
Deployment and Configuration of Security Information & Event Management (SIEM) solution for SMEs using **WAZUH** SIEM.

Presented By Okperiruisi Louis

1st November 2025

Project Deliverable

Wazuh SIEM
Deployment and
Agent
Configuration

Wazuh SIEM
integration with
virustotal for threat
intelligence.

FIM - File
Monitoring
Detection and Alert

Endpoint Threat
Detection using
Microsoft defender
and Wazuh SIEM.

Visit <https://documentation.wazuh.com/> to download wazuh

The screenshot shows the Wazuh documentation homepage. The browser address bar displays <https://documentation.wazuh.com/current/index.html>. The navigation menu includes links for Platform, Cloud, CTI, Documentation, Services, Partners, and Company. A yellow 'Install Wazuh' button and a 'Log in' button are also visible. The main content area features a large blue search bar with the text 'Documentation Index' and a placeholder 'What can we help you find?'. Below the search bar, there are three main categories: 'Getting started' (with sub-links for Components and Architecture), 'Installation guide' (with sub-links for Wazuh indexer and Wazuh server), and 'Quickstart' (highlighted with a blue background and a Wi-Fi icon).

This screenshot shows the same Wazuh documentation homepage, but with the 'Quickstart' section highlighted in blue. Below the 'Quickstart' section, there are three more categories: 'Installation alternatives' (highlighted with a red box), 'User manual' (with a sub-link for Wazuh server), and 'Cloud security' (with a sub-link for Monitoring Amazon Web Services (AWS)). The browser address bar still shows <https://documentation.wazuh.com/current/index.html>.

[//documentation.wazuh.com/current/deployment-options/index.html](https://documentation.wazuh.com/current/deployment-options/index.html)

The screenshot shows the Wazuh documentation page for 'Installing the Wazuh central components'. The browser address bar displays <https://documentation.wazuh.com/current/deployment-options/index.html>. The navigation menu includes links for Platform, Cloud, CTI, Documentation, Services, Partners, and Company. A yellow 'Version 4.14 (current)' dropdown menu is visible. The main content area features a search bar and a navigation menu with links for Getting started, Quickstart, Installation guide, and Installation alternatives (highlighted with a blue background). The main heading is 'Installing the Wazuh central components'. Below the heading, there is a paragraph: 'All the alternatives include instructions on how to install the Wazuh central components. After these are installed, you then need to deploy agents to your endpoints.' Below this, there is a section titled 'Ready-to-use machines' with a sub-section 'Virtual machine (VM)' (highlighted with a red box) containing the text: 'Wazuh provides a pre-built virtual machine image (OVA) that you can directly import using VirtualBox or other OVA compatible virtualization systems.' Below this, there is a bullet point for 'Amazon Machine Images (AMI)': 'This is a pre-built Amazon Machine Image (AMI) you can directly launch on an AWS cloud instance.' On the right side, there is a 'On this page' sidebar with links for 'Installing the Wazuh central components', 'Installing the Wazuh agent', and 'Orchestration tools'. A blue 'Contact us' button is also visible on the right side.

Search [input field]

Home / Installation alternatives / Virtual machine (VM)

Virtual machine (VM)

Wazuh provides a pre-built virtual machine image in Open Virtual Appliance (OVA) format. It includes the Amazon Linux 2023 operating system and the Wazuh central components.

- Wazuh manager 4.14.0
- Filebeat-OSS 7.10.2
- Wazuh indexer 4.14.0
- Wazuh dashboard 4.14.0

You can import the Wazuh virtual machine image to VirtualBox or other OVA-compatible virtualization systems. This VM runs only on 64-bit systems with x86_64/AMD64 architecture. It does not provide high availability or scalability out of the box. However, you can implement these using [distributed deployment](#).

Download the [virtual appliance \(OVA\)](#).

On this page

Virtual machine (VM)

Hardware requirements

Import and access the virtual machine

Access the Wazuh dashboard

Configuration files

VirtualBox time configuration

Troubleshooting

VM fails to start on AMD processors with VMware

Getting started

Quickstart

Installation guide

Installation alternatives

Virtual machine (VM)

Amazon Machine Images (AMI)

Deployment on Docker

Deployment on Kubernetes

Offline installation guide

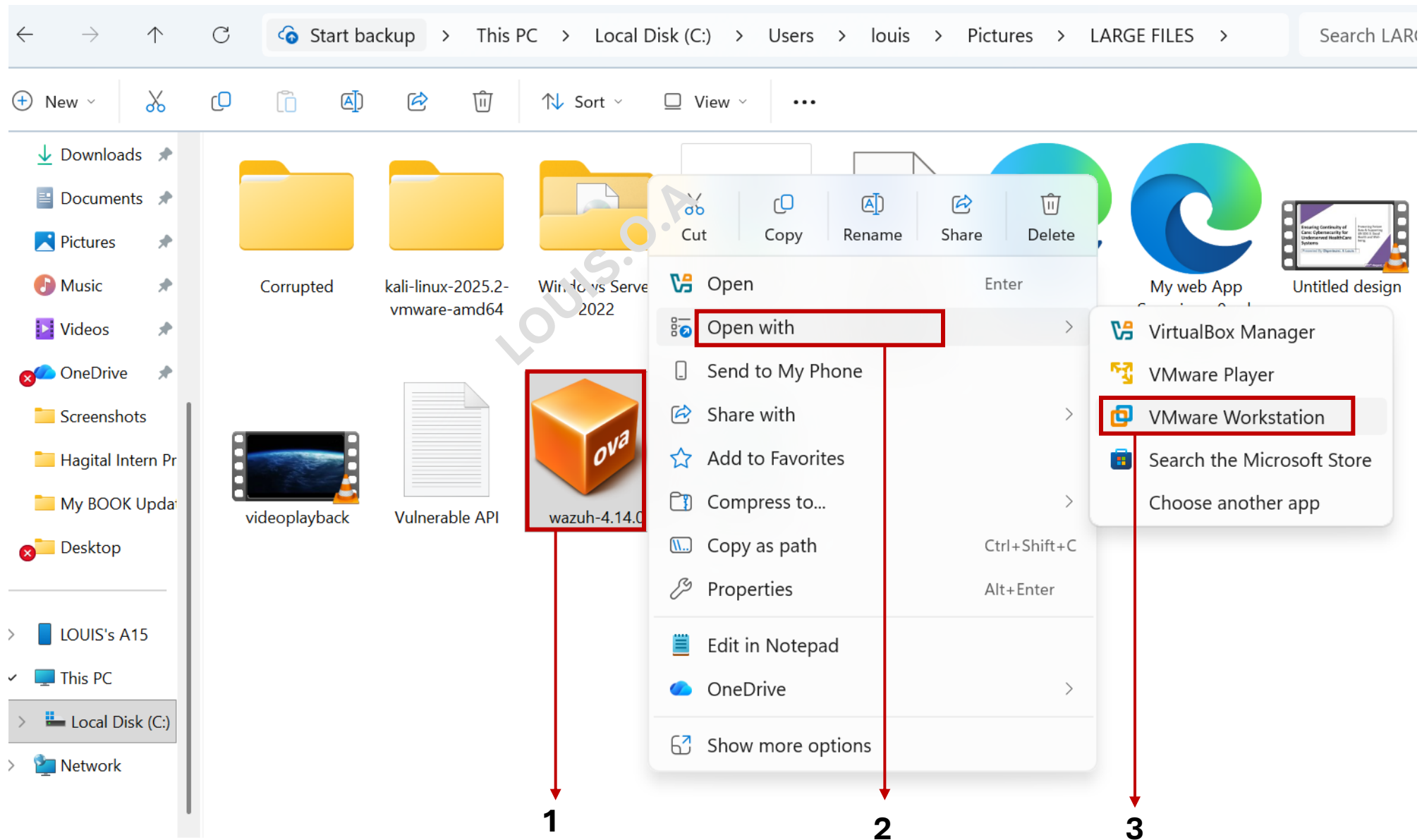
Installation from sources

Deployment with Ansible

Deployment with Puppet

User manual

Right click on the wazuh OVA file for installation





Type here t...

- My Computer
 - Windows Se
 - Windows 10
 - kali-linux-20

Home Windows 10 Windows Server 2022 kali-linux-2025.2-vmware-am...

Import Virtual Machine

Store the new Virtual Machine

Provide a name and local storage path for the new virtual machine.

Name for the new virtual machine:

Wazuh

Storage path for the new virtual machine:

C:\Users\Louis\Documents\Virtual Machines\Wazuh

Browse...

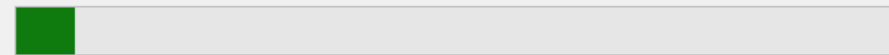
Help

Import

Cancel

VMware Workstation

Importing Wazuh



Cancel

Library

Type here t...

- My Computer
 - Windows Sel
 - Windows 10
 - kali-linux-20
 - Wazuh

Wazuh

- Power on this virtual machine
- Edit virtual machine settings**
- Upgrade this virtual machine

Devices

Memory	8 GB
Processors	4
Hard Disk (IDE)	50 GB
CD/DVD (IDE)	Using unknown
Floppy	Using drive A:
Network Adapter	Bridged (Autom
Display	Auto detect

Description

Wazuh enhances security visibility in your infrastructure by monitoring endpoints at the operating system and application levels. Its capabilities include log analysis, file integrity monitoring, intrusion detection, and compliance monitoring.

Virtual Machine Settings

Hardware Options

Device	Summary
Memory	8 GB
Processors	4
Hard Disk (IDE)	50 GB
CD/DVD (IDE)	Using unknown backend
Floppy	Using drive A:
Network Adapter	Bridged (Automatic)
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: MB

32 GB -
16 GB -
8 GB -
4 GB -
2 GB -
1 GB -
512 MB -
256 MB -
128 MB -
64 MB -
32 MB -
16 MB -
8 MB -
4 MB -

- Maximum recommended memory (Memory swapping may occur beyond this size.) 27.8 GB
- Recommended memory 384 MB
- Guest OS recommended minimum 32 MB

Add... Remove

OK Cancel Help

File Edit View VM Tabs Help

Library

My Computer

- Windows Ser
- Windows 10
- kali-linux-202
- Wazuh

Wazuh

Power on this virtual machine

Edit virtual machine settings

Upgrade this virtual machine

Devices

Memory	8 GB
Processors	4
Hard Disk (IDE)	50 GB
CD/DVD (IDE)	Using unknown .
Floppy	Using drive A:
Network Adapter	Bridged (Autom...
Display	Auto detect

Description

Wazuh enhances security visibility in your infrastructure by monitoring endpoints at the operating system and application levels. Its capabilities include log analysis, file integrity monitoring, intrusion detection, and compliance monitoring.

