

Wazuh SIEM Project

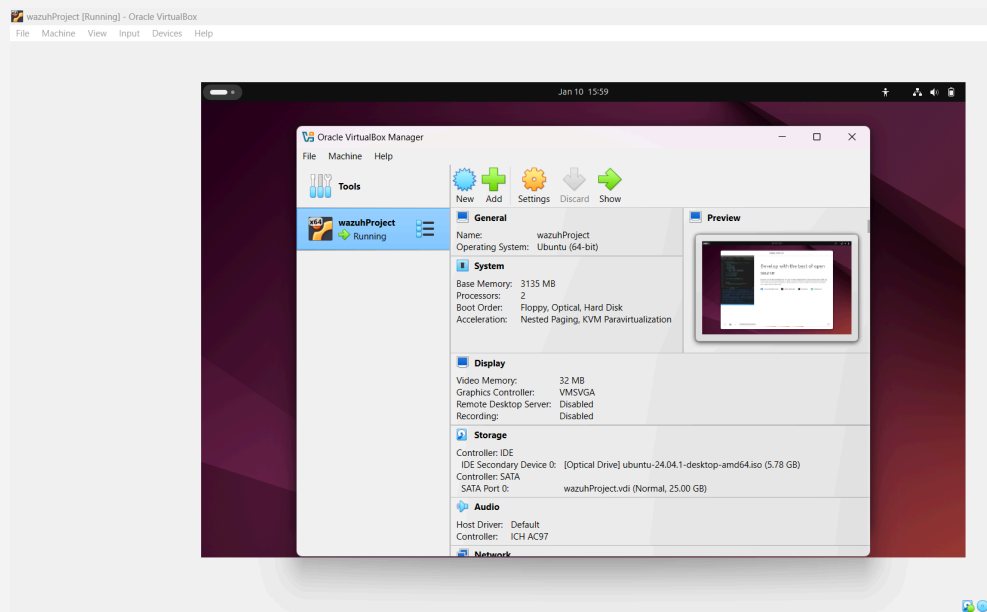
Jaleel Calhoun

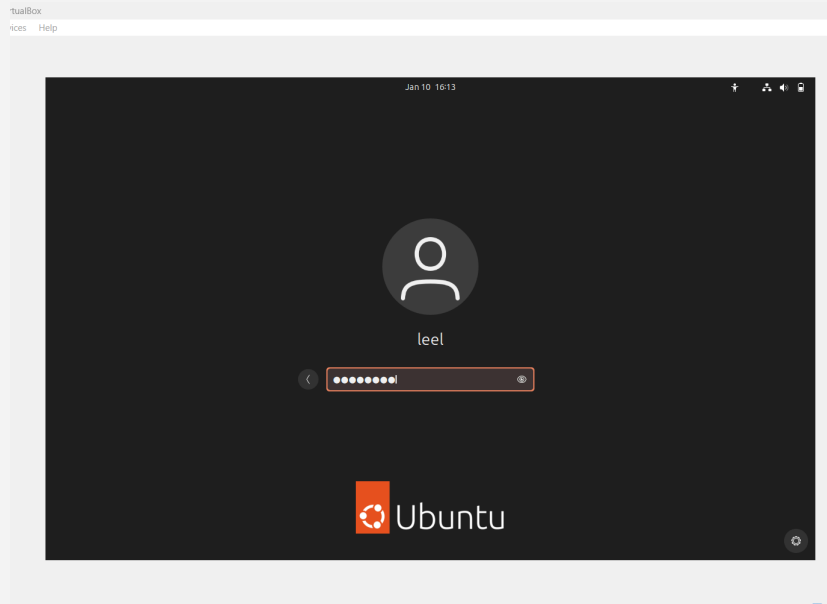
Objective:

- Install free SIEM platform “Wazuh” hosting on a linux VM to analyze endpoint device(s) and explore additional Wazuh capabilities. To then configure and utilize Wazuh to harden endpoint security/remediate vulnerabilities from added devices.

Setting up Virtual Machine and Wazuh

Installed Oracle VM and Ubuntu linux to set up a linux VM:





Installed Wazuh in the linux terminal once logged into Ubuntu. Ensured [hardware requirements](#) were met to install Wazuh.

- Received log in credentials and instructions during installation

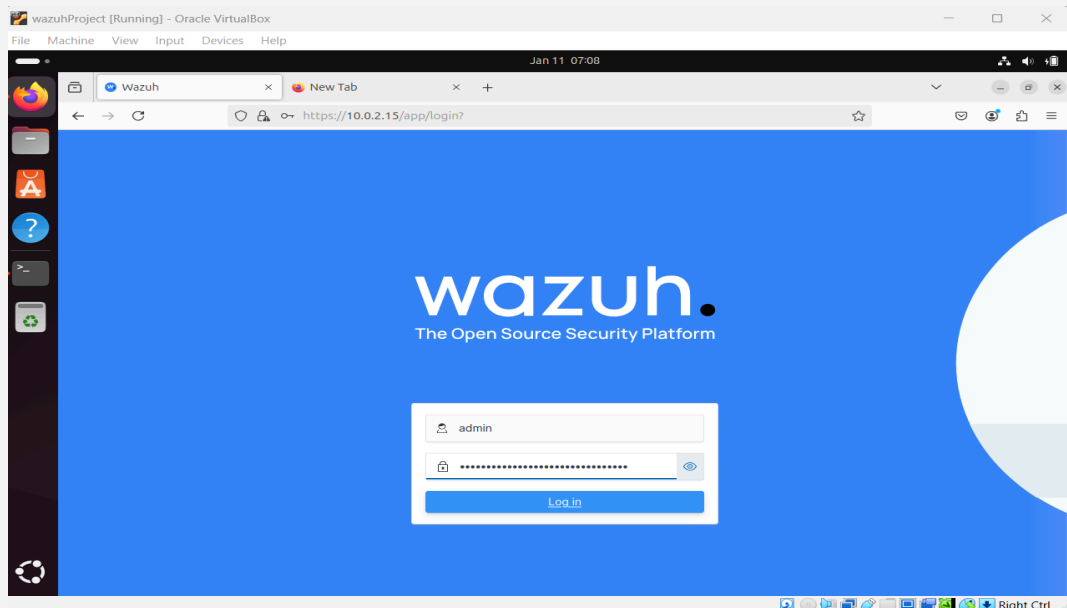
```
wazuhProject [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Jan 11 07:05
leel@wazuhProject: ~

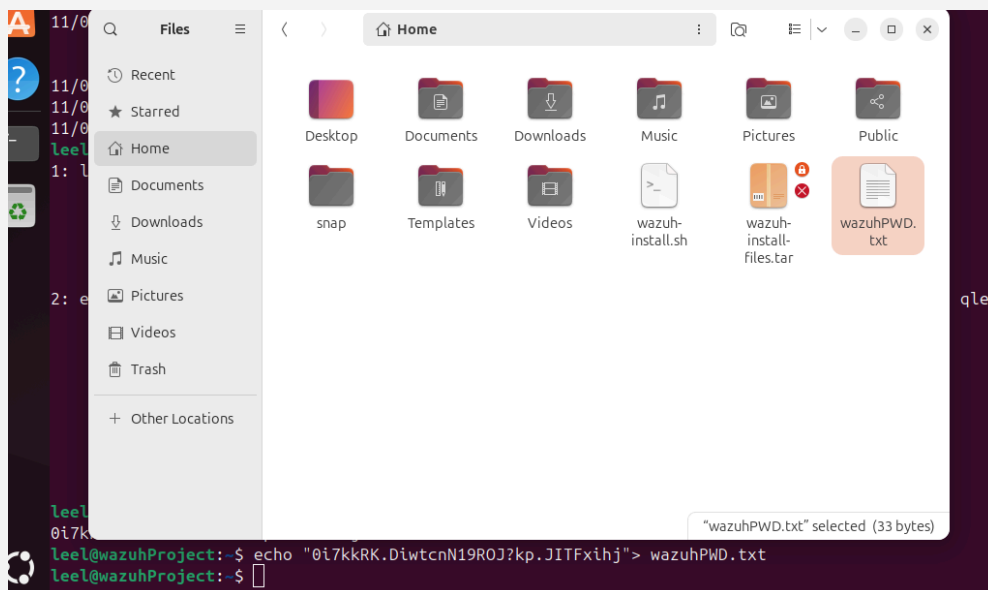
leel@wazuhProject:~$ curl -sO https://packages.wazuh.com/4.10/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
11/01/2025 06:39:04 INFO: Starting Wazuh installation assistant. Wazuh version: 4.10.0
11/01/2025 06:39:04 INFO: Verbose logging redirected to /var/log/wazuh-install.log
11/01/2025 06:39:10 INFO: --- Dependencies ---
11/01/2025 06:39:10 INFO: Installing gawk.
11/01/2025 06:54:42 INFO: Wazuh dashboard web application not yet initialized. Waiting...
11/01/2025 06:54:57 INFO: Wazuh dashboard web application initialized.
11/01/2025 06:54:57 INFO: --- Summary ---
11/01/2025 06:54:57 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
User: admin
Password: 0i7kkRK.DiwtcnN19R0J?kp.JITFxihj
11/01/2025 06:54:57 INFO: --- Dependencies ---
11/01/2025 06:54:57 INFO: Removing gawk.
11/01/2025 06:55:06 INFO: Installation finished.
leel@wazuhProject:~$
```

