

FACULTAD DE CIENCIA Y TECNOLOGÍA
CENTRO REGIONAL DE USULUTÁN
INGENIERÍA EN SISTEMAS Y REDES INFORMÁTICAS

SEGURIDAD INFORMÁTICA
CICLO II – 2025



ACTIVIDAD:

LABORATORIO 1 COMPUTO 2 – GUÍA DE INSTALACIÓN DE WAZUH.

DOCENTE:

ING. TIMOTEA GUADALUPE MENJIVAR.

ESTUDIANTES:

ANA PATRICIA GAITÁN HERNÁNDEZ	USSS017122
FREDY ADILSON CAMPOS HERNÁNDEZ	USSS017322
JOSUÉ GABRIEL CAMPOS ESCOBAR	USIS006316
LESLY CAROLINA BERMÚDEZ MEMBREÑO	USSS017722
ROMEO ALEXANDER GARCIA CASTILLO	USIS000313

FECHA DE ENTREGA:

USULUTÁN, 30 DE OCTUBRE DE 2025.



Wazuh es una plataforma de seguridad que proporciona protección XDR y SIEM unificada para terminales y cargas de trabajo en la nube. La solución está compuesta por un único agente universal y tres componentes centrales: el servidor Wazuh, el indexador Wazuh y el panel de Wazuh.

INSTALACIÓN DE WAZUH.

Recomendaciones generales.

1. Servidor de Ubuntu server 24.04, con mínimo de almacenamiento de 80 gb. (Por cache, por logs).
2. Dirección IP estática.
3. Configuración de la interfaz gráfica.
4. Configuración del resolv.conf
5. Conexión a internet.

Configuración básica para su correcto funcionamiento.

Agentes	UPC	RAM	Almacenamiento (90 días)
1–25	4 vCPU	8 GiB	50 GB
25–50	8 vCPU	8 GiB	100 GB
50–100	8 vCPU	8 GiB	200 GB

Actualizamos el Ubuntu server, utilizando el siguiente comando.

sudo apt update && sudo apt upgrade

```
root@server01:/home/ragc# sudo apt update && sudo apt upgrade
```

```
root@server01:/home/ragc# sudo apt update && sudo apt upgrade
Hit:1 http://sv.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://sv.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://sv.archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:4 http://sv.archive.ubuntu.com/ubuntu focal-security InRelease
Reading package lists... Done
```

Verificamos que el cortafuegos este activo.

ufw status numbered

```
root@server01:/home/ragc# ufw status numbered
Status: inactive
root@server01:/home/ragc#
```

Habilitamos los servicios de firewall.

ufw enable

```
root@server01:/home/ragc# ufw enable
Firewall is active and enabled on system startup
root@server01:/home/ragc#
```

Se verifica que este activo en el servidor.

ufw status numbered

```
root@server01:/home/ragc# ufw status numbered
Status: active
root@server01:/home/ragc#
```

Habilitamos los puertos necesarios de escucha con el comando:

Sudo ufw allow 22/tcp

```
root@server01:/home/ragc# sudo ufw allow 22/tcp
Rule added
Rule added (v6)
root@server01:/home/ragc# sudo ufw allow 443/tcp
Rule added
Rule added (v6)
root@server01:/home/ragc# sudo ufw allow 1514/tcp
Rule added
Rule added (v6)
root@server01:/home/ragc# sudo ufw allow 1515/tcp
Rule added
Rule added (v6)
root@server01:/home/ragc# sudo ufw allow 55000/tcp
Rule added
Rule added (v6)
root@server01:/home/ragc# sudo ufw allow 5601/tcp
Rule added
Rule added (v6)
root@server01:/home/ragc#
```

Ya que hemos activado los puertos necesarios, Podemos comenzar con la instalación de Wazuh.

Descargamos y ejecutamos el asistente de instalación de Wazuh.

```
curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh && sudo
bash ./wazuh-install.sh -a
```

```
root@server01:/home/ragc# curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh && sudo bash ./wazuh-in
stall.sh -a
27/10/2025 22:20:12 INFO: Starting Wazuh installation assistant. Wazuh version: 4.11.2 (x86_64/AMD64)
27/10/2025 22:20:12 INFO: Verbose logging redirected to /var/log/wazuh-install.log
27/10/2025 22:20:16 INFO: Verifying that your system meets the recommended minimum hardware requirements.
27/10/2025 22:20:16 INFO: Wazuh web interface port will be 443.
27/10/2025 22:20:16 WARNING: The system has UFW enabled. Please ensure that traffic is allowed on these por
ts: 1515, 1514, 443.
```

Este proceso tarda bastante, debemos recordar que si no contamos con los requerimientos necesarios no se instalará, posteriormente mostrará el medio de acceso a la interfaz web de Wazuh, algo que es bueno mencionar es que debemos percatarnos de no dejar salto de línea en el comando anterior, porque de ser así no se instalará.

```
28/10/2025 15:18:19 INFO: wazuh-manager service started.
28/10/2025 15:18:19 INFO: Starting Filebeat installation.
28/10/2025 15:18:41 INFO: Filebeat installation finished.
28/10/2025 15:18:43 INFO: Filebeat post-install configuration finished.
28/10/2025 15:18:43 INFO: Starting service filebeat.
28/10/2025 15:18:46 INFO: filebeat service started.
28/10/2025 15:18:46 INFO: --- Wazuh dashboard ---
28/10/2025 15:18:46 INFO: Starting Wazuh dashboard installation.
28/10/2025 15:21:30 INFO: Wazuh dashboard installation finished.
28/10/2025 15:21:31 INFO: Wazuh dashboard post-install configuration finished.
28/10/2025 15:21:31 INFO: Starting service wazuh-dashboard.
28/10/2025 15:21:32 INFO: wazuh-dashboard service started.
28/10/2025 15:21:33 INFO: Updating the internal users.
28/10/2025 15:21:38 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/internalusers-backup folder.
28/10/2025 15:21:50 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and password.
28/10/2025 15:22:23 INFO: Initializing Wazuh dashboard web application.
28/10/2025 15:22:24 INFO: Wazuh dashboard web application initialized.
28/10/2025 15:22:24 INFO: --- Summary ---
28/10/2025 15:22:24 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
  User: admin
  Password: *SGv?s5bR?R+.DSDyH48sLTCVC8jUADP
28/10/2025 15:22:24 INFO: Installation finished.
root@server01:/home/radc#
```

En este caso la rut del dashboard, usuario y contraseña:

https://<wazuh-dashboard-ip>:443

User: admin

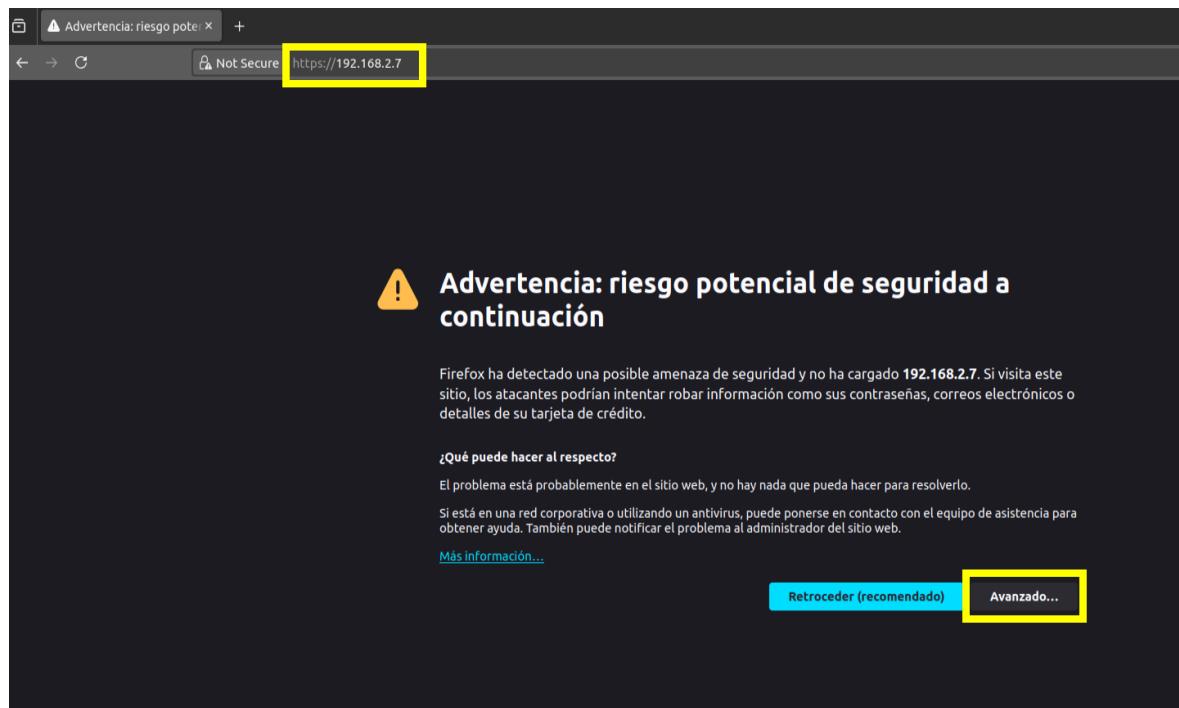
Password: *SGv?s5bR?R+.DSDyH48sLTCVC8jUADP

