025.2w | Green | No | Open | 2mb | 2mb | 3994 | 0 | 1 | 0 |
| wazuh-statistics-2025.1w | Green | No | Open | 1.6mb | 1.6mb | 2850 | 0 | 1 | 0 |
| wazuh-statistics-2024.9w | Green | No | Open | 1.9mb | 1.9mb | 3986 | 0 | 1 | 0 |
| wazuh-statistics-2024.8w | Green | No | Open | 2mb | 2mb | 3999 | 0 | 1 | 0 |
| wazuh-statistics-2024.7w | Green | No | Open | 2mb | 2mb | 4001 | 0 | 1 | 0 |
| wazuh-statistics-2024.6w | Green | No | Open | 1.6mb | 1.6mb | 3595 | 0 | 1 | 0 |

# Wazuh-Indexer – La bibliothèque


| Index | Health | Managed by policy | Status | Total size | Size of primaries | Total documents | Deleted documents | Primaries | Replicas |
|---|---|---|---|---|---|---|---|---|---|
| wazuh-monitoring-2025.9w | Green | No | Open | 208b | 208b | 0 | 0 | 1 | 0 |
| wazuh-monitoring-2025.8w | Green | No | Open | 44.6kb | 44.6kb | 5 | 0 | 1 | 0 |
| wazuh-monitoring-2025.7w | Green | No | Open | 87.5kb | 87.5kb | 47 | 0 | 1 | 0 |
| wazuh-monitoring-2025.6w | Green | No | Open | 208b | 208b | 0 | 0 | 1 | 0 |
| wazuh-monitoring-2025.5w | Green | No | Open | 208b | 208b | 0 | 0 | 1 | 0 |
| wazuh-monitoring-2025.4w | Green | No | Open | 208b | 208b | 0 | 0 | 1 | 0 |
| wazuh-monitoring-2025.3w | Green | No | Open | 208b | 208b | 0 | 0 | 1 | 0 |
| wazuh-monitoring-2025.2w | Green | No | Open | 208b | 208b | 0 | 0 | 1 | 0 |
| wazuh-monitoring-2025.1w | Green | No | Open | 208b | 208b | 0 | 0 | 1 | 0 |
| wazuh-monitoring-2024.9w | Green | No | Open | 746.5kb | 746.5kb | 1935 | 0 | 1 | 0 |
| wazuh-monitoring-2024.8w | Green | No | Open | 399.4kb | 399.4kb | 750 | 0 | 1 | 0 |
| wazuh-monitoring-2024.7w | Green | No | Open | 204.5kb | 204.5kb | 332 | 0 | 1 | 0 |
| wazuh-monitoring-2024.6w | Green | No | Open | 36.7mb | 36.7mb | 167458 | 0 | 4 | 0 |