- Used “ip a s” command to receive the ip address of the VM to be able to access the Wazuh interface/dashboard in the browser.

```
11/01/2025 06:54:57 INFO: Removing gawk.
11/01/2025 06:55:06 INFO: Installation finished.
leel@wazuhProject:~$ ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:5b:0c:71 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 84798sec preferred_lft 84798sec
    inet6 fd00::332e:bfff:b89a:251f/64 scope global temporary dynamic
        valid_lft 84798sec preferred_lft 84798sec
```

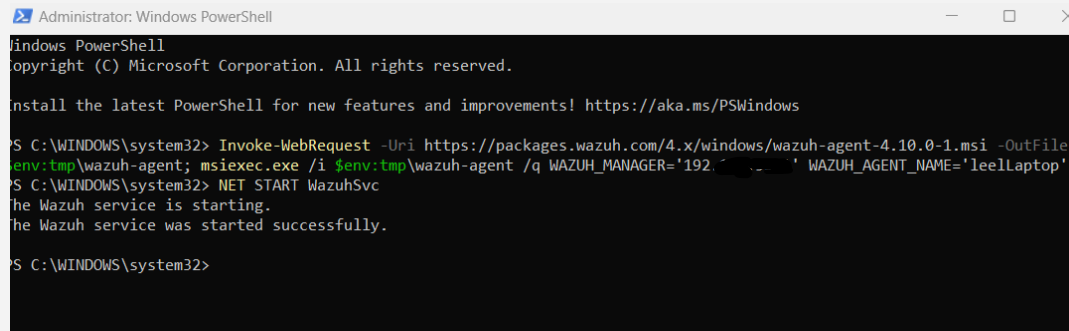


- Used command (echo "provided_password_txt"> file_Name.txt) to place the provided password in a text file for future use.



Add endpoint device to Wazuh once able to log in to the platform

- Utilizing Windows device and used the following commands to connect device to Wazuh server
- Used Windows Powershell as admin



```
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-4.10.0-1.msi -OutFile
env:tmp\wazuh-agent; msixexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.1.100' WAZUH_AGENT_NAME='leellaptop'
PS C:\WINDOWS\system32> NET START WazuhSvc
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\WINDOWS\system32>
```

Obstacles

Troubleshooting process I had endured:

- After running the commands above to add a Windows device to Wazuh, I noticed the device did not add properly.
- Tested the network connection of the VM to Windows device, and the status failed.
- Confirmed the ip addresses of both machines were accurate and analyzed the VM's network settings.
- Found a solution of switching the network adapter from NAT to bridged to enable a shared network.
- Tested the network connection of the two machines and it was successful. Enabling myself to add the Windows machine properly.
- Would have analyzed if the necessary ports were open and view if there were any network security such as firewalls preventing access

```

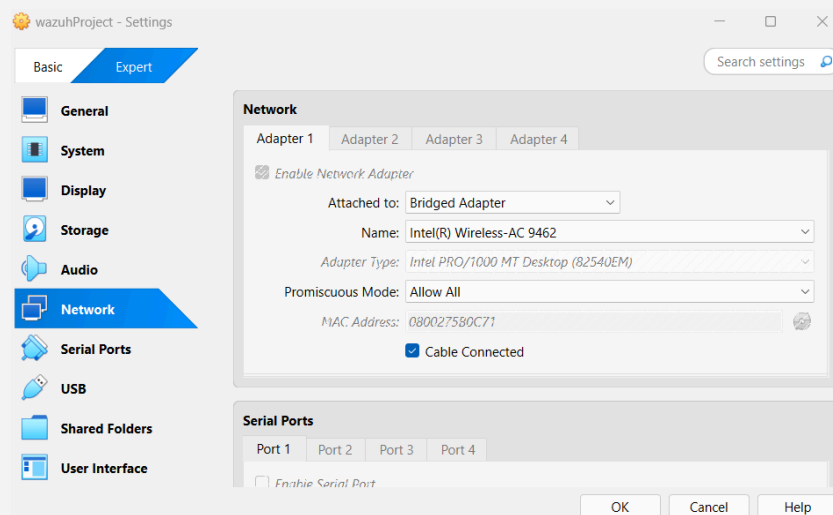
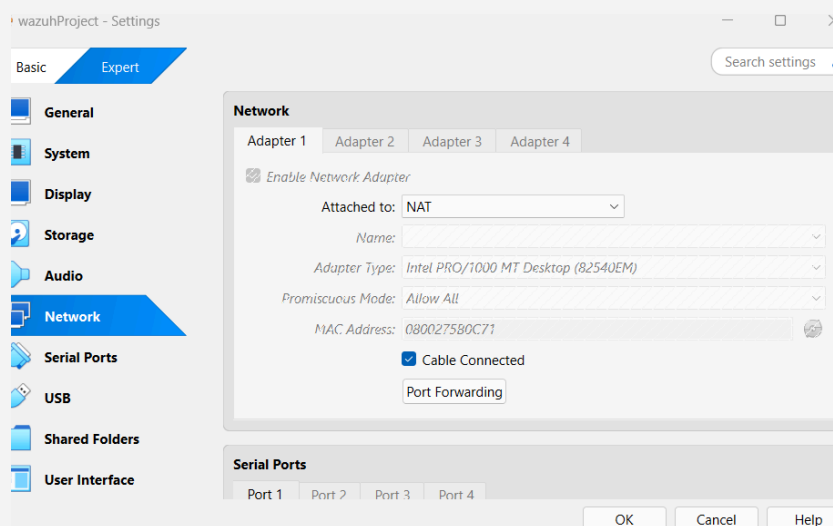
PS C:\Program Files (x86)\ossec-agent> Test-NetConnection -ComputerName 10.0.2.15 -Port 1555
WARNING: TCP connect to (10.0.2.15 : 1555) failed
WARNING: Ping to 10.0.2.15 failed with status: TimedOut

ComputerName      : 10.0.2.15
RemoteAddress     : 10.0.2.15
RemotePort        : 1555
InterfaceAlias    : Wi-Fi
SourceAddress     : 192.168.1.100
PingSucceeded     : False
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded  : False

PS C:\Program Files (x86)\ossec-agent> Test-NetConnection -ComputerName 192.168.1.100 -Port 1555

ComputerName      : 192.168.1.100
RemoteAddress     : 192.168.1.100
RemotePort        : 1555
InterfaceAlias    : Wi-Fi
SourceAddress     : 192.168.1.100
PingSucceeded     : True
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded  : True

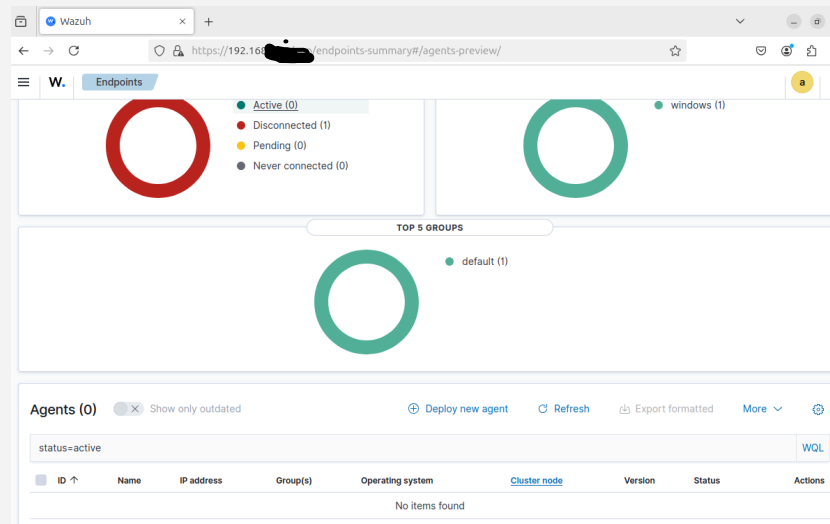
```



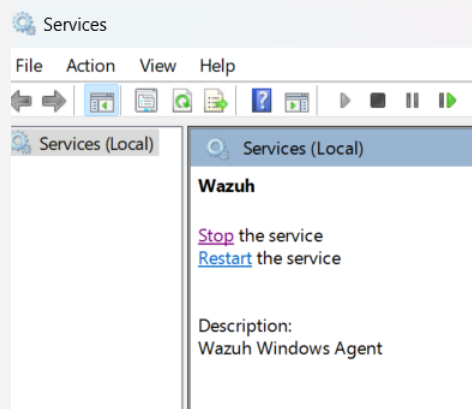
Reconnecting Windows machine to Wazuh server

- Continued this project on a new day and was unable to load up Wazuh log in page due to a VM ip address change
- Obtained current ip address from VM to use for Wazuh's login page

```
leel@wazuhProject: ~  
leel@wazuhProject:~$ ip a s  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500  
    group default qlen 1000  
    link/ether 08:00:27:5b:0c:71 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.1.10/24 brd 192.168.1.255 scope global enp0s3
```



- As presented above, the Window machine disconnected
- So I stopped the current Wazuh server connection on Window machine



- Updated Wazuh's configuration file on the windows machine and modified the updated ip address into the <Address> tag
- Saved the "Ossec.conf" file

```

ossec.conf
File Edit View

<!--
Wazuh - Agent - Default configuration for Windows
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>

  <client>
    <server>
      <address>192.168.1.100</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>windows, windows10</config-profile>
    <crypto_method>aes</crypto_method>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
  </client>

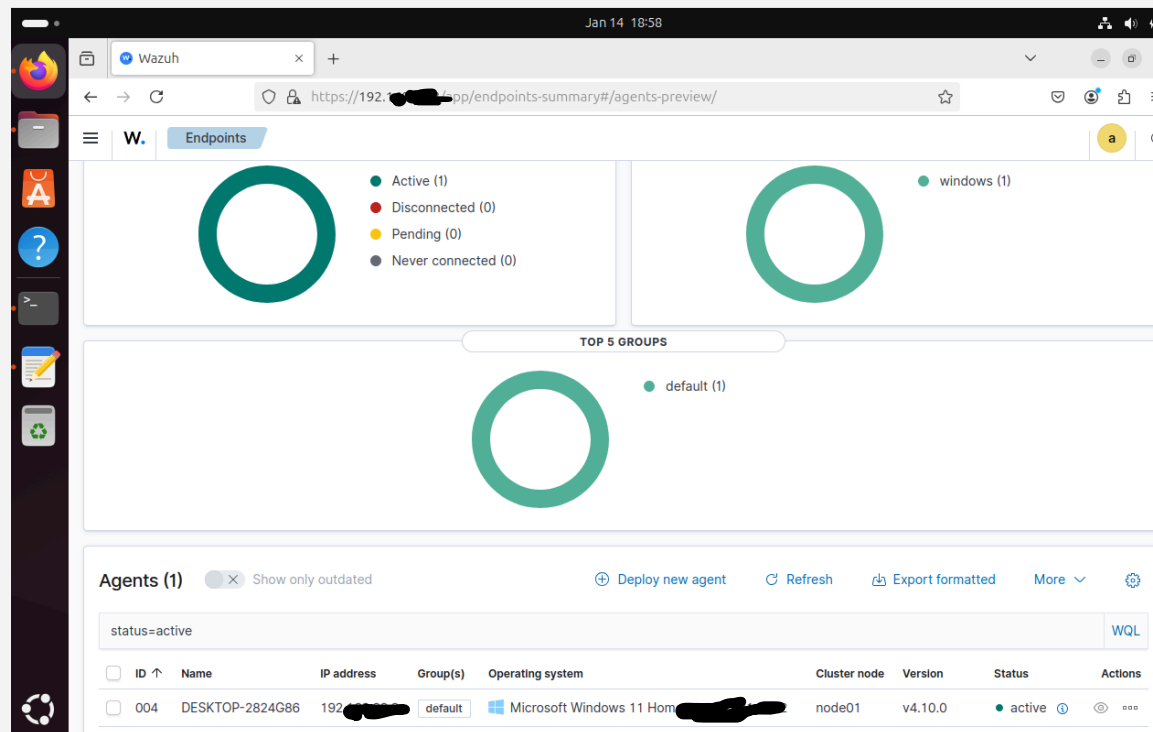
```

