

Gestión de Logs con Wazuh

Este laboratorio demostrará la implementación de Wazuh como sistema de gestión de logs (SIEM) y monitorización de seguridad en tiempo real. Se recopilarán y analizarán eventos de seguridad provenientes de distintos sistemas para detectar incidentes.

Objetivos:

- * **Implementar un servidor Wazuh en Ubuntu.**
- * **Configurar agentes para recolectar logs de hosts y servidores.**
- * **Centralizar logs de autenticación, sistema y red.**
- * **Detectar eventos de seguridad relevantes ej: (ataques de fuerza bruta, escaladas de privilegios).**
- * **Visualizar métricas y alertas mediante Wazuh Dashboards.**

Entorno del laboratorio:

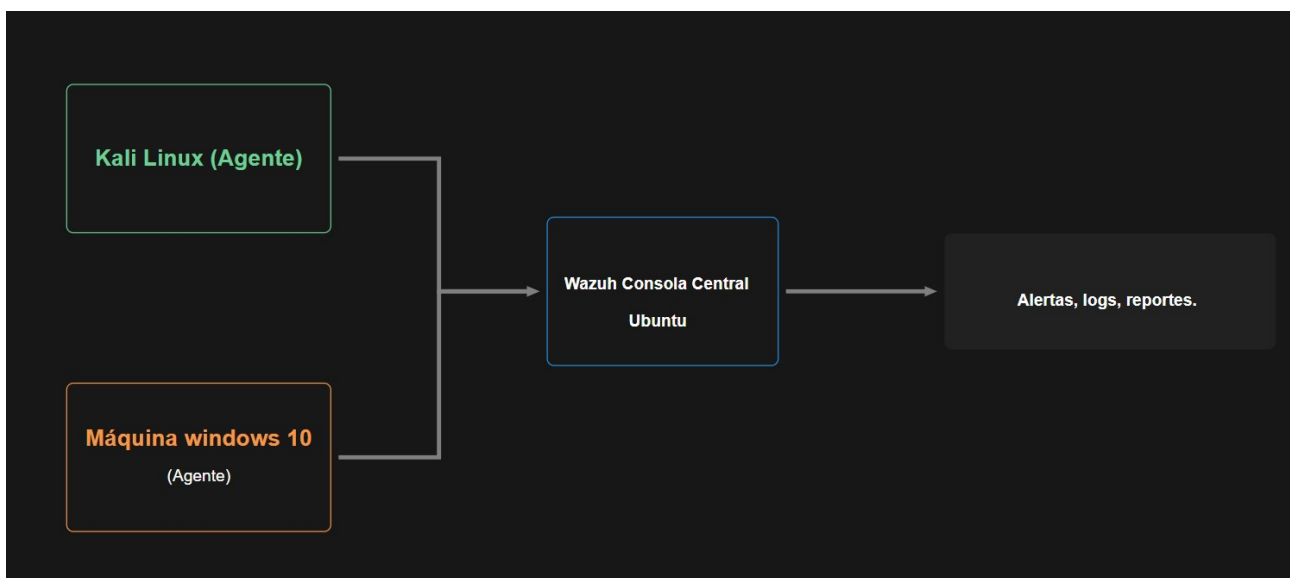
* Servidor SIEM (Wazuh Manager + Filebeat + Dashboards): Ubuntu Server 22.04 LTS → consola central.

*Agentes a monitorear:

- Máquina Kali Linux: Logs de autenticación (/var/log/auth.log) y sistema (/var/log/syslog).
- Windows 10: Logs de eventos de seguridad (Inicios de sesión, escaladas de privilegios, etc).

Red: Entorno en Vmware. (Aplicable también en AWS).

Arquitectura del laboratorio:



1) Implementación

Instalación del Wazuh Manager (Ubuntu).

Comandos:

```
$ sudo curl -O https://packages.wazuh.com/4.8/wazuh-install.sh
```

```
$ sudo bash wazuh-install.sh -a
```

(Instalamos wazuh)

```
mauricio@mauricio-VMware-Virtual-Platform:~$ sudo bash wazuh-install.sh -a
[sudo] contraseña para mauricio:
02/10/2025 01:54:00 INFO: Starting Wazuh installation assistant. Wazuh version: 4.8.2
02/10/2025 01:54:00 INFO: Verbose logging redirected to /var/log/wazuh-install.log
02/10/2025 01:54:01 INFO: Verifying that your system meets the recommended minimum hardware requirements.
02/10/2025 01:54:08 INFO: --- Dependencies ---
02/10/2025 01:54:08 INFO: Installing gawk.
02/10/2025 01:54:13 INFO: Wazuh web interface port will be 443.
02/10/2025 01:54:20 INFO: Wazuh repository added.
02/10/2025 01:54:20 INFO: --- Configuration files ---
```

* Se instaló Wazuh Manager, Filebeat y Dashboards.


* Acceso web: <https://<wazuh-dashboard-ip>:443>


* <https://192.168.220.149:443>

Accedemos a la interfaz gráfica de Wazuh:

wazuh.