Hay que tomar en cuenta que estos datos varían, así que debemos guardar los que proporciona wazuh en la instalación que realicemos.

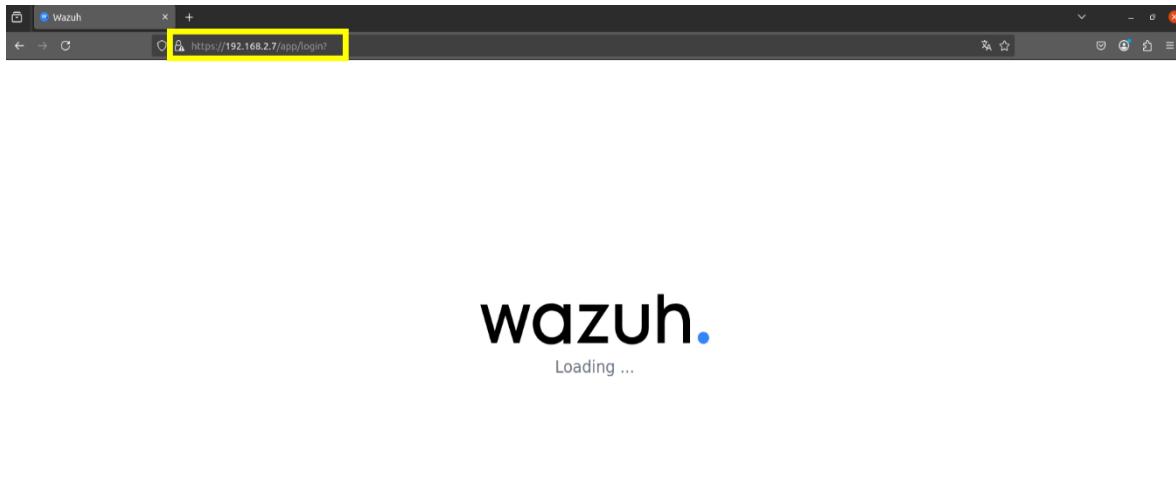
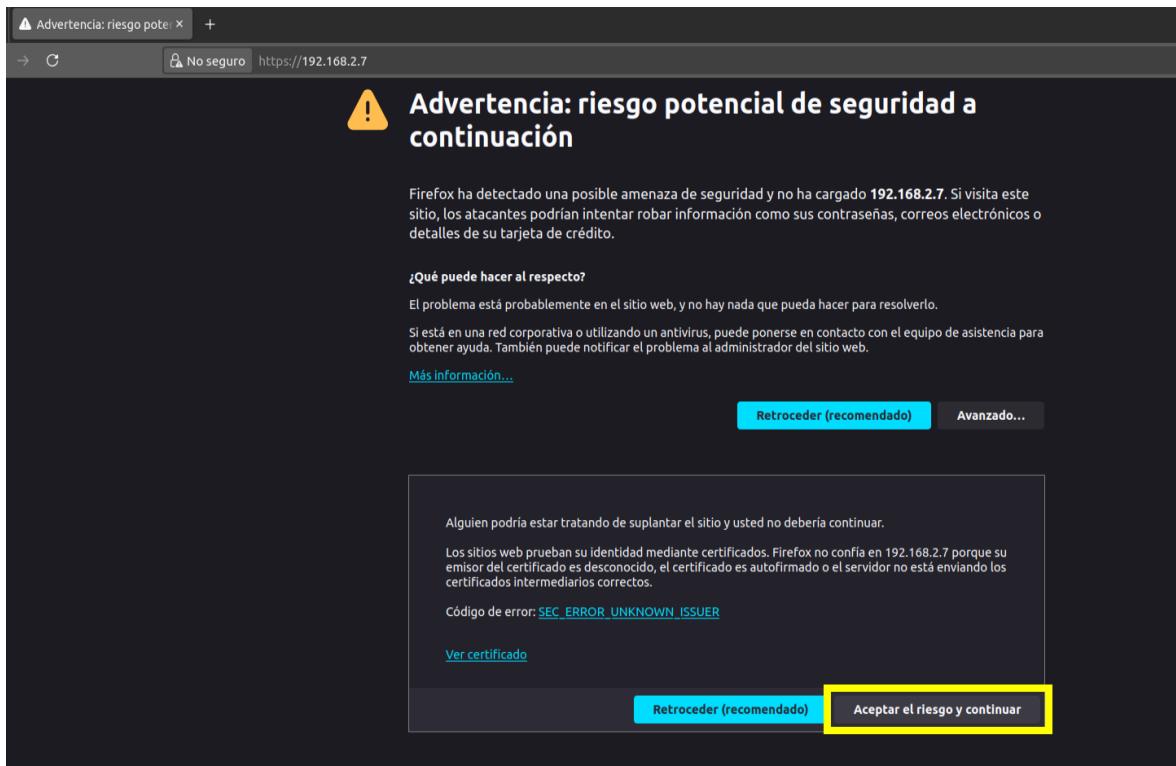
CARGANDO EL DASHBOARD.

Debemos poner la ip de Nuestro servidor en el navegador, en este caso es la 192.168.2.7, se colocará de la siguiente manera:

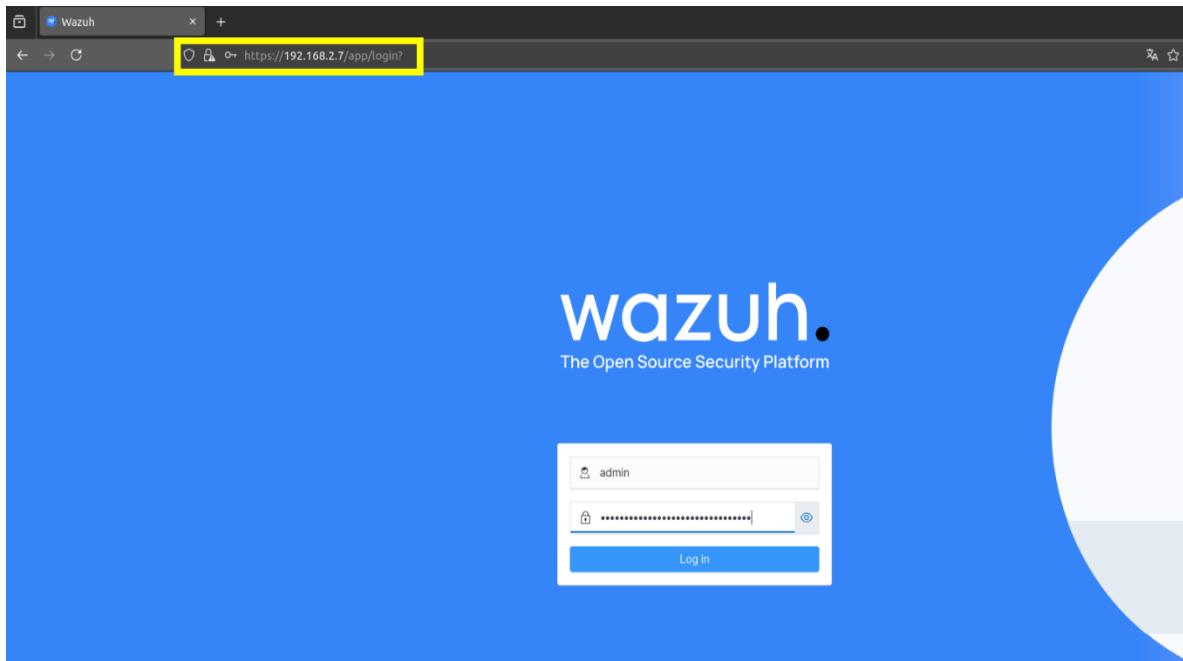
<https://192.168.2.7:443>



Debemos seleccionar la opción que dice “Avanzado”, luego nos mostrará la siguiente ventana advirtiendo el riesgo de seguir, seleccionamos la opción “Aceptar el riesgo y continuar”.



Una vez que inicie, nos pedirá loguearnos, para ello debemos ingresar los datos proporcionados anteriormente por la herramienta.



Finalmente, tenemos acceso al panel de administración:

A screenshot of the Wazuh dashboard. At the top, there's a summary section with "LAST 24 HOURS ALERTS": Critical severity 0, High severity 0, Medium severity 130, and Low severity 107. Below this are sections for "AGENTS SUMMARY" (no agents registered, "Deploy new agent" button), "ENDPOINT SECURITY" (Configuration Assessment, Malware Detection, File Integrity Monitoring), and "THREAT INTELLIGENCE" (Threat Hunting, MITRE ATT&CK, Vulnerability Detection).

AGREGANDO UN NUEVO AGENTE.

Agregando un agente Windows.

Seleccionamos la opción “Desplegar nuevo agente”.

This screenshot shows the 'Overview' page of a security monitoring application. At the top left, there's a message: 'This instance has no agents registered. Please deploy agents to begin monitoring your endpoints.' Below this, a green arrow points to a blue button labeled '+ Deploy new agent'. To the right, there's a section titled 'LAST 24 HOURS ALERTS' with four categories: Critical severity (0), High severity (0), Medium severity (130), and Low severity (107). Below these sections are 'ENDPOINT SECURITY' and 'THREAT INTELLIGENCE' modules, each containing two cards with icons and descriptions.

Seleccionamos la distribución del nuevo agente, en este caso será windows.

This screenshot shows the 'Deploy new agent' page. A blue checkmark icon indicates the 'Select the package to download and install on your system:' step is selected. Under this step, there are three options: 'LINUX', 'WINDOWS', and 'macOS'. The 'WINDOWS' option is highlighted with a green border. Below each option, there are specific package details: 'LINUX' shows 'RPM amd64', 'DEB amd64', 'RPM aarch64', and 'DEB aarch64'; 'WINDOWS' shows 'MSI 32/64 bits'; and 'macOS' shows 'Intel' and 'Apple silicon'. At the bottom, there's a note: 'For additional systems and architectures, please check our documentation'.

Llenamos los datos del servidor:

This screenshot shows the 'Server address' configuration page. It includes a section for 'Assign a server address' with a note: 'This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).'. A text input field contains '192.168.2.7'. Below the input field is a checkbox labeled 'Remember server address' with a checked status.

Asignamos un nombre al agente windows, uno que nos permita reconocerlo fácilmente y además de su ip estática que le hemos configurado, siendo este el nombre:

WIN10-192.168.2.8

 **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: [?](#)

 The agent name must be unique. It can't be changed once the agent has been enrolled. [?](#)

Lo siguiente es copiar el código de configuración que debemos ejecutar en powershell en la máquina cliente, es decir en el agente windows.

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

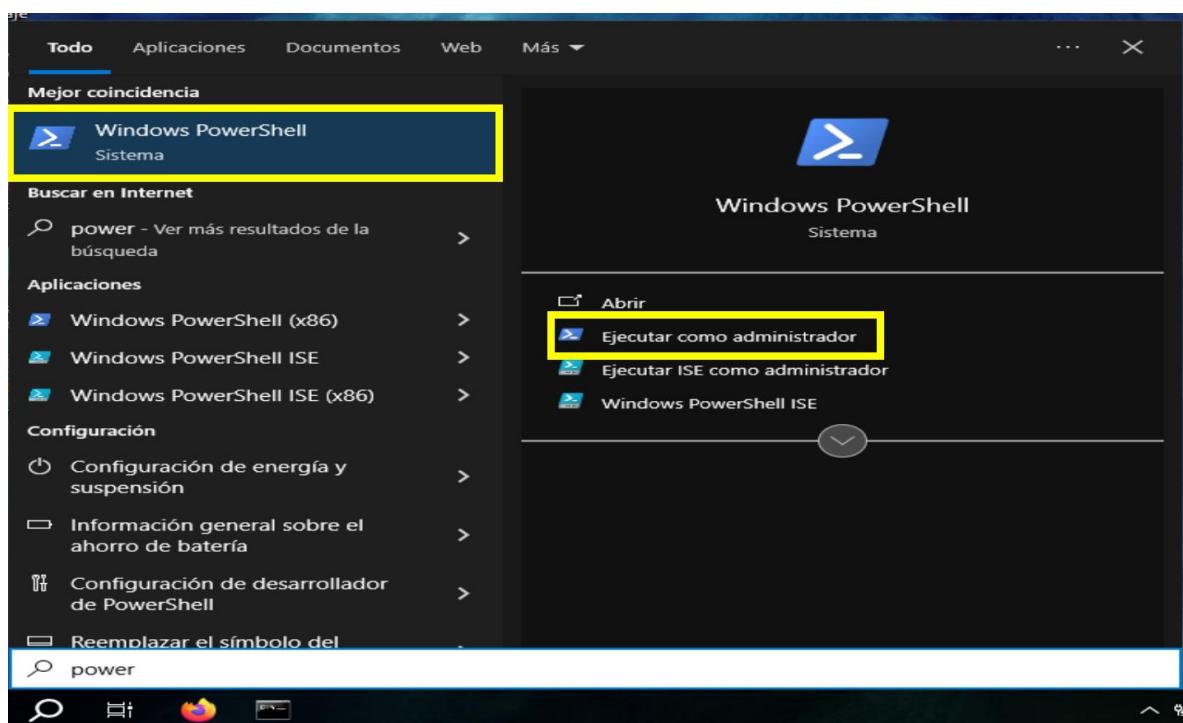
```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.11.2-1.msi -OutFile $env:tmp\wazuh-agent; msieexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.2.7' WAZUH_AGENT_NAME='WIN10-192.168.2.8'
```

 **Requirements**

- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

Keep in mind you need to run this command in a Windows PowerShell terminal.