- Reconnected to Wazuh server on Windows Powershell as admin

```

PS C:\WINDOWS\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.10.0-1.msi -OutFile
env:tmp\wazuh-agent; msixexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.1.100' WAZUH_AGENT_NAME='leelLaptop'
PS C:\WINDOWS\system32> NET START WazuhSvc
The Wazuh service is starting.
The Wazuh service was started successfully.
PS C:\WINDOWS\system32>

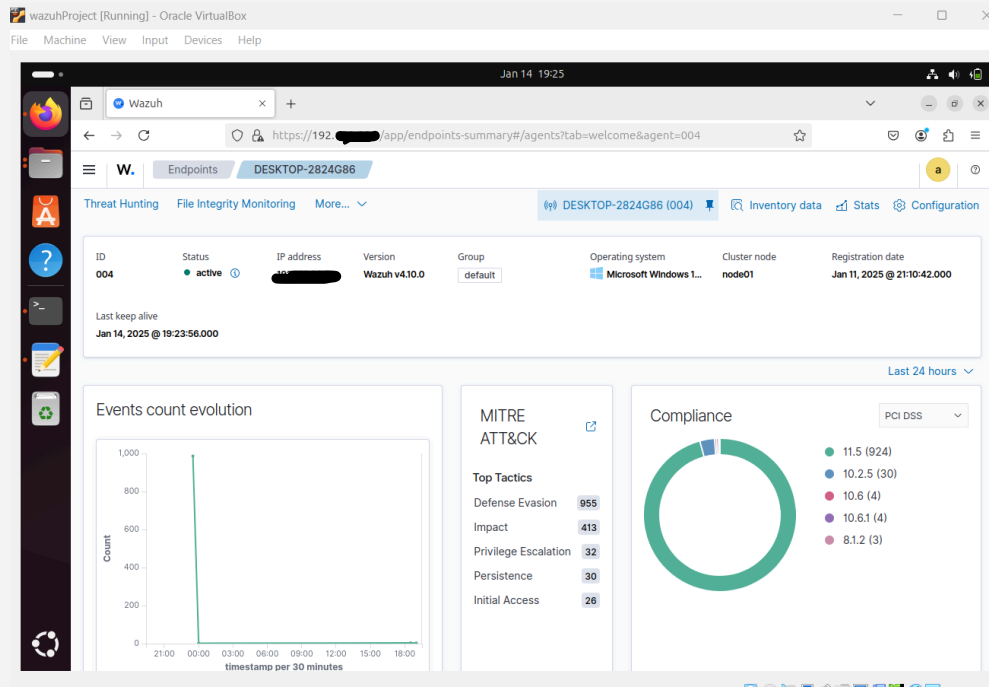
```



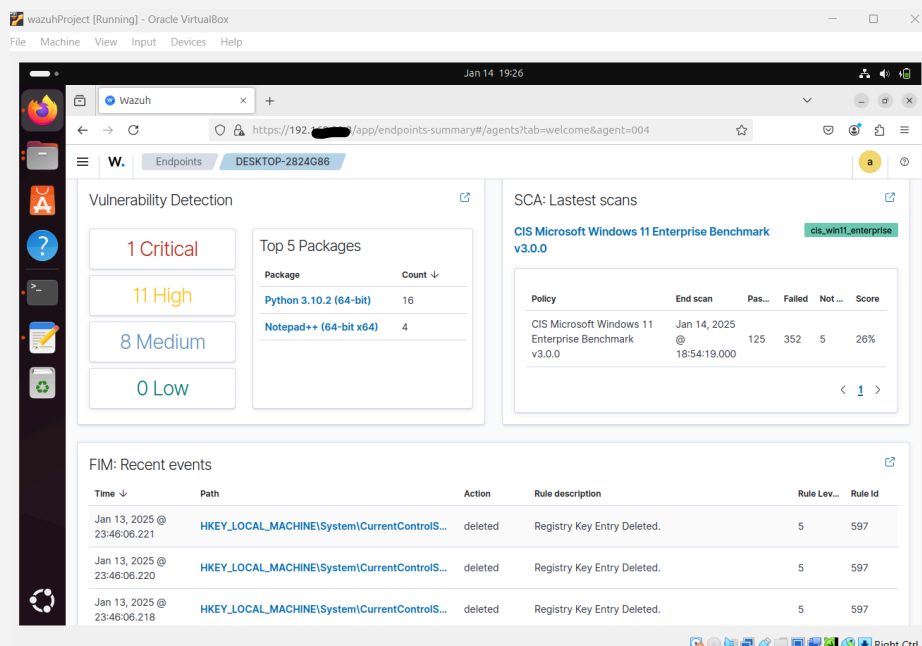
- Successfully reconnected Window machine to Wazuh

Wazuh Dashboard

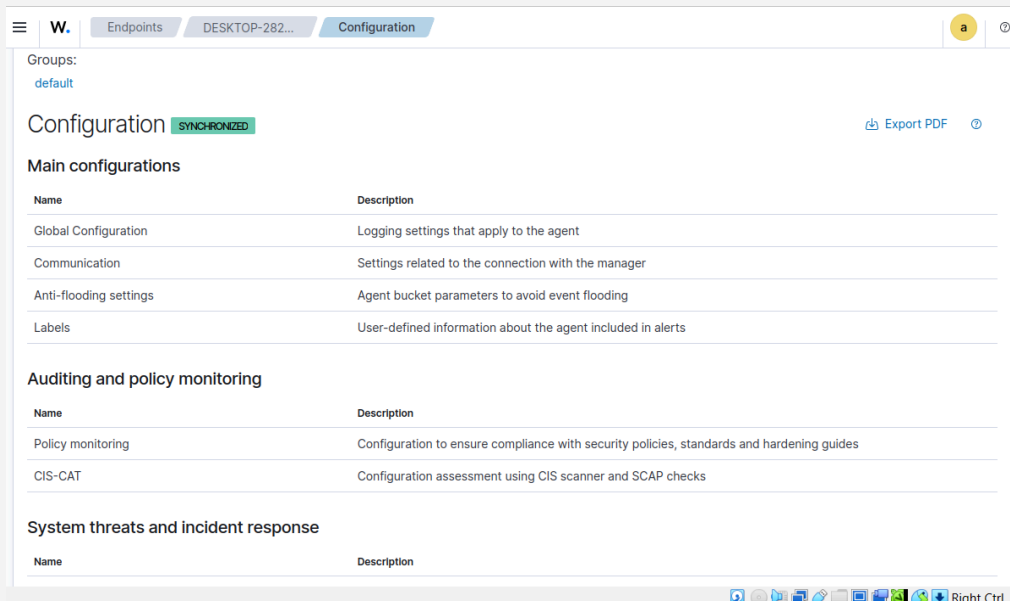
Endpoint monitoring:



- Provides essential information of each endpoint to help monitor and improve security structure. Wazuh utilizes industry known standards/regulations and databases aligned with known vulnerabilities/malware to scan endpoint devices to highlight important insights.



