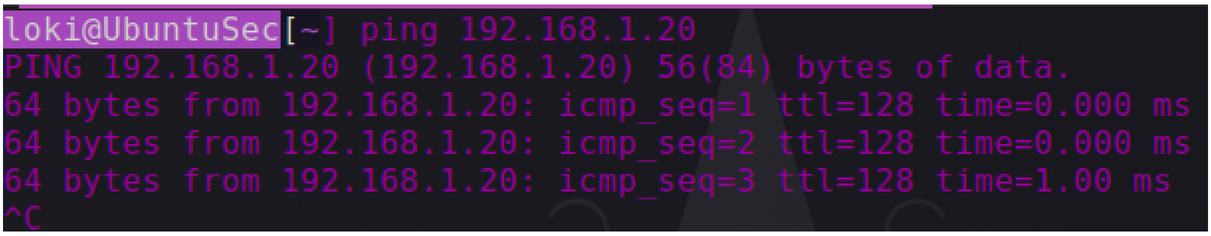
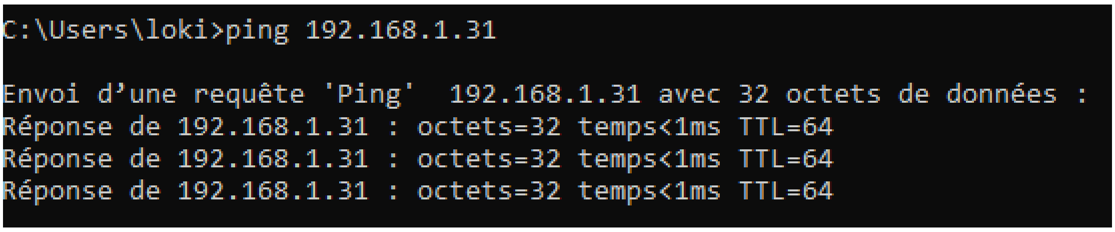
Mini-SOC SIEM (Wazuh)

To initiate this project we need to setup 2 VMs (Virtual Machines), running on Linux (Ubuntu for mine) and Windows. The Linux one is our Wazuh server and the Windows our victim machine.

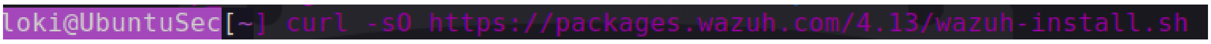


```
loki@UbuntuSec[~] ping 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
64 bytes from 192.168.1.20: icmp_seq=1 ttl=128 time=0.000 ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=128 time=0.000 ms
64 bytes from 192.168.1.20: icmp_seq=3 ttl=128 time=1.00 ms
^C
```



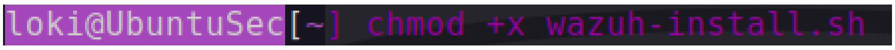
```
C:\Users\loki>ping 192.168.1.31

Envoi d’une requête 'Ping'  192.168.1.31 avec 32 octets de données :
Réponse de 192.168.1.31 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.31 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.31 : octets=32 temps<1ms TTL=64
```

We can see that the 2 VMs can ping eachothers (don’t forget to add Windows firewall rules otherwise impossible to ping back the Windows VM. (192.168.1.20 is Windows and 192.168.1.31 is Wazuh server)



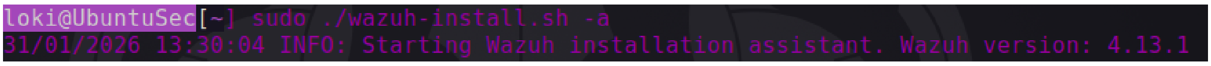
```
loki@UbuntuSec[~] curl -sO https://packages.wazuh.com/4.13/wazuh-install.sh
```

Next need to get the Wazuh installer by using curl package

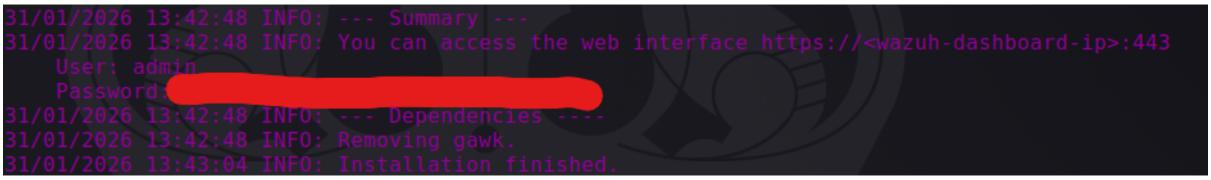


```
loki@UbuntuSec[~] chmod +x wazuh-install.sh
```