Virtual Machine Settings

Hardware Options

Device	Summary
Memory	8 GB
Processors	4
Hard Disk (IDE)	50 GB
CD/DVD (IDE)	Using unknown backend
Floppy	Using drive A:
Network Adapter	Bridged (Automatic)
Display	Auto detect

Device status

Connected

Connect at power on **1**

Network connection

Bridged: Connected directly to the physical network **2**

Replicate physical network connection state

NAT: Used to share the host's IP address **3**

Host-only: A private network shared with the host

Custom: Specific virtual network

VMnet0

LAN segment:

LAN Segments... Advanced...

Add... Remove

OK Cancel Help **4**



Library

Type here to search

- My Computer
 - Windows Server 2022
 - Windows 10
 - kali-linux-2025.2-vmware-am...
 - Wazuh

- Home
- Windows 10
- Windows Server 2022
- kali-linux-2025.2-vmware-am...
- Wazuh

Wazuh

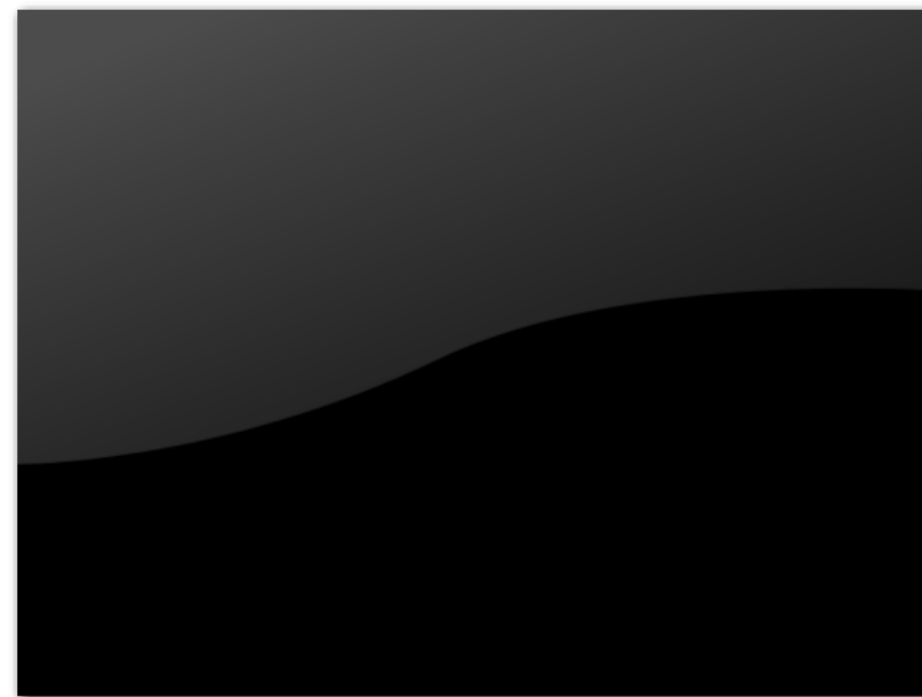
[▶ Power on this virtual machine](#)[✎ Edit virtual machine settings](#)[⬆ Upgrade this virtual machine](#)

Devices

Memory	8 GB
Processors	4
Hard Disk (IDE)	50 GB
CD/DVD (IDE)	Using unknown ...
Floppy	Using drive A:
Network Adapter	NAT
Display	Auto detect

Description

Wazuh enhances security visibility in your infrastructure by monitoring endpoints at the operating system and application levels. Its capabilities include log analysis, file integrity monitoring, intrusion detection, and compliance monitoring.



Virtual Machine Details

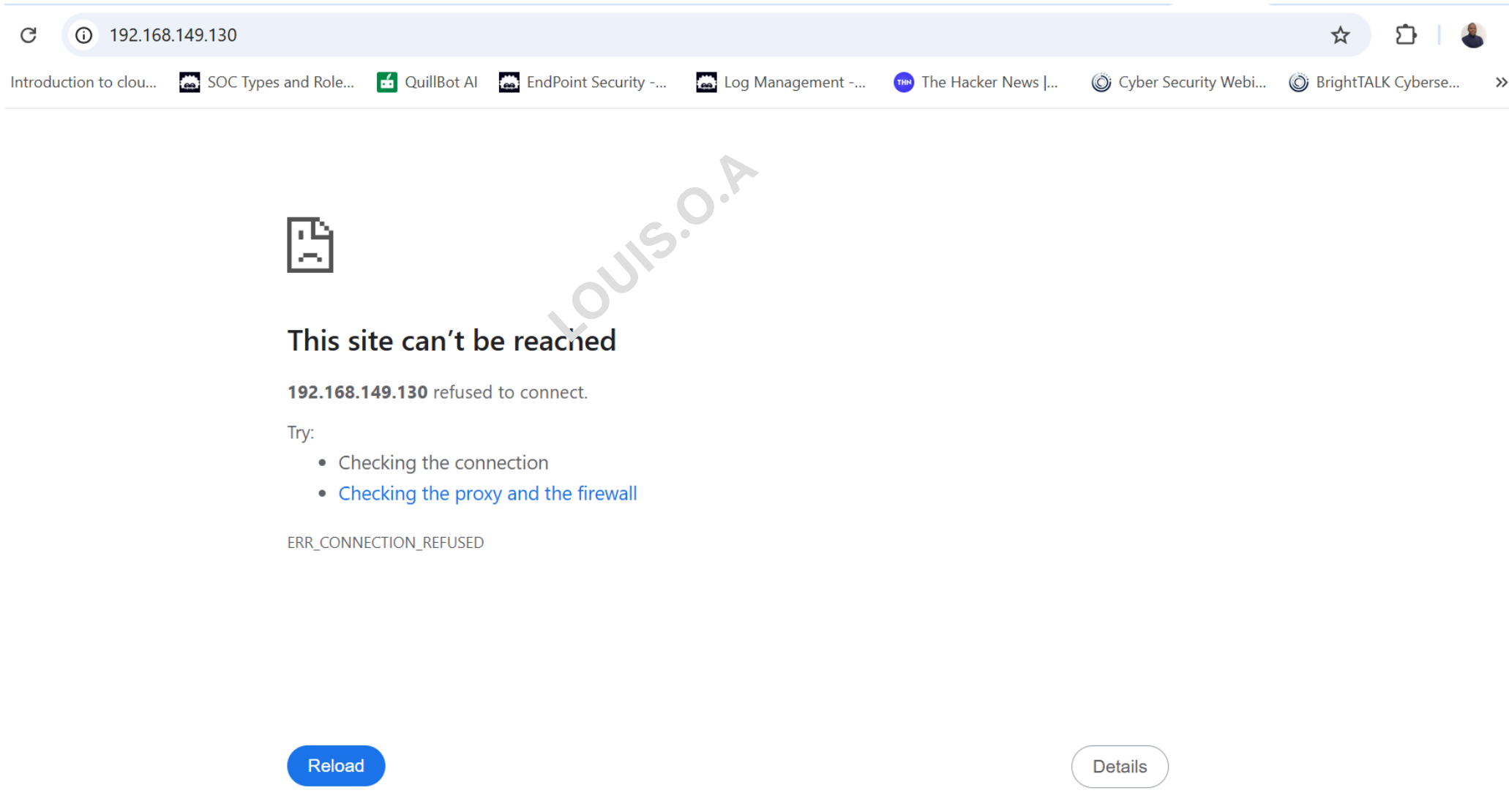
State: Powered off

Configuration file: C:\Users\louis\Documents\Virtual Machines\Wazuh\Wazuh.vmx

Hardware compatibility: Workstation 6.5-7.x virtual machine

Primary IP address: Network information is not available


If you cannot access the wazuh dashboard using the ip address, kindly manually start wazuh dashboard server, wazuh manager, and wazuh indexer.



The screenshot shows a web browser window with the address bar displaying '192.168.149.130'. The browser's tab bar contains several open tabs, including 'Introduction to clou...', 'SOC Types and Role...', 'QuillBot AI', 'EndPoint Security -...', 'Log Management -...', 'The Hacker News [...]', 'Cyber Security Webi...', and 'BrightTALK Cyberse...'. The main content area displays a 'This site can't be reached' error message. The error message includes a sad face icon, the text 'This site can't be reached', and the specific error '192.168.149.130 refused to connect.'. Below this, it suggests trying to check the connection or check the proxy and firewall. At the bottom of the error message, the code 'ERR_CONNECTION_REFUSED' is visible. At the bottom of the browser window, there are two buttons: a blue 'Reload' button and a white 'Details' button.

192.168.149.130

Introduction to clou... SOC Types and Role... QuillBot AI EndPoint Security -... Log Management -... The Hacker News [...] Cyber Security Webi... BrightTALK Cyberse... >>



This site can't be reached

192.168.149.130 refused to connect.

