

## **Laboratorio #2**

### **Estudiante:**

Andrés Arias Medina

### **Curso**

Seguridad en los Datos

### **Profesor**

Javier Omar Contreras Rodriguez



Universidad Pontificia Bolivariana

10 de septiembre de 2024

Medellín, Colombia

Lo primero a realizar fue la instalación de Wazuh localmente siguiendo los pasos de la documentación. Se habilitaron los certificados para permitir los certificados entre los tres contenedores y se ejecutó el docker-compose dentro de la carpeta de single-node.

```
andresariasmedina@Andress-MacBook-Pro ~ % cd Documents/UPB/SeguridadDatos
andresariasmedina@Andress-MacBook-Pro SeguridadDatos % git clone https://github.com/wazuh/wazuh-docker.git -b v4.9.0
Cloning into 'wazuh-docker'...
remote: Enumerating objects: 13558, done.
remote: Counting objects: 100% (878/878), done.
remote: Compressing objects: 100% (470/470), done.
remote: Total 13558 (delta 437), reused 779 (delta 377), pack-reused 12680 (from 1)
Receiving objects: 100% (13558/13558), 314.63 MiB | 19.92 MiB/s, done.
Resolving deltas: 100% (7062/7062), done.
Note: switching to 'cb63566719ce2e78b9d3c111a0a61d743fc699fc'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

    git switch -c <new-branch-name>

Or undo this operation with:

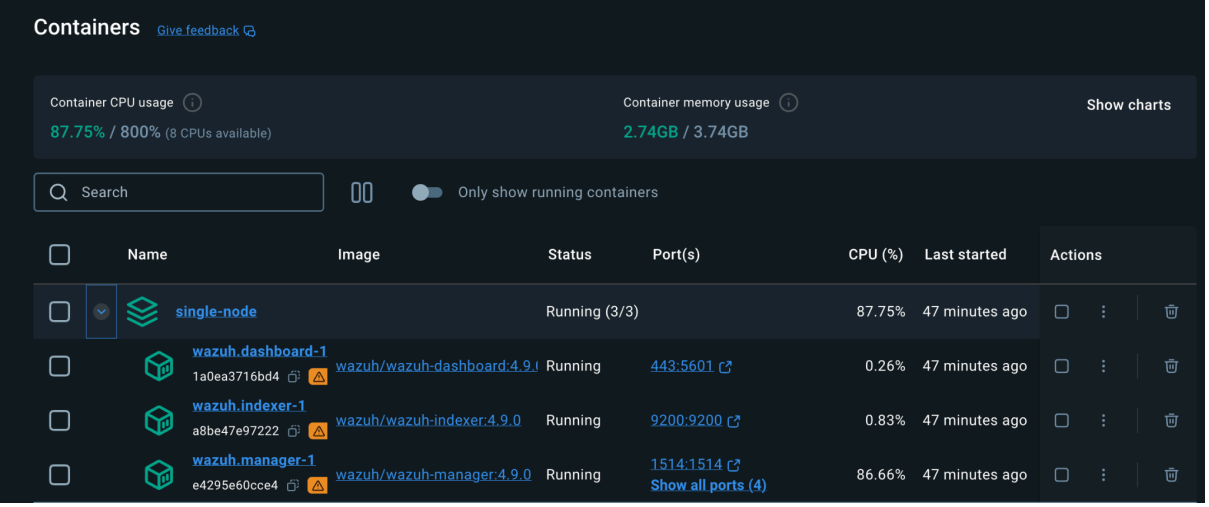
    git switch -

Turn off this advice by setting config variable advice.detachedHead to false
```

```
andresariasmedina@Andress-MacBook-Pro SeguridadDatos % cd wazuh-docker/single-node
andresariasmedina@Andress-MacBook-Pro single-node % docker-compose -f generate-indexer-certs.yml run --rm generator
WARN[0000] /Users/andresariasmedina/Documents/UPB/SeguridadDatos/wazuh-docker/single-node/generate-indexer-certs.yml: 'version' is obsolete
The tool to create the certificates exists in the in Packages bucket
15/09/2024 09:03:40 INFO: Generating the root certificate.
15/09/2024 09:03:40 INFO: Generating Admin certificates.
15/09/2024 09:03:41 INFO: Admin certificates created.
15/09/2024 09:03:41 INFO: Generating Wazuh indexer certificates.
15/09/2024 09:03:41 INFO: Wazuh indexer certificates created.
15/09/2024 09:03:41 INFO: Generating Filebeat certificates.
15/09/2024 09:03:41 INFO: Wazuh Filebeat certificates created.
15/09/2024 09:03:41 INFO: Generating Wazuh dashboard certificates.
15/09/2024 09:03:41 INFO: Wazuh dashboard certificates created.
Moving created certificates to the destination directory
Changing certificate permissions
Setting UID indexer and dashboard
Setting UID for wazuh manager and worker
```

```
andresariasmedina@Andress-MacBook-Pro single-node % docker-compose up -d
WARN[0000] /Users/andresariasmedina/Documents/UPB/SeguridadDatos/wazuh-docker/single-node/docker-compose.yml: 'version' is obsolete
[*] Running 44/3
  ✓ wazuh.manager Pulled
  ✓ wazuh.dashboard Pulled
  ✓ wazuh.indexer Pulled
[*] Running 17/16
  ✓ Volume "single-node_wazuh_api_configuration"
    Created 0.0s Created0.0s single-node_wazuh_etc"
s* Created 0.0s Created0.0s single-node_wazuh_var_multigroup
  ✓ Volume "single-node_wazuh_agentless"
    Created 0.0s Created0.0s single-node_wazuh_wodles"
  ✓ Volume "single-node_wazuh_var_multigroups"
    Created 0.0s Created0.0s single-node_filebeat_var"
  ✓ Volume "single-node_wazuh-dashboard-config"
    Created 0.0s Created0.0s single-node_wazuh_queue"
  ✓ Volume "single-node_wazuh_wodles"
    Created 0.0s Created0.0s single-node_wazuh-dashboard-cust
on* Created 0.0s Created0.0s single-node_filebeat_etc"
  ✓ Volume "single-node_wazuh_logs"
    Created 0.0s Created0.0s single-node-wazuh.indexer-1
  ✓ Volume "single-node_filebeat_var"
    Created 0.0s
  Creating
  ✓ Volume "single-node_wazuh_integrations"
  ✓ Volume "single-node_wazuh_api_configuration"
  ✓ Volume "single-node_wazuh_etc"
  ✓ Volume "single-node_wazuh_agentless"
  ✓ Volume "single-node_wazuh_var_multigroups"
  ✓ Volume "single-node_wazuh-dashboard-config"
  ✓ Volume "single-node_wazuh_wodles"
  ✓ Volume "single-node_wazuh_logs"
  ✓ Volume "single-node_filebeat_var"
  ✓ Volume "single-node_wazuh_integrations"
  ✓ Volume "single-node_wazuh_queue"
  ✓ Volume "single-node_wazuh_api_configuration"
  ✓ Volume "single-node_wazuh_etc"
  ✓ Volume "single-node_wazuh_agentless"
  ✓ Volume "single-node_wazuh_var_multigroups"
  ✓ Volume "single-node_wazuh-dashboard-config"
  ✓ Volume "single-node_wazuh_wodles"
  ✓ Volume "single-node_wazuh_logs"
  ✓ Volume "single-node_filebeat_var"
  ✓ Volume "single-node_wazuh_integrations"
  ✓ Volume "single-node_wazuh_queue"
```