Give it the right privilege to execute it

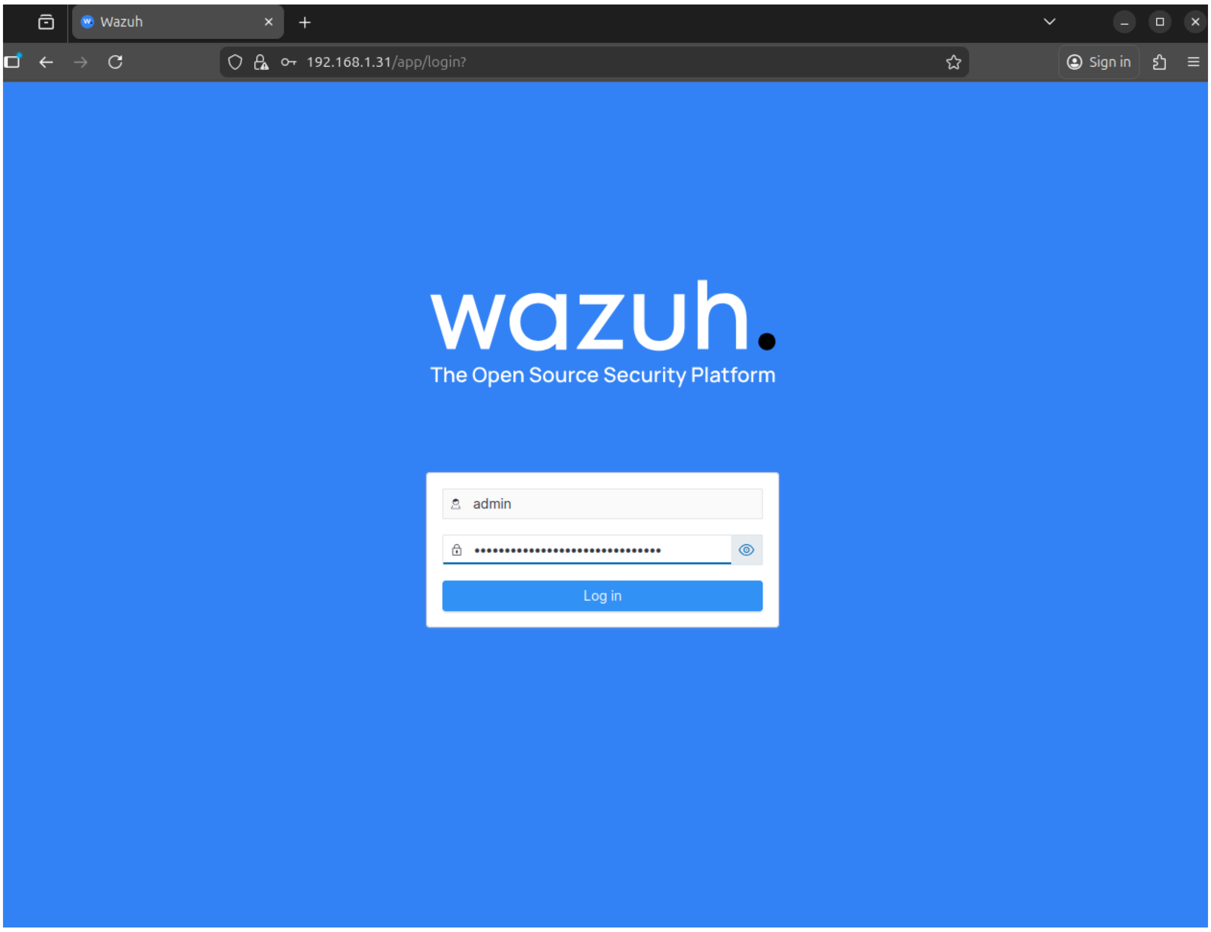


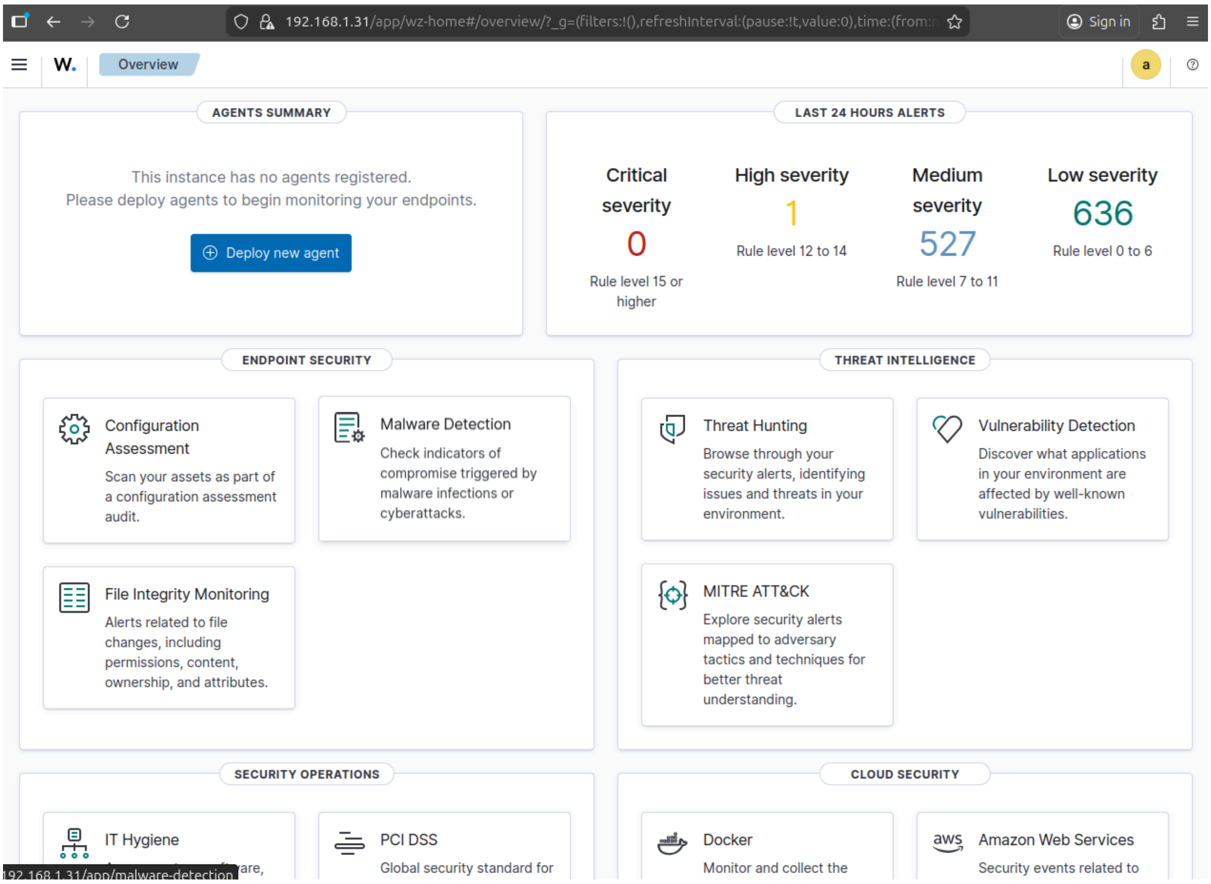
```
loki@UbuntuSec[~] sudo ./wazuh-install.sh -a
31/01/2026 13:30:04 INFO: Starting Wazuh installation assistant. Wazuh version: 4.13.1
```



```
31/01/2026 13:42:48 INFO: --- Summary ---
31/01/2026 13:42:48 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: [redacted]
31/01/2026 13:42:48 INFO: --- Dependencies ----
31/01/2026 13:42:48 INFO: Removing gawk.
31/01/2026 13:43:04 INFO: Installation finished.
```

Once Wazuh is installed you need to keep your credentials, we need them to login into our Wazuh GUI (access via linuxIP:443)




192.168.1.31/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:
Sign in
W.
Overview
a

AGENTS SUMMARY

This instance has no agents registered.
Please deploy agents to begin monitoring your endpoints.