The Open Source Security Platform

Username

Password

Log in

Instalación del Agente en Kali Linux

Objetivo: Instalar y configurar el Wazuh Agent en Kali Linux para enviar los eventos de seguridad al Wazuh Manager (Ubuntu).

Comandos:

```
$ sudo curl -O https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.8.2-1_amd64.deb
```

```
(mauricio@kali)-[~]
$ curl -O https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.8.2-1_amd64.deb
```

% Total	% Received	% Xferd	Average Speed	Time	Time	Time	Current
			Dload Upload	Total	Spent	Left	Speed
100	9.7M	100	9.7M	0	0	2374k	0
				0:00:04	0:00:04	--:--:--	2374k

```
$ sudo dpkg -i wazuh-agent_4.8.2-1_amd64.deb
```

```
(mauricio@kali)-[~]
└─$ sudo dpkg -i wazuh-agent_4.8.2-1_amd64.deb
Seleccionando el paquete wazuh-agent previamente no seleccionado.
(Leyendo la base de datos ... 410710 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar wazuh-agent_4.8.2-1_amd64.deb ...
Desempaquetando wazuh-agent (4.8.2-1) ...
Configurando wazuh-agent (4.8.2-1) ...
```

Registrar agente en Wazuh Manager

Comandos:

```
$ sudo /var/ossec/bin/agent-auth -m 192.168.220.149 -p 1515
```

```
(mauricio@kali)-[~]
└─$ sudo /var/ossec/bin/agent-auth -m 192.168.220.149 -p 1515
2025/10/02 02:44:57 agent-auth: INFO: Started (pid: 66415).
2025/10/02 02:44:57 agent-auth: INFO: Requesting a key from server: 192.168.220.149
2025/10/02 02:44:57 agent-auth: INFO: No authentication password provided
2025/10/02 02:44:57 agent-auth: INFO: Using agent name as: kali
2025/10/02 02:44:57 agent-auth: INFO: Waiting for server reply
2025/10/02 02:44:57 agent-auth: INFO: Valid key received
```

- Editamos manualmente el archivo principal del agente para que reconozca el Manager.

```
$ sudo nano /var/ossec/etc/ossec.conf
```

-Reemplazamos

```
<server>
  <address>192.168.220.149</address>
</server>
```

- Reiniciamos el agente y comprobamos status.

```
$ sudo systemctl restart wazuh-agent
```

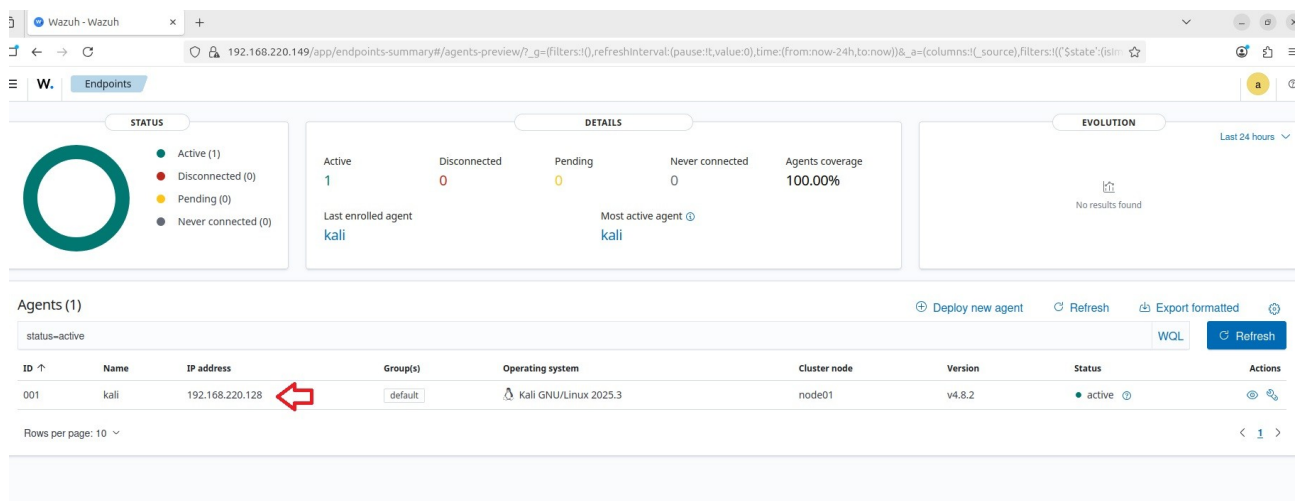
```
$ sudo systemctl status wazuh-agent
```

```
(mauricio@kali)-[~]
└─$ sudo systemctl restart wazuh-agent
sudo systemctl status wazuh-agent

● wazuh-agent.service - Wazuh agent
   Loaded: loaded (/usr/lib/systemd/system/wazuh-agent.service; enabled; preset: disabled)
   Active: active (running) since Thu 2025-10-02 03:35:26 -03; 34ms ago
 Invocation: 45faa0aca99d4f43bd75e53848240ee1
   Process: 68346 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
    Tasks: 32 (limit: 9327)
   Memory: 523.6M (peak: 523.8M)
      CPU: 5.123s
   CGroup: /system.slice/wazuh-agent.service
           └─68368 /var/ossec/bin/wazuh-execd
             └─68376 /var/ossec/bin/wazuh-agentd
               └─68383 /bin/sh active-response/bin/restart.sh agent
                 └─68387 /bin/sh /var/ossec/bin/wazuh-control restart
                   └─68409 /var/ossec/bin/wazuh-syscheckd
                     └─68425 /var/ossec/bin/wazuh-logcollector
                       └─68447 /var/ossec/bin/wazuh-modulesd
                         └─68493 sleep 1

oct 02 03:35:20 kali systemd[1]: Starting wazuh-agent.service - Wazuh agent ...
```