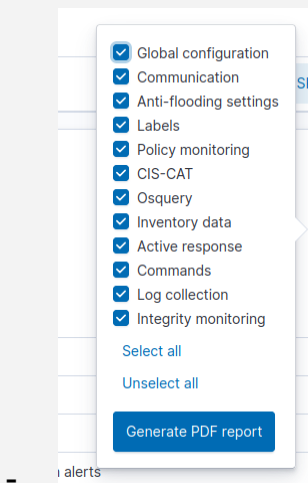
Endpoint configuration:



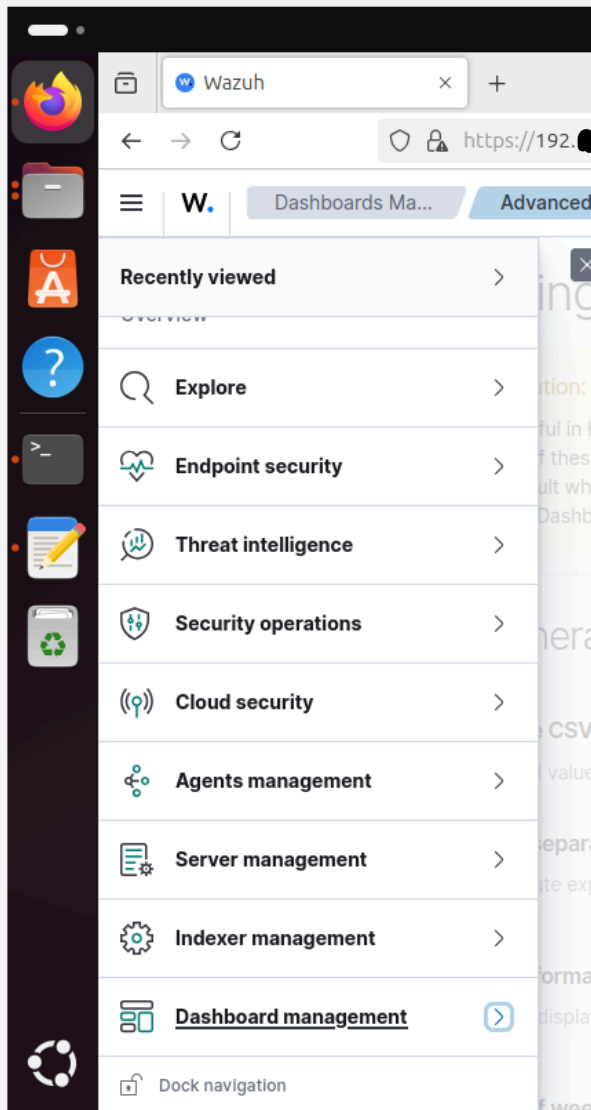
Main configurations such as:

- Auditing and policy monitoring
- System threats and incident response
- Log data analysis
- Cloud security monitoring

May also export a PDF report of selected sections:

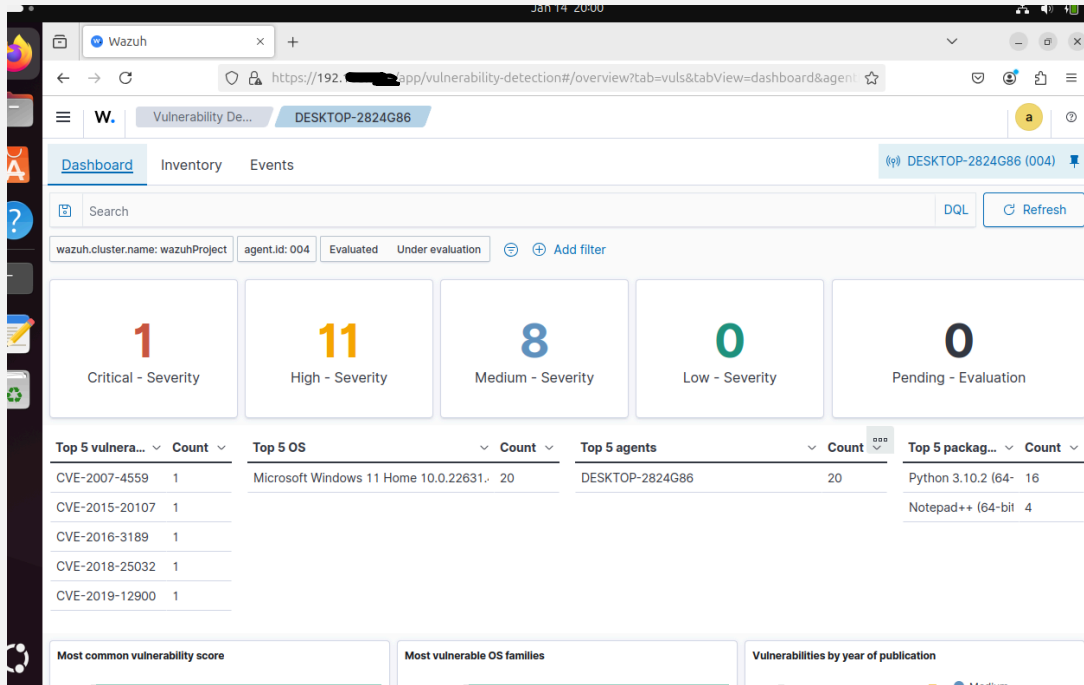


Tabs to navigate to:

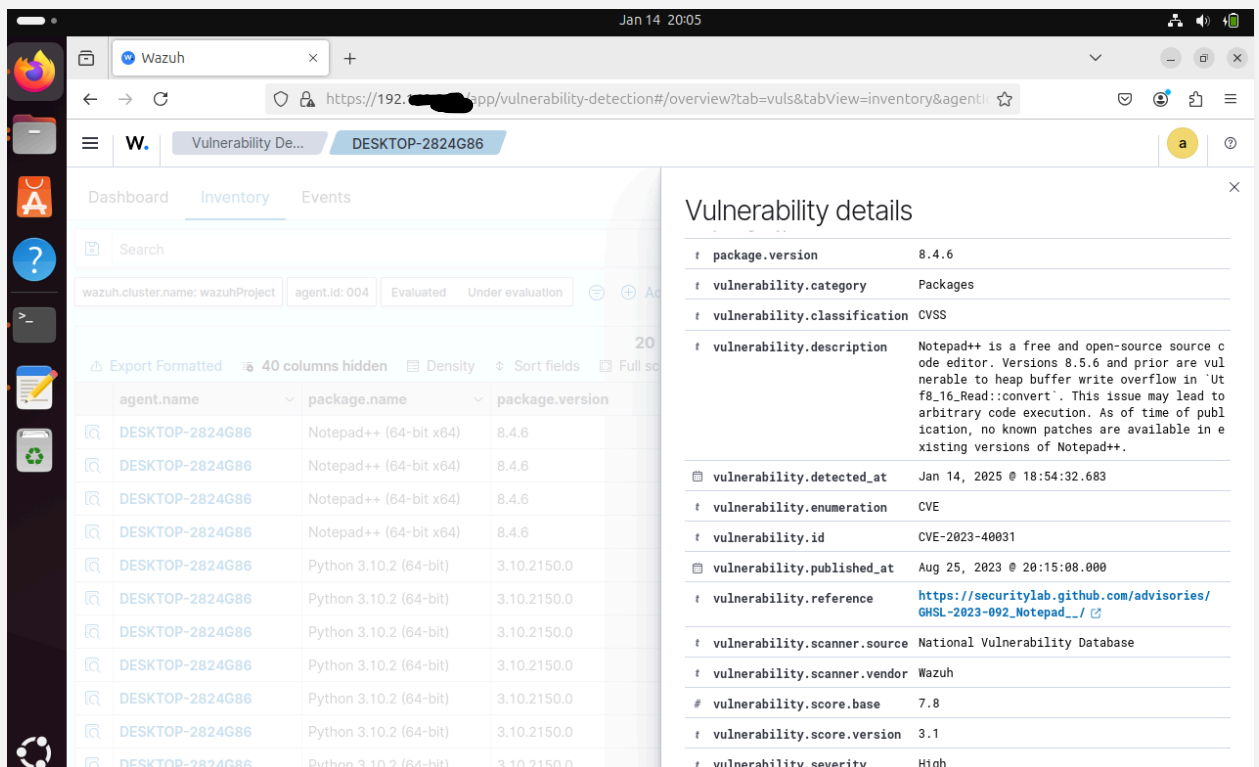


Many great capabilities with this tool. Opportunities for integrations with other tools and even cloud. Exploring each tab enables further options to enhance an individual's or group's security structure and security operations.

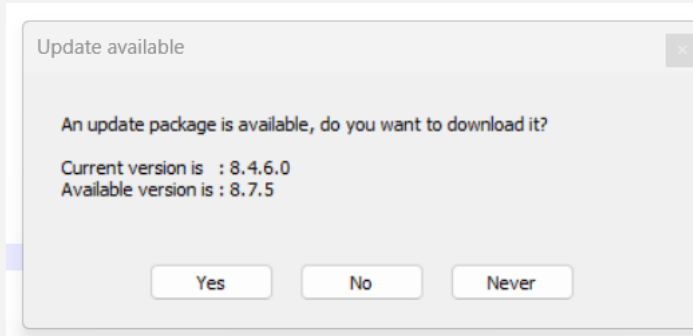
Mitigating Vulnerabilities and Improving Security Structure



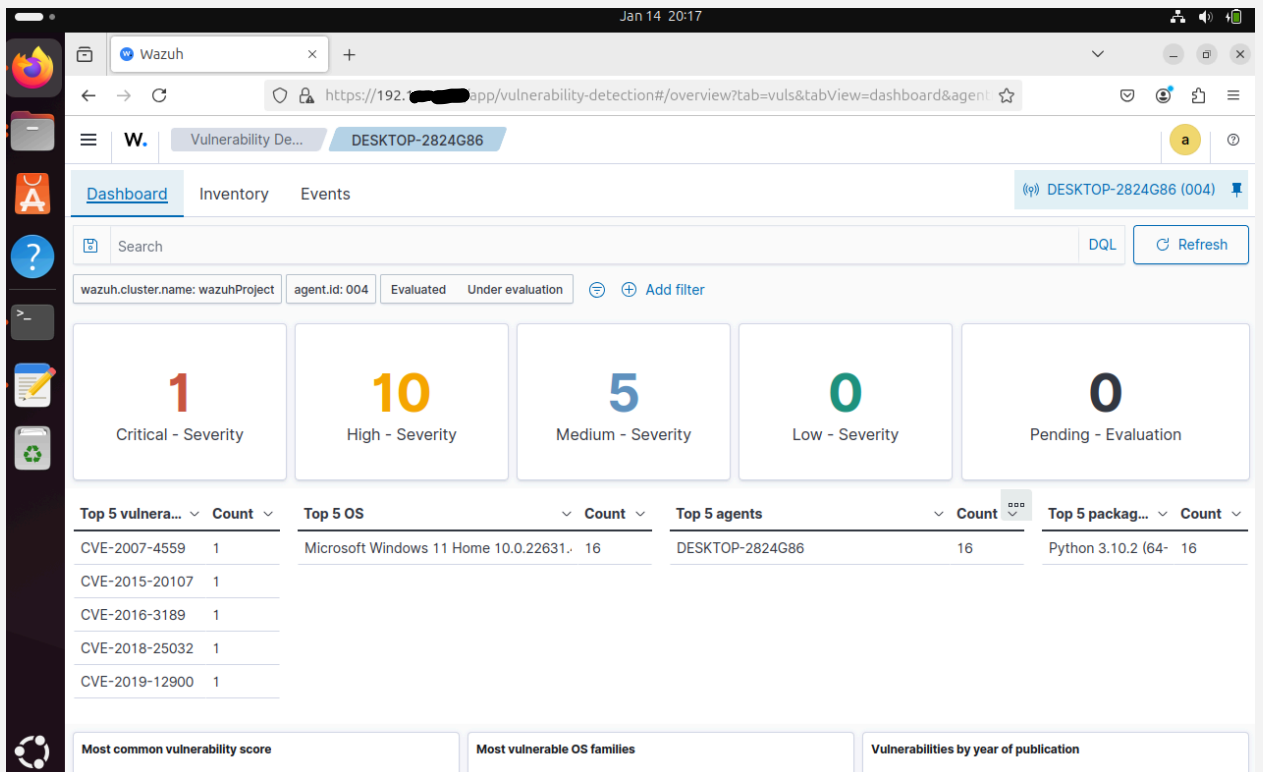
- Python v 3.10.2 and Notepad++ are presented as the packages that contain vulnerabilities
- Inspected a listed vulnerability and updated the app's version to view updated Wazuh dashboard



Updating notepad ++



- Restarted Wazuh server on Window Machine
- Would like to possibly modify the config file on Windows machine to have Wazuh server automatically refresh when apps are updated in future scope