El último paso es abrir el powershell de la máquina windows como administrador.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.11.2-1.msi
-OutFile $env:tmp\wazuh-agent; msieexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.2.7' WAZUH_AGENT
_NAME='WIN10-192.168.2.8'
```

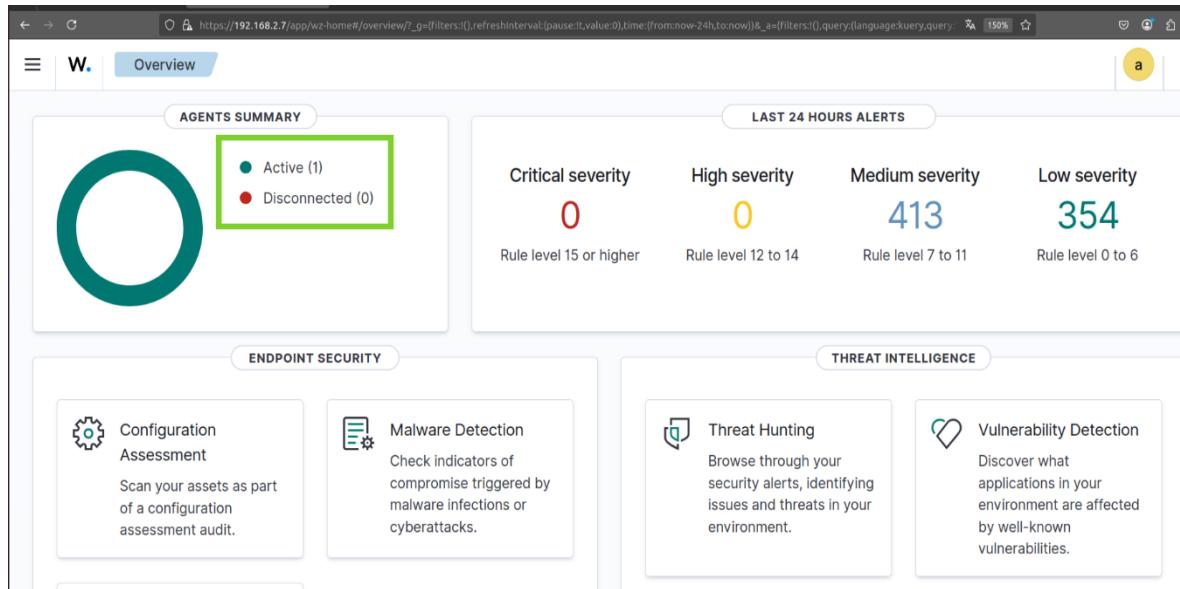
Ahora ejecutamos el comando de inicio del agente:

NET START WazuhSvc

```
PS C:\Windows\system32> NET START WazuhSvc
El servicio de Wazuh se ha iniciado correctamente.

PS C:\Windows\system32>
```

Podemos notar que el agente se instaló correctamente:



Método alternativo si no aparece después del comando: NET START

WazuhSvc:

Si no nos aparece hasta este punto el agente, entonces debemos agregarlo con la terminal de nuestro Ubuntu server.

Para ello debemos abrir nuestra terminal y escribir el siguiente comando:

```
sudo /var/ossec/bin/manage_agents
```

```
ragc@server01:~$ sudo /var/ossec/bin/manage_agents
```

```
*****
* Wazuh v4.11.2 Agent manager.          *
* The following options are available: *
*****  
(A)dd an agent (A).  
(E)xtract key for an agent (E).  
(L)ist already added agents (L).  
(R)emove an agent (R).  
(Q)uit.  
Choose your action: A,E,L,R or Q:
```

Se abre un menú de opciones y debemos seleccionar la letra “A” (Add), para agregar el agente:

```
ragc@server01:~$ sudo /var/ossec/bin/manage_agents
```

```
*****
* Wazuh v4.11.2 Agent manager.          *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
```

```
Choose your action: A,E,L,R or Q: A
```

Nos pedirá el nombre de nuestro agente, para lo cual le pondremos WIN10 y la ip del agente, que en este caso es la 192.168.2.8 (máquina windows) y por último confirmamos el hecho de agregar el agente con la letra “y”, damos enter y listo hemos agregado el agente windows:

```
ragc@server01:~$ sudo /var/ossec/bin/manage_agents
[sudo] password for ragc:
```

```
*****
* Wazuh v4.11.2 Agent manager.          *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
```

```
Choose your action: A,E,L,R or Q: A
```

```
- Adding a new agent (use '\q' to return to the main menu).
Please provide the following:
```

```
* A name for the new agent: WIN10
* The IP Address of the new agent: 192.168.2.8
Confirm adding it?(y/n): y
```

Ya Podremos notar que se ha agregado el agente:

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
005	WIN10-192.168.2.8	192.168.2.8	default	Microsoft Windows 10 Education 10.0.19045.6216	node01	v4.11.2	active	...

Pasos que debemos tener en cuenta antes de apagar nuestro agente windows.

PASO 1:

Verifica que el servicio esté en buen estado (opcional):

En PowerShell (Administrador):

Get-Service WazuhSvc

```
PS C:\Windows\system32> Get-Service WazuhSvc
Status     Name                           DisplayName
-----   ----                           -----------
Running   WazuhSvc                       Wazuh

PS C:\Windows\system32>
```

Si dice Running, está funcionando correctamente.

PASO 2:

Detenemos el servicio manualmente. Utilizamos el comando, de esta forma desconectamos limpiamente el agente del servidor.

NET STOP WazuhSvc

```
PS C:\Windows\system32> NET STOP WazuhSvc
El servicio de Wazuh se detuvo correctamente.
PS C:\Windows\system32>
```

PASO 3:

Apagamos windows normalmente:

shutdown /s /t 0

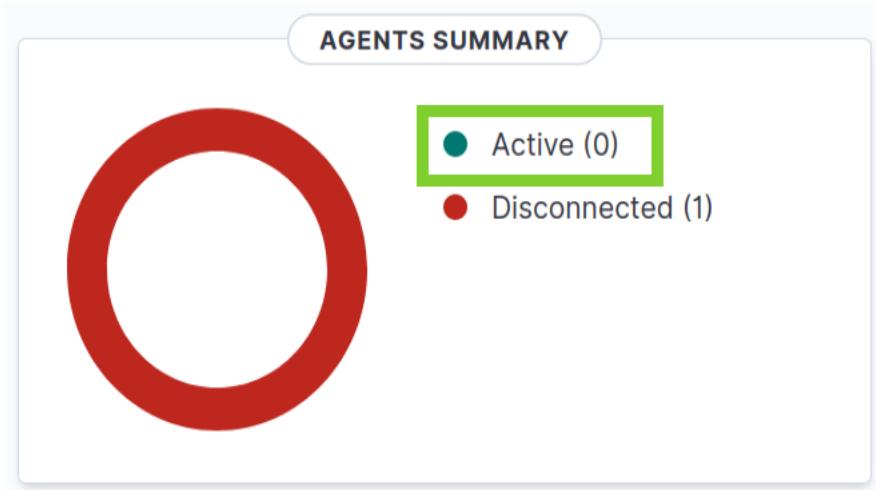
Notaremos que ahora no aparece la máquina windows 10 en “Active”, sino en “Disconected(1)”.

The screenshot shows the Wazuh user interface. At the top, there's a summary section with a large red circle icon. To its right, under 'AGENTS SUMMARY', it shows 0 Active agents and 1 Disconnected agent. A green box highlights the 'Disconnected (1)' count. Below this is a 'LAST 24 HOURS ALERTS' section with counts for Critical, High, Medium, and Low severity alerts. The main part of the screen is a table titled 'Agents (1)'. It shows one row for a disconnected Windows 10 agent. The table includes columns for ID, Name, IP address, Group(s), Operating system, Cluster node, Version, Status, and Actions. The status column shows 'disconnected' with a red dot. The 'Actions' column contains a refresh icon and three dots. At the bottom of the table, there are pagination controls and a note about rows per page.

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
005	WIN10-192.168.2.8	192.168.2.8	default	Microsoft Windows 10 Education 10.0.19045.6216	node01	v4.11.2	disconnected	

Agregando un agente Libre.

Debemos dar clic en la parte de Wazuh, donde dice “Active”, esto nos mostrará el panel de los agentes activos.



Una vez estando en ese panel, debemos dar clic en “Deploy new agent”, con el objetivo de agregar un nuevo agente.

The screenshot shows a table header for "Agents (0)" with columns: ID, Name, IP address, Group(s), Operating system, Cluster node, Version, Status, and Actions. A search bar at the top contains "status=active". A button labeled "Deploy new agent" is highlighted with a green border. The message "No items found" is displayed below the table.

Nos desplegará el panel donde vamos a seleccionar el tipo de arquitectura que usaremos, en este caso es un S.O libre. Por lo tanto usamos esa opción:

The screenshot shows a step-by-step guide for deploying a new agent. Step 1: "Select the package to download and install on your system:". It has three sections: "LINUX" (selected and highlighted with a green border), "WINDOWS", and "macOS". Under "LINUX", there are two groups of options: "RPM" (RPM amd64, RPM aarch64) and "DEB" (DEB amd64, DEB aarch64). A note at the bottom says "For additional systems and architectures, please check our documentation".

Ahora debemos saber la arquitectura de nuestro sistema operativo para que podamos elegir la opción correcta, para ello en la terminal de nuestro agente debian 13 (agente), vamos a poner el siguiente comando:

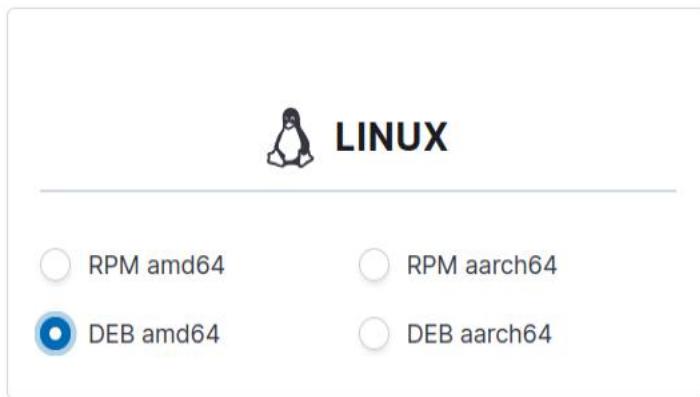
uname -a

