WAZUH SIEM - HOME TEST LAB

Objective: This mini-project aims to demonstrate the features of Wazuh within a home SIEM lab environment using my own Windows PC, focusing on FIM, SCA, and Vulnerability Detection. My goal is to highlight how Wazuh can be used as both an IDS and XDR strategy to identify and mitigate potential security risks. The configuration settings used in this setup will be discussed in detail, along with customizable scanning options based on the desired targets whether directories, systems or compliance benchmarks.

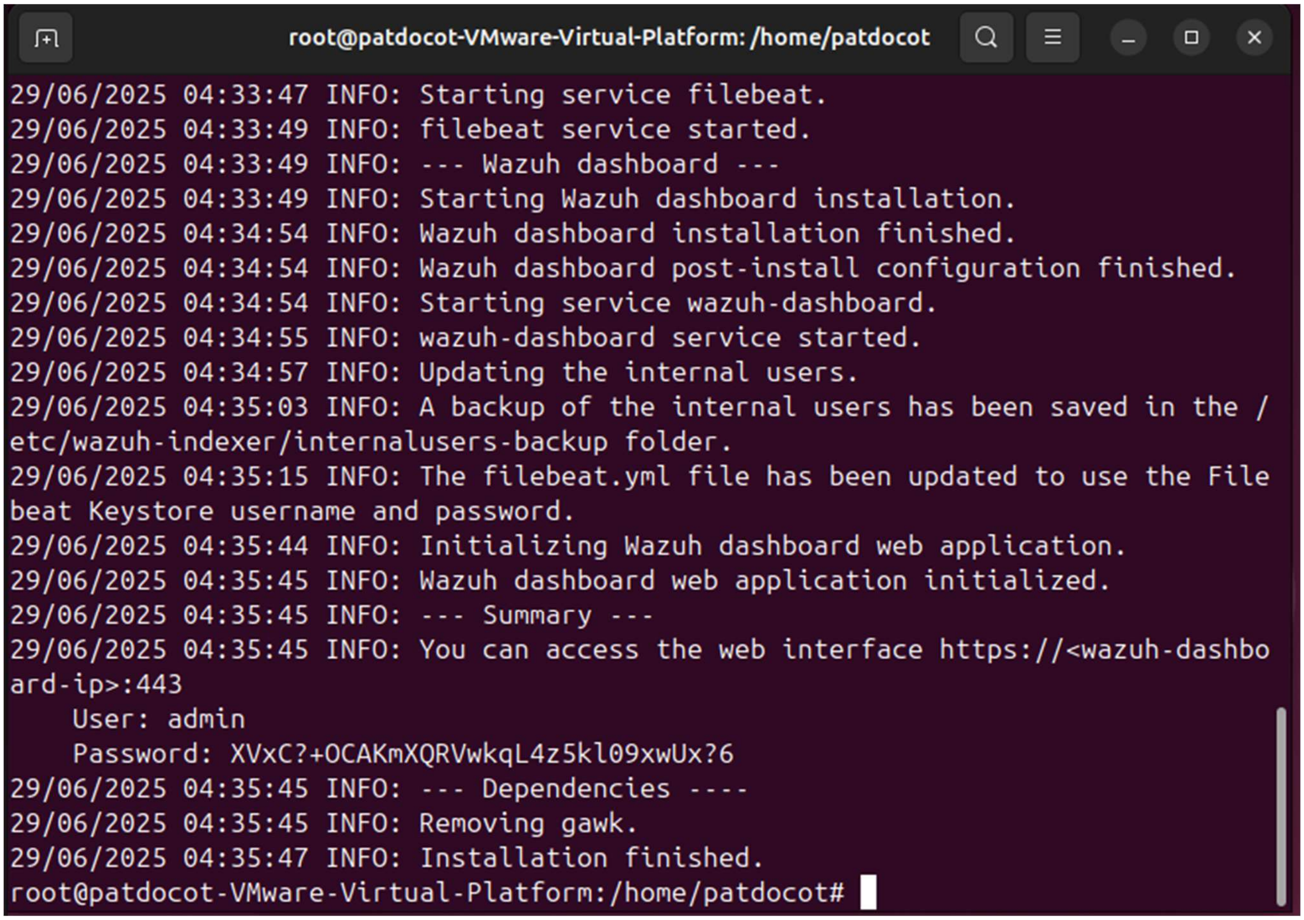
Lab Setup Components - Wazuh Server and Agent:

Download and run the Wazuh installation assistant

- >Sudo apt update && sudo apt upgrade

Enter all-in-one command which will install the dashboard, server, and indexer.

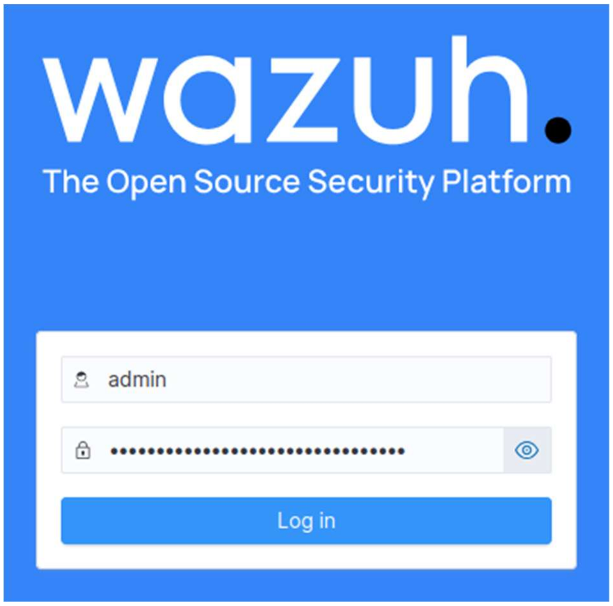
- >curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash ./wazuh-install.sh –a