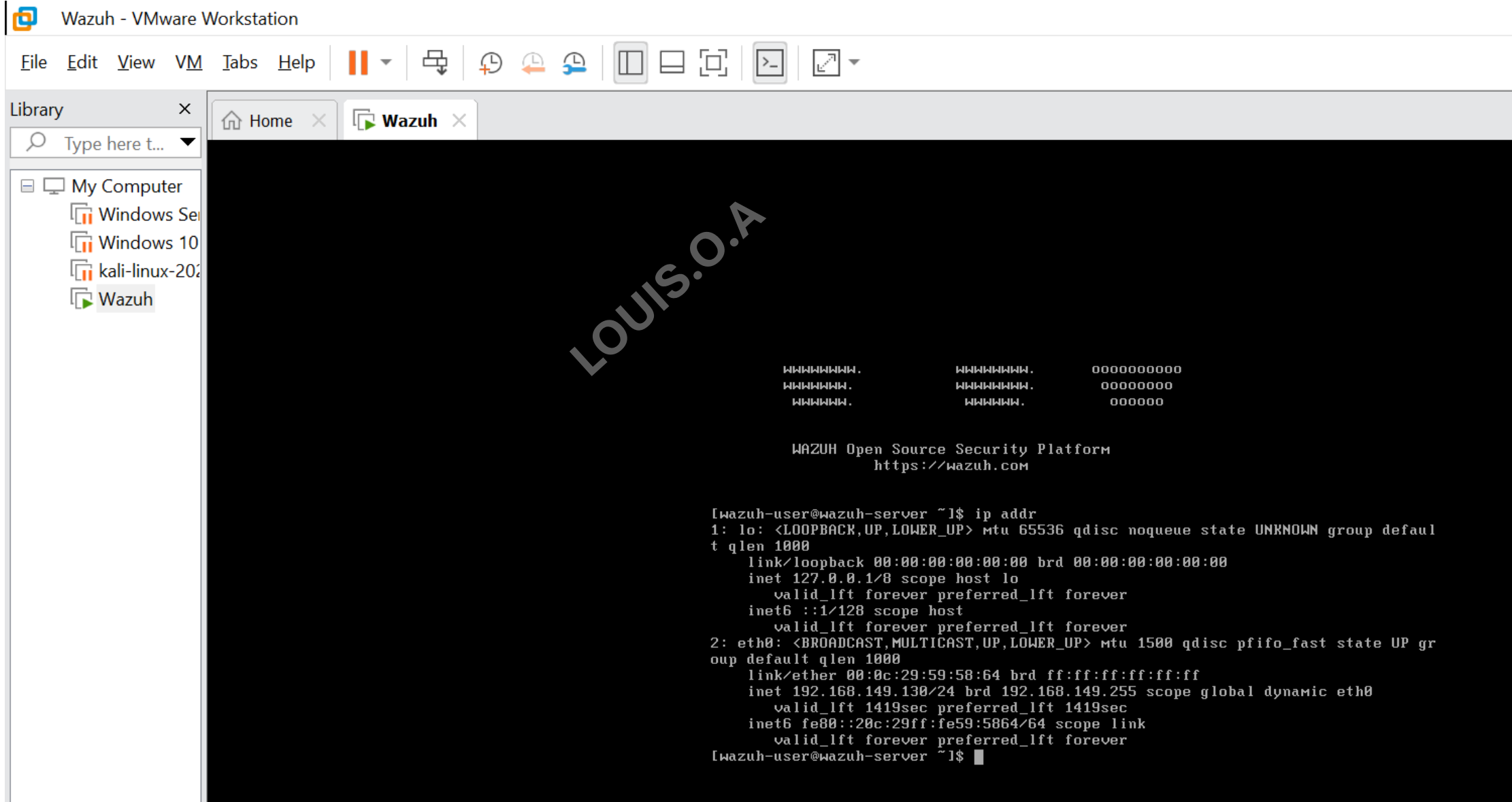
Try:

- Checking the connection
- [Checking the proxy and the firewall](#)

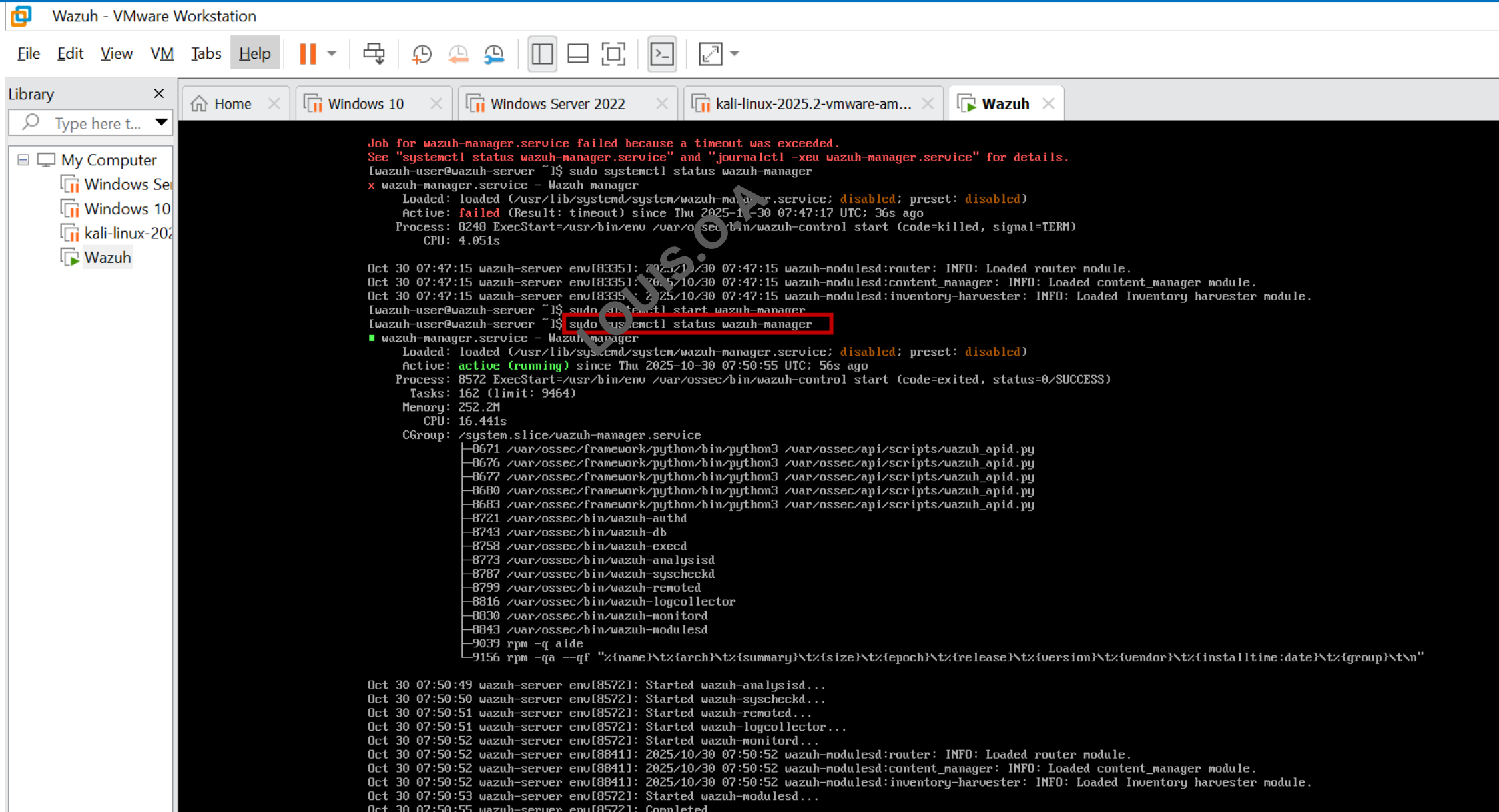
ERR_CONNECTION_REFUSED

[Reload](#) [Details](#)

Firstly, let us start wazuh manager by typing-in “sudo systemctl start wazuh-manager”



To check if the wazuh manager has started type this command "sudo systemctl status wazuh-manager" and hit enter key. Once you see these write up, it shows the wazuh is running now.