```
ragc@romeoDebian:~$ uname -a
Linux romeoDebian 6.12.48+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.48
-1 (2025-09-20) x86_64 GNU/Linux
ragc@romeoDebian:~$ █
```

Aquí lo importante es ver la parte de la arquitectura:

```
ragc@romeoDebian:~$ uname -a
Linux romeoDebian 6.12.48+deb13 amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.48
-1 (2025-09-20) x86_64 GNU/Linux
ragc@romeoDebian:~$ █
```

Ahora que ya tenemos la arquitectura de nuestro debian, podemos seleccionar la opción correcta en nuestro Wazuh:



Una vez seleccionada la opción correcta, pasamos a la siguiente opción, aunque debemos aclarar que, ya que es el segundo agente, entonces automáticamente estará disponible la ip de nuestro servidor.

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 [?](#)

Remember server address

Solo si marcamos en el primer agente esta opción

El siguiente paso es darle un nombre con el que podamos identificar fácilmente la máquina, en este caso le pondremos:

Debian-192.168.2.9

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: [?](#)

Debian-192.168.2.9

ⓘ The agent name must be unique. It can't be changed once the agent has been enrolled. [?](#)

Select one or more existing groups: [?](#)

Default

Ahora lo siguiente, antes de pasar a pegar el comando de descarga e instalación del agente, debemos instalar las siguientes dependencias en Debian 11, 12 y 13 con el objetivo de obtener primero las llaves que el sistema necesita para poder **descargar y verificar con seguridad** el paquete del agente Wazuh desde internet.

Los comandos de las dependencias son, aunque es posible que ya estén instalados por defecto en el sistema:

sudo apt-get install gnupg apt-transport-https -y

```
ragc@romeoDebian:~$ sudo apt-get install gnupg apt-transport-https -y
[sudo] contraseña para ragc:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
gnupg ya está en su versión más reciente (2.4.7-21).
apt-transport-https ya está en su versión más reciente (3.0.3).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
ragc@romeoDebian:~$
```

sudo apt-get install curl -y

```
ragc@romeoDebian:~$ sudo apt-get install curl -y
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
curl ya está en su versión más reciente (8.14.1-2).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
ragc@romeoDebian:~$
```

Ahora copiamos el comando de instalación del agente y lo pegamos en la terminal de debian 13.

Run the following commands to download and install the agent:

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.11.2-1_amd64.deb && sudo WAZUH_MANAGER='192.168.2.7' WAZUH_AGENT_NAME='Debian-192.168.2.9' dpkg -i ./wazuh-agent_4.11.2-1_amd64.deb
```

```
ragc@romeoDebian:~$ sudo wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.11.2-1_amd64.deb && sudo WAZUH_MANAGER='192.168.2.7' WAZUH_AGENT_NAME='Debian-192.168.2.9' dpkg -i ./wazuh-agent_4.11.2-1_amd64.deb
[sudo] contraseña para ragc:
```

```
[sudo] contraseña para ragc:  
--2025-10-29 20:24:29-- https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.11.2-1_amd64.deb  
Resolviendo packages.wazuh.com (packages.wazuh.com)... 18.173.166.9, 18.173.166.107, 18.173.166.17, ...  
Conectando con packages.wazuh.com (packages.wazuh.com)[18.173.166.9]:443... conectado.  
Petición HTTP enviada, esperando respuesta... 200 OK  
Longitud: 11075686 (11M) [application/vnd.debian.binary-package]  
Grabando a: «wazuh-agent_4.11.2-1_amd64.deb»  
  
wazuh-agent_4.11.2- 100%[=====] 10.56M 15.3MB/s en 0.7s  
  
2025-10-29 20:24:30 (15.3 MB/s) - «wazuh-agent_4.11.2-1_amd64.deb» guardado [11075686/11075686]  
  
Seleccionando el paquete wazuh-agent previamente no seleccionado.  
(Leyendo la base de datos ... 142593 ficheros o directorios instalados actualmente.)  
Preparando para desempaquetar .../wazuh-agent_4.11.2-1_amd64.deb ...  
Desempaquetando wazuh-agent (4.11.2-1) ...  
Configurando wazuh-agent (4.11.2-1) ...  
ragc@romeoDebian:~$ █
```

Una vez configurado lo anterior, debemos ingresar los siguientes comandos para el inicio del agente.

PRIMER COMANDO:

sudo systemctl daemon-reload

Este comando nos permite recargar la lista de servidores para detectar el nuevo agente wazuh que acabamos de instalar.

```
ragc@romeoDebian:~$ sudo systemctl daemon-reload  
ragc@romeoDebian:~$ █
```

SEGUNDO COMANDO:

sudo systemctl enable wazuh-agent

Este comando nos permite ejecutar automáticamente cada vez que encienda el debian.

```
ragc@romeoDebian:~$ sudo systemctl enable wazuh-agent
Created symlink '/etc/systemd/system/multi-user.target.wants/wazuh-agent.service
' → '/usr/lib/systemd/system/wazuh-agent.service'.
ragc@romeoDebian:~$
```

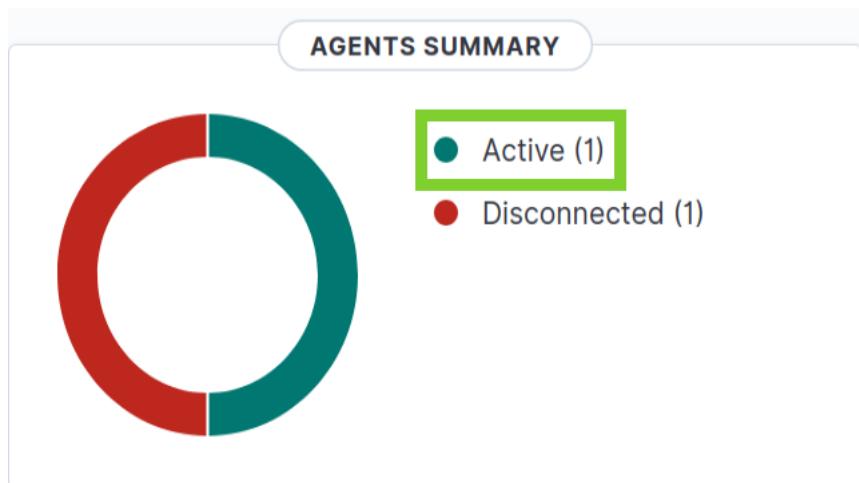
TERCER COMANDO:

sudo systemctl start wazuh-agent

Este comando enciende el servicio inmediatamente, sin necesidad de reiniciar.

```
ragc@romeoDebian:~$ sudo systemctl start wazuh-agent
ragc@romeoDebian:~$
```

Ahora solo falta recargar el dashboard de wazuh para que se cargue el nuevo agente y el estado activo del mismo, notaremos que ya nos muestra uno activo y uno desectivado, recordemos que solo teníamos conectado el agente windows:



Damos clic en el que dice “Active” y este nos llevara a la ventana donde están todos los agentes activos, pero que en este momento solo es uno, mostrándonos el agente libre, el cual es Debian 13.