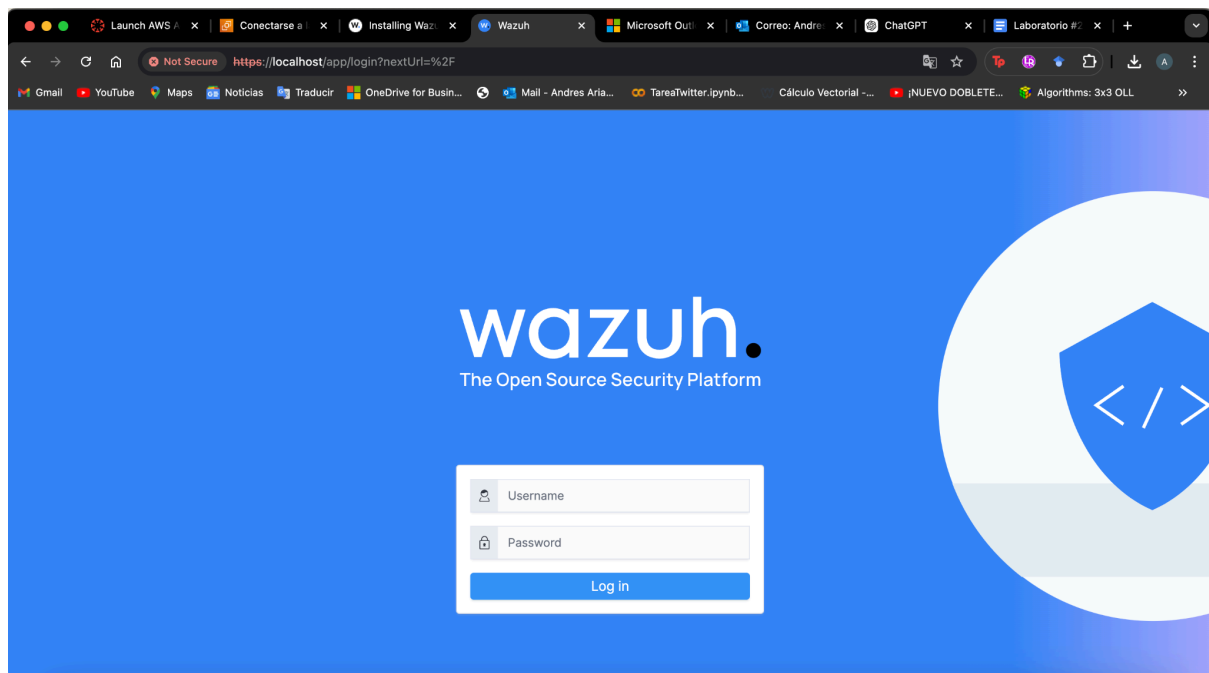
Una vez se clonó el repo de Wazuh y se ejecutó lo anterior el resultado en Docker Desktop fue el siguiente.