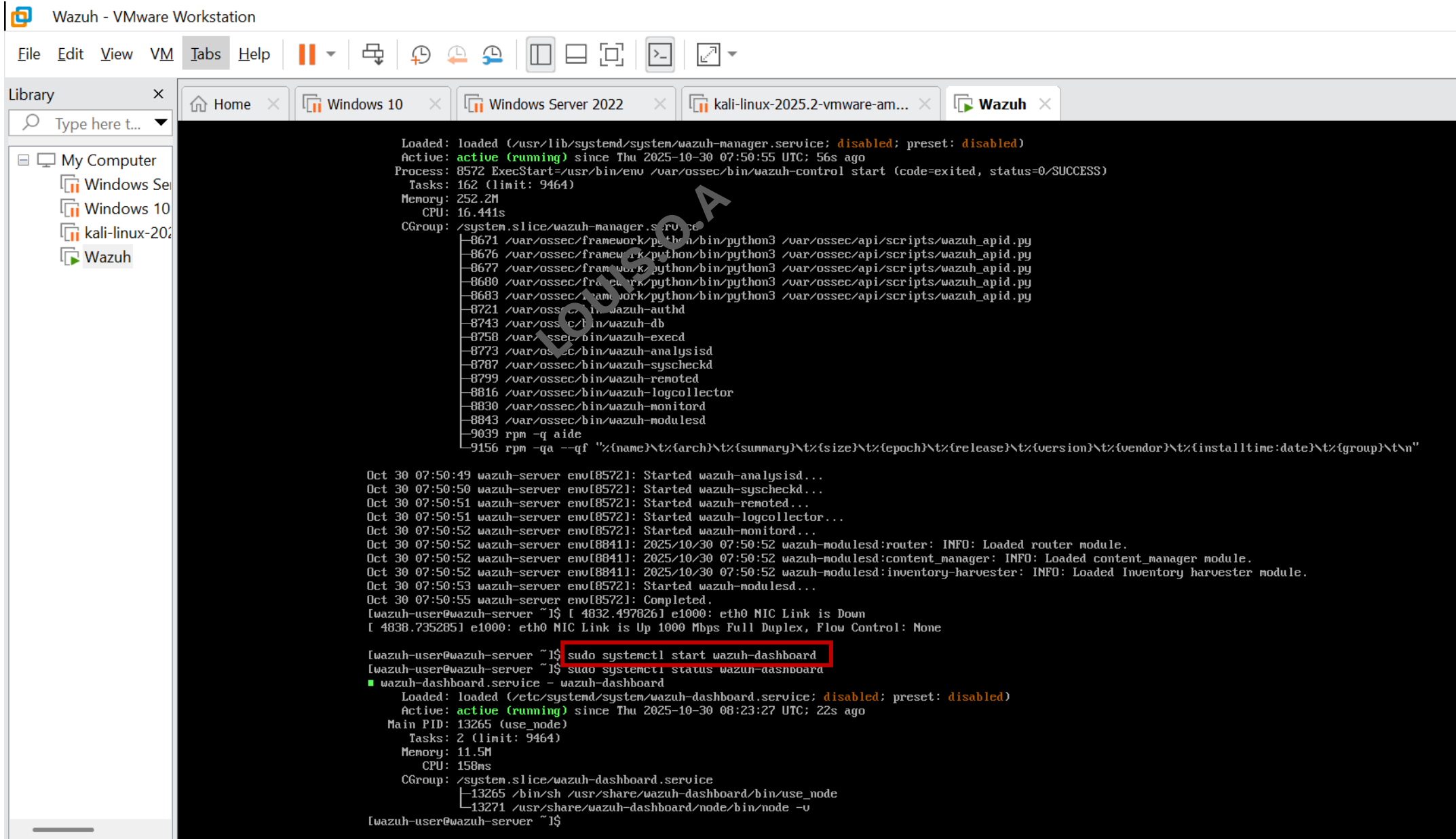
The screenshot shows a VMware Workstation interface with a terminal window titled "Wazuh". The terminal displays the following output:

```
Job for wazuh-manager.service failed because a timeout was exceeded.
See "systemctl status wazuh-manager.service" and "journalctl -xeu wazuh-manager.service" for details.
[wazuh-user@wazuh-server ~]$ sudo systemctl status wazuh-manager
x wazuh-manager.service - Wazuh manager
   Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; disabled; preset: disabled)
   Active: failed (Result: timeout) since Thu 2025-10-30 07:47:17 UTC; 36s ago
   Process: 8248 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=killed, signal=TERM)
   CPU: 4.051s

Oct 30 07:47:15 wazuh-server env[8335]: 2025/10/30 07:47:15 wazuh-modulesd:router: INFO: Loaded router module.
Oct 30 07:47:15 wazuh-server env[8335]: 2025/10/30 07:47:15 wazuh-modulesd:content_manager: INFO: Loaded content_manager module.
Oct 30 07:47:15 wazuh-server env[8335]: 2025/10/30 07:47:15 wazuh-modulesd:inventory-harvester: INFO: Loaded Inventory harvester module.
[wazuh-user@wazuh-server ~]$ sudo systemctl start wazuh-manager
[wazuh-user@wazuh-server ~]$ sudo systemctl status wazuh-manager
■ wazuh-manager.service - Wazuh manager
   Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; disabled; preset: disabled)
   Active: active (running) since Thu 2025-10-30 07:50:55 UTC; 56s ago
   Process: 8572 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
   Tasks: 162 (limit: 9464)
   Memory: 252.2M
   CPU: 16.441s
   CGroup: /system.slice/wazuh-manager.service
├─8671 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
├─8676 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
├─8677 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
├─8680 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
├─8683 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
├─8721 /var/ossec/bin/wazuh-authd
├─8743 /var/ossec/bin/wazuh-db
├─8758 /var/ossec/bin/wazuh-execd
├─8773 /var/ossec/bin/wazuh-analysisd
├─8787 /var/ossec/bin/wazuh-syscheckd
├─8799 /var/ossec/bin/wazuh-remoted
├─8816 /var/ossec/bin/wazuh-logcollector
├─8830 /var/ossec/bin/wazuh-monitord
├─8843 /var/ossec/bin/wazuh-modulesd
├─9039 rpm -q aide
└─9156 rpm -qa --qf "%{name}\t%{arch}\t%{summary}\t%{size}\t%{epoch}\t%{release}\t%{version}\t%{vendor}\t%{installtime:date}\t%{group}\t\n"

Oct 30 07:50:49 wazuh-server env[8572]: Started wazuh-analysisd...
Oct 30 07:50:50 wazuh-server env[8572]: Started wazuh-syscheckd...
Oct 30 07:50:51 wazuh-server env[8572]: Started wazuh-remoted...
Oct 30 07:50:51 wazuh-server env[8572]: Started wazuh-logcollector...
Oct 30 07:50:52 wazuh-server env[8572]: Started wazuh-monitord...
Oct 30 07:50:52 wazuh-server env[8841]: 2025/10/30 07:50:52 wazuh-modulesd:router: INFO: Loaded router module.
Oct 30 07:50:52 wazuh-server env[8841]: 2025/10/30 07:50:52 wazuh-modulesd:content_manager: INFO: Loaded content_manager module.
Oct 30 07:50:52 wazuh-server env[8841]: 2025/10/30 07:50:52 wazuh-modulesd:inventory-harvester: INFO: Loaded Inventory harvester module.
Oct 30 07:50:53 wazuh-server env[8572]: Started wazuh-modulesd...
Oct 30 07:50:55 wazuh-server env[8572]: Completed.
```

To start the wazuh dashboard type this command "sudo systemctl start wazuh-dashboard" and hit enter key. Once you see these write, it shows the wazuh dashboard is running now.



The screenshot shows a terminal window titled "Wazuh - VMware Workstation" with a menu bar (File, Edit, View, VM, Tabs, Help) and a toolbar. The terminal output displays the status of the wazuh-manager.service and the wazuh-dashboard.service. The wazuh-manager.service is active and running, with a list of child processes including wazuh-api, wazuh-authd, wazuh-db, wazuh-execd, wazuh-analysisd, wazuh-syscheckd, wazuh-remoted, wazuh-logcollector, wazuh-monitord, and wazuh-modulesd. The wazuh-dashboard.service is also active and running. The terminal shows the command "sudo systemctl start wazuh-dashboard" being executed, and the output "wazuh-dashboard.service - wazuh-dashboard" followed by its status details. A red box highlights the command "sudo systemctl start wazuh-dashboard".

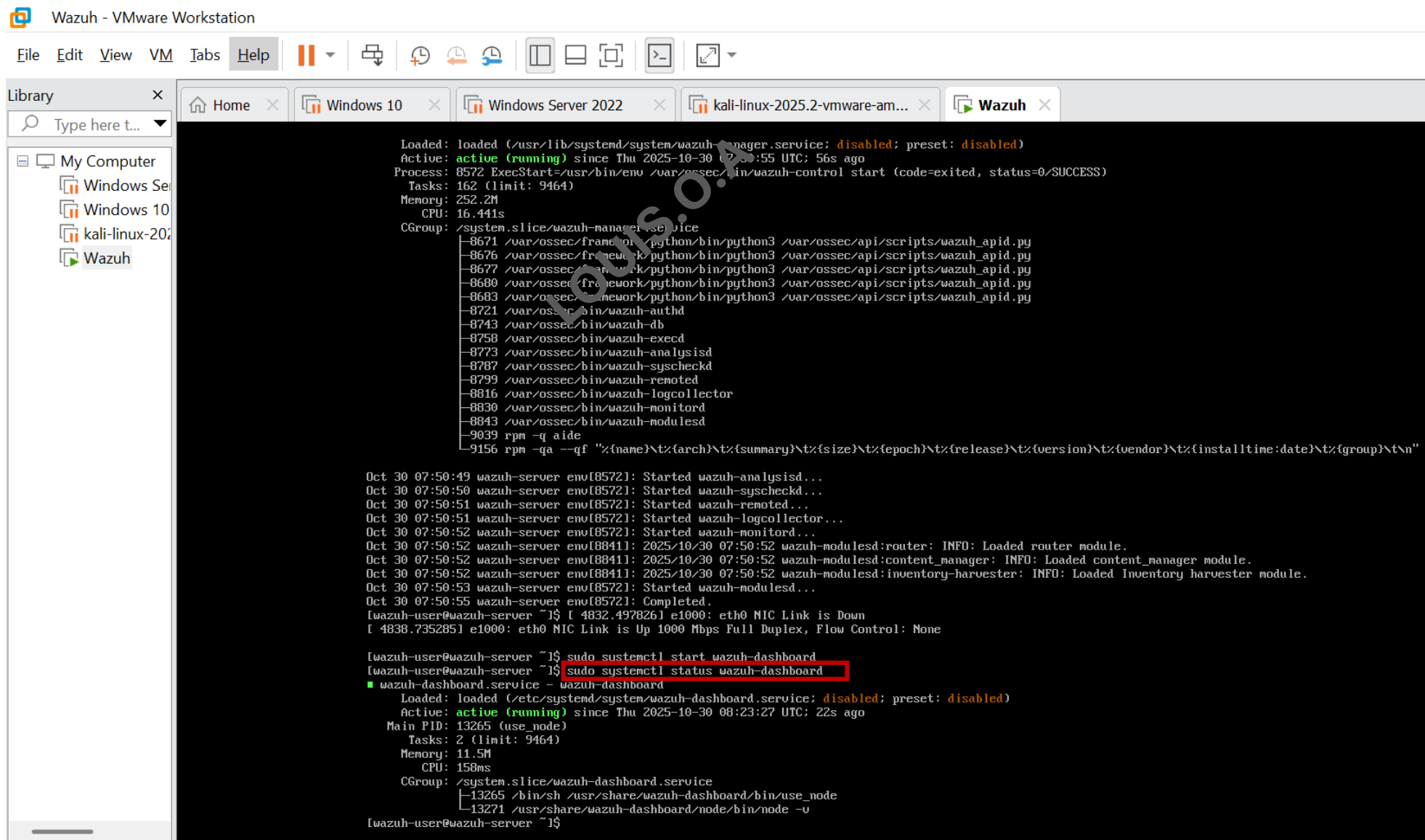
```
Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; disabled; preset: disabled)
Active: active (running) since Thu 2025-10-30 07:50:55 UTC; 56s ago
Process: 8572 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
Tasks: 162 (limit: 9464)
Memory: 252.2M
CPU: 16.441s
CGroup: /system.slice/wazuh-manager.service
├─8671 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
├─8676 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
├─8677 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
├─8680 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
├─8683 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
├─8721 /var/ossec/bin/wazuh-authd
├─8743 /var/ossec/bin/wazuh-db
├─8758 /var/ossec/bin/wazuh-execd
├─8773 /var/ossec/bin/wazuh-analysisd
├─8787 /var/ossec/bin/wazuh-syscheckd
├─8799 /var/ossec/bin/wazuh-remoted
├─8816 /var/ossec/bin/wazuh-logcollector
├─8830 /var/ossec/bin/wazuh-monitord
├─8843 /var/ossec/bin/wazuh-modulesd
├─9039 rpm -q aide
└─9156 rpm -qa --qf "%{name}\t:{arch}\t:{summary}\t:{size}\t:{epoch}\t:{release}\t:{version}\t:{vendor}\t:{installtime:date}\t:{group}\t\n"

Oct 30 07:50:49 wazuh-server env[8572]: Started wazuh-analysisd...
Oct 30 07:50:50 wazuh-server env[8572]: Started wazuh-syscheckd...
Oct 30 07:50:51 wazuh-server env[8572]: Started wazuh-remoted...
Oct 30 07:50:51 wazuh-server env[8572]: Started wazuh-logcollector...
Oct 30 07:50:52 wazuh-server env[8572]: Started wazuh-monitord...
Oct 30 07:50:52 wazuh-server env[8841]: 2025/10/30 07:50:52 wazuh-modulesd:router: INFO: Loaded router module.
Oct 30 07:50:52 wazuh-server env[8841]: 2025/10/30 07:50:52 wazuh-modulesd:content_manager: INFO: Loaded content_manager module.
Oct 30 07:50:52 wazuh-server env[8841]: 2025/10/30 07:50:52 wazuh-modulesd:inventory-harvester: INFO: Loaded Inventory harvester module.
Oct 30 07:50:53 wazuh-server env[8572]: Started wazuh-modulesd...
Oct 30 07:50:55 wazuh-server env[8572]: Completed.
[wazuh-user@wazuh-server ~]# [ 4832.497826] e1000: eth0 NIC Link is Down
[ 4838.735285] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None

[wazuh-user@wazuh-server ~]# sudo systemctl start wazuh-dashboard
[wazuh-user@wazuh-server ~]# sudo systemctl status wazuh-dashboar
■ wazuh-dashboard.service - wazuh-dashboard
Loaded: loaded (/etc/systemd/system/wazuh-dashboard.service; disabled; preset: disabled)
Active: active (running) since Thu 2025-10-30 08:23:27 UTC; 22s ago
Main PID: 13265 (use_node)
Tasks: 2 (limit: 9464)
Memory: 11.5M
CPU: 158ms
CGroup: /system.slice/wazuh-dashboard.service
├─13265 /bin/sh /usr/share/wazuh-dashboard/bin/use_node
└─13271 /usr/share/wazuh-dashboard/node/bin/node -u

[wazuh-user@wazuh-server ~]#
```