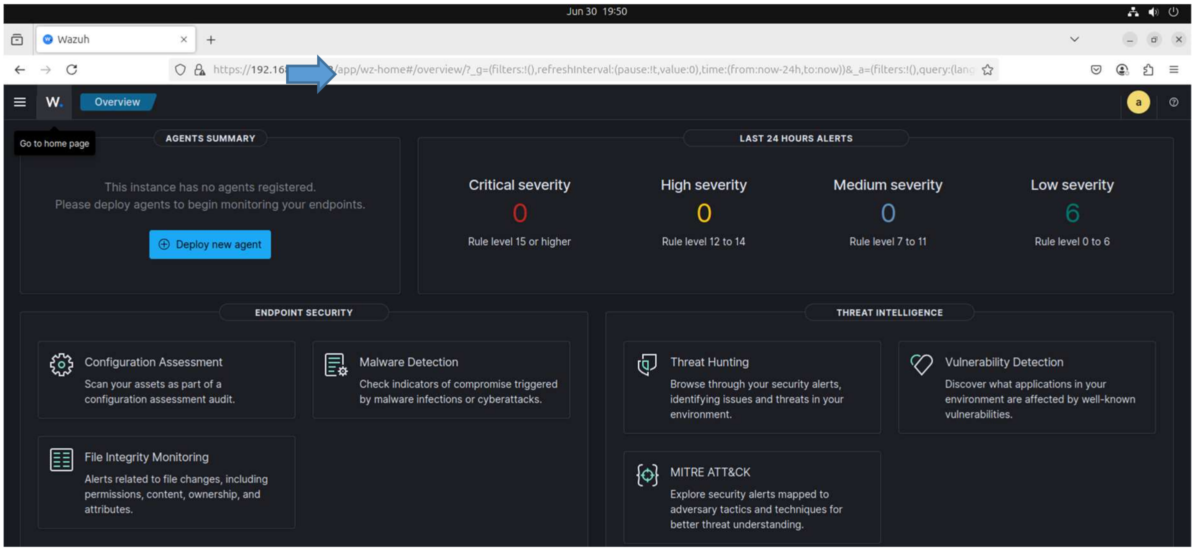
```
29/06/2025 04:33:47 INFO: Starting service filebeat.
29/06/2025 04:33:49 INFO: filebeat service started.
29/06/2025 04:33:49 INFO: --- Wazuh dashboard ---
29/06/2025 04:33:49 INFO: Starting Wazuh dashboard installation.
29/06/2025 04:34:54 INFO: Wazuh dashboard installation finished.
29/06/2025 04:34:54 INFO: Wazuh dashboard post-install configuration finished.
29/06/2025 04:34:54 INFO: Starting service wazuh-dashboard.
29/06/2025 04:34:55 INFO: wazuh-dashboard service started.
29/06/2025 04:34:57 INFO: Updating the internal users.
29/06/2025 04:35:03 INFO: A backup of the internal users has been saved in the /
etc/wazuh-indexer/internalusers-backup folder.
29/06/2025 04:35:15 INFO: The filebeat.yml file has been updated to use the File
beat Keystore username and password.
29/06/2025 04:35:44 INFO: Initializing Wazuh dashboard web application.
29/06/2025 04:35:45 INFO: Wazuh dashboard web application initialized.
29/06/2025 04:35:45 INFO: --- Summary ---
29/06/2025 04:35:45 INFO: You can access the web interface https://<wazuh-dashbo
ard-ip>:443
    User: admin
    Password: XVxC?+OCAKmXQRVwkqL4z5kl09xwUx?6
29/06/2025 04:35:45 INFO: --- Dependencies ----
29/06/2025 04:35:45 INFO: Removing gawk.
29/06/2025 04:35:47 INFO: Installation finished.
root@patdocot-VMware-Virtual-Platform:/home/patdocot#
```

To log in, secure IP and type “ip a” in the command line.

Open Firefox to and paste the IP address 192.168.223.*** to log in



Dashboard view: Connected IP address 192.168.223.*** to the Wazuh manager.



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

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.

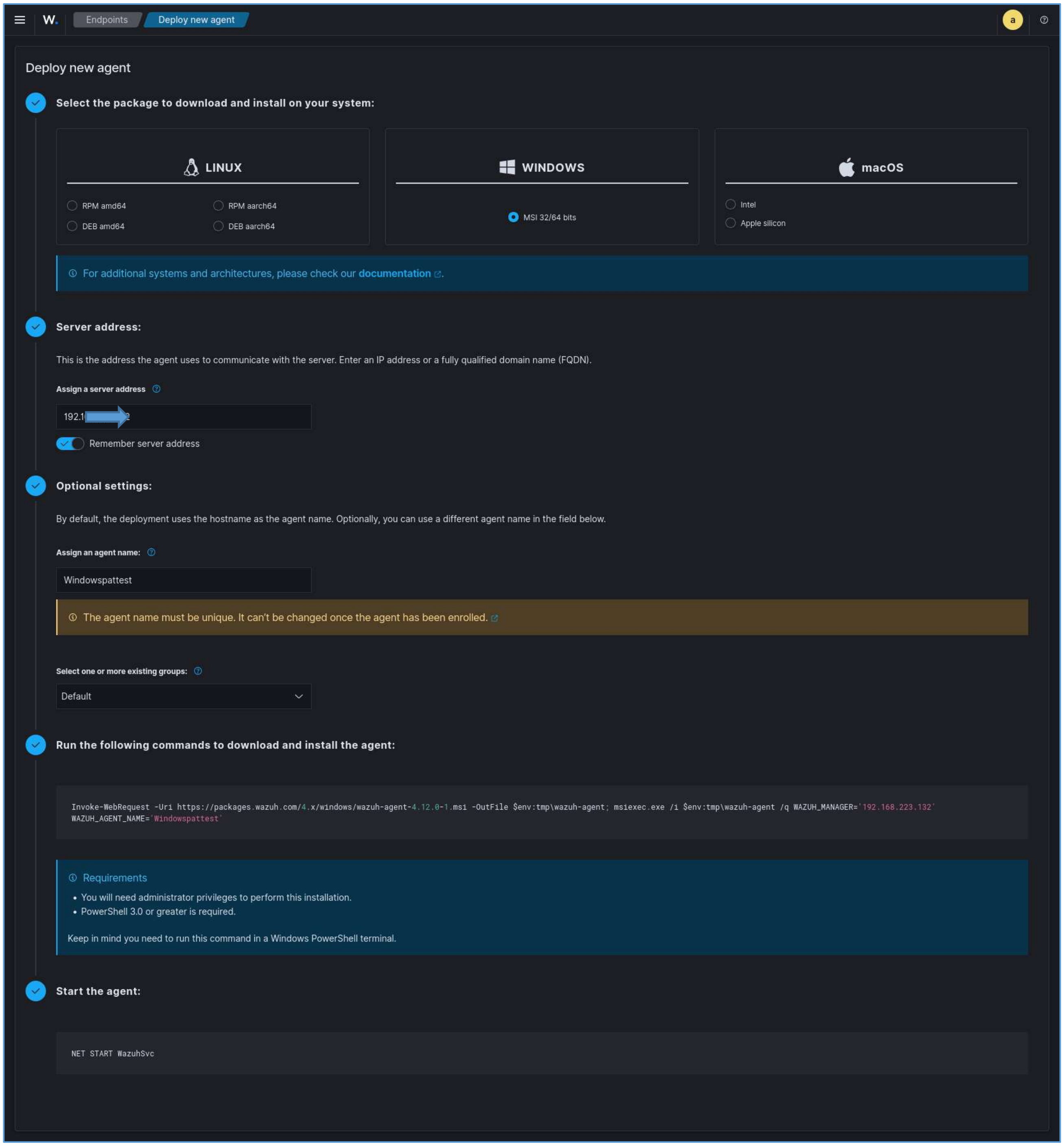
Threat Hunting: Browse through your security alerts, identifying issues and threats in your environment.

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.

I will showcase key Wazuh features by connecting it to my Windows PC. In this project, I will monitor Vulnerability Management (CVEs), Security Configuration Audit (SCA), and File Integrity Monitoring

Here are the quicks steps to connect Windows PC to the Wazuh Manager



Deploy new agent

Select the package to download and install on your system:

LINUX

○ RPM amd64 ○ RPM aarch64
○ DEB amd64 ○ DEB aarch64

WINDOWS

● MSI 32/64 bits

macOS

○ Intel
○ Apple silicon

For additional systems and architectures, please check our documentation.

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

192.1[redacted]2

Remember server address

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:

Windowspattest

The agent name must be unique. It can't be changed once the agent has been enrolled.