The screenshot shows the Docker Desktop interface. At the top, it displays 'Containers' with a 'Give feedback' link. Below this, there are two summary cards: 'Container CPU usage' at 87.75% / 800% (8 CPUs available) and 'Container memory usage' at 2.74GB / 3.74GB. A 'Show charts' link is also present. A search bar and a toggle for 'Only show running containers' are located below the summary cards. The main part of the interface is a table of containers.

	Name	Image	Status	Port(s)	CPU (%)	Last started	Actions
<input type="checkbox"/>	single-node		Running (3/3)		87.75%	47 minutes ago	<input type="checkbox"/> ⋮ 🗑️
<input type="checkbox"/>	wazuh.dashboard-1 1a0ea3716bd4	wazuh/wazuh-dashboard:4.9.0	Running	443:5601	0.26%	47 minutes ago	<input type="checkbox"/> ⋮ 🗑️
<input type="checkbox"/>	wazuh.indexer-1 a8be47e97222	wazuh/wazuh-indexer:4.9.0	Running	9200:9200	0.83%	47 minutes ago	<input type="checkbox"/> ⋮ 🗑️
<input type="checkbox"/>	wazuh.manager-1 e4295e60cce4	wazuh/wazuh-manager:4.9.0	Running	1514:1514 <a href="#">Show all ports (4)</a>	86.66%	47 minutes ago	<input type="checkbox"/> ⋮ 🗑️