To check if the wazuh dashboard has started type this command "sudo systemctl status wazuh-dashboard" and hit enter key. Once you see "active running", it shows the wazuh dashboard is running now.



The screenshot shows a VMware Workstation window titled "Wazuh - VMware Workstation". The interface includes a menu bar (File, Edit, View, VM, Tabs, Help), a toolbar with various icons, and a tab bar with several open windows: Home, Windows 10, Windows Server 2022, kali-linux-2025.2-vmware-am..., and Wazuh. The main terminal window displays the output of the command `sudo systemctl status wazuh-dashboard`. The output shows that the service is loaded and active (running). The status is "active (running) since Thu 2025-10-30 07:50:55 UTC; 56s ago". The process is 8572, and the status is 0/SUCCESS. The terminal also shows a list of processes for the wazuh-manager.service and a log of system events for the wazuh-server. The command `sudo systemctl start wazuh-dashboard` is also visible in the terminal output.

```
Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; disabled; preset: disabled)
Active: active (running) since Thu 2025-10-30 07:50:55 UTC; 56s ago
Process: 8572 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
Tasks: 162 (limit: 9464)
Memory: 252.2M
CPU: 16.441s
CGroup: /system.slice/wazuh-manager.service
├─8671 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
├─8676 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
├─8677 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
├─8680 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
├─8683 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
├─8721 /var/ossec/bin/wazuh-authd
├─8743 /var/ossec/bin/wazuh-db
├─8758 /var/ossec/bin/wazuh-execd
├─8773 /var/ossec/bin/wazuh-analysisd
├─8787 /var/ossec/bin/wazuh-syscheckd
├─8799 /var/ossec/bin/wazuh-remoted
├─8816 /var/ossec/bin/wazuh-logcollector
├─8830 /var/ossec/bin/wazuh-monitord
├─8843 /var/ossec/bin/wazuh-modulesd
├─9039 rpm -q aide
└─9156 rpm -qa --qf "%{name}\t%{arch}\t%{summary}\t%{size}\t%{epoch}\t%{release}\t%{version}\t%{vendor}\t%{installtime:date}\t%{group}\t\n"

Oct 30 07:50:49 wazuh-server env[8572]: Started wazuh-analysisd...
Oct 30 07:50:50 wazuh-server env[8572]: Started wazuh-syscheckd...
Oct 30 07:50:51 wazuh-server env[8572]: Started wazuh-remoted...
Oct 30 07:50:51 wazuh-server env[8572]: Started wazuh-logcollector...
Oct 30 07:50:52 wazuh-server env[8572]: Started wazuh-monitord...
Oct 30 07:50:52 wazuh-server env[8841]: 2025/10/30 07:50:52 wazuh-modulesd:router: INFO: Loaded router module.
Oct 30 07:50:52 wazuh-server env[8841]: 2025/10/30 07:50:52 wazuh-modulesd:content_manager: INFO: Loaded content_manager module.
Oct 30 07:50:52 wazuh-server env[8841]: 2025/10/30 07:50:52 wazuh-modulesd:inventory-harvester: INFO: Loaded Inventory harvester module.
Oct 30 07:50:53 wazuh-server env[8572]: Started wazuh-modulesd...
Oct 30 07:50:55 wazuh-server env[8572]: Completed.
[wazuh-user@wazuh-server ~]$ [ 4832.497826] e1000: eth0 NIC Link is Down
[ 4838.735285] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None

[wazuh-user@wazuh-server ~]$ sudo systemctl start wazuh-dashboard
[wazuh-user@wazuh-server ~]$ sudo systemctl status wazuh-dashboard
■ wazuh-dashboard.service - wazuh-dashboard
Loaded: loaded (/etc/systemd/system/wazuh-dashboard.service; disabled; preset: disabled)
Active: active (running) since Thu 2025-10-30 08:23:27 UTC; 22s ago
Main PID: 13265 (use_node)
Tasks: 2 (limit: 9464)
Memory: 11.5M
CPU: 158ms
CGroup: /system.slice/wazuh-dashboard.service
├─13265 /bin/sh /usr/share/wazuh-dashboard/bin/use_node
└─13271 /usr/share/wazuh-dashboard/node/bin/node -v

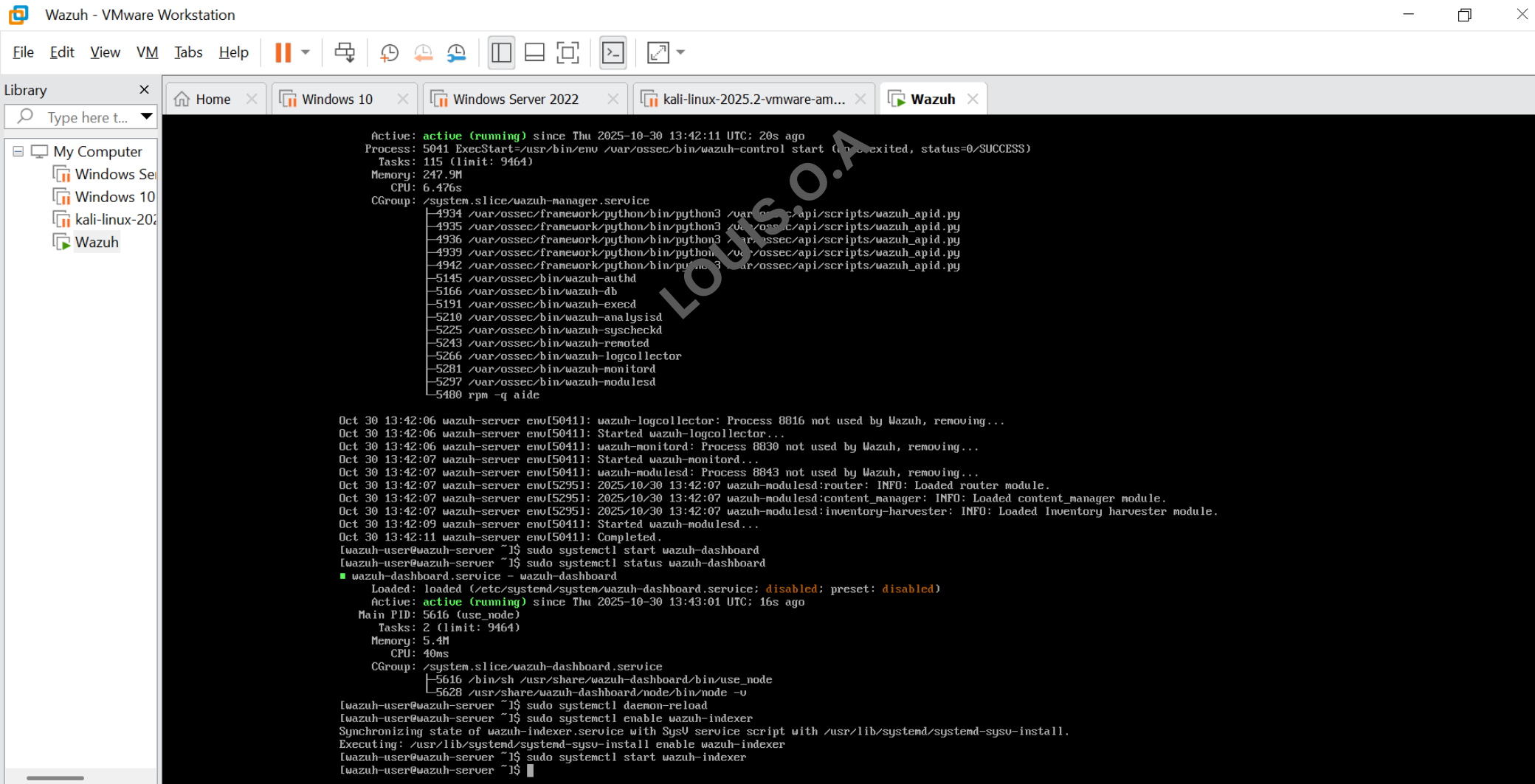
[wazuh-user@wazuh-server ~]$
```

To start the indexer, firstly, enter

"sudo systemctl daemon-reload"

"sudo systemctl enable wazuh-indexer"

"sudo systemctl start wazuh-indexer"