Select one or more existing groups:

Default

Run the following commands to download and install the agent:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.12.0-1.msi -OutFile $env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.223.132'
WAZUH_AGENT_NAME='Windowspattest'
```

Requirements

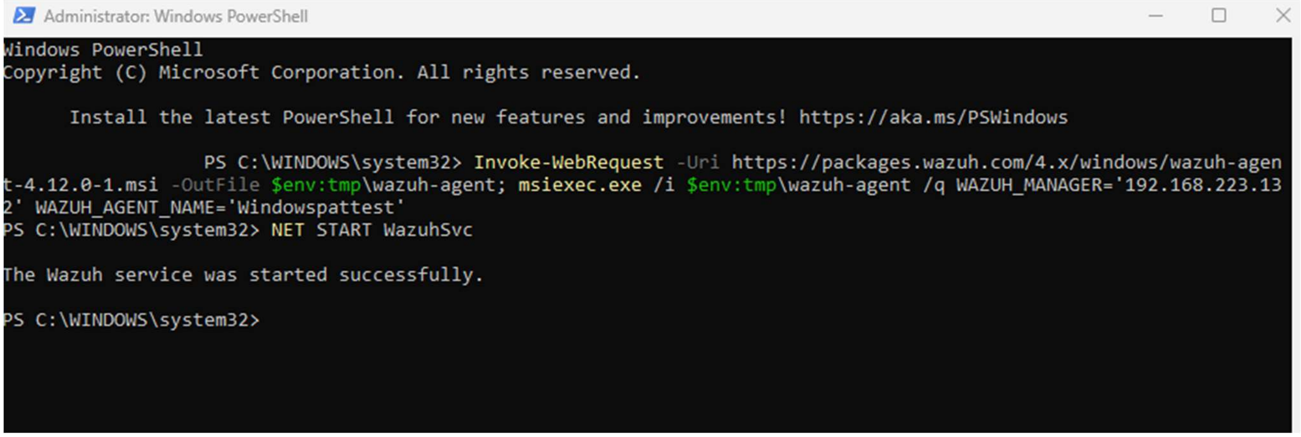
- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

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

Start the agent:

```
NET START WazuhSvc
```

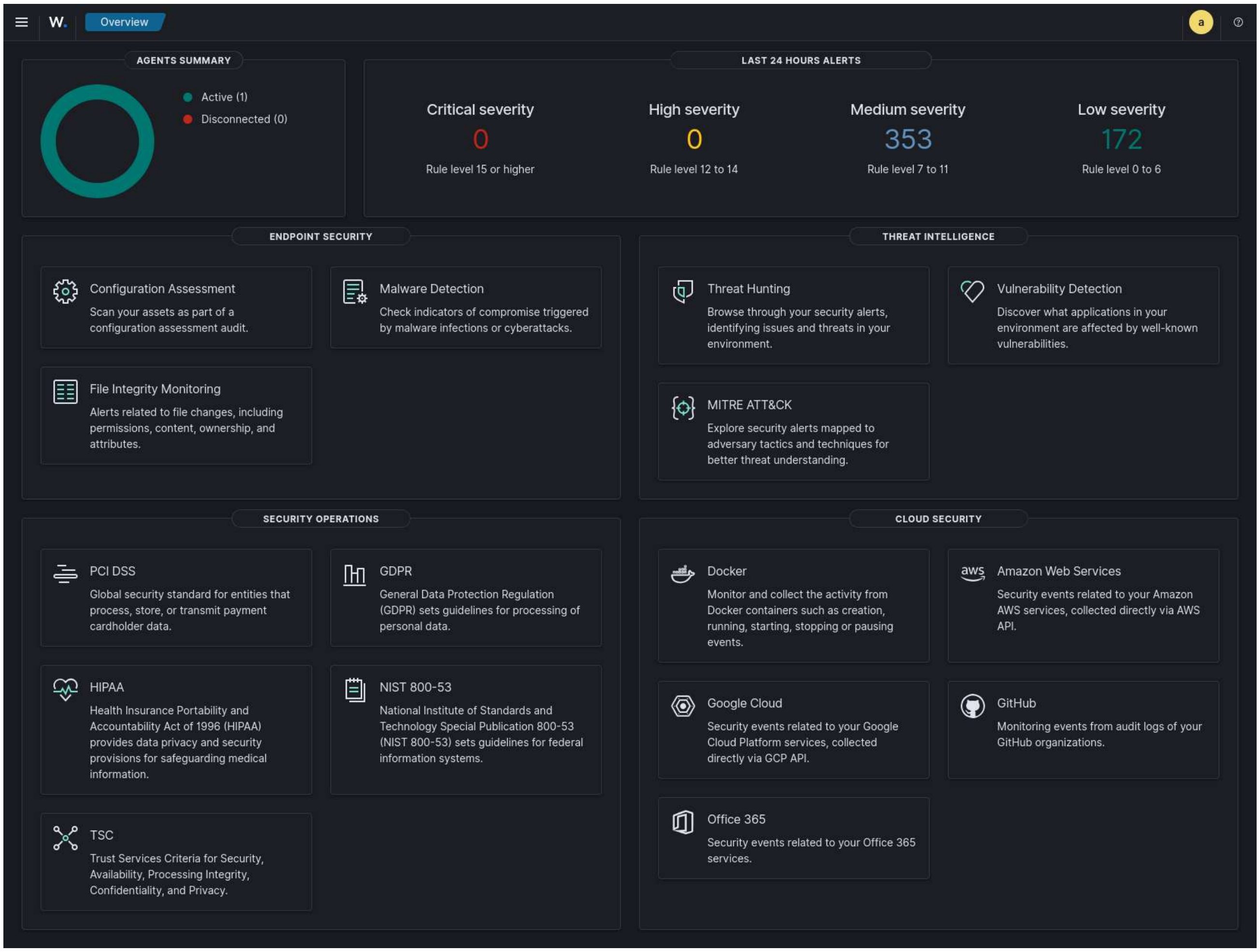
Open Powershell as administrator mode and connect to the Wazuh Server.



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-agen
t-4.12.0-1.msi -OutFile $env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.223.13
2' WAZUH_AGENT_NAME='Windowspattest'
PS C:\WINDOWS\system32> NET START WazuhSvc

The Wazuh service was started successfully.

PS C:\WINDOWS\system32>
```

Successfully connected. The dashboard shows the Windows PC is on Active status



AGENTS SUMMARY

● Active (1)
● Disconnected (0)

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	353	172
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

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

GDPR
General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.

HIPAA
Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides data privacy and security provisions for safeguarding medical information.

NIST 800-53
National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

TSC
Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

CLOUD SECURITY

Docker
Monitor and collect the activity from Docker containers such as creation, running, starting, stopping or pausing events.