Luego ingresamos en un browser a <https://localhost:443>

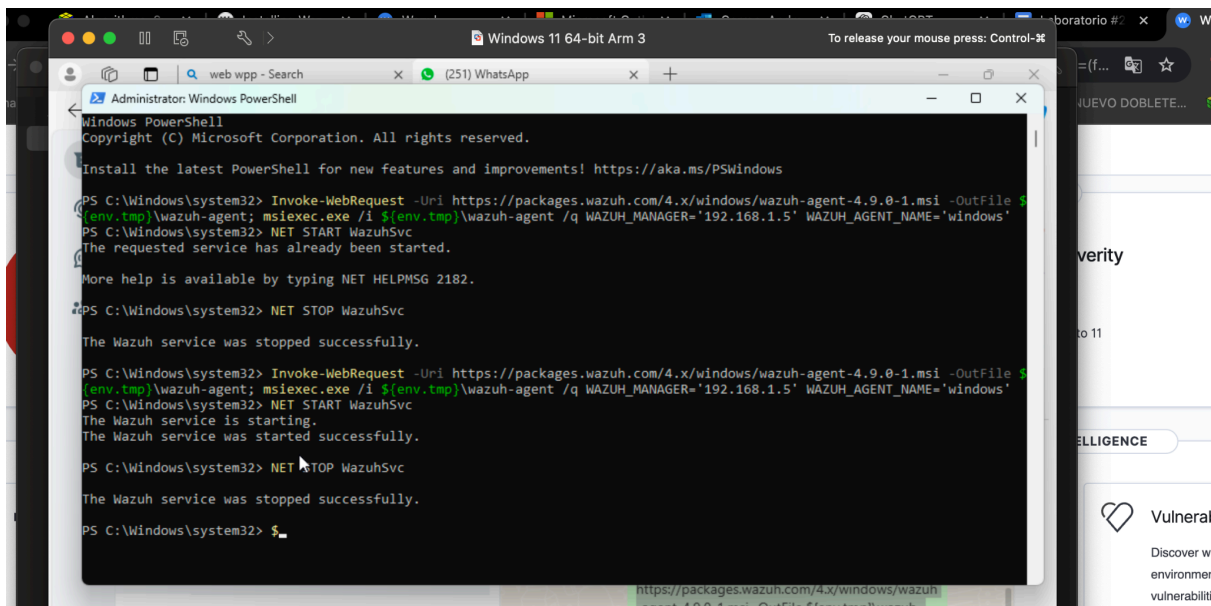


Nos autenticamos con el usuario y clave que da la documentación por defecto.

El siguiente paso es crear una máquina virtual para desplegar el agente. En mi caso creé dos VM, una en la nube con AWS y otra local con VMWare.

Cuando intente desplegar el agente en la máquina de VMWare arrojaba error a la hora inicializar el agente con NET START Wazuh. Traté de corregirlo de todas las formas posibles pero de ninguna forma funcionó. Abandoné esta alternativa debido a que mi computador no aguantó la cantidad de procesos simultáneos generados por los contenedores activos y el particionamiento de los recursos con la máquina virtual.

De veras que intente de todo, al final ya me tocó dejarlo. También implementé la solución propuesta en clase pero tampoco funcionó.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.9.0-1.msi -OutFile $(env:tmp)\wazuh-agent; msixexec.exe /i $(env:tmp)\wazuh-agent /q WAZUH_MANAGER='192.168.1.5' WAZUH_AGENT_NAME='windows'
PS C:\Windows\system32> NET START WazuhSvc
The requested service has already been started.