Deploy new agent

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	1	527	636
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Check indicators of compromise triggered by malware infections or cyberattacks.

File Integrity Monitoring
Alerts related to file changes, including permissions, content, ownership, and attributes.

THREAT INTELLIGENCE

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK
Explore security alerts mapped to adversary tactics and techniques for better threat understanding.

SECURITY OPERATIONS

IT Hygiene

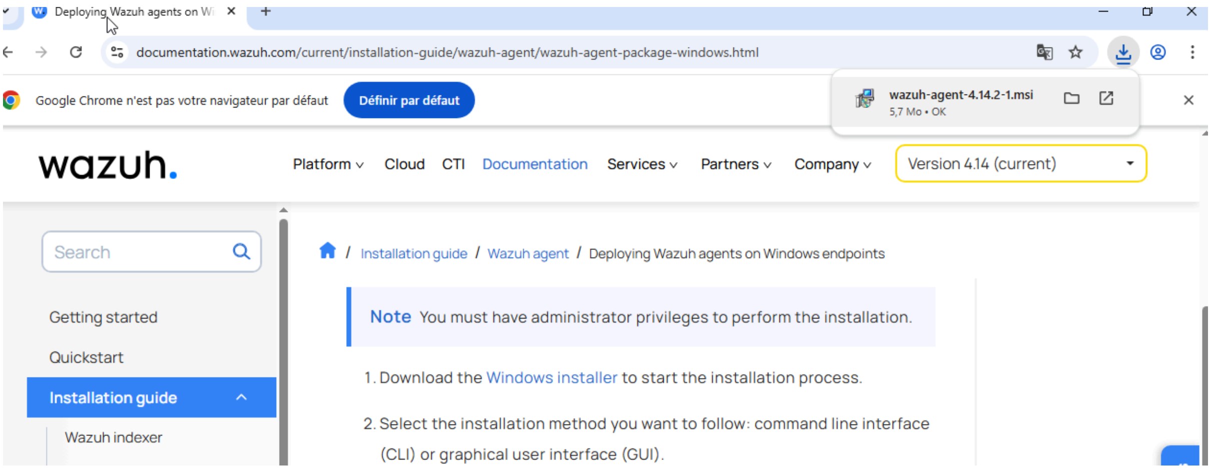
PCI DSS
Global security standard for

CLOUD SECURITY

Docker
Monitor and collect the

Amazon Web Services
Security events related to

This our Home page we can already see that due to my Windows 10 machine (no more supported) Wazuh raise alerts



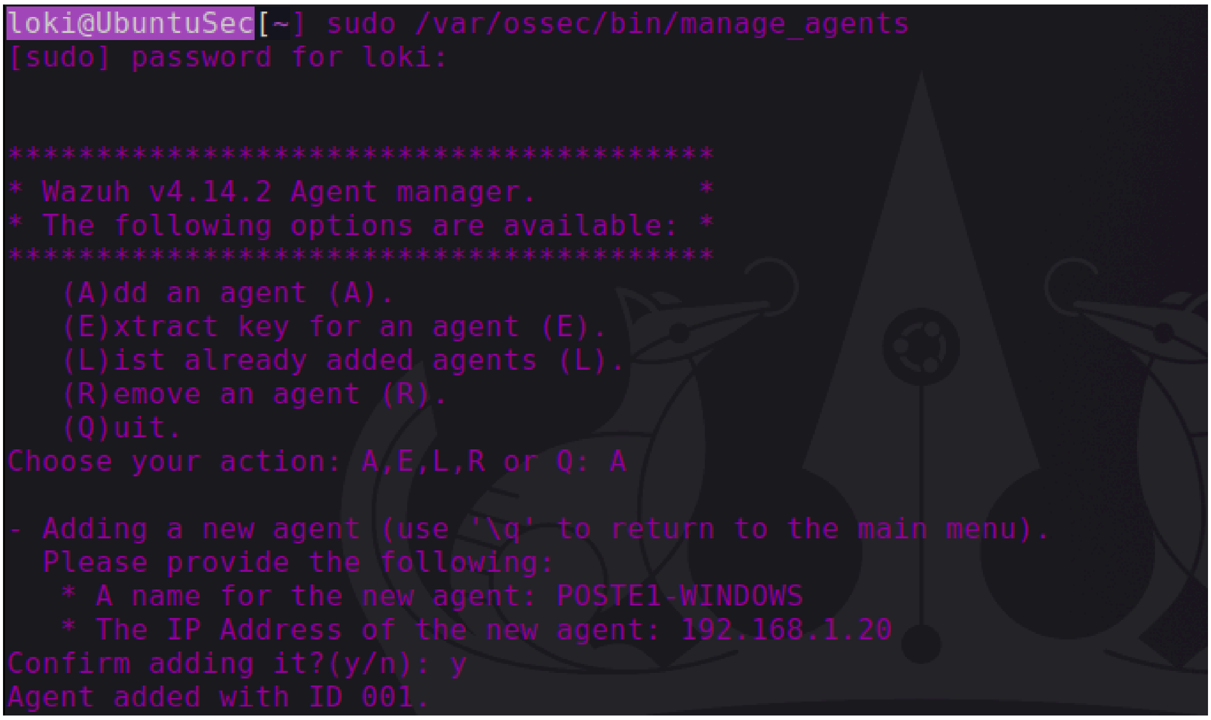
Installation guide / Wazuh agent / Deploying Wazuh agents on Windows endpoints

Note You must have administrator privileges to perform the installation.

1. Download the Windows installer to start the installation process.
2. Select the installation method you want to follow: command line interface (CLI) or graphical user interface (GUI).