The screenshot shows the Wazuh Agents interface. At the top, it says "Agents (1)". Below that is a search bar with "status=active". To the right are buttons for "Deploy new agent", "Refresh", "Export formatted", and "More". A "WQL" button is also present. The main table has columns: ID, Name, IP address, Group(s), Operating system, Cluster node, Version, Status, and Actions. One row is shown, corresponding to the agent listed in the search bar. The status is "active". At the bottom, it says "Rows per page: 10" and shows a page number "1".

Si queremos volver a la página principal de Wazuh, basta con presionar el botón superior izquierdo que tiene una “W”.

The screenshot shows the Wazuh homepage. On the left is a navigation bar with a "W" icon highlighted in green, followed by "Endpoints" and other options. In the center is a donut chart with two segments: "default (2)" in green and "N/A (1)" in blue. Below the chart is a section titled "Agents (1)" with a "status=active" filter. It contains a table with the same columns as the previous screenshot, showing one active agent (Debian 13). The bottom of the screen shows "Rows per page: 10" and a page number "1".

MÓDULOS DE WAZUH.

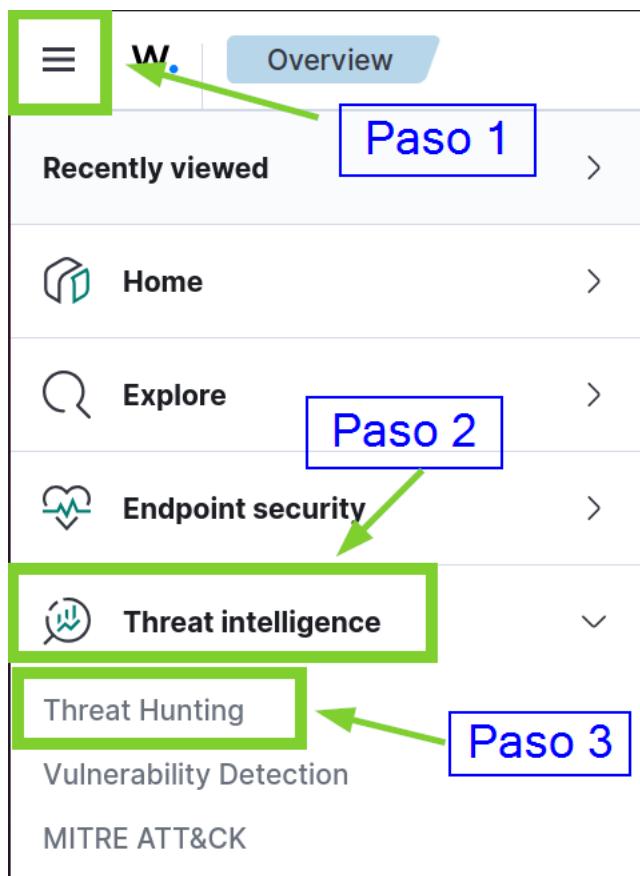
Módulo 1 – Análisis de logs (recolección y normalización).

Lo realiza el agente y el manager al recibir los logs. Los decodificadores (decoders) y las reglas que transforman y normalizan los eventos, están en el conjunto de reglas (ruleset).

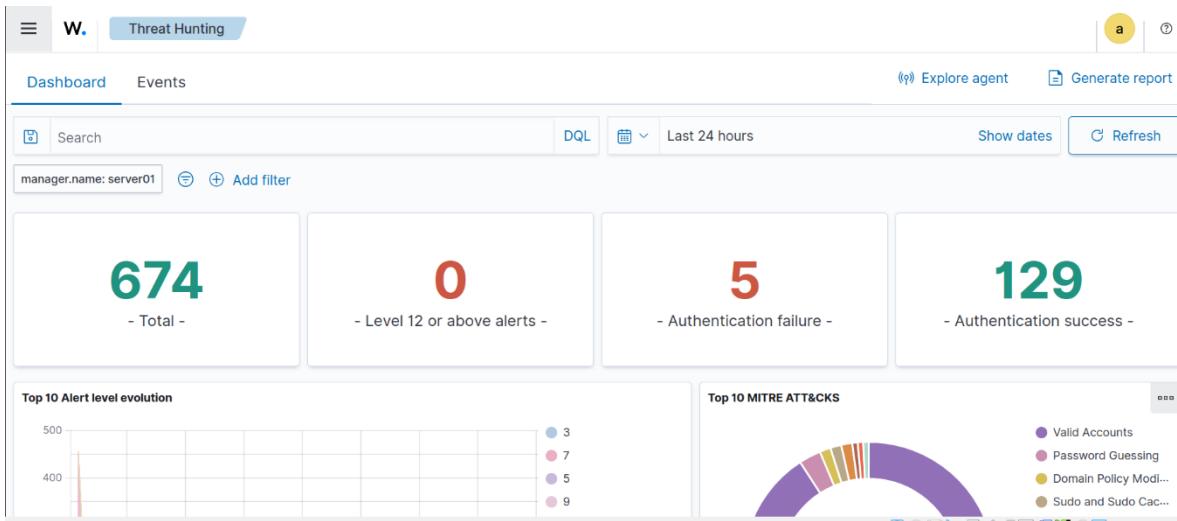
En resumen, este módulo se encarga de recolectar, normalizar y almacenar los logs que envían los agentes.

Pasos para entrar al módulo 1 (Análisis de logs).

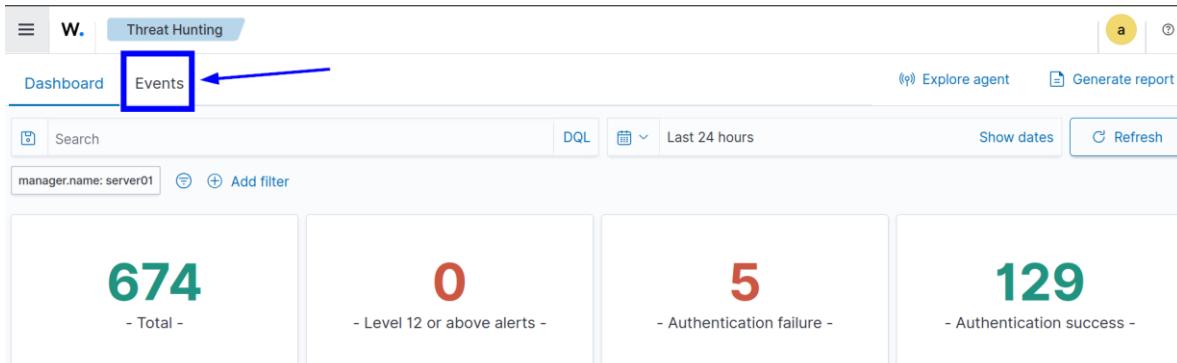
Primero abrimos el panel, dando clic en el botón superior izquierdo. Luego buscamos el módulo Threat Hunting. Aquí es donde se visualizan los resultados combinados del **Módulo 1 (Análisis de logs)**, **Módulo 2 (Detección de intrusos)** y **Módulo 3 (Análisis de seguridad)**.