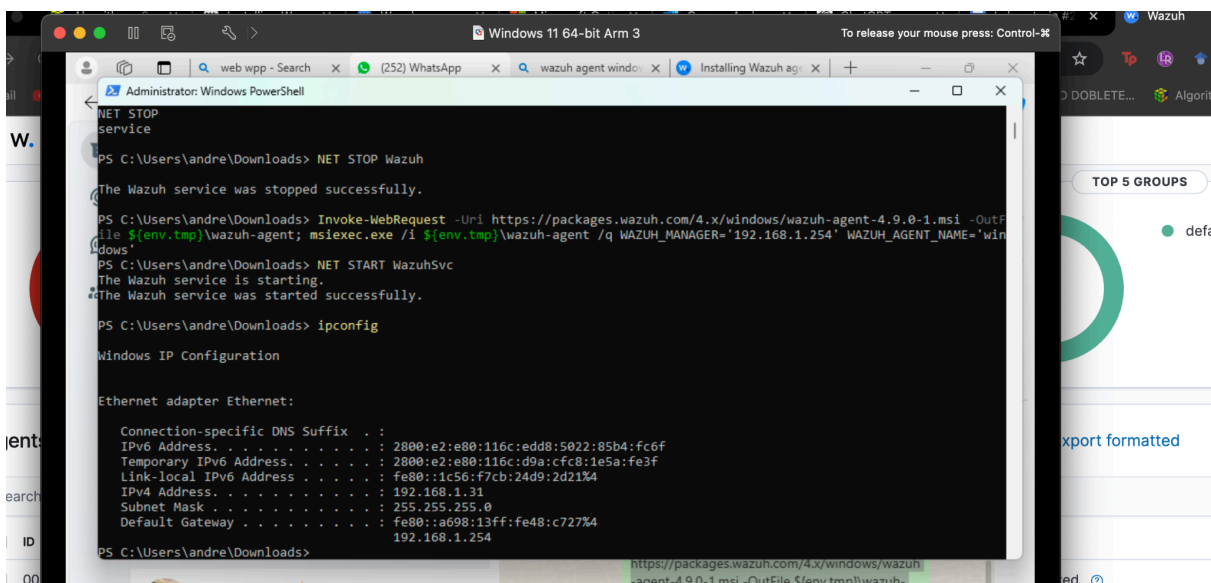
More help is available by typing NET HELPMSG 2182.

PS C:\Windows\system32> NET STOP WazuhSvc
The Wazuh service was stopped successfully.

PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.9.0-1.msi -OutFile $(env:tmp)\wazuh-agent; msixexec.exe /i $(env:tmp)\wazuh-agent /q WAZUH_MANAGER='192.168.1.5' WAZUH_AGENT_NAME='windows'
PS C:\Windows\system32> NET START WazuhSvc
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\Windows\system32> NET STOP WazuhSvc
The Wazuh service was stopped successfully.

PS C:\Windows\system32> $
```



```
Administrator: Windows PowerShell
NET STOP
Service
PS C:\Users\andre\Downloads> NET STOP Wazuh
The Wazuh service was stopped successfully.

PS C:\Users\andre\Downloads> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.9.0-1.msi -OutFile $(env:tmp)\wazuh-agent; msixexec.exe /i $(env:tmp)\wazuh-agent /q WAZUH_MANAGER='192.168.1.254' WAZUH_AGENT_NAME='windows'
PS C:\Users\andre\Downloads> NET START WazuhSvc
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\Users\andre\Downloads> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . : 
IPv6 Address. . . . . : 2800:e2:e80:116c:edd8:5022:85b4:fc6f
Temporary IPv6 Address. . . . . : 2800:e2:e80:116c:d9a:cfc8:1e5a:fe3f
Link-local IPv6 Address . . . . . : fe80::1c56:f7cb:24d9:2d21%4
IPv4 Address. . . . . : 192.168.1.31
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::a698:13ff:fe48:c727%4
192.168.1.254