- Accedemos a la interfaz gráfica de Wazuh Manager para comprobar que efectivamente el Agente se conectó a la consola central.

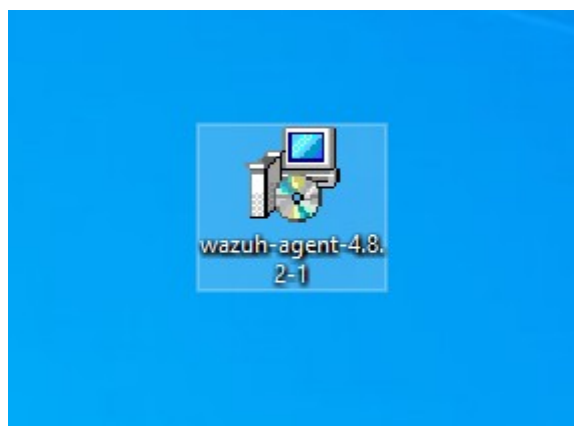


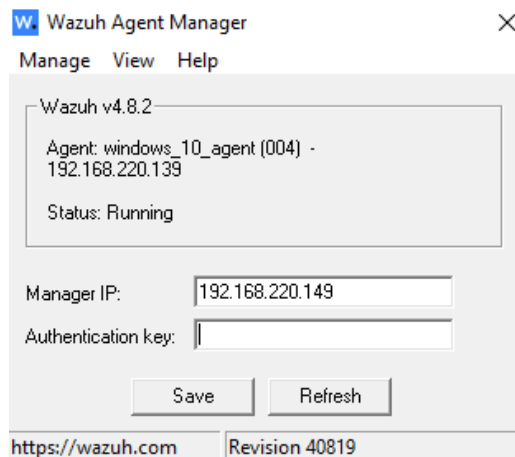
Instalación del segundo Agente en Windows 10

Objetivo: Enviar eventos de seguridad al Wazuh Manager.

- Descargamos el agente <https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-windows.html>

- Ejecutamos el instalador con privilegios de administrador.





- Obtener Authentication key de Wazuh-Manager.

Comandos:

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

- Seleccionar opción “A”.

```
mauricio@mauricio-VMware-Virtual-Platform:~$ sudo /var/ossec/bin/manage_agents
[sudo] contraseña para mauricio:

*****
* Wazuh v4.8.2 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: █
```

- Introducir credenciales del agente Windows 10.

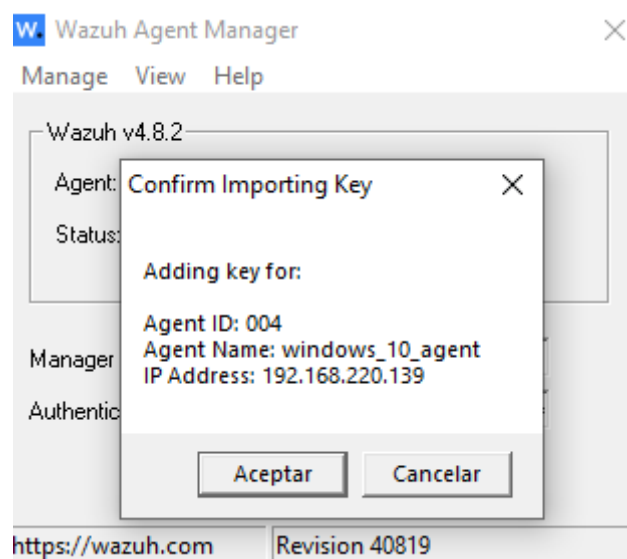
- Credenciales introducidas:

- * A name for the new agent: windows_10_agent
- * The IP Address of the new agent: 192.168.220.139
- Agente agregado como ID 004.
- Seleccionar (E) Extract key for an agent.