Ahora, nos mostrará el siguiente panel:



Lo que debemos hacer ahora es dar clic en la etiqueta que dice “Eventos”. Ahí podremos ver los logs que Wazuh esta recibiendo de los agentes.



Al dar clic ahí podremos ver los logs que son enviados a Wazuh.

675 hits					
Oct 30, 2025 @ 03:13:31.637 - Oct 31, 2025 @ 03:13:31.637					
Export Formatted		706 available fields		Columns	
Density				1 fields sorted	Full screen
↓ timestamp	agent.name	rule.description	rule.level	rule.id	rule.level
Oct 31, 2025 @ 03:07:59.285	WIN10-192.168.2.8	Windows Logon Success	3	60106	
Oct 31, 2025 @ 02:55:19.846	WIN10-192.168.2.8	Service startup type was changed	3	61104	
Oct 31, 2025 @ 02:54:54.091	WIN10-192.168.2.8	Windows application error event.	9	60602	
Oct 31, 2025 @ 02:53:08.066	WIN10-192.168.2.8	Windows Logon Success	3	60106	
Oct 31, 2025 @ 02:49:32.982	WIN10-192.168.2.8	Service startup type was changed	3	61104	
Oct 31, 2025 @ 02:48:25.253	WIN10-192.168.2.8	Service startup type was changed	3	61104	
Oct 31, 2025 @ 02:47:26.376	WIN10-192.168.2.8	Service startup type was changed	3	61104	
Oct 31, 2025 @ 02:47:25.828	WIN10-192.168.2.8	Windows Logon Success	3	60106	

Módulo 2 – Detección de intrusos.

El Módulo 2 de Wazuh se centra en la detección de intrusos dentro del sistema y la red. Su función principal es identificar actividades sospechosas o maliciosas mediante el análisis continuo de los registros y eventos que provienen de los agentes instalados en los equipos monitorizados.

En resumen, este módulo es la alarma del sistema:

- Analiza continuamente los registros de los agentes.
- Detecta patrones de intrusión conocidos y comportamientos anómalos.
- Correlaciona eventos para detectar ataques complejos.
- Ayuda a responder rápidamente ante incidentes de seguridad.

En otras palabras, se encarga de analizar los logs que ya procesó el **Módulo 1**, compararlos con sus **reglas de detección**, y generar alertas según el nivel de riesgo.

Pasos para entrar al módulo 2 (Detección de intrusos).

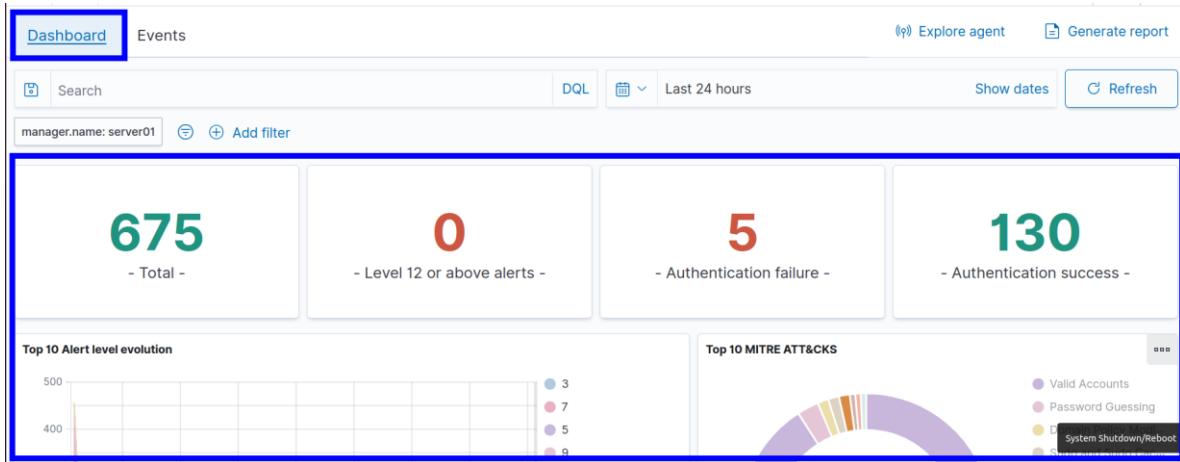
Nos quedamos siempre en el apartado del módulo 1, es decir en la ruta:

Threat Hunting → Dashboard.

Ahí debemos ver los cuadros que dicen:

- Authentication success.
- Authentication failure.
- Level 12 or above alerts
- Total.

Tal como podemos ver en la imagen:



Si nosotros hacemos clic en un número o gráfico, Wazuh abre los eventos que dispararon esas alertas.

Módulo 3 – Análisis de seguridad.

Se enfoca en el **análisis de seguridad integral** del sistema. Su propósito es **evaluar el estado general de la seguridad** de los equipos y servidores monitorizados, verificando configuraciones, políticas, vulnerabilidades y cumplimiento de normas.

Este módulo **recopila y correlaciona los datos de los agentes** para ofrecer una visión completa del nivel de protección y los riesgos existentes.

El análisis de seguridad ayuda a los administradores a **prevenir ataques antes de que ocurran**, reforzando las defensas del sistema mediante acciones correctivas basadas en los reportes generados por Wazuh.

En resumen, este módulo actúa como un auditor de seguridad automatizado que revisa la postura general de los sistemas:

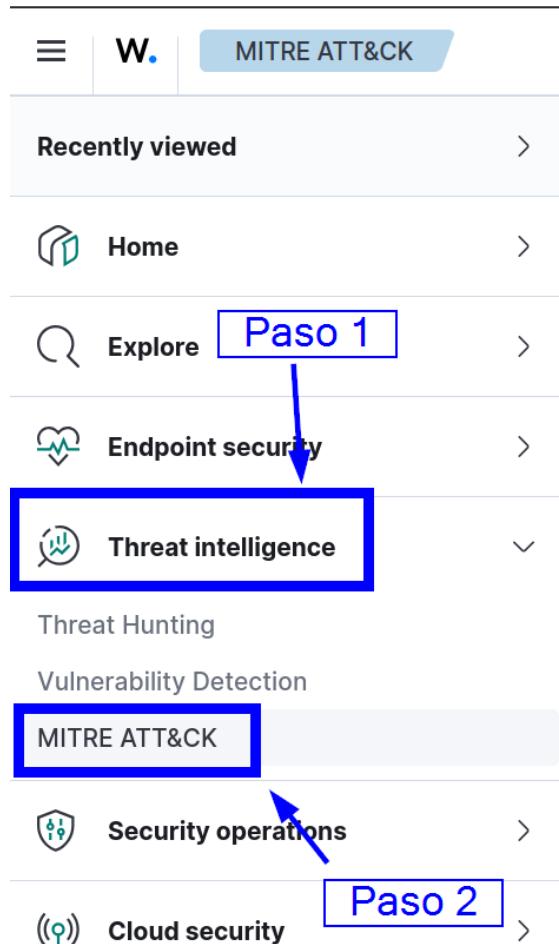
- Evalúa configuraciones y políticas de seguridad.
- Detecta vulnerabilidades y fallos en el sistema.
- Correlaciona eventos para medir el nivel de riesgo.
- Verifica el cumplimiento de estándares y normativas.

Evalúa vulnerabilidades y cumplimiento normativo.

Pasos para entrar al módulo 3 – Análisis de seguridad.