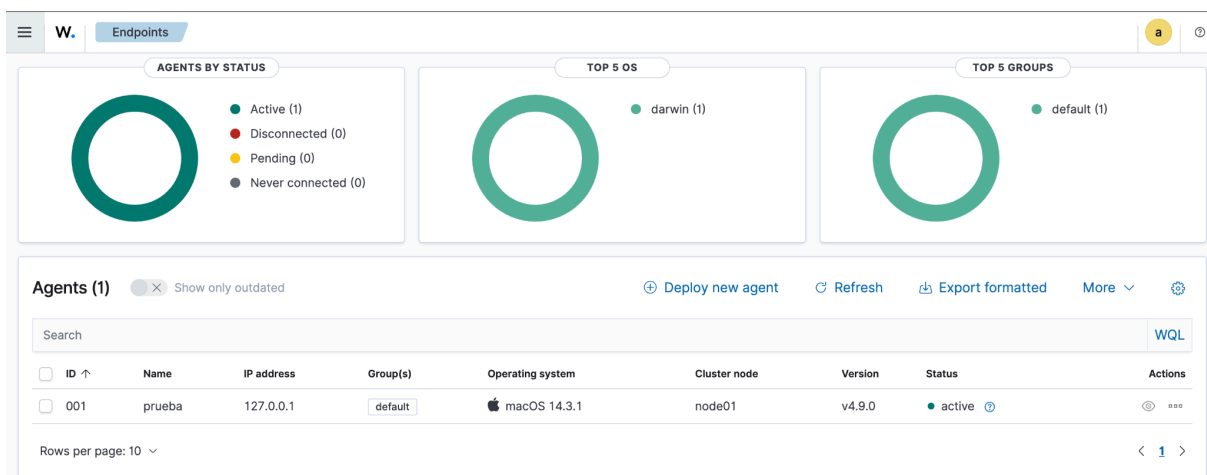
PS C:\Users\andre\Downloads>
```

Procedí con AWS generando una VM con Windows. En este caso sí pude activar el agente pero a la hora de conectar el agente con el Wazuh de mi

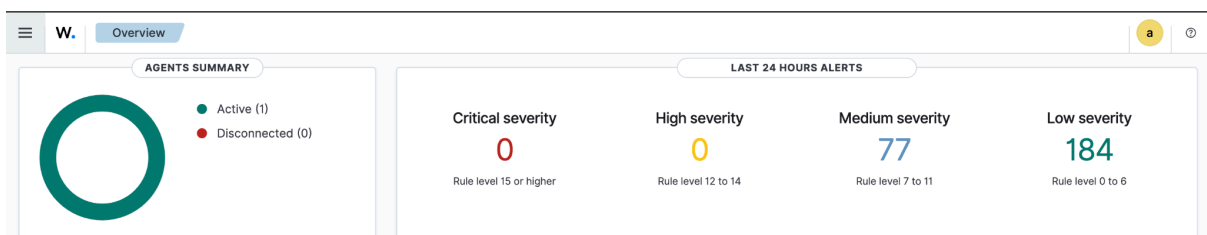
máquina local fue otro problemón. De veras que dedique horas a intentar solucionarlo, probando alternativas de configuraciones, habilitación de puertos y manejo de direcciones IP. De ninguna forma funcionó.

Así que, como última instancia desplegué el agente de forma local en mi Mac con procesador ARM.