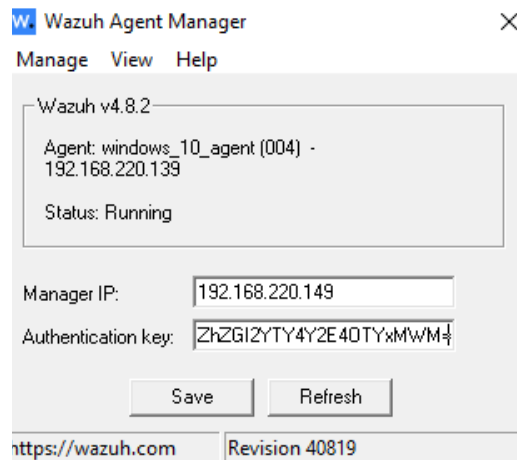
```
*****
* Wazuh v4.8.2 Agent manager.                *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: E

Available agents:
  ID: 001, Name: kali, IP: any
  ID: 004, Name: windows_10_agent, IP: 192.168.220.139
Provide the ID of the agent to extract the key (or '\q' to quit): 004

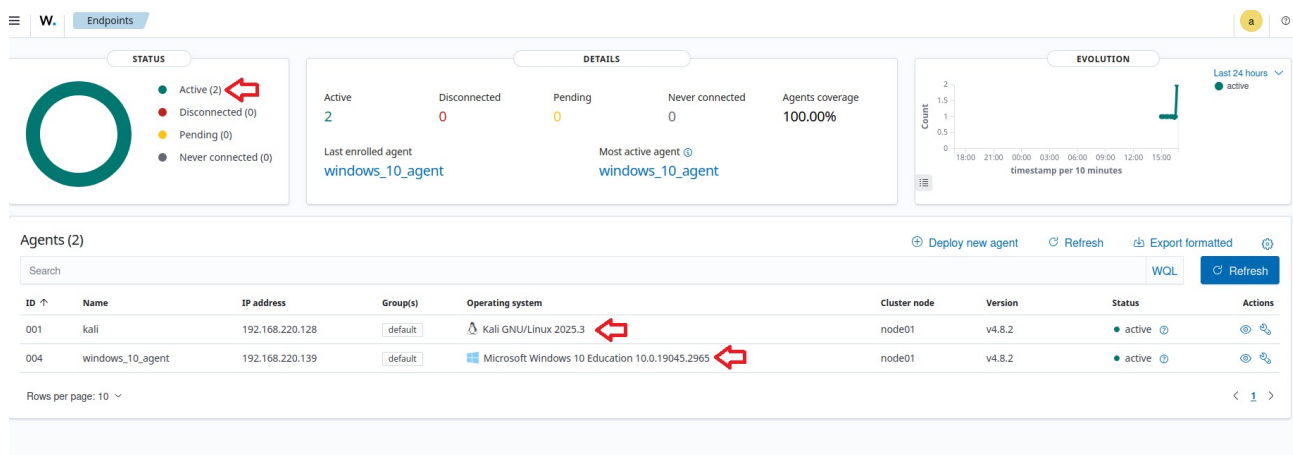
Agent key information for '004' is:
MDA0IHdpbmRvd3NfMTBfYWdlbnQgMTkyLjE2OC4yMjAuMTM5IGU0MWMzMmE2Y2ZkNGRkYTRhNTM1YjRm
OGUzOWE5MmU0ODNkNGM5ZTQzOTNjZTFLOWZhZGI2YTY4Y2E4OTYxMWM=
```



- Introducir el auth key en el agente de Windows 10.



Una vez hecho esto, el Wazuh Manager reconoce ambos endpoints (Kali y Windows 10).