Debemos ir a la ruta:

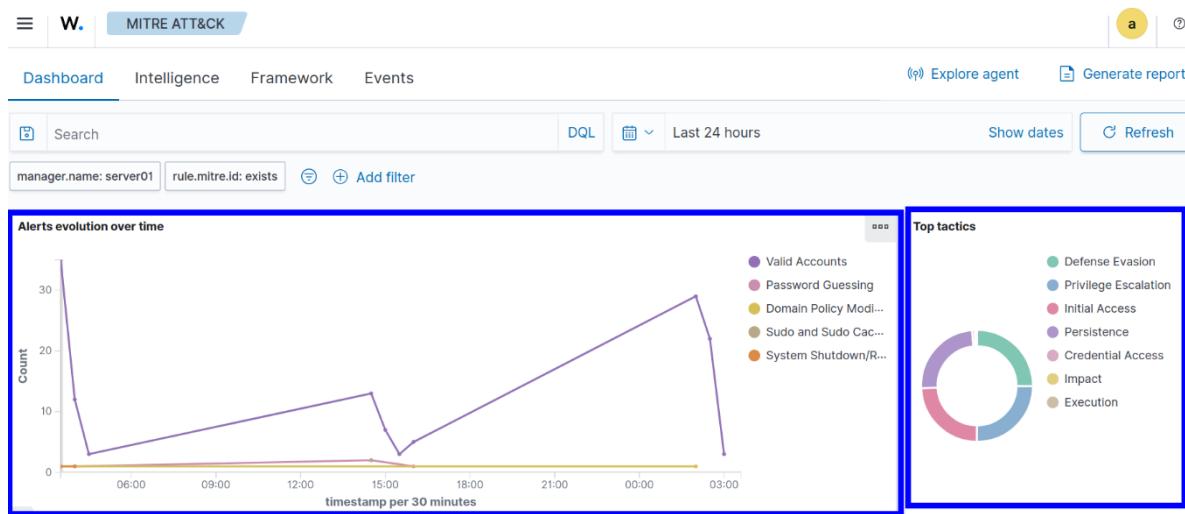
Threat Intelligence → MITRE ATT&CK.



El gráfico de la izquierda (evolución) muestra **cuántas alertas** relacionadas con cada *técnica* ocurrieron a lo largo del tiempo (por ejemplo *Valid Accounts*, *Password Guessing*).

El gráfico circular / Top tactics muestra las tácticas (ej. Credential Access, Privilege Escalation) y la proporción de alertas asociadas.

Estos datos vienen de las reglas que incluyen campos rule.mitre.* (p. ej. rule.mitre.id, rule.mitre.tactic, rule.mitre.technique) — por eso ves rule.mitre.id: exists en el filtro.



Módulo 4 – Detección de vulnerabilidades.

Este módulo analiza los paquetes y programas instalados en tus agentes (Windows, Linux, etc.) y los compara con la base de datos de vulnerabilidades (CVE). Cuando detecta que un software tiene una versión vulnerable, genera una alerta.

Por ejemplo si nuestro agente tiene OpenSSL 1.0.2 y existe una CVE crítica para esa versión, Wazuh mostrará esa vulnerabilidad aquí, con su nivel de riesgo.

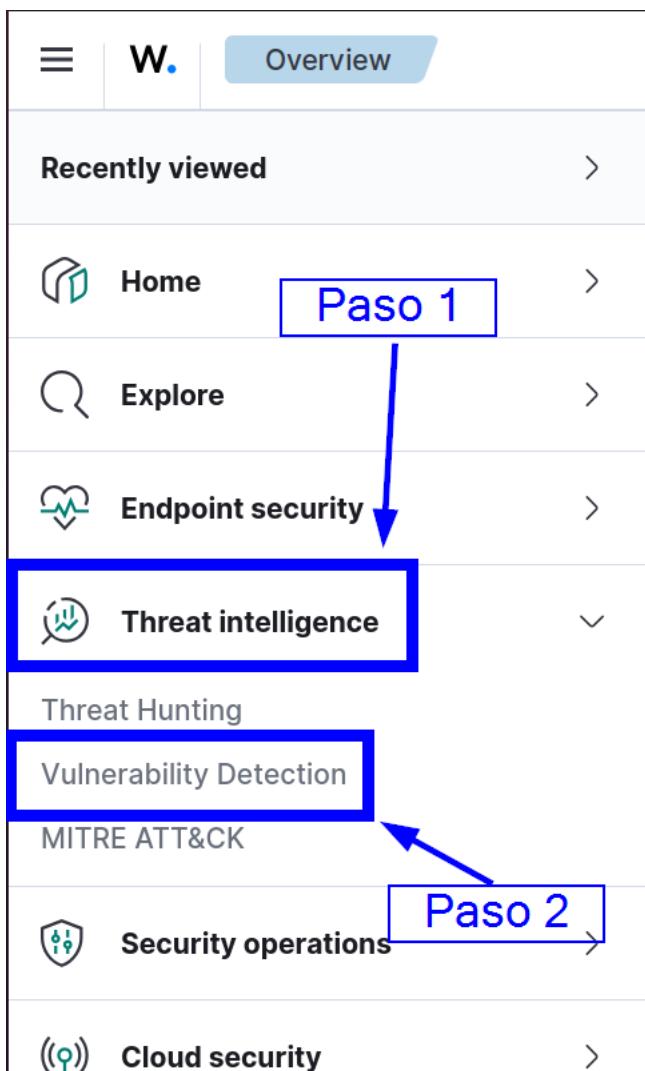
Aquí podemos ver:

- Listado de vulnerabilidades detectadas.
- CVE ID (por ejemplo, CVE-2024-1234).
- Severidad (Critical, High, Medium, Low).
- Nombre del paquete afectado y su versión.

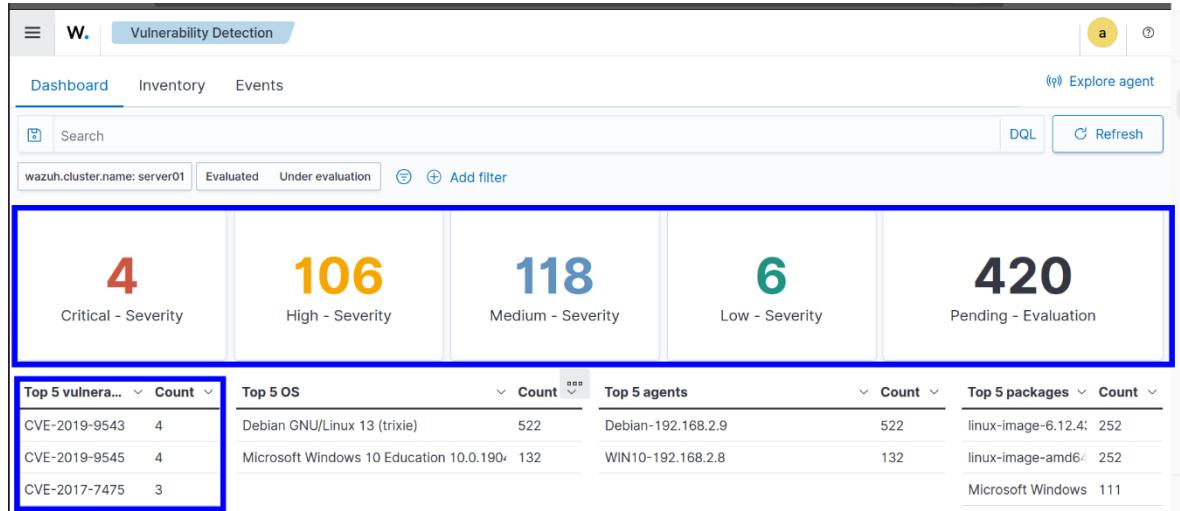
Pasos para entrar al módulo 4 – Detección de vulnerabilidades.

En el menú lateral, debemos seleccionar:

Threat Intelligence → Vulnerability Detection.



Nos abrirá el dashboard donde podremos ver todas las vulnerabilidades detectadas en los agentes, desde las más leves hasta las más graves.



Módulo 5 – Respuesta ante incidentes.

El módulo Active Response ejecuta acciones inmediatas y automáticas cuando se genera una alerta o se detecta un comportamiento peligroso.

Estas acciones pueden incluir:

- Bloquear una IP atacante (por ejemplo, tras un ataque de fuerza bruta).
- Eliminar procesos maliciosos.
- Desconectar un usuario o detener un servicio sospechoso.
- Restaurar configuraciones seguras automáticamente.

Estas respuestas se definen mediante scripts de acción almacenados en el servidor Wazuh (por defecto en /var/ossec/active-response/bin/).