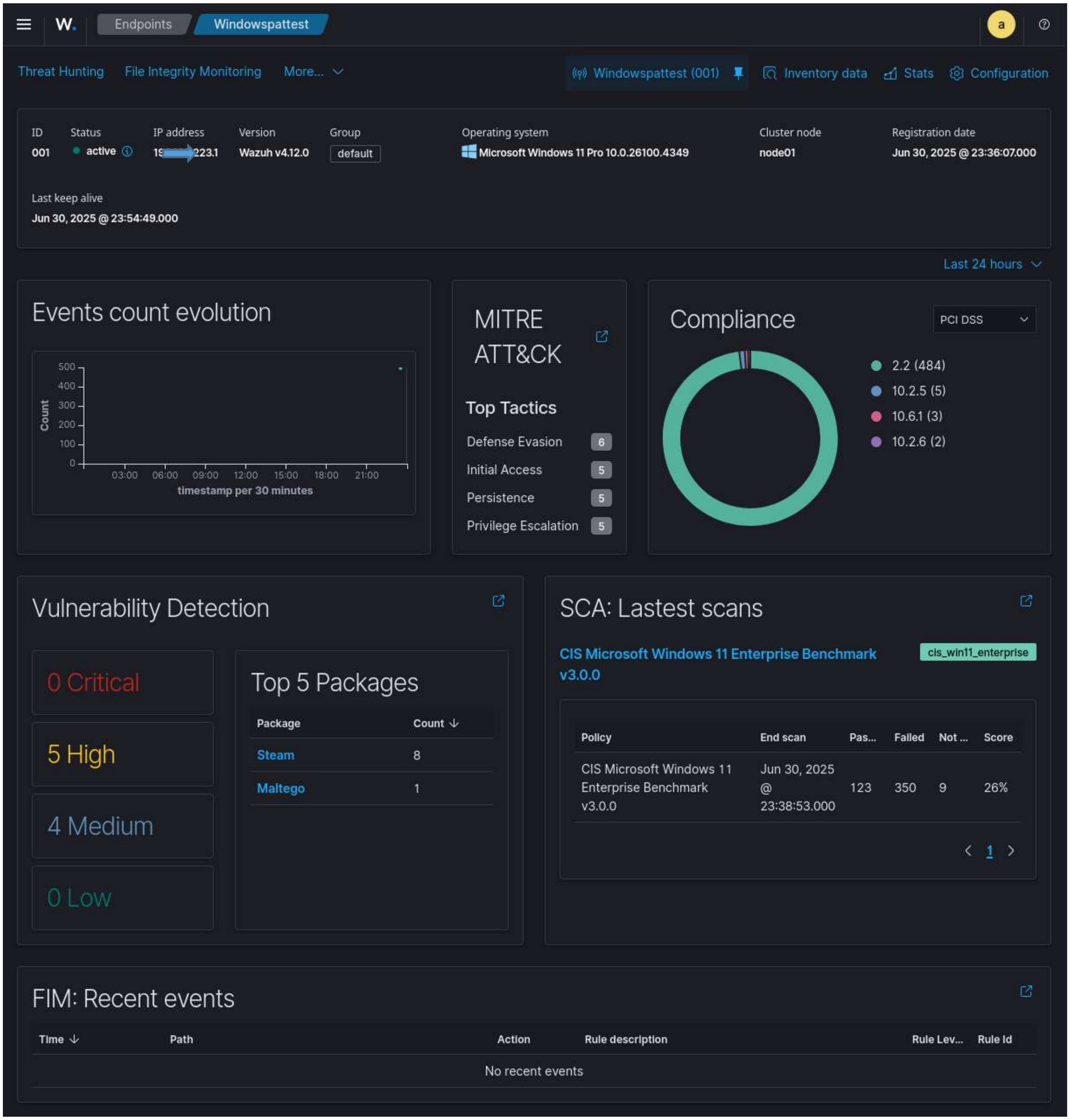
Amazon Web Services
Security events related to your Amazon AWS services, collected directly via AWS API.

Google Cloud
Security events related to your Google Cloud Platform services, collected directly via GCP API.

GitHub
Monitoring events from audit logs of your GitHub organizations.

Office 365
Security events related to your Office 365 services.

Wazuh Main Dashboard



ID	Status	IP address	Version	Group	Operating system	Cluster node	Registration date
001	● active	19[redacted]223.1	Wazuh v4.12.0	default	Microsoft Windows 11 Pro 10.0.26100.4349	node01	Jun 30, 2025 @ 23:36:07.000

Last keep alive
Jun 30, 2025 @ 23:54:49.000

Last 24 hours

Events count evolution

MITRE ATT&CK

Top Tactics

Defense Evasion	6
Initial Access	5
Persistence	5
Privilege Escalation	5

Compliance

PCI DSS

- ● 2.2 (484)
- ● 10.2.5 (5)
- ● 10.6.1 (3)
- ● 10.2.6 (2)

Vulnerability Detection

0 Critical

5 High

4 Medium

0 Low

Top 5 Packages

Package	Count ↓
Steam	8
Maltego	1

SCA: Lastest scans

CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0 cis_win11_enterprise

Policy	End scan	Pas...	Failed	Not ...	Score
CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0	Jun 30, 2025 @ 23:38:53.000	123	350	9	26%

< 1 >

FIM: Recent events

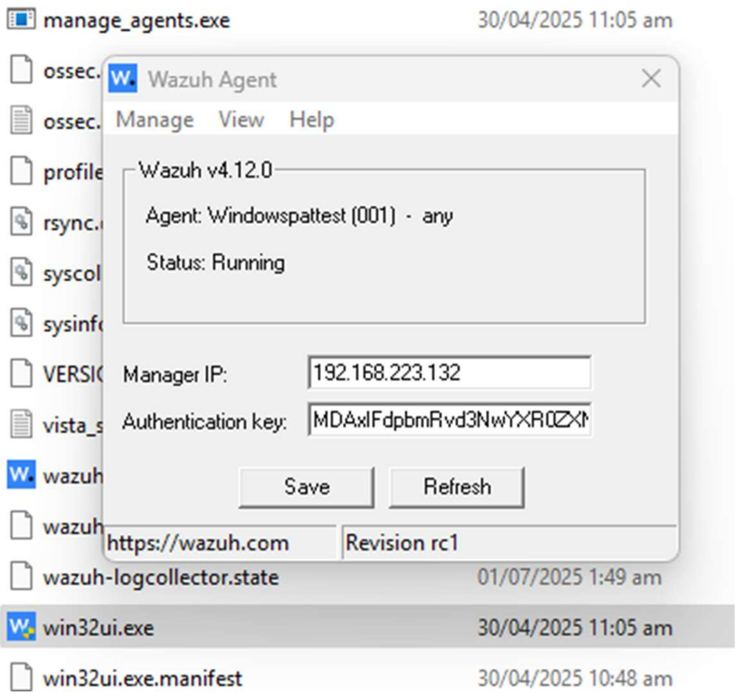
Time ↓	Path	Action	Rule description	Rule Lev...	Rule Id
No recent events					

Hands-on FIM, SCA and Vulnerability Scans

1) **File Integrity Monitoring (FIM)** is a feature in Wazuh SIEM to monitor files and directories whenever there are changes in real time or on a scheduled basis. It helps detect suspicious, unauthorized or unexpected file activity. Moreover, it detects creations, modifications, deletions, permission and ownership changes of files and folders.

   Configuration:

- Enable FIM configuration by editing ossec.conf file. \
- Find the location at C:\Program Files (86)\ossec agent
- Select win32ui.exe and view config to make changes on the FIM



```
manage_agents.exe        30/04/2025 11:05 am
ossec.
ossec.
profile
rsync.
syscol
sysinf
VERSIC
vista_s
wazuh
wazuh
wazuh-logcollector.state 01/07/2025 1:49 am
win32ui.exe              30/04/2025 11:05 am
win32ui.exe.manifest     30/04/2025 10:48 am
```

Wazuh Agent

Wazuh v4.12.0

Agent: Windowspattest (001) - any

Status: Running

Manager IP: 192.168.223.132

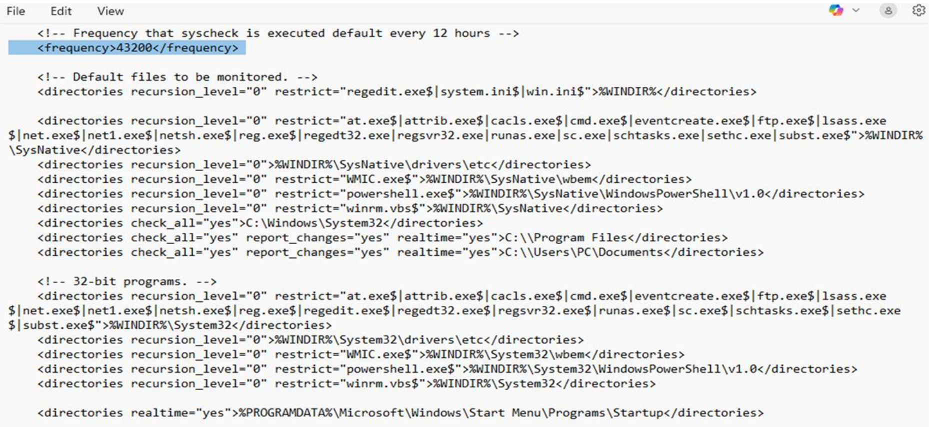
Authentication key: MDAxIFdpbmRvd3NwYXR0ZXN