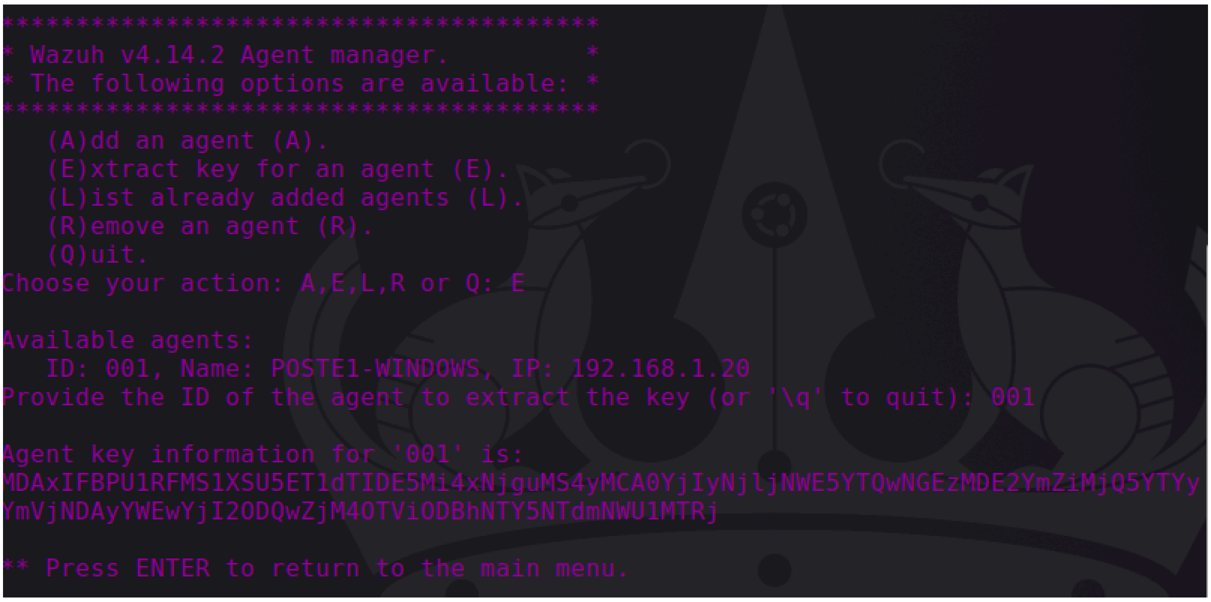
Now, we can download the Wazuh Agent on our Windown VM and create the link between the server and the victim machine

Once the agent is installed we need to create a new agent on the server to identify our Windows machine.



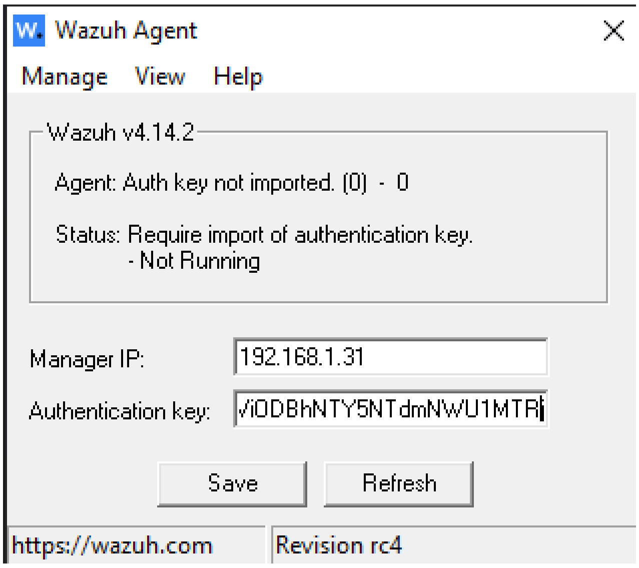
```
loki@UbuntuSec[~] sudo /var/ossec/bin/manage_agents
[sudo] password for loki:


****************************************
* Wazuh v4.14.2 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: POSTE1-WINDOWS
   * The IP Address of the new agent: 192.168.1.20
Confirm adding it?(y/n): y
Agent added with ID 001.
```

Execute the manage agent binary and press A to add a new agent, provide a name and an IP address (the Windows IP one)



```
****************************************
* Wazuh v4.14.2 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: POSTE1-WINDOWS, IP: 192.168.1.20
Provide the ID of the agent to extract the key (or '\q' to quit): 001

Agent key information for '001' is:
MDAxIFBPU1RFMS1XSU5ET1dTIDE5Mi4xNjguMS4yMCA0YjIyNjljNWE5YTQwNGEzMDE2YmZiMjQ5YTYy
YmVjNDAyYWEwYjI2ODQwZjM4OTViODBhNTY5NTdmNWU1MTRj

** Press ENTER to return to the main menu.
```

Next, press E to redeem your Windows Vm agent key



Wazuh Agent

Wazuh v4.14.2

Agent: Auth key not imported. (0) - 0

Status: Require import of authentication key.
- Not Running

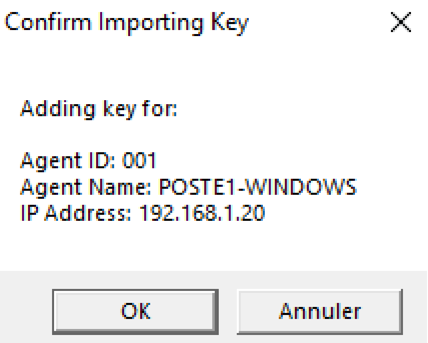
Manager IP: 192.168.1.31

Authentication key: ViODBhNTY5NTdmNWU1MTR

https://wazuh.com

Revision rc4

Back in our Windows environment we can provide the manager IP (linux server) and our authentication key so the server can figure out who this machine is. Save and go to manage and restart the agent