Wazuh - VMware Workstation

File Edit View VM Tabs Help

Library

My Computer

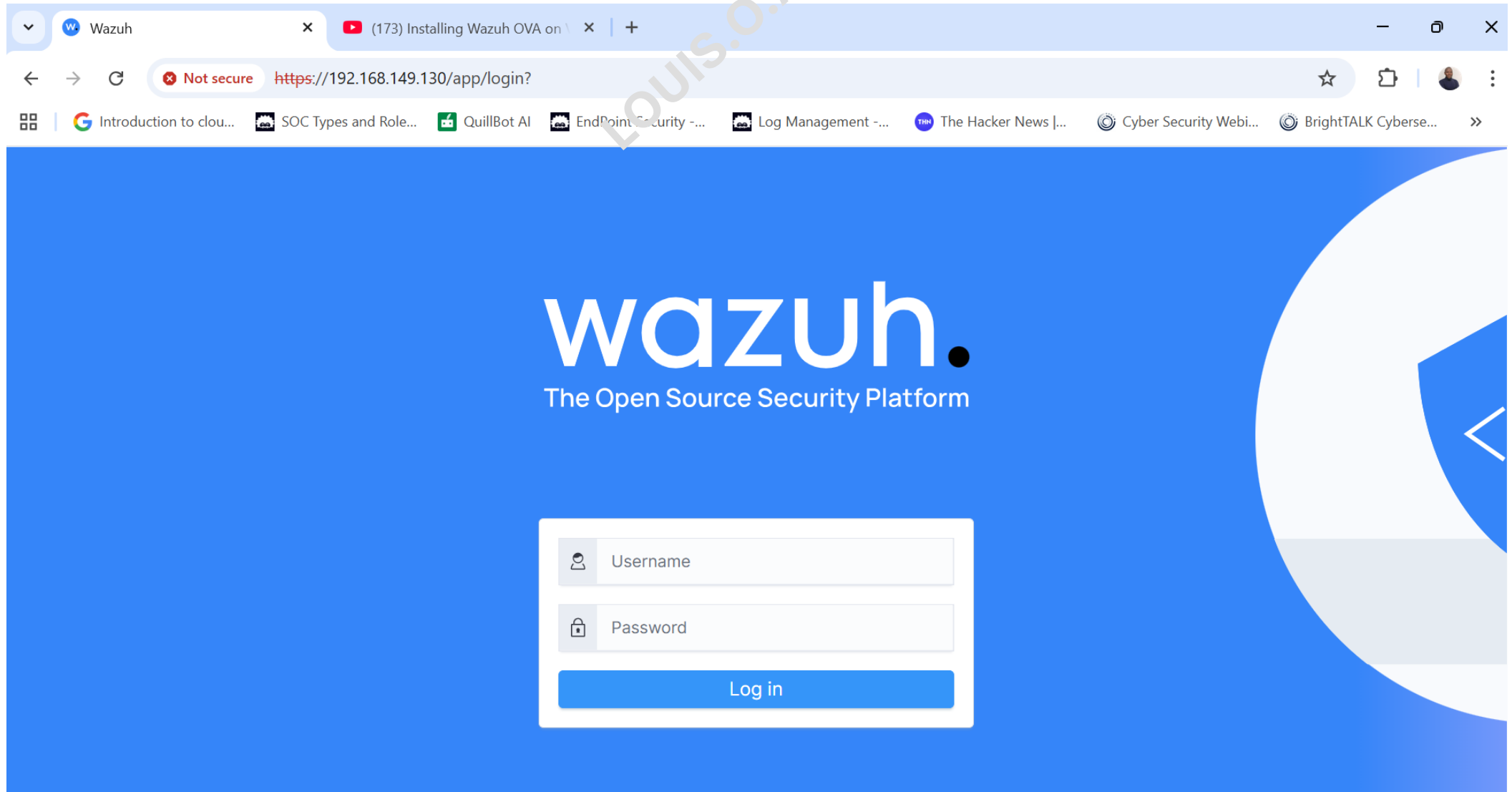
- Windows Server 2022
- Windows 10
- kali-linux-2025.2-vmware-am...
- Wazuh

```
Active: active (running) since Thu 2025-10-30 13:42:11 UTC; 20s ago
Process: 5041 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
Tasks: 115 (limit: 9464)
Memory: 247.9M
CPU: 6.476s
CGroup: /system.slice/wazuh-manager.service
├─4934 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
├─4935 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
├─4936 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
├─4939 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
├─4942 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
├─5145 /var/ossec/bin/wazuh-authd
├─5166 /var/ossec/bin/wazuh-db
├─5191 /var/ossec/bin/wazuh-execd
├─5210 /var/ossec/bin/wazuh-analysisd
├─5225 /var/ossec/bin/wazuh-syscheckd
├─5243 /var/ossec/bin/wazuh-remoted
├─5266 /var/ossec/bin/wazuh-logcollector
├─5281 /var/ossec/bin/wazuh-monitord
├─5297 /var/ossec/bin/wazuh-modulesd
└─5480 rpm -q aide

Oct 30 13:42:06 wazuh-server env[5041]: wazuh-logcollector: Process 8816 not used by Wazuh, removing...
Oct 30 13:42:06 wazuh-server env[5041]: Started wazuh-logcollector...
Oct 30 13:42:06 wazuh-server env[5041]: wazuh-monitord: Process 8830 not used by Wazuh, removing...
Oct 30 13:42:07 wazuh-server env[5041]: Started wazuh-monitord...
Oct 30 13:42:07 wazuh-server env[5041]: wazuh-modulesd: Process 8843 not used by Wazuh, removing...
Oct 30 13:42:07 wazuh-server env[5295]: 2025/10/30 13:42:07 wazuh-modulesd:router: INFO: Loaded router module.
Oct 30 13:42:07 wazuh-server env[5295]: 2025/10/30 13:42:07 wazuh-modulesd:content_manager: INFO: Loaded content_manager module.
Oct 30 13:42:07 wazuh-server env[5295]: 2025/10/30 13:42:07 wazuh-modulesd:inventory-harvester: INFO: Loaded inventory harvester module.
Oct 30 13:42:09 wazuh-server env[5041]: Started wazuh-modulesd...
Oct 30 13:42:11 wazuh-server env[5041]: Completed.
[wazuh-user@wazuh-server ~]$ sudo systemctl start wazuh-dashboard
[wazuh-user@wazuh-server ~]$ sudo systemctl status wazuh-dashboard
■ wazuh-dashboard.service - wazuh-dashboard
   Loaded: loaded (/etc/systemd/system/wazuh-dashboard.service; disabled; preset: disabled)
   Active: active (running) since Thu 2025-10-30 13:43:01 UTC; 16s ago
 Main PID: 5616 (use_node)
   Tasks: 2 (limit: 9464)
  Memory: 5.4M
     CPU: 40ms
  CGroup: /system.slice/wazuh-dashboard.service
          └─5616 /bin/sh /usr/share/wazuh-dashboard/bin/use_node
            └─5628 /usr/share/wazuh-dashboard/node/bin/node -v

[wazuh-user@wazuh-server ~]$ sudo systemctl daemon-reload
[wazuh-user@wazuh-server ~]$ sudo systemctl enable wazuh-indexer
Synchronizing state of wazuh-indexer.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable wazuh-indexer
[wazuh-user@wazuh-server ~]$ sudo systemctl start wazuh-indexer
[wazuh-user@wazuh-server ~]$
```

Login with the ip address (192.168.149.130) as in my case and enter the default password and username which are both "admin"



Add an Agent (Windows Computer)

The screenshot shows the Wazuh web interface in a browser. The address bar displays the URL: `https://192.168.149.130/app/wazuh#/overview/?_g=(filters:!,refreshInterval:(pause:!,value:0),time:(from:now-24h,to:now))&_a=(columns:!(...`. The interface features a navigation bar with the Wazuh logo and a 'Modules' dropdown. Below this, a summary section displays agent statistics:

Total agents	Active agents	Disconnected agents	Pending agents	Never connected agents
0	0	0	0	0

A yellow warning banner below the statistics states: "No agents were added to this manager." A red box highlights the "Add agent" link within this banner.

The main content area is divided into two sections:

- SECURITY INFORMATION MANAGEMENT**
 - Security events**: Browse through your security alerts, identifying issues and threats in your environment.
 - Integrity monitoring**: Alerts related to file changes, including permissions, content, ownership and attributes.
- AUDITING AND POLICY MONITORING**
 - Policy monitoring**: Verify that your systems are configured according to your security policies baseline.
 - System auditing**: Audit users behavior, monitoring command execution and alerting on access to critical files.
 - Security configuration**

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 Wazuh server. Enter an IP address or a fully qualified domain name (FDQN).

Assign a server address

192.168.149.130

Optional settings

The deployment sets the endpoint hostname as the agent name by default. Optionally, you can set your own name in the field below.

Assign an agent name

Louis-Machine

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 Wazuh agent:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.0-1.msi -OutFile
${env.tmp}\wazuh-agent; msixec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='192.168.149.130'
WAZUH_AGENT_NAME='Louis-Machine' WAZUH_REGISTRATION_SERVER='192.168.149.130'
```

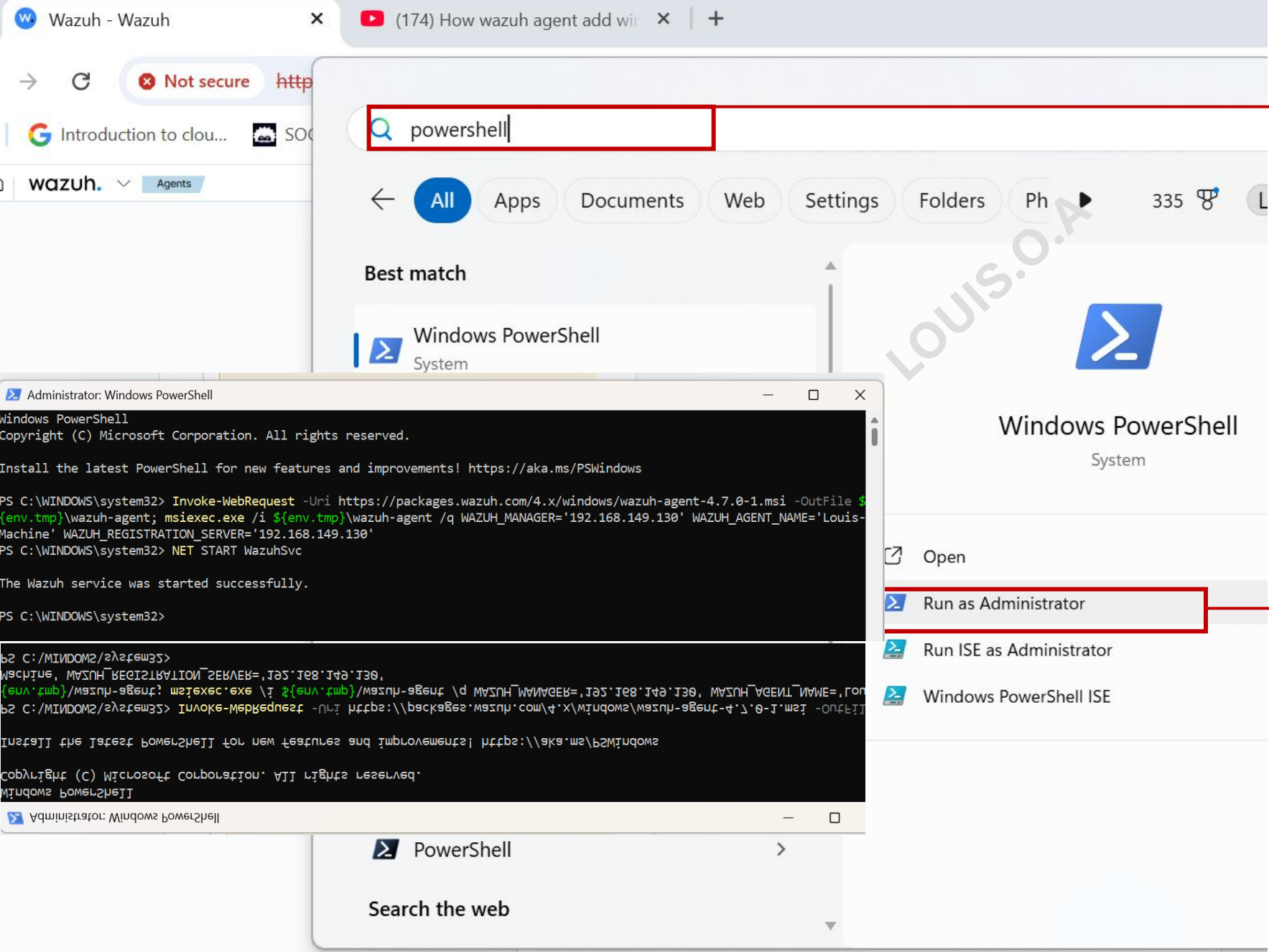
Start the Wazuh agent:

```
NET START WazuhSvc
```

READ ME

Close

1. Chose the Agent you want to add e.g Windows PC
2. Type-in the ip address of the Wazuh Server e.g 192.168.149.130
3. Name the Agent you want to add e.g Louis-Machine
4. Open PowerShell in **administrative** mode as shown in the **next slide to run No. 4 & 5** command.
5. Click close & go back to wazuh dashboard to see the agent



Type powershell

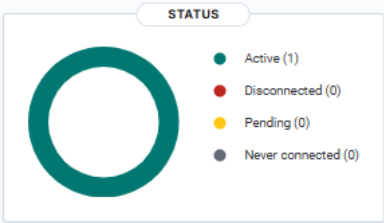
2

Run as administrator

3

Search powershell

1

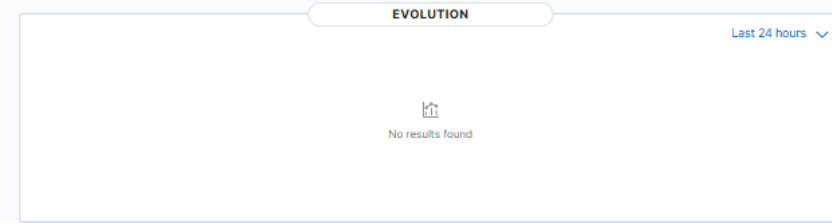


DETAILS

Active	1	Disconnected	0	Pending	0	Never connected	0	Agents coverage	100.00%
--------	---	--------------	---	---------	---	-----------------	---	-----------------	---------

Last registered agent: [Louis-Machine](#)

Most active agent: [Louis-Machine](#)

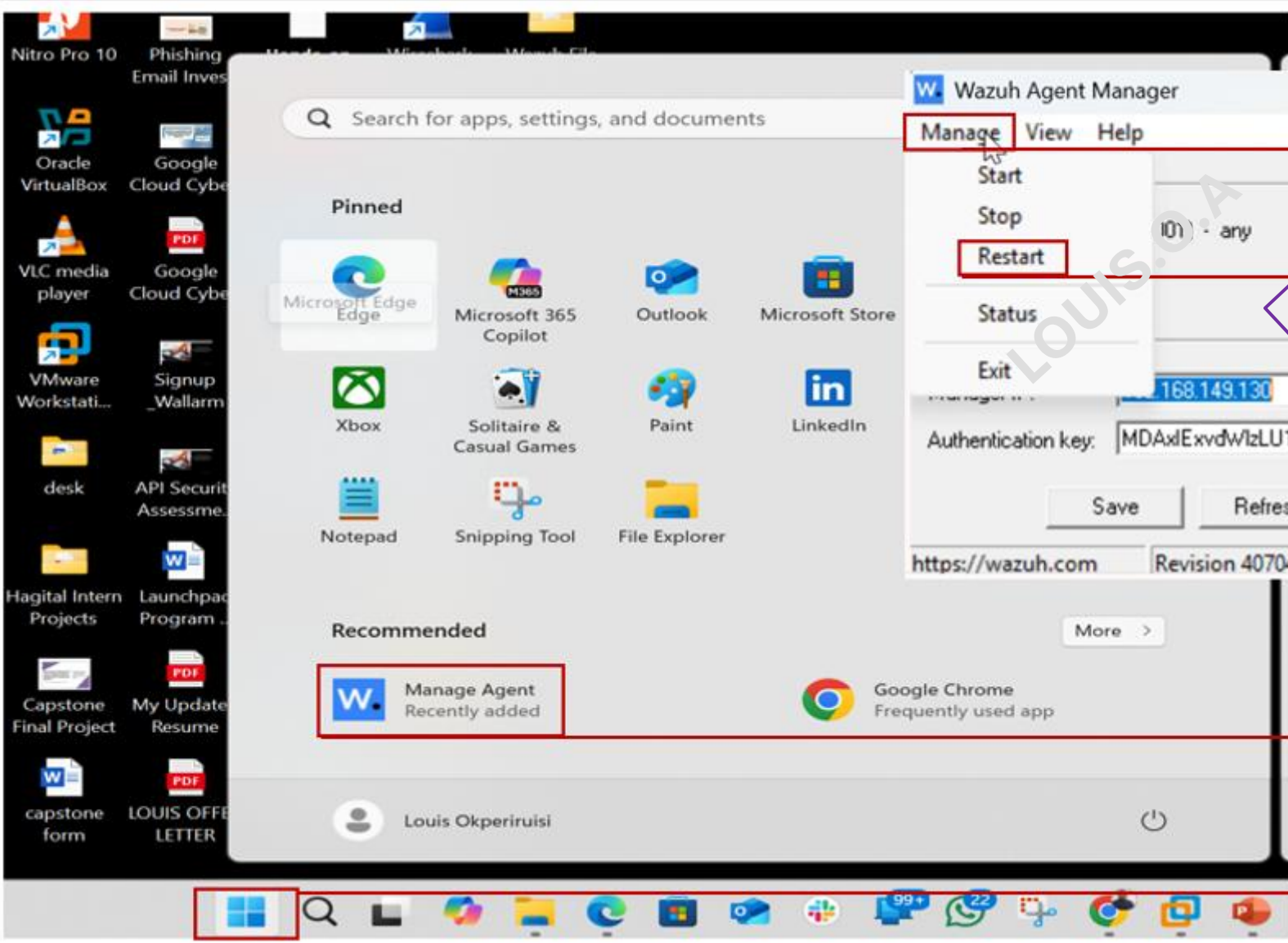


Agents (1)

Deploy new agent Refresh Export formatted WQL Refresh

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	Louis-Machine	192.168.149.1	default	Microsoft Windows 11 Pro 10.0.26200.7019	node01	v4.7.0	active	

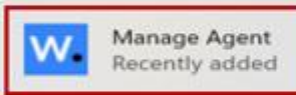
Rows per page: 10 < 1 >



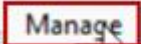
Restart wazuh once the agent has been added to the wazuh server



1



2



3

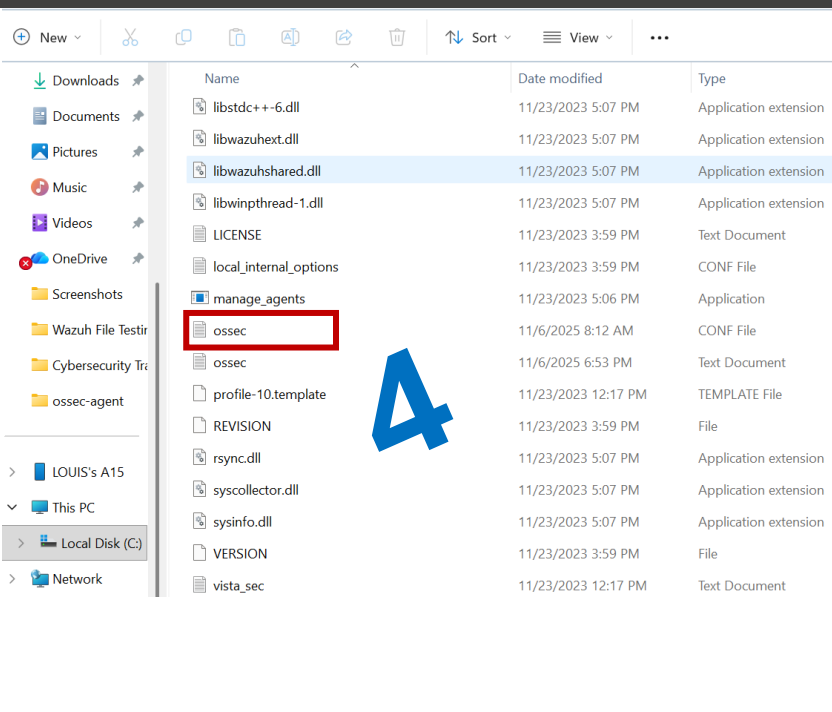
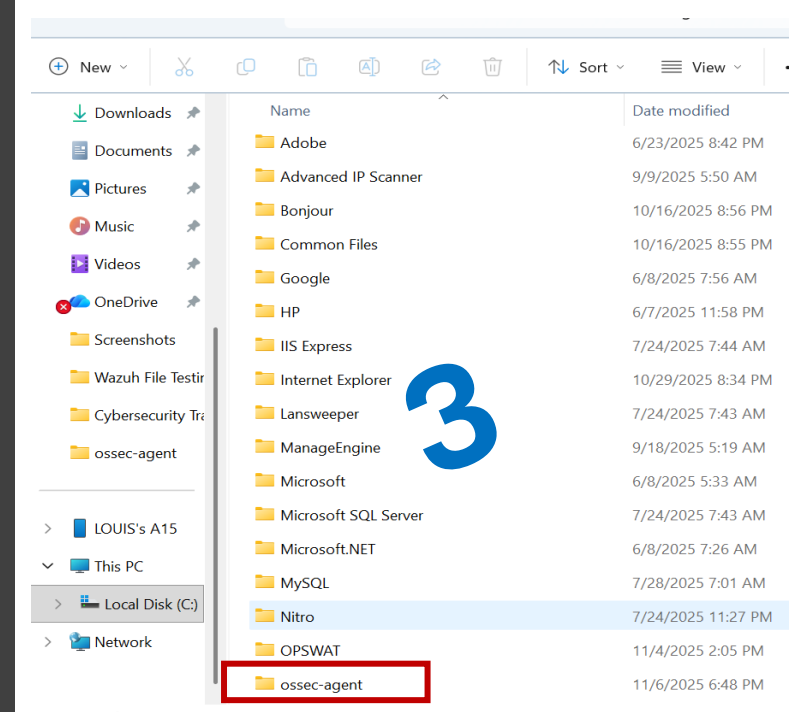
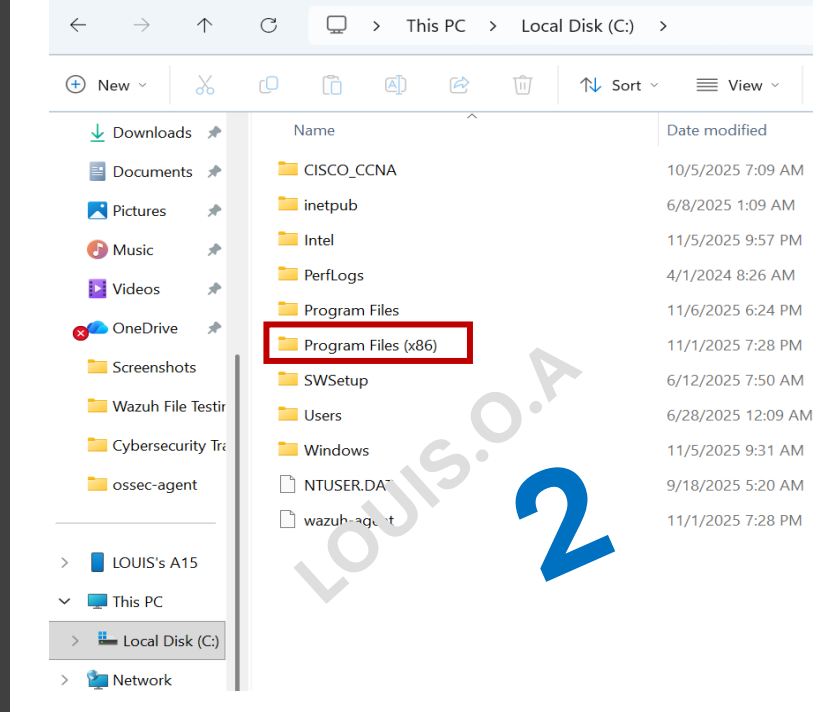
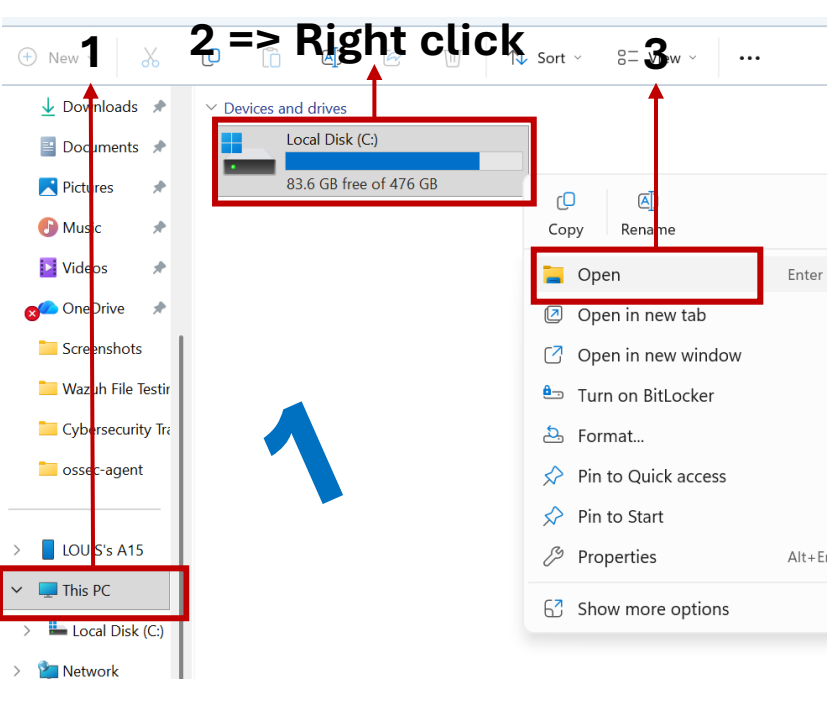


4

File Integrity Monitoring Configuration

[On Windows-Agent in ossec.conf file]





View all monitored directories by wazuh.

The screenshot shows the Wazuh web interface with the following navigation steps highlighted by red boxes and arrows:

1. Click on the **Configuration** tab in the top navigation bar.
2. Click on the **Management** menu item in the left sidebar.
3. Click on the **Configuration** sub-menu item in the expanded sidebar.
4. Click on the **Integrity monitoring** item in the 'Log data analysis' table.

The 'Log data analysis' table contains the following data:

Name	Description
Log collection	Log analysis from text files, Windows events or syslog outputs
Integrity monitoring	Identify changes in content, permissions, ownership, and attributes of files
Agentless	Run integrity checks on devices such as routers, firewalls and switches

The 'Cloud security monitoring' table contains the following data:

Name	Description
Amazon S3	Security events related to Amazon AWS services, collected directly via AWS API

Wazuh - Wazuh x +
Not secure https://192.168.149.130/app/wazuh#/manager/?tab=configuration

wazuh. Management Configuration

Integrity monitoring ENABLED

Identify changes in content, permissions, ownership, and attributes of files

General **Monitored** Ignored No diff Who-data Synchronization Files limit

General

The settings shown below are applied globally

Integrity monitoring status	enabled
Interval (in seconds) to run the integrity scan	43200
Time of day to run integrity scans	-
Day of the week to run integrity scans	-
Ignore files that change too many times	no
Alert when new files are created	no
Scan on start	yes