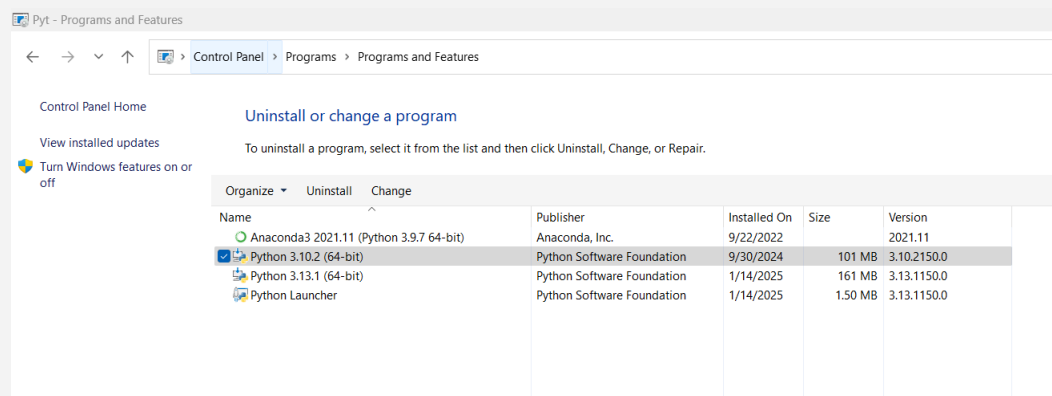
The screenshot shows the Wazuh Vulnerability Detection dashboard for agent DESKTOP-2824G86. The dashboard includes a search bar, filters for cluster name (wazuhProject) and agent ID (004), and a table of vulnerabilities. The table is organized into four columns: Top 5 vulnerabilities by severity, Top 5 OS, Top 5 agents, and Top 5 packages. The severity counts are: Critical (1), High (10), Medium (5), Low (0), and Pending (0). The OS is Microsoft Windows 11 Home 10.0.22631.0 with 16 vulnerabilities. The agent is DESKTOP-2824G86 with 16 vulnerabilities. The package is Python 3.10.2 (64-bit) with 16 vulnerabilities. The dashboard also includes a sidebar with navigation links (Dashboard, Inventory, Events) and a bottom section with charts for most common vulnerability scores, most vulnerable OS families, and vulnerabilities by year of publication.

Top 5 vuln...	Count	Top 5 OS	Count	Top 5 agents	Count	Top 5 packag...	Count
CVE-2007-4559	1	Microsoft Windows 11 Home 10.0.22631.0	16	DESKTOP-2824G86	16	Python 3.10.2 (64-bit)	16
CVE-2015-20107	1						
CVE-2016-3189	1						
CVE-2018-25032	1						
CVE-2019-12900	1						

Upgraded current python to newest version



- Navigate to control panel - Program and features - Search up the package name to uninstall on windows machine



- Restarted Wazuh server on windows machine and viewed updated dashboard

Jan 14 21:38

Wazuh

https://192.168.1.100/app/endpoints-summary#/agents?tab=welcome&agent=004

Endpoints

DESKTOP-2824G86

0 Critical

0 High

0 Medium

0 Low

Top 5 Packages

Package

Count ↓

No recent events

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	Jan 14, 2025 @ 21:36:06.000	125	352	5	26%

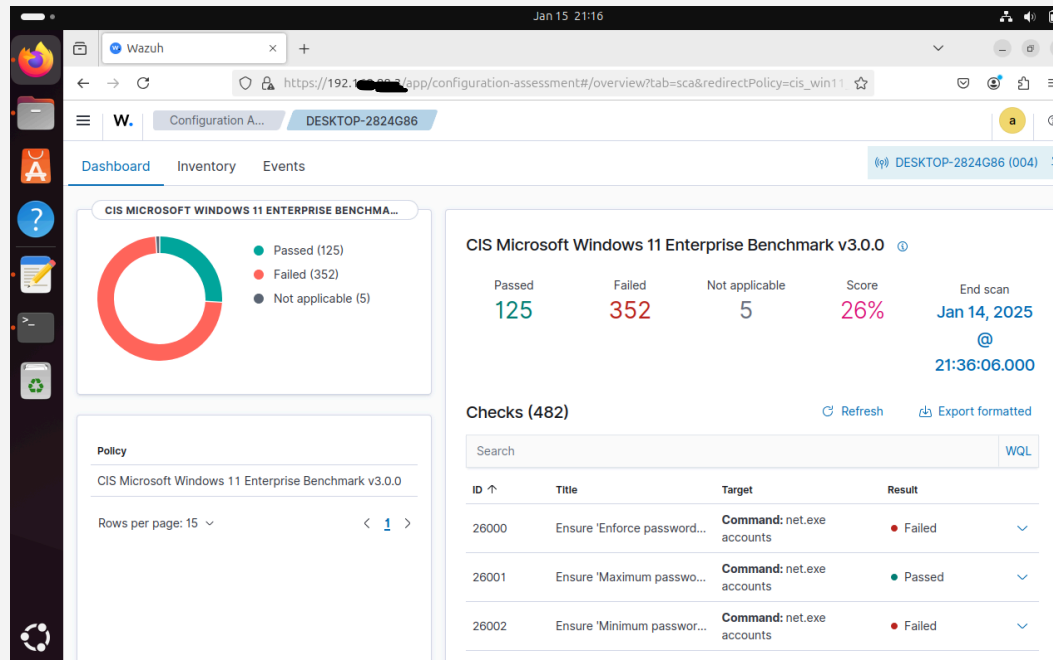
< 1 >

FIM: Recent events

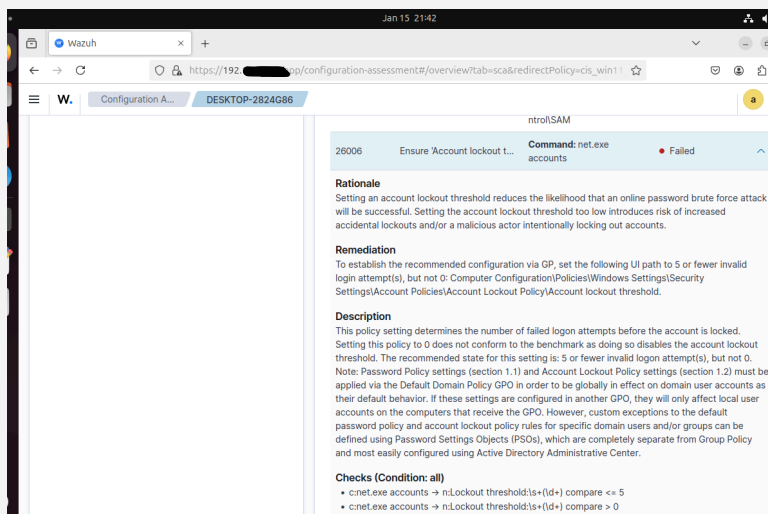
Time ↓	Path	Action	Rule description	Rule Lev...	Rule Id
Jan 13, 2025 @ 23:46:06.221	HKEY_LOCAL_MACHINE\System\CurrentControlS...	deleted	Registry Key Entry Deleted.	5	597
Jan 13, 2025 @ 23:46:06.220	HKEY_LOCAL_MACHINE\System\CurrentControlS...	deleted	Registry Key Entry Deleted.	5	597
Jan 13, 2025 @	HKEY_LOCAL_MACHINE\System\CurrentControlS...	deleted	Registry Key Entry Deleted.	5	597

SCA implements

SCA (Security Configuration Assessment) latest scan compliance/noncompliance with CIS (Center for Internet Security) Microsoft windows 11 Enterprise benchmark v3.0.0:



- Window device's configurations/misconfigurations that do or do not meet CIS standards.
- Used analysis to remediate risks and harden device(s) based on CIS standards to improve security settings.
- Remediated a failed control for account lockout:



- Provides essential information such as descriptions and remediation suggestions

- Navigated to Windows powershell and run the following command to set threshold:

```
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

S C:\WINDOWS\system32> net accounts /lockoutthreshold:5
The command completed successfully.

S C:\WINDOWS\system32>
```

- Restarted Wazuh server on windows machine and restarted window machine
- Control updated to “pass” status, ensuring compliance with CIS policy

26006

Ensure 'Account lockout t...