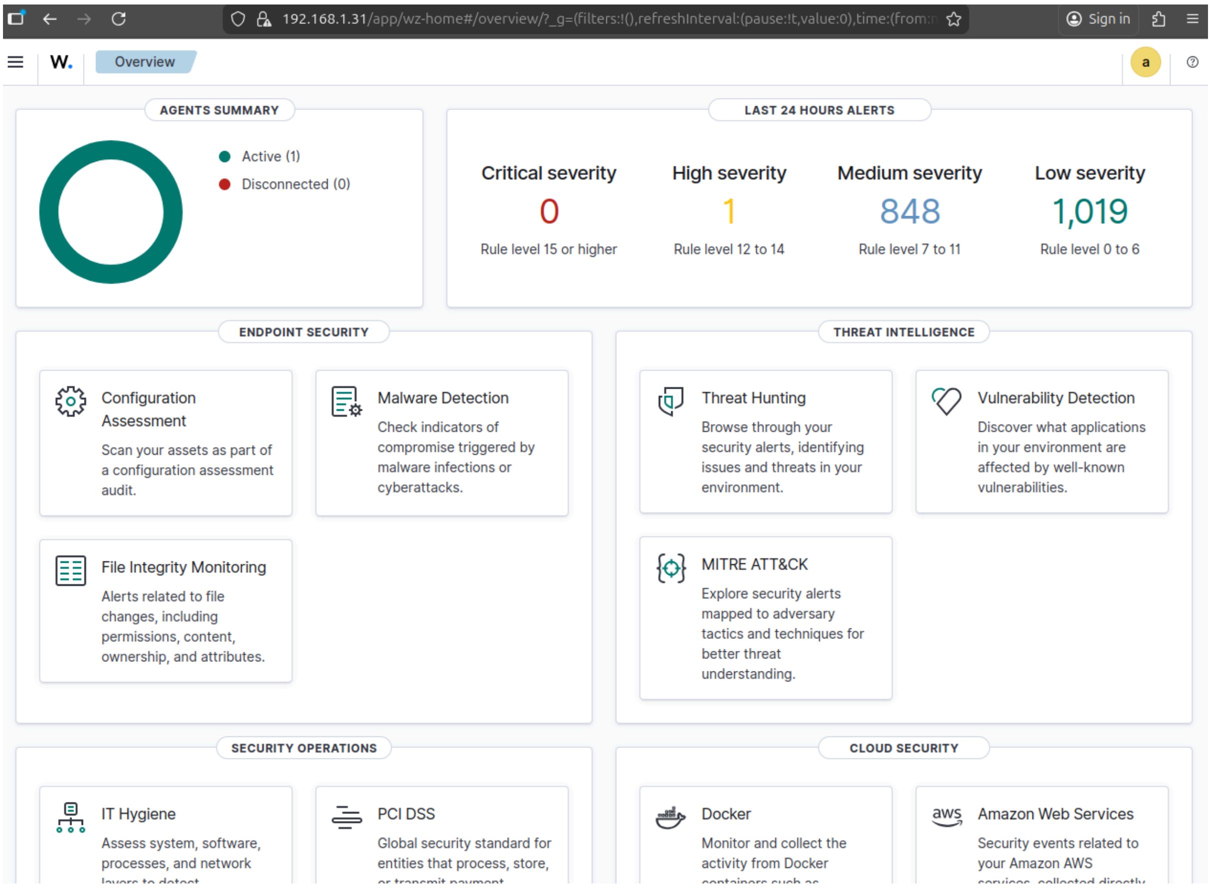


Confirm Importing Key

Adding key for:

Agent ID: 001
Agent Name: POSTE1-WINDOWS
IP Address: 192.168.1.20

Success !
Back in our Wazuh GUI we can see that our Windows is "Active"



192.168.1.31/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:n
Sign in
W.
Overview
a

AGENTS SUMMARY

● Active (1)

● Disconnected (0)

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	1	848	1,019
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Check indicators of compromise triggered by malware infections or cyberattacks.

File Integrity Monitoring
Alerts related to file changes, including permissions, content, ownership, and attributes.

THREAT INTELLIGENCE

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK
Explore security alerts mapped to adversary tactics and techniques for better threat understanding.

SECURITY OPERATIONS

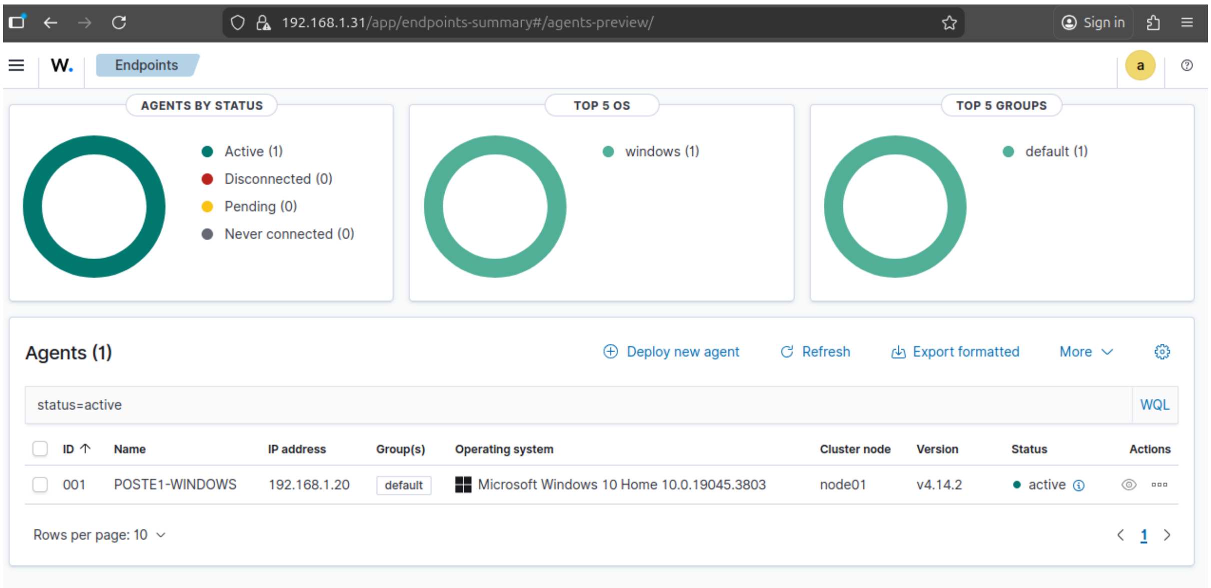
IT Hygiene
Assess system, software, processes, and network layers to detect

PCI DSS
Global security standard for entities that process, store, or transmit payment

CLOUD SECURITY

Docker
Monitor and collect the activity from Docker containers such as

Amazon Web Services
Security events related to your Amazon AWS services, collected directly



AGENTS BY STATUS

● Active (1)

● Disconnected (0)

● Pending (0)

● Never connected (0)

TOP 5 OS

● windows (1)

TOP 5 GROUPS

● default (1)