Visualización de eventos por terminal

- Ubicación de los logs en Wazuh Manager

`/var/ossec/logs/alerts/alerts.json`

`$ sudo tail -f /var/ossec/logs/alerts/alerts.json`

- Logs generales de Wazuh

`/var/ossec/logs/ossec.log`

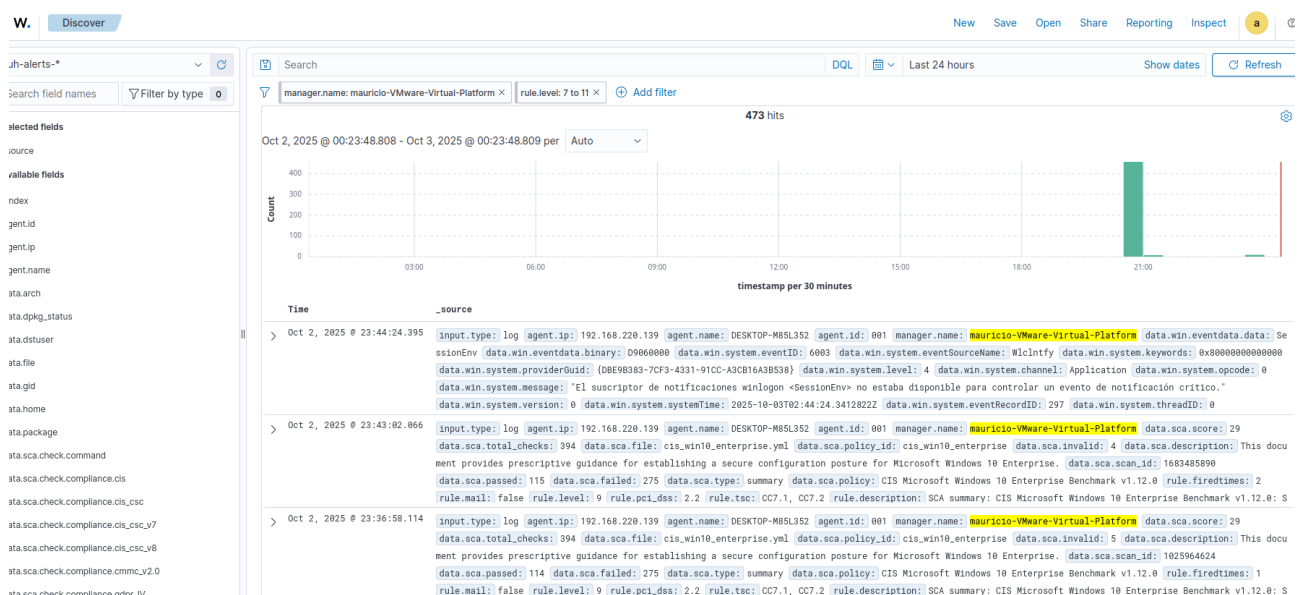
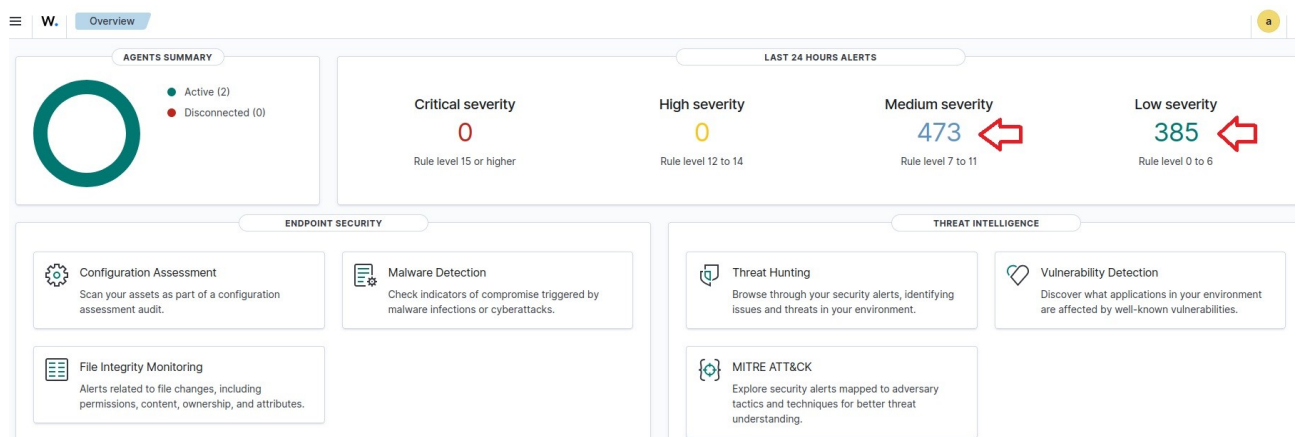
`$ sudo tail -f /var/ossec/logs/ossec.log`

- Comando para ver logs en tiempo real

\$ sudo tail -f /var/ossec/logs/alerts/alerts.json

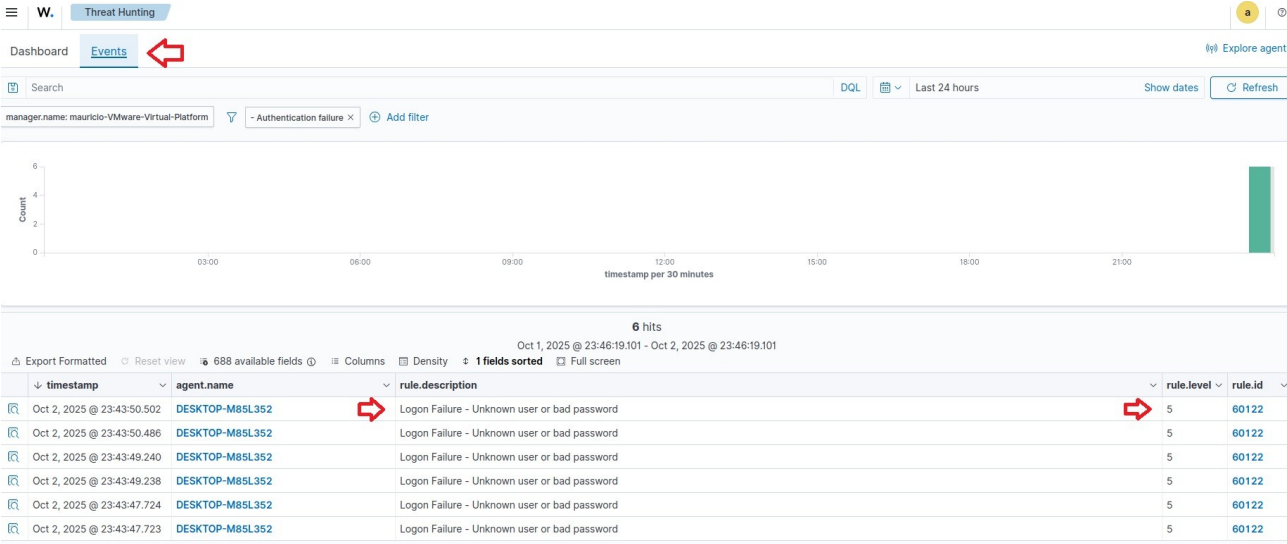
```
mauricio@mauricio-VMware-Virtual-Platform:~$ sudo tail -f /var/ossec/logs/alerts/alerts.json
[sudo] contraseña para mauricio:
{"timestamp":"2025-10-02T23:37:17.429-0300","rule":{"level":3,"description":"Service startup type was changed","id":"61104","info":"This does not appear to be logged on Windows 2000","firedtimes":2,"mail":false,"groups":["windows","windows_system","policy_changed"],"pci_dss":["10.6"],"gdpr":["IV_35.7.d"],"hipaa":["164.312.b"],"nist_800_53":["AU.6"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"001","name":"DESKTOP-M85L352","ip":"192.168.220.139"},"manager":{"name":"mauricio-VMware-Virtual-Platform","id":"1759459037.2858265"},"decoder":{"name":"windows_eventchannel"},"data":{"win":{"system":{"providerName":"Service Control Manager","providerGuid":"{555908d1-a6d7-4695-8e1e-26931d2012f4}","eventSourceName":"Service Control Manager","eventID":"7040","version":"0","level":"4","task":"0","opcode":"0","keywords":"0x8080000000000000","systemTime":"2025-10-03T02:37:16.3594368Z","eventRecordID":"840","processID":"628","threadID":"732","channel":"System","computer":"DESKTOP-M85L352","severityValue":"INFORMATION","message":"\n
```