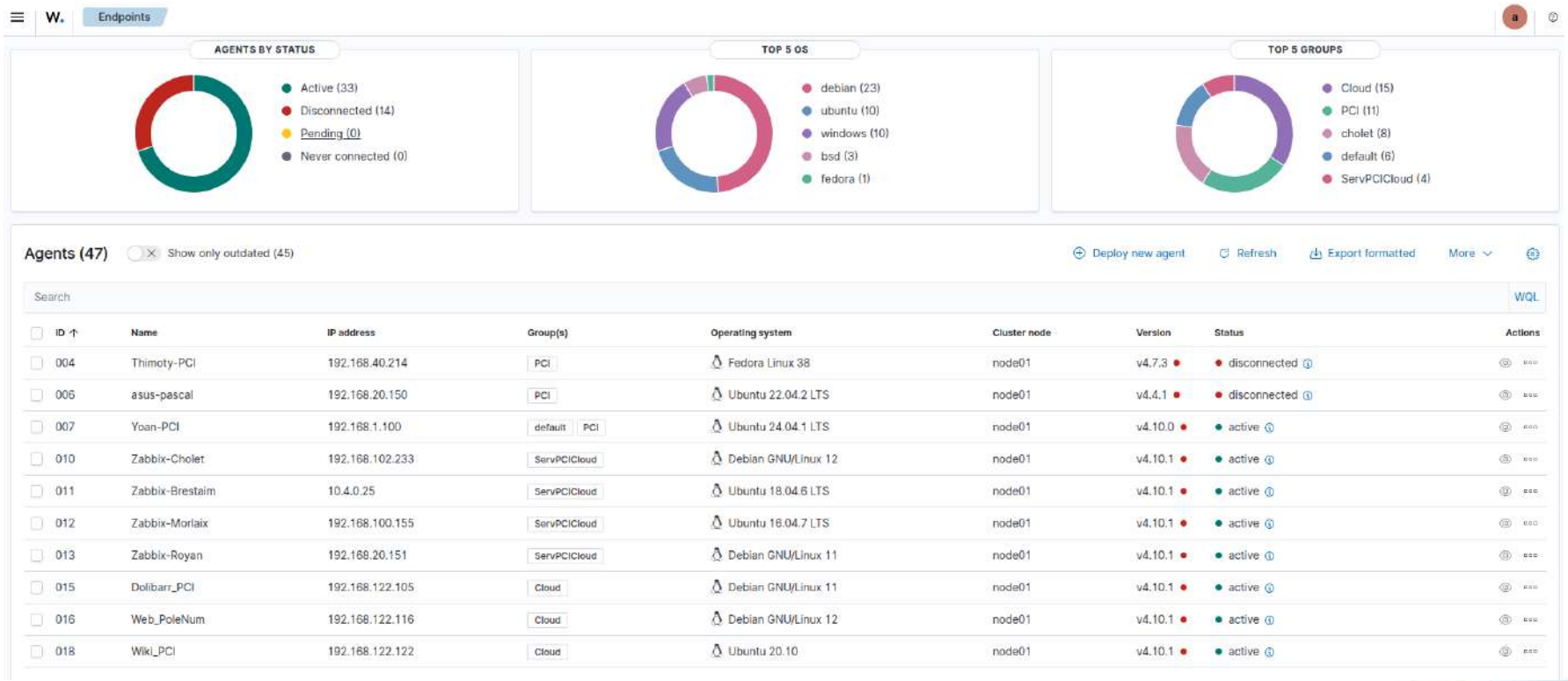
# Wazuh-Indexer – La bibliothèque


| Index ↓ | Health | Managed by policy | Status | Total size | Size of primaries | Total documents | Deleted documents |
|---|---|---|---|---|---|---|---|
| wazuh-states-vulnerabilities-mutualise-wazuh | Green | No | Open | 93mb | 93mb | 109374 | 1321 |