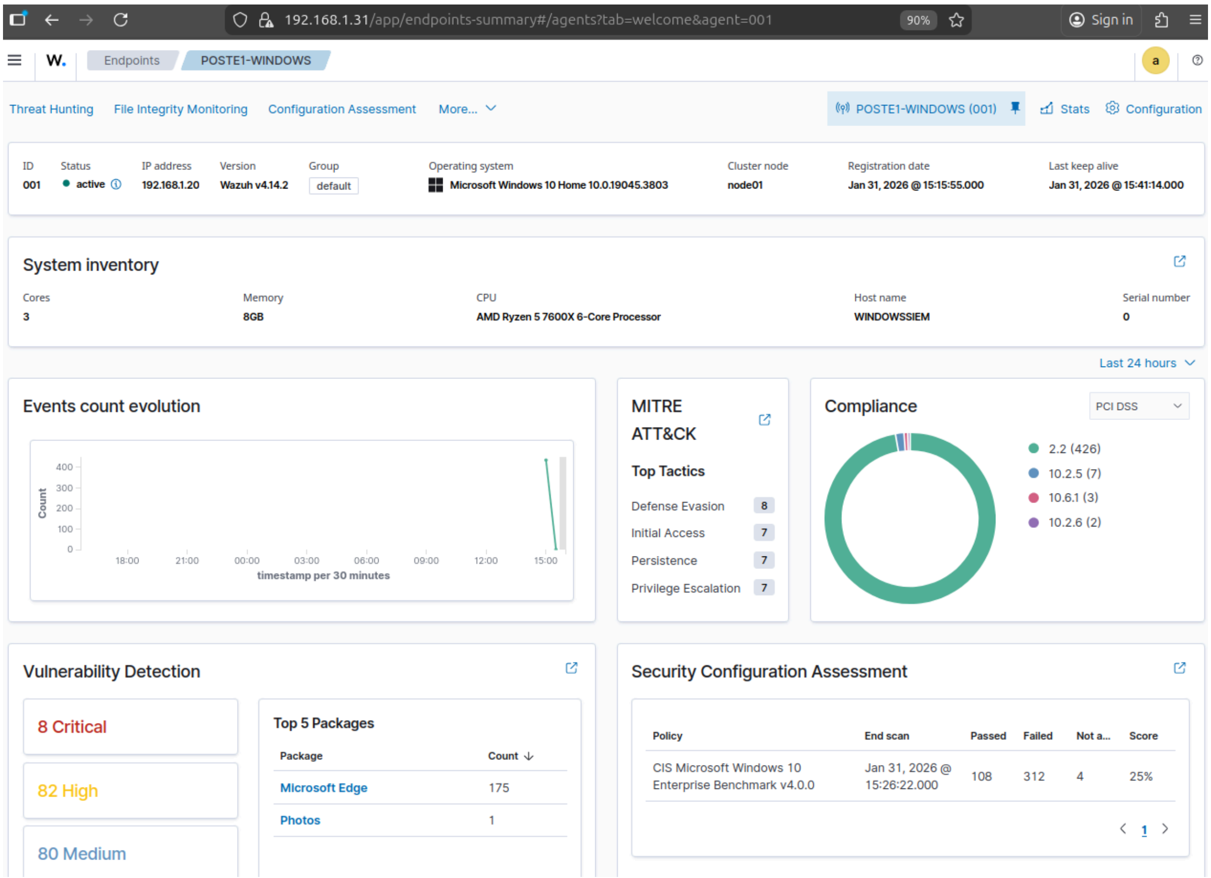
Agents (1)

status=active

□	ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
□	001	POSTE1-WINDOWS	192.168.1.20	default	Microsoft Windows 10 Home 10.0.19045.3803	node01	v4.14.2	● active	

Rows per page: 10

< 1 >



ID	Status	IP address	Version	Group	Operating system	Cluster node	Registration date	Last keep alive
001	active	192.168.1.20	Wazuh v4.14.2	default	Microsoft Windows 10 Home 10.0.19045.3803	node01	Jan 31, 2026 @ 15:15:55.000	Jan 31, 2026 @ 15:41:14.000

System inventory

Cores	Memory	CPU	Host name	Serial number
3	8GB	AMD Ryzen 5 7600X 6-Core Processor	WINDOWSSIEM	0