https://wazuh.com

Revision rc1

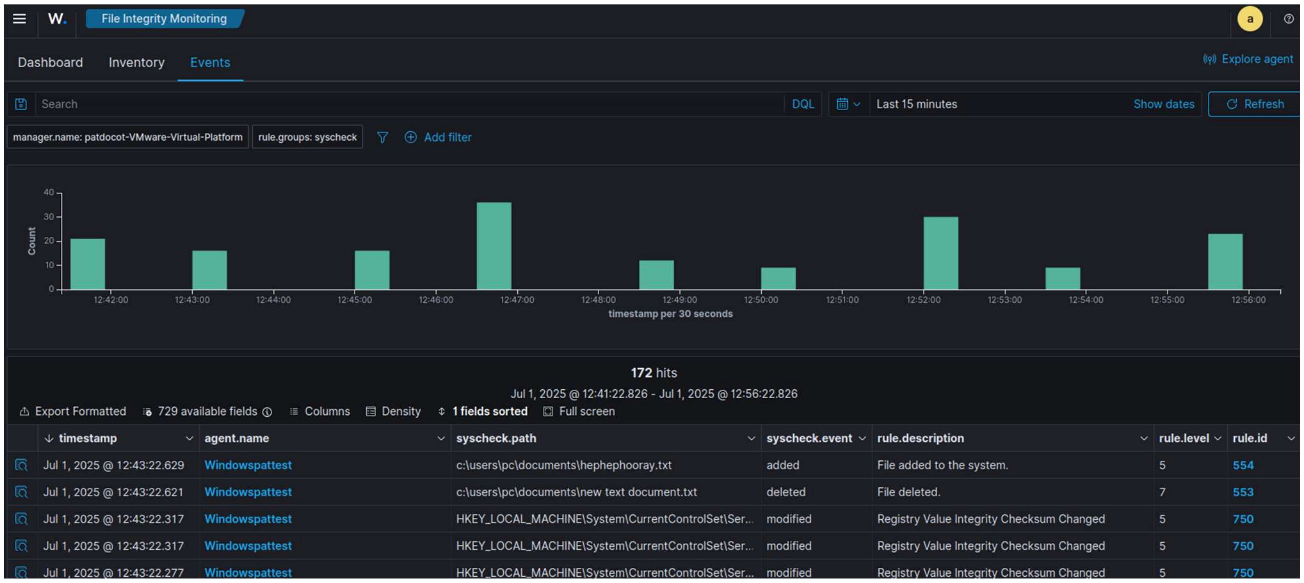
Roadblock/Challenge/s

There was a few delay in monitoring because I had challenges configuring the script. I thought there were mistakes in the script but I noticed that the frequency of the scan is 12 hours. I changed it to 10 seconds and I immediately saw the report of the changes in the Wazuh Dashboard.



```
    <!-- 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$|ftp.exe$|lsass.exe
$|net.exe$|net1.exe$|netsh.exe$|reg.exe$|regedt32.exe|regsvr32.exe|runas.exe|sc.exe|schtasks.exe|sethc.exe|subst.exe$">%WINDIR%
\SysNative</directories>
    <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</directories>
    <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\SysNative</directories>
    <directories check_all="yes">C:\Windows\System32</directories>
    <directories check_all="yes" report_changes="yes" realtime="yes">C:\\Program Files</directories>
    <directories check_all="yes" report_changes="yes" realtime="yes">C:\\Users\PC\Documents</directories>

    <!-- 32-bit programs. -->
    <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe
$|net.exe$|net1.exe$|netsh.exe$|reg.exe$|regedit.exe$|regedt32.exe$|regsvr32.exe$|runas.exe$|sc.exe$|schtasks.exe$|sethc.exe
$|subst.exe$">%WINDIR%\System32</directories>
    <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</directories>
    <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\System32</directories>

    <directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>
```

The image below shows the changes in different directories: Public, User, Documents, and Systems



172 hits

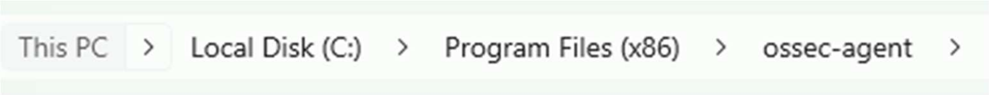
Jul 1, 2025 @ 12:41:22.826 - Jul 1, 2025 @ 12:56:22.826

timestamp	agent.name	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Jul 1, 2025 @ 12:43:22.629	Windowspattest	c:\users\pc\documents\hephephooray.txt	added	File added to the system.	5	554
Jul 1, 2025 @ 12:43:22.621	Windowspattest	c:\users\pc\documents\new text document.txt	deleted	File deleted.	7	553
Jul 1, 2025 @ 12:43:22.317	Windowspattest	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checksum Changed	5	750
Jul 1, 2025 @ 12:43:22.317	Windowspattest	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checksum Changed	5	750
Jul 1, 2025 @ 12:43:22.277	Windowspattest	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checksum Changed	5	750

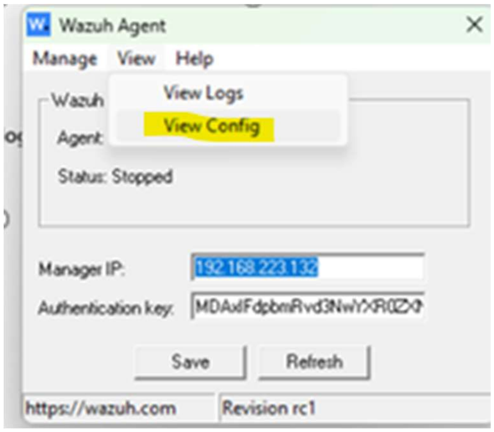
2) **Security Configuration Audit** or SCA is a security configuration feature that audits systems based on industry standards or custom policies. SCA checks whether a system's configuration complies with CIS Benchmarks, HIPAA, GDPR, and PCI-DSS.

Configuration:

Go to C:\Program Files (x86)\ossec-agent and run win32ui.exe>click view config. Once Wazuh is activated, it automatically starts scanning. You can add more scripts depending on the type of scan you want to perform.



This PC > Local Disk (C:) > Program Files (x86) > ossec-agent >

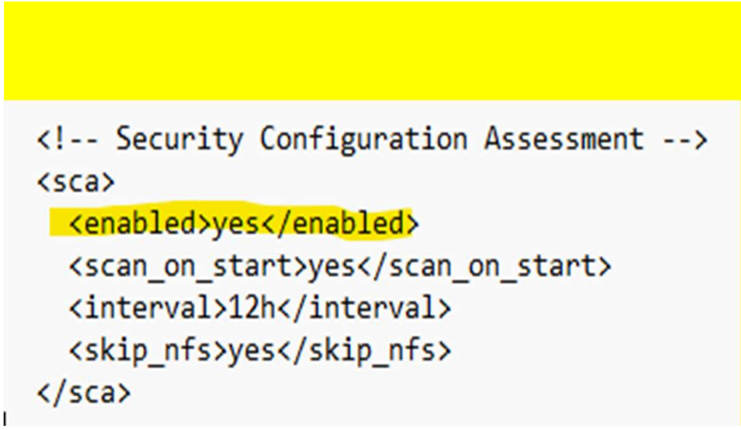


Agent:

Status: Stopped

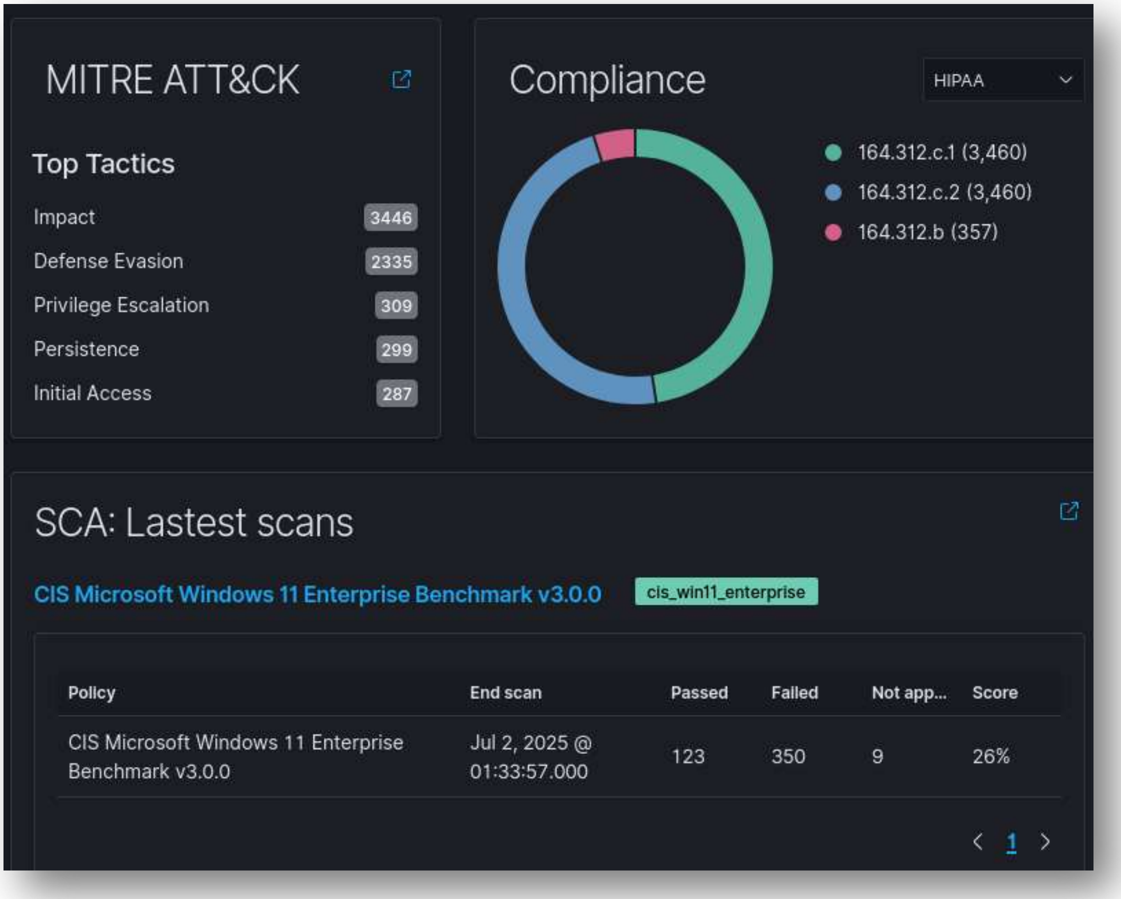
Manager IP: 192.168.223.132

Authentication key: MDAxIFdpbmRvd3NwYXR0ZX



```
<!-- Security Configuration Assessment -->
<sca>
  <enabled>yes</enabled>
  <scan_on_start>yes</scan_on_start>
  <interval>12h</interval>
  <skip_nfs>yes</skip_nfs>
</sca>
```

Here’s a quick look of the SCA dashboard. There is a dropdown option at the top right of the image and you can choose HIPAA, CIS Benchmarks, GDPR, PCI-DSS and see if the system complies to the standards or policies.



MITRE ATT&CK

Top Tactics

Impact	3446
Defense Evasion	2335
Privilege Escalation	309
Persistence	299
Initial Access	287

Compliance

HIPAA

- ● 164.312.c.1 (3,460)
- ● 164.312.c.2 (3,460)
- ● 164.312.b (357)

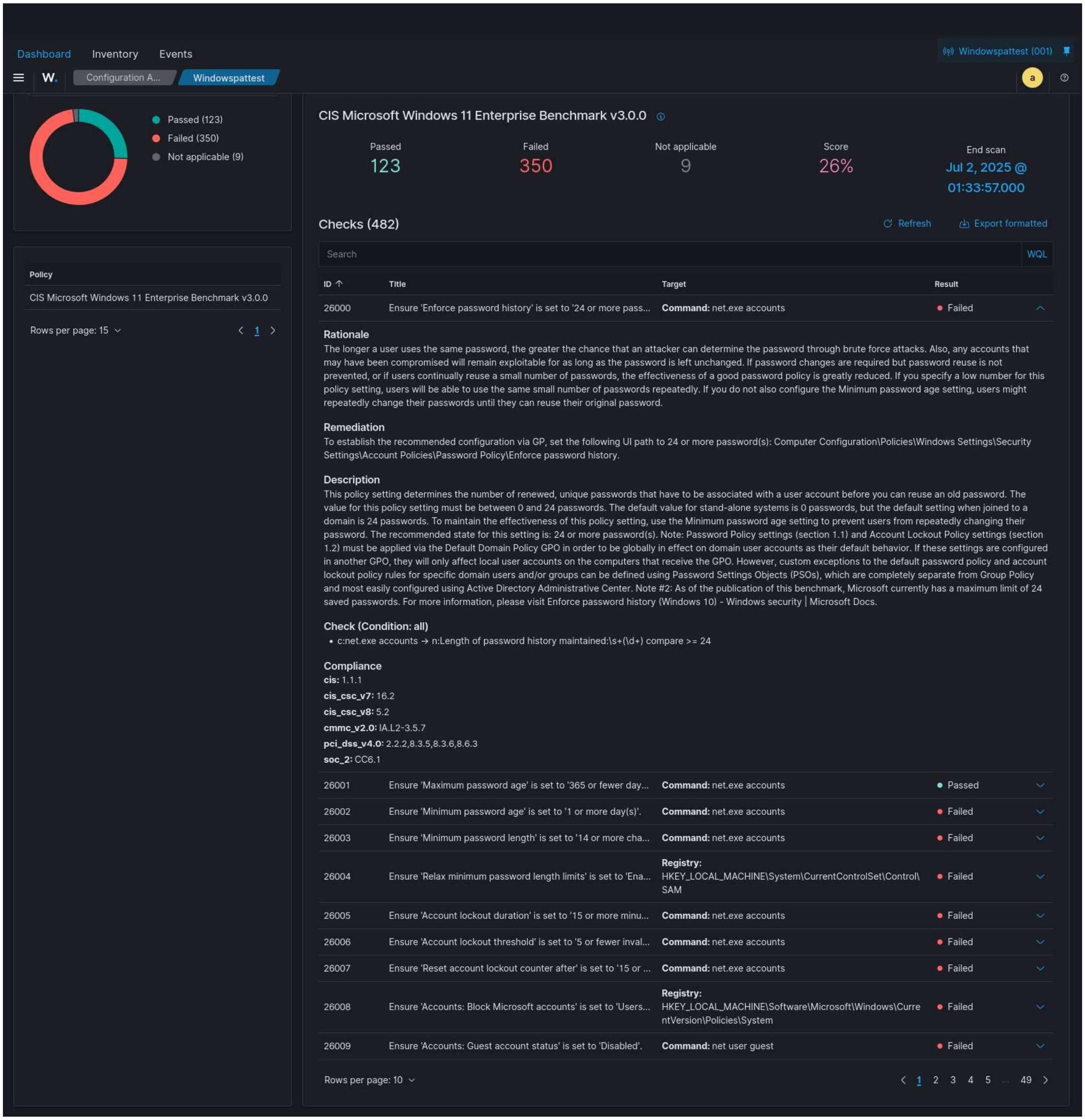
SCA: Lastest scans

CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0 cis_win11_enterprise

Policy	End scan	Passed	Failed	Not app...	Score
CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0	Jul 2, 2025 @ 01:33:57.000	123	350	9	26%

The dashboard displays results based on the most recent scan, including a clear pass/fail status for each item. By clicking on any failed item, you can view detailed information such as the vulnerability description, rationale, recommended solutions, and more.