```
andresariasmedina@Andress-MacBook-Pro ~ % curl -so wazuh-agent.pkg https://packages.wazuh.com/4.x/macos/wazuh-agent-4.9.0-1.arm64.pkg && echo "WAZUH_MANAGER='127.0.0.1' && WAZUH_AGENT_NAME='prueba'" > /tmp/wazuh_envs && sudo installer -pkg ./wazuh-agent.pkg -target /
Password:
installer: Package name is Wazuh Agent
installer: Installing at base path /
installer: The install was successful.
andresariasmedina@Andress-MacBook-Pro ~ % sudo /Library/OSsec/bin/wazuh-control start
Starting Wazuh v4.9.0...
Started wazuh-execd...
Started wazuh-agentd...
Started wazuh-syscheckd...
Started wazuh-logcollector...
Started wazuh-modulesd...
Completed.
```



Para realizar el análisis podemos seleccionar alguna de las categorías.



0

Critical - Severity

44

High - Severity

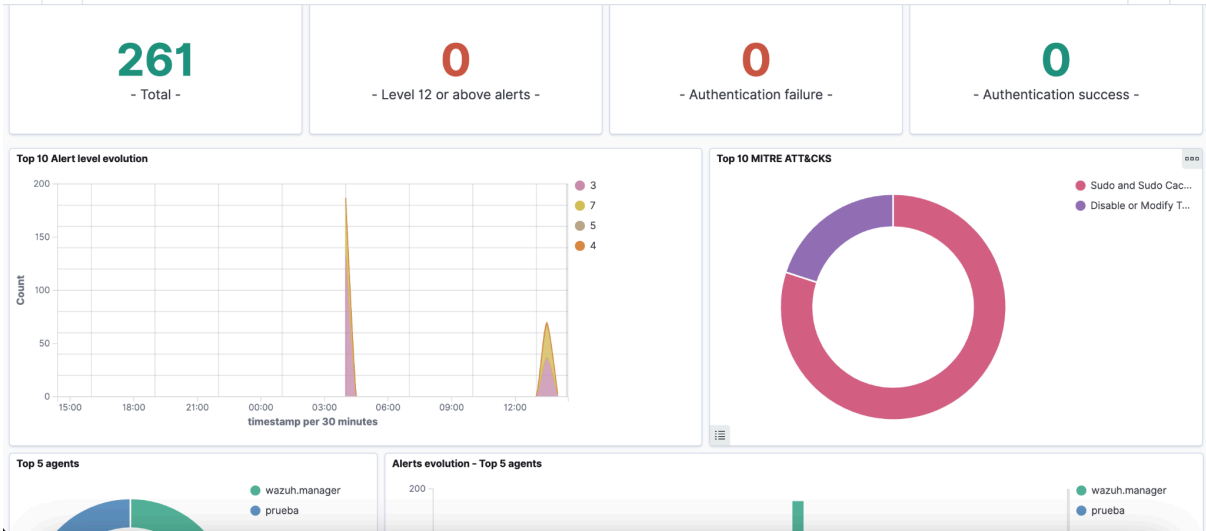
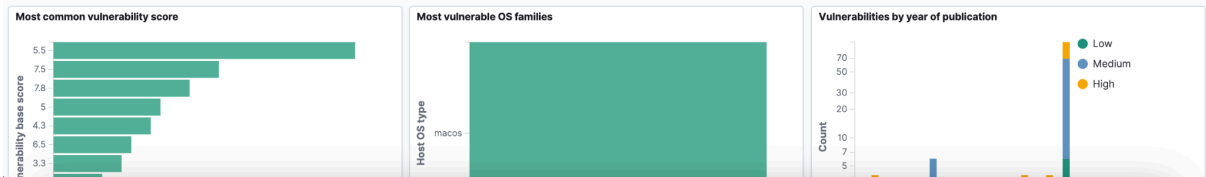
88

Medium - Severity

14

Low - Severity

Top 5 vulnerabilities	Count	Top 5 OS	Count	Top 5 agents	Count	Top 5 packages	Count
CVE-2001-0718	2	macOS Sonoma	146	prueba	146	macOS Sonoma	87
CVE-2022-40898	2					Safari	30
CVE-2022-40899	2					Docker	8
CVE-2023-5752	2					Excel	4
CVE-2024-23273	2					Outlook	4



261 hits							
Sep 14, 2024 @ 14:23:53.694 - Sep 15, 2024 @ 14:23:53.694							
<a href="#">Export Formated</a> <a href="#">484 columns hidden</a> <a href="#">Density</a> <a href="#">1 fields sorted</a> <a href="#">Full screen</a>							
↓ timestamp	agent.id	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description	rule.level	rule.id
Sep 15, 2024 @ 14:05:...	001	prueba			Listened ports status (...)	7	533
Sep 15, 2024 @ 14:01:...	001	prueba	T1548.003	Privilege EscalationDe...	Successful sudo to RO...	3	5402
Sep 15, 2024 @ 14:00:...	001	prueba	T1548.003	Privilege EscalationDe...	Successful sudo to RO...	3	5402
Sep 15, 2024 @ 13:58:...	001	prueba			Listened ports status (...)	7	533
Sep 15, 2024 @ 13:53:...	001	prueba			SCA summary: CIS_Ap...	5	19003