Last 24 hours

Events count evolution

MITRE ATT&CK

Top Tactics

Defense Evasion	8
Initial Access	7
Persistence	7
Privilege Escalation	7

Compliance

Vulnerability Detection

8 Critical

82 High

80 Medium

Top 5 Packages

Package	Count
Microsoft Edge	175
Photos	1

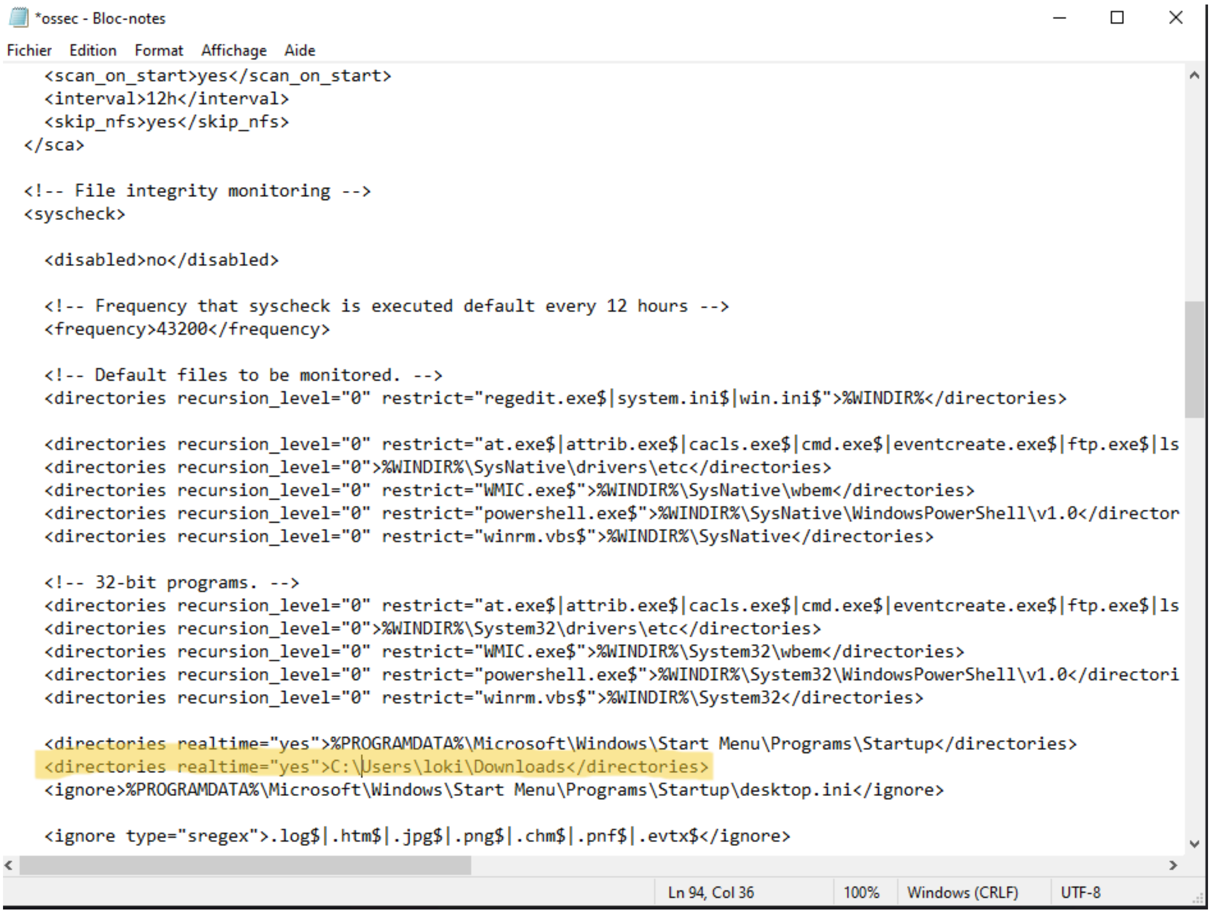
Security Configuration Assessment

Policy	End scan	Passed	Failed	Not a...	Score
CIS Microsoft Windows 10 Enterprise Benchmark v4.0.0	Jan 31, 2026 @ 15:26:22.000	108	312	4	25%

We want now to setup our own File Integrity Monitoring rule because we do not trust the user about his downloadings

Go to C:/Program Files (x86)/ossec-agent/ossec.conf

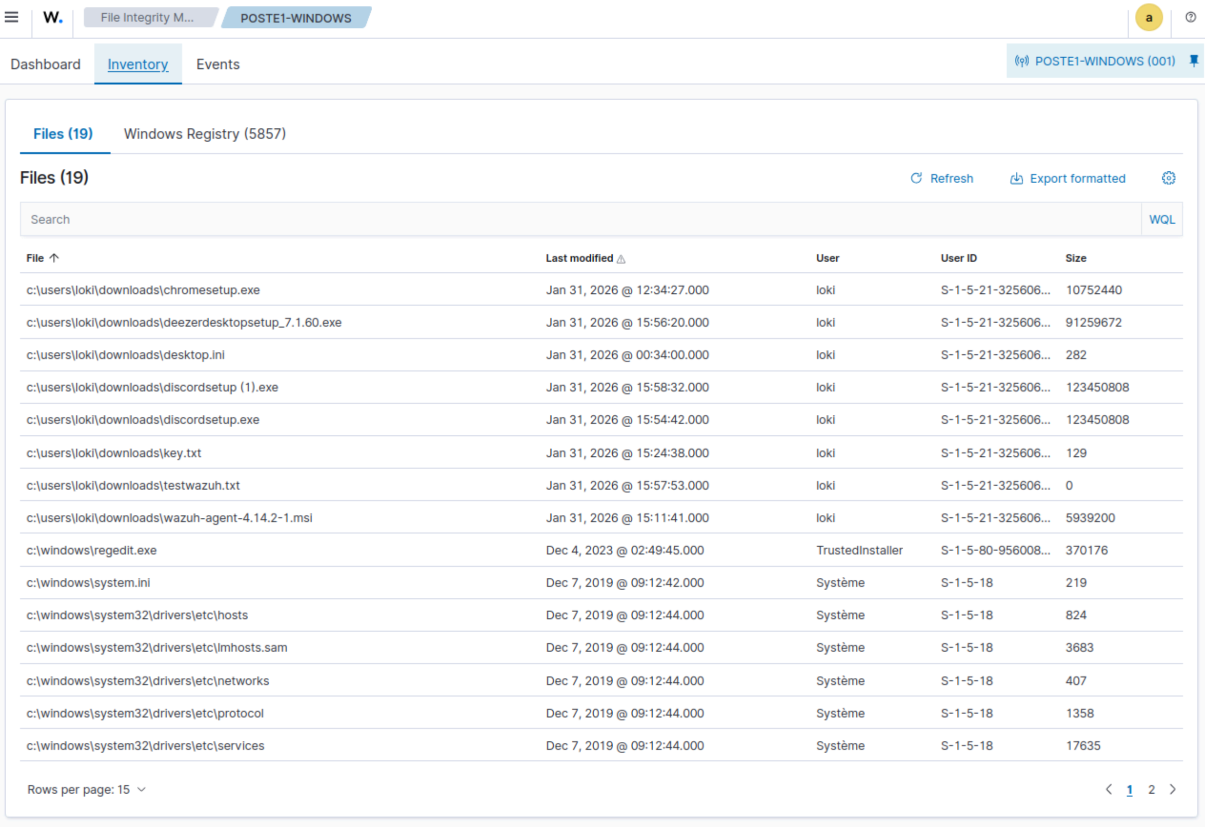
And add this line (change the user)



```
    <scan_on_start>yes</scan_on_start>
    <interval>12h</interval>
    <skip_nfs>yes</skip_nfs>
  </sca>

  <!-- File integrity monitoring -->
  <syscheck>

    <disabled>no</disabled>

    <!-- Frequency that syscheck is executed default every 12 hours -->
    <frequency>43200</frequency>

    <!-- Default files to be monitored. -->
    <directories recursion_level="0" restrict="regedit.exe$|system.ini$|win.ini$">%WINDIR%</directories>

    <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|ls
    <directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>
    <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\SysNative\wbem</directories>
    <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\SysNative\WindowsPowerShell\v1.0</director
    <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\SysNative</directories>

    <!-- 32-bit programs. -->
    <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|ls
    <directories recursion_level="0">%WINDIR%\System32\drivers\etc</directories>
    <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\System32\wbem</directories>
    <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\System32\WindowsPowerShell\v1.0</directori
    <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\System32</directories>

    <directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>
    <directories realtime="yes">C:\Users\loki\Downloads</directories>
    <ignore>%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini</ignore>

    <ignore type="sregex">.log$|.htm$|.jpg$|.png$|.chm$|.pnf$|.evtx$</ignore>
```

Download some softwares, delete some files in your downloads and go back to your Wazuh GUI