Command: net.exe accounts

Passed

Rationale

Setting an account lockout threshold reduces the likelihood that an online password brute force attack will be successful. Setting the account lockout threshold too low introduces risk of increased accidental lockouts and/or a malicious actor intentionally locking out accounts.

Remediation

To establish the recommended configuration via GP, set the following UI path to 5 or fewer invalid login attempt(s), but not 0: Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold.

Description

This policy setting determines the number of failed logon attempts before the account is locked. Setting this policy to 0 does not conform to the benchmark as doing so disables the account lockout threshold. The recommended state for this setting is: 5 or fewer invalid logon attempt(s), but not 0.

Wazuh

https://localhost:55000/configuration-assessment#/overview?tab=sca&redirectPolicy=cis_win11

Configuration A... DESKTOP-2824G88

Dashboard Inventory Events

DESKTOP-2824G88 (004)

CIS MICROSOFT WINDOWS 11 ENTERPRISE BENCHMARK v3.0.0

Passed (126)

Failed (351)

Not applicable (5)

CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0

Passed 126

Failed 351

Not applicable 5

Score 26%

End scan Jan 15, 2025 22:17:34.000

Checks (482)

Refresh Export formatted

Search WQL

ID	Title	Target	Result
26000	Ensure 'Enforce password...	Command: net.exe accounts	Failed
26001	Ensure 'Maximum passwo...	Command: net.exe accounts	Passed

File integrity monitoring:

Windows Wazuh agent:

- Opened config file “ossec.conf” with admin role on Windows powershell:

```
S C:\WINDOWS\system32> notepad "C:\Program Files (x86)\ossec-agent\ossec.conf"
```

- Added Downloads directory within <syscheck> tag in config file for file monitoring in *realtime*:


```

</sca>

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

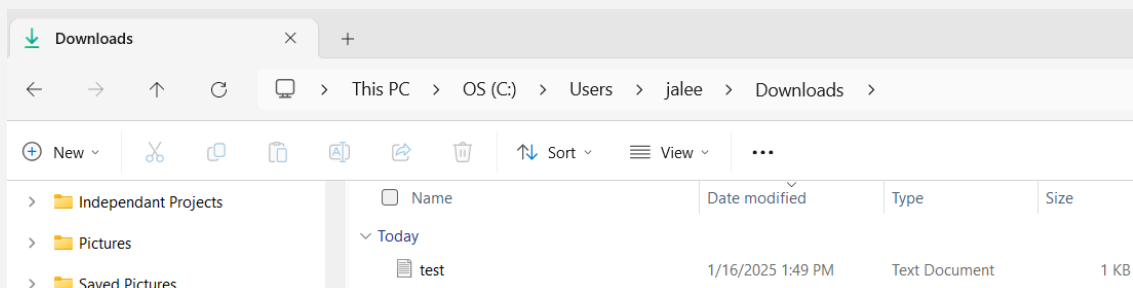
  <disabled>no</disabled>

  <!-- 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 check_all="yes" report_changes="yes" realtime="yes">C:\Users\jalee\Downloads</directories>

```

- Saved file and restarted Wazuh server on Windows agent's machine
- Added a test text file in Downloads directory.
- Modified test text file adding a sample text.



- Wazuh dashboard provided events based on the above actions

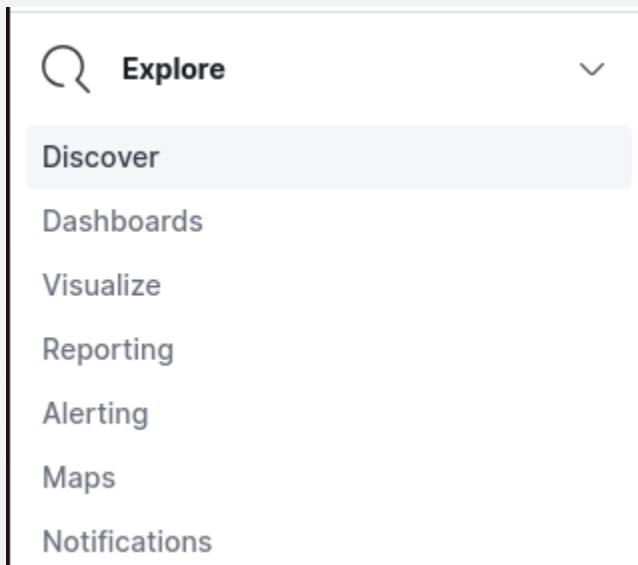
FIM: Recent events 					
Time ↓	Path	Action	Rule description	Rule Lev...	Rule Id
Jan 16, 2025 @ 18:49:34.507	c:\users\jalee\downloads\test.txt	modified	Integrity checksum changed.	7	550
Jan 16, 2025 @ 18:48:24.317	c:\users\jalee\downloads\test.txt	added	File added to the system.	5	554

- Can inspect each FIM event and analyze the info Wazuh provides:

Document Details		View surrounding documents	View single document
# rule.level	7		
rule.mail	false		
rule.mitre.id	T1565.001		
rule.mitre.tactic	Impact		
rule.mitre.technique	Stored Data Manipulation		
rule.nist_800_53	SI.7		
rule.pci_dss	11.5		
rule.tsc	PI1.4, PI1.5, CC6.1, CC6.8, CC7.2, CC7.3		
syscheck.attrs_after	ARCHIVE		
syscheck.changed_attributes	size, mtime, md5, sha1, sha256		
syscheck.diff	--- > Sample text for SIEM project.		
syscheck.event	modified		
syscheck.md5_after	b3ee85c54fd39db0952005dd4f4e2b59		
syscheck.md5_before	d41d8cd98f00b204e9800998ecf8427e		
syscheck.mode	realtime		
syscheck.mtime_after	Jan 16, 2025 @ 18:49:34.000	🔍	📄
syscheck.mtime_before	Jan 16, 2025 @ 18:48:18.000		
syscheck.path	c:\users\ialee\downloads\test.txt		

- Data such as hash values before and after file modification
- Agent's id and ip address
- Event type
- Text value modified of before and after
- Time frames of last file modification or creation and most recent file modification
- Compliance assurance

Additional capabilities:



- Dashboard, visual, reporting capabilities for creating visualization or clustered information from Wazuh and its resources.

- Alerting enables Wazuh server logs to be reviewed and contains capabilities of using the Alert Ids in the “Ossec.conf” file to set up alert rules
- Notification options such as by email for reporting or alerts
- Detecting and removing malware using VirusTotal integration using file monitoring feature Wazuh obtains
- Blocking a known malicious actor
- Integrating a network IDS and various security tools