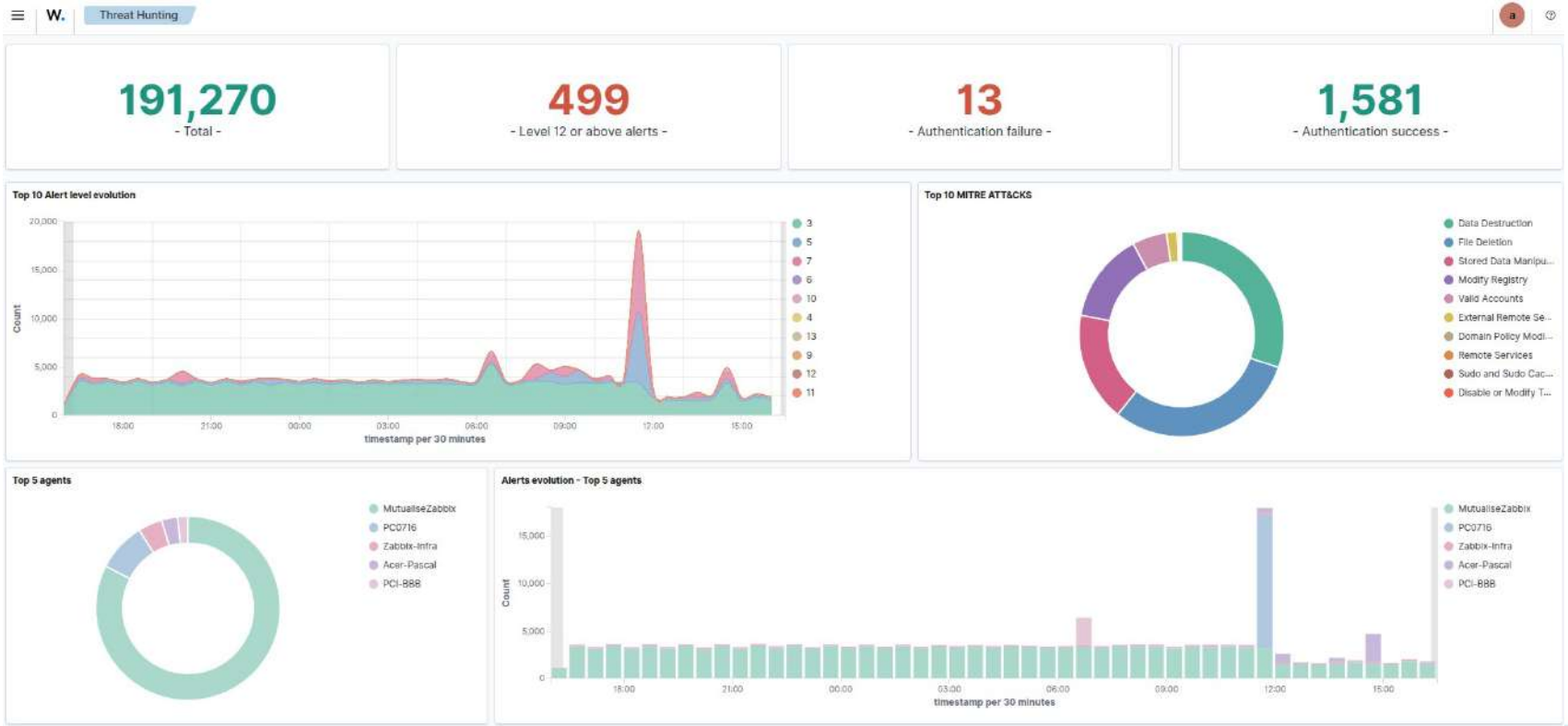
# Wazuh-Dashboard – L’oncle SAM

- Visualisation des données
- Gestion des agents
- Gestion des indexes

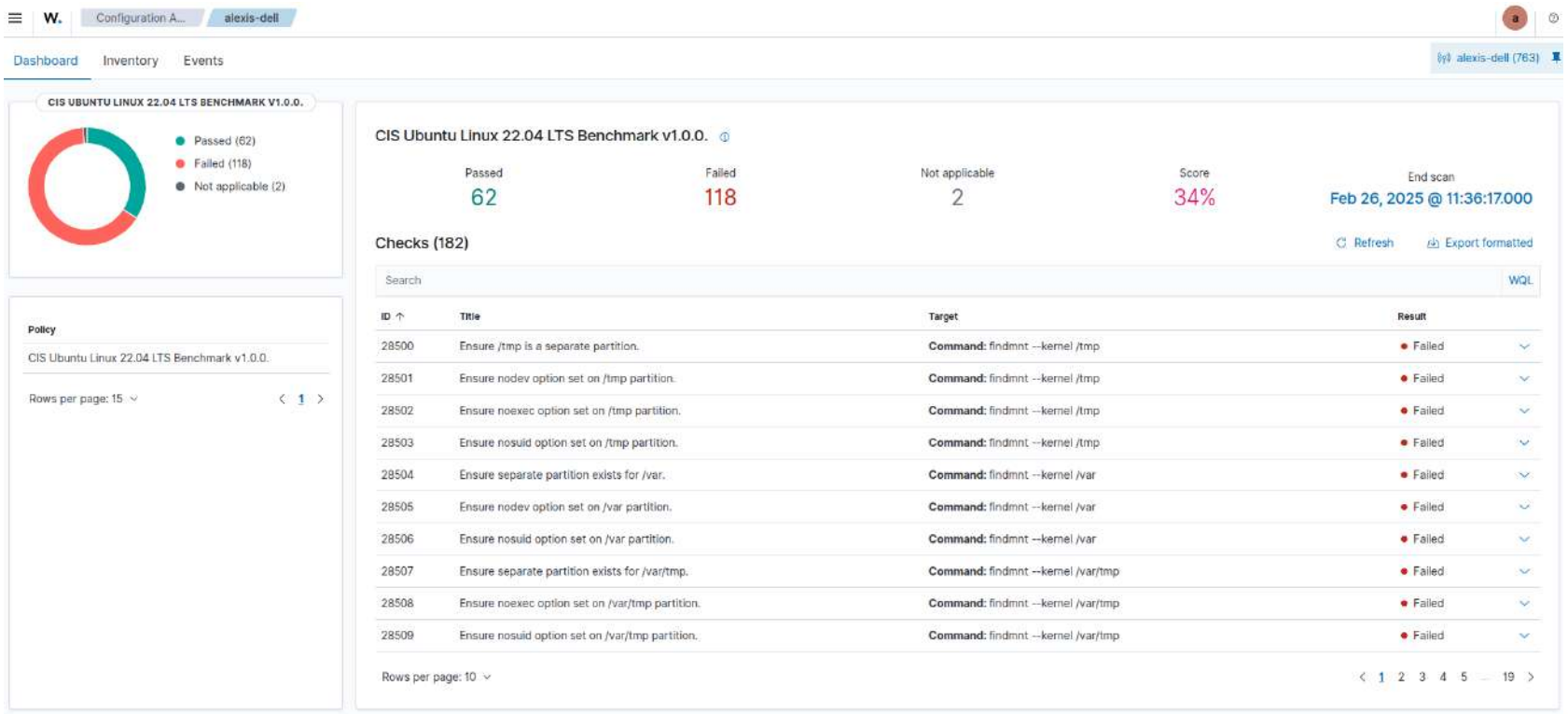
# Wazuh-Dashboard – L'oncle SAM



# Wazuh-Dashboard – L'oncle SAM



# Wazuh-Dashboard – L'oncle SAM



# Wazuh

Activités pratique :

- Installation d’un agent ;
- Changement de valeur d’un fichier pour file integrity checking ;
- Bruteforce avec blocage actif (EDR + XDR);