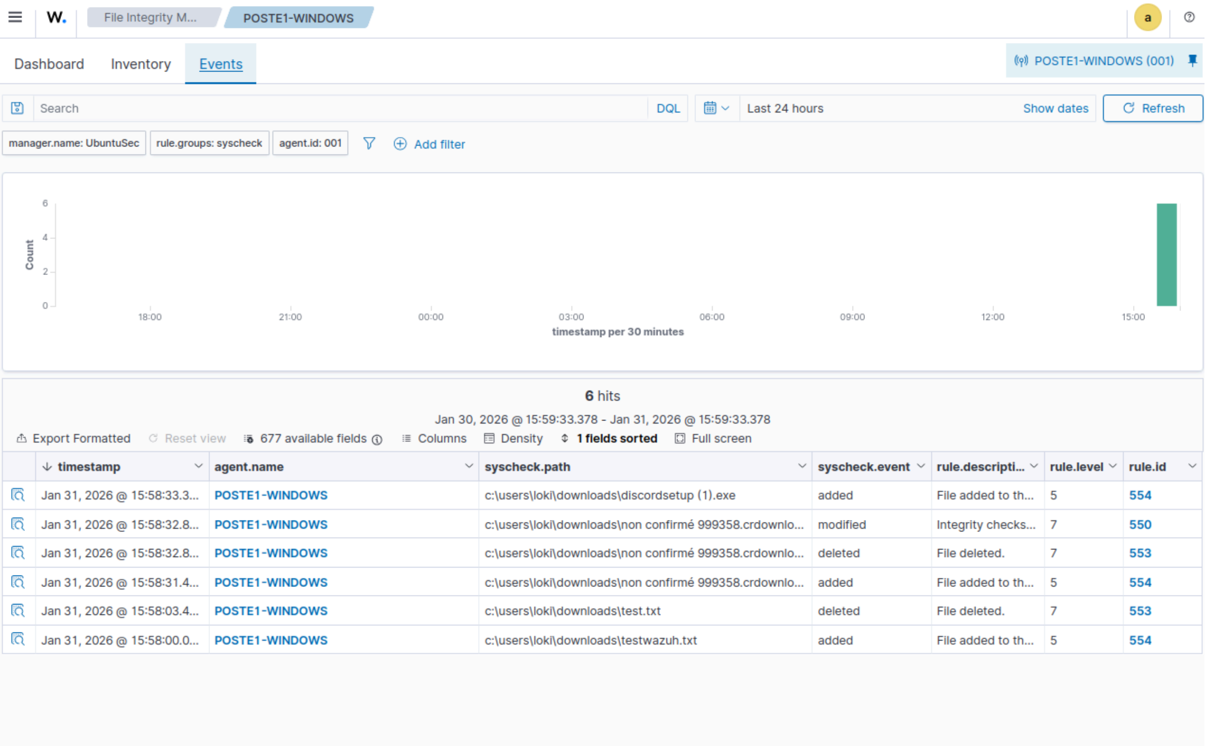
We can see that we generate some “noise” by downloading and modifying files



Files (19)

File ↑	Last modified	User	User ID	Size
c:\users\loki\downloads\chromesetup.exe	Jan 31, 2026 @ 12:34:27.000	loki	S-1-5-21-325606...	10752440
c:\users\loki\downloads\deezerdesktopsetup_7.1.60.exe	Jan 31, 2026 @ 15:56:20.000	loki	S-1-5-21-325606...	91259672
c:\users\loki\downloads\desktop.ini	Jan 31, 2026 @ 00:34:00.000	loki	S-1-5-21-325606...	282
c:\users\loki\downloads\discordsetup (1).exe	Jan 31, 2026 @ 15:58:32.000	loki	S-1-5-21-325606...	123450808
c:\users\loki\downloads\discordsetup.exe	Jan 31, 2026 @ 15:54:42.000	loki	S-1-5-21-325606...	123450808
c:\users\loki\downloads\key.txt	Jan 31, 2026 @ 15:24:38.000	loki	S-1-5-21-325606...	129
c:\users\loki\downloads\testwazuh.txt	Jan 31, 2026 @ 15:57:53.000	loki	S-1-5-21-325606...	0
c:\users\loki\downloads\wazuh-agent-4.14.2-1.msi	Jan 31, 2026 @ 15:11:41.000	loki	S-1-5-21-325606...	5939200
c:\windows\regedit.exe	Dec 4, 2023 @ 02:49:45.000	TrustedInstaller	S-1-5-80-956008...	370176
c:\windows\system.ini	Dec 7, 2019 @ 09:12:42.000	Système	S-1-5-18	219
c:\windows\system32\drivers\etc\hosts	Dec 7, 2019 @ 09:12:44.000	Système	S-1-5-18	824
c:\windows\system32\drivers\etc\lmhosts.sam	Dec 7, 2019 @ 09:12:44.000	Système	S-1-5-18	3683
c:\windows\system32\drivers\etc\networks	Dec 7, 2019 @ 09:12:44.000	Système	S-1-5-18	407
c:\windows\system32\drivers\etc\protocol	Dec 7, 2019 @ 09:12:44.000	Système	S-1-5-18	1358
c:\windows\system32\drivers\etc\services	Dec 7, 2019 @ 09:12:44.000	Système	S-1-5-18	17635

Rows per page: 15



6 hits

Jan 30, 2026 @ 15:59:33.378 - Jan 31, 2026 @ 15:59:33.378

↓ timestamp	agent.name	syscheck.path	syscheck.event	rule.descripti...	rule.level	rule.id
Jan 31, 2026 @ 15:58:33.3...	POSTE1-WINDOWS	c:\users\loki\downloads\discordsetup (1).exe	added	File added to th...	5	554
Jan 31, 2026 @ 15:58:32.8...	POSTE1-WINDOWS	c:\users\loki\downloads\non confirmé 999358.crdownlo...	modified	Integrity checks...	7	550
Jan 31, 2026 @ 15:58:32.8...	POSTE1-WINDOWS	c:\users\loki\downloads\non confirmé 999358.crdownlo...	deleted	File deleted.	7	553
Jan 31, 2026 @ 15:58:31.4...	POSTE1-WINDOWS	c:\users\loki\downloads\non confirmé 999358.crdownlo...	added	File added to th...	5	554
Jan 31, 2026 @ 15:58:03.4...	POSTE1-WINDOWS	c:\users\loki\downloads\test.txt	deleted	File deleted.	7	553
Jan 31, 2026 @ 15:58:00.0...	POSTE1-WINDOWS	c:\users\loki\downloads\testwazuh.txt	added	File added to th...	5	554