It is crucial to follow the recommended steps to harden the system. Vulnerabilities, misconfigurations, or other security risks can potentially compromise the operating system, applications, and other system components.



Policy

CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0

Rows per page: 15 ⌄ ‹ 1 ›

CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0

Passed	Failed	Not applicable	Score	End scan
123	350	9	26%	Jul 2, 2025 @ 01:33:57.000

Checks (482)

ID ↑	Title	Target	Result
26000	Ensure 'Enforce password history' is set to '24 or more pass...	**Command:** net.exe accounts	● Failed

Rationale
The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced. If you specify a low number for this policy setting, users will be able to use the same small number of passwords repeatedly. If you do not also configure the Minimum password age setting, users might repeatedly change their passwords until they can reuse their original password.

Remediation
To establish the recommended configuration via GP, set the following UI path to 24 or more password(s): Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history.

Description
This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value for stand-alone systems is 0 passwords, but the default setting when joined to a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password. The recommended state for this setting is: 24 or more password(s). Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the Default Domain Policy GPO in order to be globally in effect on domain user accounts as their default behavior. If these settings are configured in another GPO, they will only affect local user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center. Note #2: As of the publication of this benchmark, Microsoft currently has a maximum limit of 24 saved passwords. For more information, please visit Enforce password history (Windows 10) - Windows security | Microsoft Docs.

Check (Condition: all)
- c:net.exe accounts → n:Length of password history maintained:\s+(\d+) compare >= 24

Compliance
cis: 1.1.1
cis_csc_v7: 16.2
cis_csc_v8: 5.2
cmmc_v2.0: IA.L2-3.5.7
pci_dss_v4.0: 2.2.2,8.3.5,8.3.6,8.6.3
soc_2: CC6.1

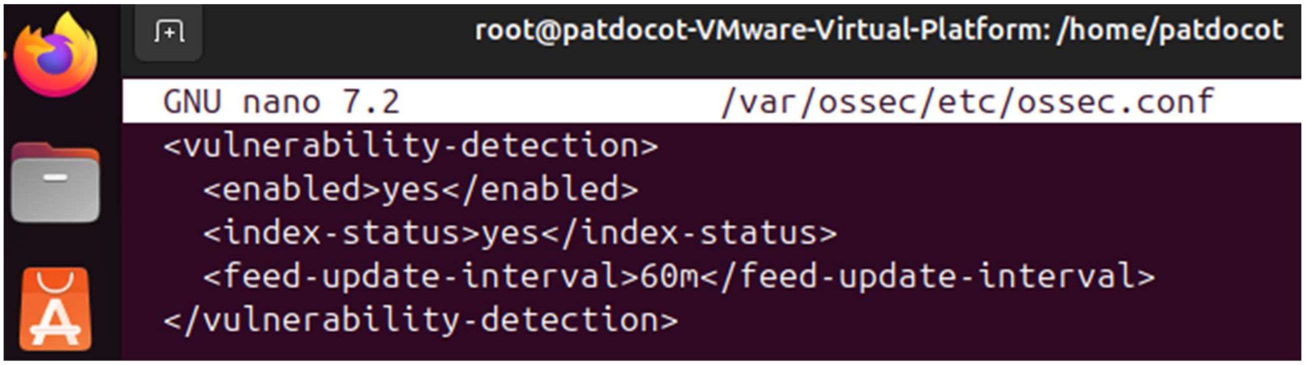
ID ↑	Title	Target	Result
26001	Ensure 'Maximum password age' is set to '365 or fewer day...	**Command:** net.exe accounts	● Passed
26002	Ensure 'Minimum password age' is set to '1 or more day(s)'.	**Command:** net.exe accounts	● Failed
26003	Ensure 'Minimum password length' is set to '14 or more cha...	**Command:** net.exe accounts	● Failed
26004	Ensure 'Relax minimum password length limits' is set to 'Ena...	**Registry:** HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SAM	● Failed
26005	Ensure 'Account lockout duration' is set to '15 or more minu...	**Command:** net.exe accounts	● Failed
26006	Ensure 'Account lockout threshold' is set to '5 or fewer inval...	**Command:** net.exe accounts	● Failed
26007	Ensure 'Reset account lockout counter after' is set to '15 or ...	**Command:** net.exe accounts	● Failed
26008	Ensure 'Accounts: Block Microsoft accounts' is set to 'Users...	**Registry:** HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	● Failed
26009	Ensure 'Accounts: Guest account status' is set to 'Disabled'.	**Command:** net user guest	● Failed

Rows per page: 10 ⌄ ‹ 1 2 3 4 5 ... 49 ›

3) **Vulnerability Detection.** There are few ways to find the ways on how it operates.

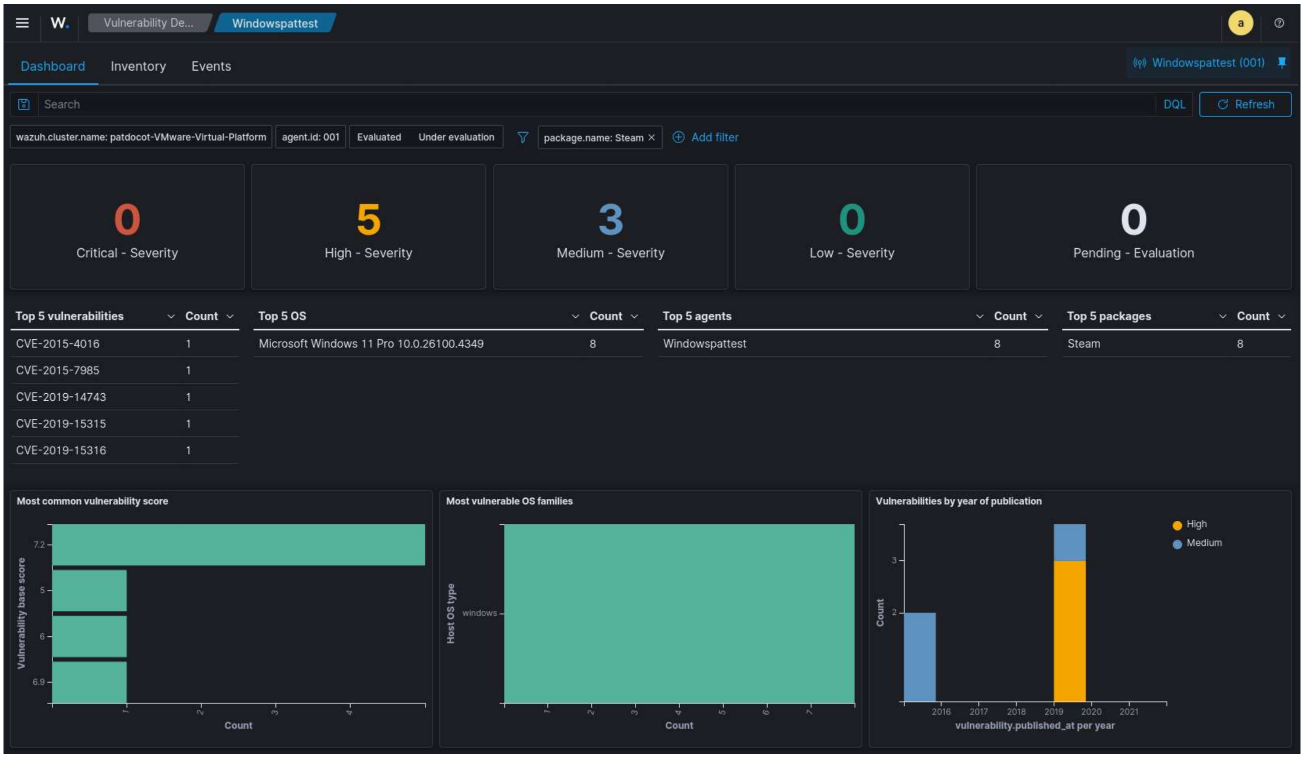
Configuration:

- First, you can find the script through C:\Program Files (x86)\ossec-agent>win32ui.exe>view config.
- This time, I will use the command >sudo nano /var/ossec/etc/ossec.conf (see image below)



```
root@patdocot-VMware-Virtual-Platform: /home/patdocot
GNU nano 7.2                    /var/ossec/etc/ossec.conf
<vulnerability-detection>
  <enabled>yes</enabled>
  <index-status>yes</index-status>
  <feed-update-interval>60m</feed-update-interval>
</vulnerability-detection>
```

The image below displays the Vulnerability Detection Dashboard. It provides an overview of the system inventory and related events, highlighting various CVE-linked vulnerabilities along with their severity levels. The dashboard also includes filter options and other helpful features. This visibility enables SOC analysts to effectively prioritize vulnerabilities that may pose a risk to systems and applications.



wazuh.cluster.name: patdocot-VMware-Virtual-Platform | agent.id: 001 | Evaluated Under evaluation | package.name: Steam

0 Critical - Severity | 5 High - Severity | 3 Medium - Severity | 0 Low - Severity | 0 Pending - Evaluation

Top 5 vulnerabilities	Count
CVE-2015-4016	1
CVE-2015-7985	1
CVE-2019-14743	1
CVE-2019-15315	1
CVE-2019-15316	1

Top 5 OS	Count
Microsoft Windows 11 Pro 10.0.26100.4349	8

Top 5 agents	Count
Windowspattest	8

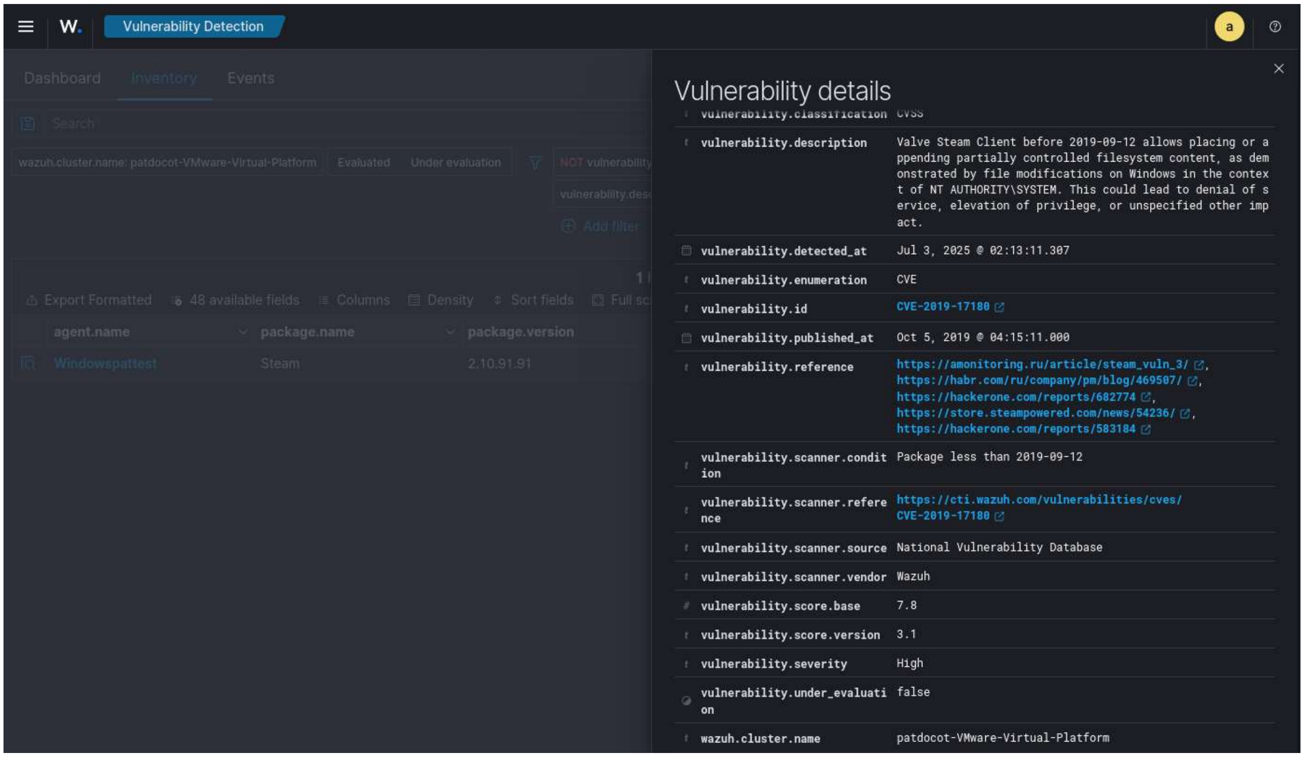
Top 5 packages	Count
Steam	8

Most common vulnerability score
Vulnerability base score
7.2
5
6
6.9
1
2
3
4
Count
Most vulnerable OS families
Host OS type
windows
1
2
3
4
5
6
7
Count
Vulnerabilities by year of publication
High
Medium
Count
3
2
2016
2017
2018
2019
2020
2021
vulnerability.published_at per year

The primary role of an SOC analyst is to prioritize vulnerabilities based on their severity. The highest-severity vulnerabilities are given top priority, as they pose the greatest potential threat to systems, web applications, and other assets.

Here are the steps on how to investigate and mitigate a vulnerability:

- Click the magnifying glass icon to inspect the vulnerability details.
- A pop-up window will provide the necessary details of the vulnerability.
- Vulnerability ID will show the associated CVE number as reference or track the vulnerability across systems and tools
- Vulnerability reference provides a clearer context, analysis and possible solutions from sources such as NVD, and other security advisories.



agent.name	package.name	package.version
Windowspattest	Steam	2.10.91.91

Vulnerability details

vulnerability.classification	CVSS
vulnerability.description	Valve Steam Client before 2019-09-12 allows placing or appending partially controlled filesystem content, as demonstrated by file modifications on Windows in the context of NT AUTHORITY\SYSTEM. This could lead to denial of service, elevation of privilege, or unspecified other impact.
vulnerability.detected_at	Jul 3, 2025 @ 02:13:11.307
vulnerability.enumeration	CVE
vulnerability.id	CVE-2019-17180
vulnerability.published_at	Oct 5, 2019 @ 04:15:11.000
vulnerability.reference	https://amonitoring.ru/article/steam_vuln_3/, https://habr.com/ru/company/pm/blog/469507/, https://hackerone.com/reports/682774, https://store.steampowered.com/news/54236/, https://hackerone.com/reports/583184
vulnerability.scanner.condition	Package less than 2019-09-12
vulnerability.scanner.reference	https://cti.wazuh.com/vulnerabilities/cves/CVE-2019-17180
vulnerability.scanner.source	National Vulnerability Database
vulnerability.scanner.vendor	Wazuh
vulnerability.score.base	7.8
vulnerability.score.version	3.1
vulnerability.severity	High
vulnerability.under_evaluation	false
wazuh.cluster.name	patdocot-VMware-Virtual-Platform