Visualización de eventos en Interfaz gráfica:



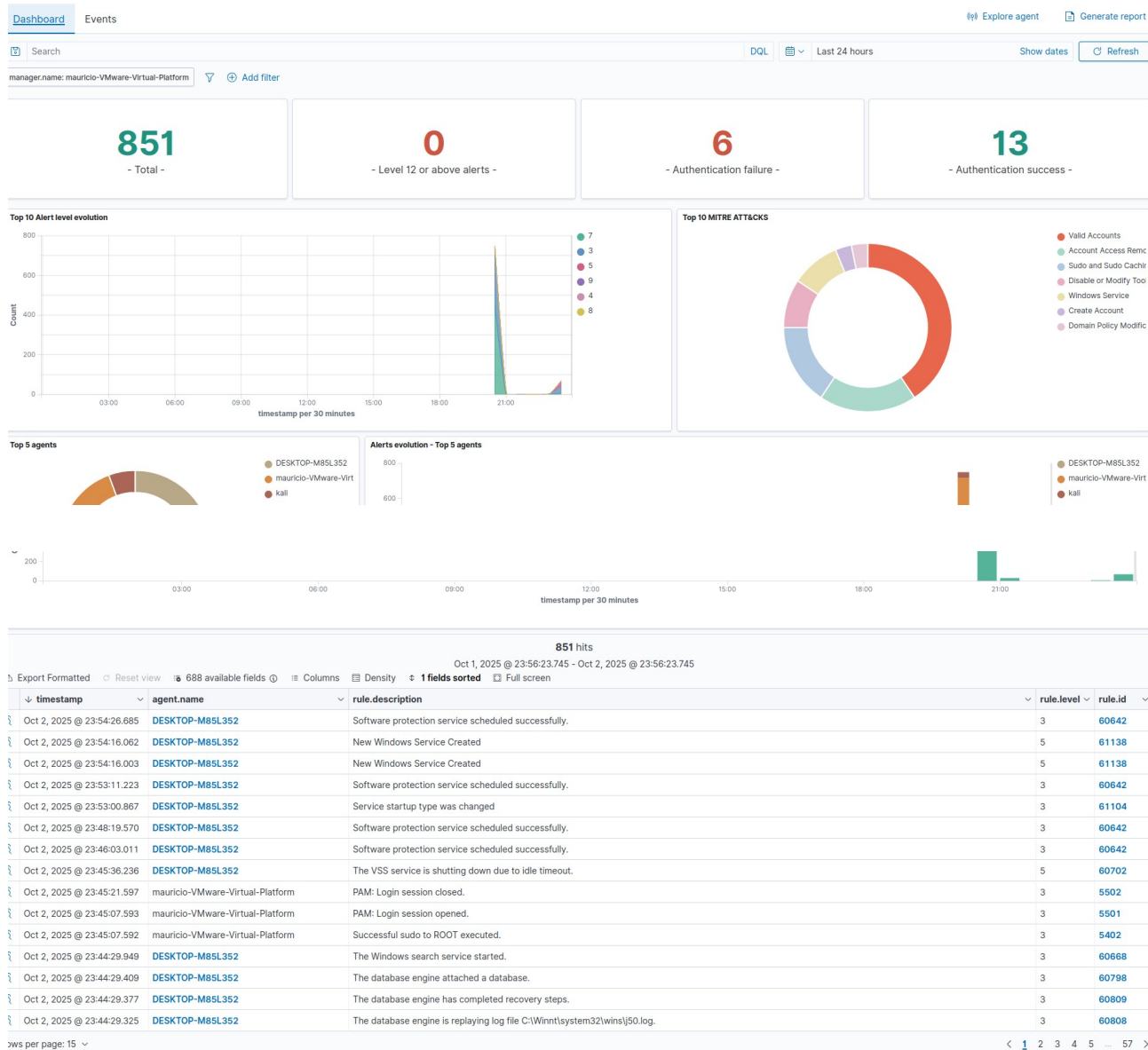
- Generar un evento en Windows 10 fallando repetidamente el login:

Alertas:

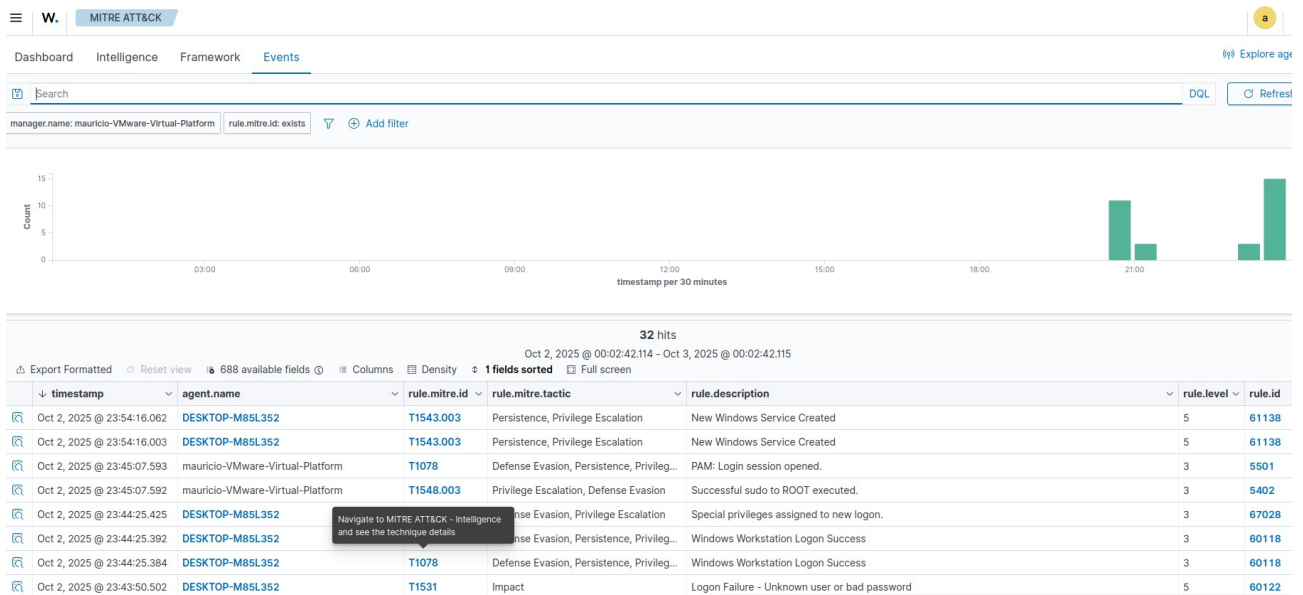


timestamp	agent.name	rule.description	rule.level	rule.id
Oct 2, 2025 @ 23:43:50.502	DESKTOP-M85L352	Logon Failure - Unknown user or bad password	5	60122
Oct 2, 2025 @ 23:43:50.486	DESKTOP-M85L352	Logon Failure - Unknown user or bad password	5	60122
Oct 2, 2025 @ 23:43:49.240	DESKTOP-M85L352	Logon Failure - Unknown user or bad password	5	60122
Oct 2, 2025 @ 23:43:49.238	DESKTOP-M85L352	Logon Failure - Unknown user or bad password	5	60122
Oct 2, 2025 @ 23:43:47.724	DESKTOP-M85L352	Logon Failure - Unknown user or bad password	5	60122
Oct 2, 2025 @ 23:43:47.723	DESKTOP-M85L352	Logon Failure - Unknown user or bad password	5	60122

Eventos centralizados por Wazuh la infraestructura:



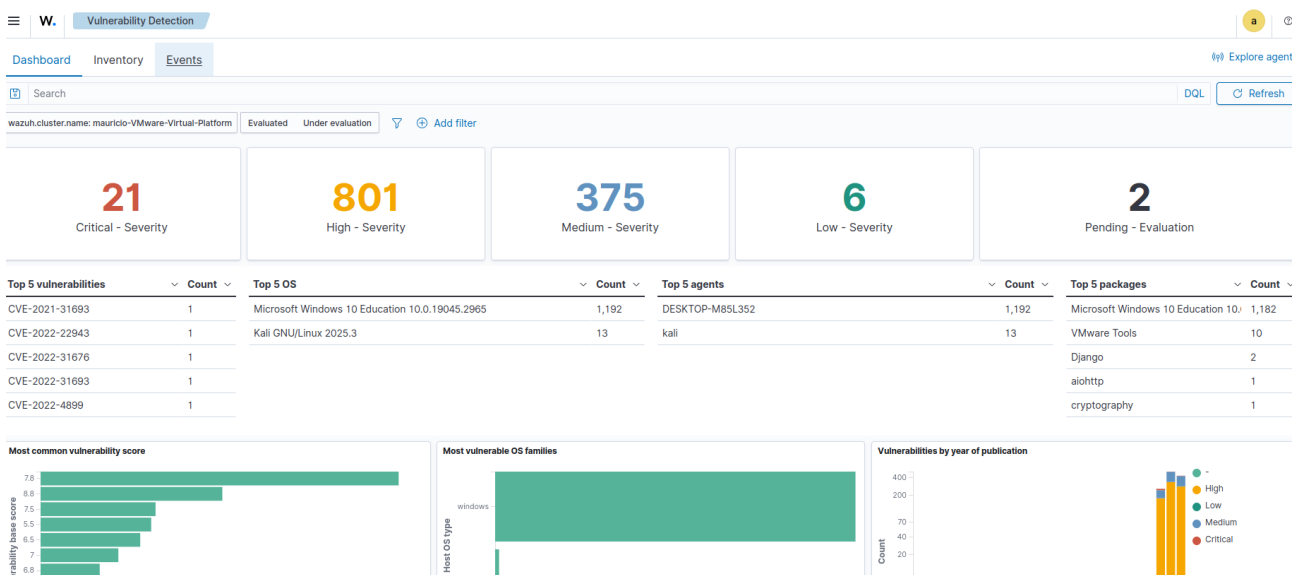
MITRE ATT&CK



- MITRE ATT&CK es un framework público que describe técnicas y tácticas utilizadas por atacantes en entornos de TI.

* Táctica: El objetivo o categoría del comportamiento del atacante por ejemplo:(Privilege Escalation, Persistence).

Detección de vulnerabilidades:



W. Vulnerability Detection

DashboardInventoryEvents

Search

wazuh.cluster.name: mauricio-VMware-Virtual-Platform

EvaluatedUnder evaluation

Add filter

1,205 hits

Export Formatted

Reset view

48 available fields

Columns

Density

Sort fields

Full screen

agent.name	package.name	package.version	vulnerability.description	vulnerability.severity	vulnerability.id
DESKTOP-M85L352	Microsoft Windows 10 Education 10.0.19...	10.0.19045.2965	Concurrent execution using shared resour...	High	CVE-2025-59220
DESKTOP-M85L352	Microsoft Windows 10 Education 10.0.19...	10.0.19045.2965	Time-of-check time-of-use (toctou) race ...	High	CVE-2025-55236
DESKTOP-M85L352	Microsoft Windows 10 Education 10.0.19...	10.0.19045.2965	SMB Server might be susceptible to relay ...	High	CVE-2025-55234
DESKTOP-M85L352	Microsoft Windows 10 Education 10.0.19...	10.0.19045.2965	Improper verification of cryptographic sig...	Medium	CVE-2025-55229
DESKTOP-M85L352	Microsoft Windows 10 Education 10.0.19...	10.0.19045.2965	Concurrent execution using shared resour...	High	CVE-2025-55223
DESKTOP-M85L352	Microsoft Windows 10 Education 10.0.19...	10.0.19045.2965	Concurrent execution using shared resour...	High	CVE-2025-54919
DESKTOP-M85L352	Microsoft Windows 10 Education 10.0.19...	10.0.19045.2965	Missing authentication for critical functio...	High	CVE-2025-53789
DESKTOP-M85L352	Microsoft Windows 10 Education 10.0.19...	10.0.19045.2965	Access of resource using incompatible ty...	High	CVE-2025-53724
DESKTOP-M85L352	Microsoft Windows 10 Education 10.0.19...	10.0.19045.2965	Use after free in Windows Connected De...	High	CVE-2025-53721
DESKTOP-M85L352	Microsoft Windows 10 Education 10.0.19...	10.0.19045.2965	Null pointer dereference in Windows Loca...	Medium	CVE-2025-53716
DESKTOP-M85L352	Microsoft Windows 10 Education 10.0.19...	10.0.19045.2965	Null pointer dereference in Windows Ancil...	High	CVE-2025-53154
DESKTOP-M85L352	Microsoft Windows 10 Education 10.0.19...	10.0.19045.2965	Use after free in Windows Kernel allows a...	High	CVE-2025-53151
DESKTOP-M85L352	Microsoft Windows 10 Education 10.0.19...	10.0.19045.2965	Heap-based buffer overflow in Kernel Str...	High	CVE-2025-53149

Beneficios demostrados:

- Permite ver logs centralizados.
- Monitorización en tiempo real y detección de incidentes de seguridad.
- Facilita correlación de eventos entre distintos sistemas y hosts.
- Permite auditorías y cumplimiento normativo (PCI DSS, HIPAA, GDPR, etc.).
- Clasifica eventos según MITRE ATT&CK, ayudando a identificar tácticas y técnicas usadas por posibles atacantes.

En resumen: Wazuh ayuda a que una empresa cumpla con regulaciones al demostrar que registra, monitorea y responde a eventos de seguridad relevantes. Esto reduce riesgos legales y financieros y facilita las auditorías.