Skip scan on CIFS/NFS mounts	yes
Skip scan of /dev directory	yes

Wazuh - Wazuh x +
Not secure https://192.168.149.130/app/wazuh#/manager/?tab=configuration

wazuh. Management Configuration

Integrity monitoring ENABLED

Identify changes in content, permissions, ownership, and attributes of files

General **Monitored** Ignored No diff Who-data Synchronization Files limit

Monitored directories

These directories are included on the integrity scan

/bin	Selected item	/bin
/boot	Enable realtime monitoring	no
/etc	Enable auditing (who-data)	no
/sbin	Report file changes	no
/usr/bin	Perform all checksums	no
/usr/sbin	Check sums (MD5 & SHA1)	no
C:\Users\emma.okperiruisi\...	Check MD5 sum	yes
C:\Users\louis\Desktop\Wa...	Check SHA1 sum	yes

Total agents: 2
Active agents: 2
Disconnected agents: 0
Pending agents: 0
Never connected agents: 0

SECURITY INFORMATION MANAGEMENT

AUDITING AND POLICY MONITORING

Security events
Browse through your security alerts, identifying issues and threats in your environment.


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

Policy monitoring
Verify that your systems are configured according to your security policies baseline.

System auditing
Audit users behavior, monitoring command execution and alerting on access to critical files.

Security configuration assessment
Scan your assets as part of a configuration assessment audit.

wazuh. Agents

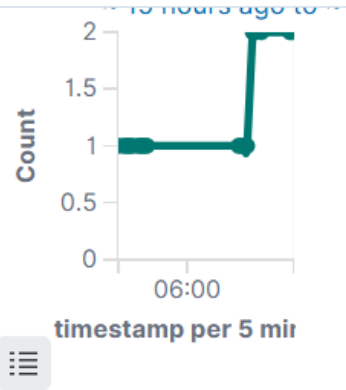


- Active (2)
- Disconnected (0)
- Pending (0)
- Never connected (0)

Active: 2, Disconnected: 0, Pending: 0, Never connected: 0. Agents coverage: 100.00%

Last registered agent: **virtualMachine**

Most active agent: **Louis-Machine**



Count vs timestamp per 5 min

Agents (2)

Deploy new agent Refresh Export for

id!=000 and status=active WQL

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status
001	Louis-Machine	192.168.149.1	default	Microsoft Windows 11 Pro 10.0.26200.7019	node01	v4.7.0	active
002	virtualMachine	192.168.149.128	default	Microsoft Windows 10 Pro 10.0.19043.928	node01	v4.7.0	active

Rows per page: 10

The three (3) cases of file integrity check (**Modify, Add, & Delete**)

Wazuh - Wazuh | VirusTotal integration - M | VirusTotal integration - M | (178) File Integrity Monit | Download Anti Malware | +

Not secure https://192.168.149.130/app/wazuh#/agents?tab=welcome&agent=001&g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(fro... ☆ | 📄 | 📌 | 🗑️ | 👤 | ⋮

Introduction to clou... | SOC Types and Role... | QuillBot AI | EndPoint Security -... | Log Management -... | The Hacker News [...] | Cyber Security Webi... | BrightTALK Cyberse...

☰ | 🏠 | **wazuh.** | Agents | **Louis-Machine** | a | ?

Security events | **Integrity monitoring** | SCA | More... | Inventory data | Stats | Configuration

ID	Status	IP address	Version	Groups	Operating system	Cluster node	Registration date
001	● active ?	192.168.149.1	Wazuh v4.7.0	default	Microsoft Windows 1...	node01	Nov 1, 2025 @ 19:29:39.000

Last keep alive
Nov 2, 2025 @ 15:22:28.000

~ 15 hours ago to ~ a few seconds ago

MITRE

Top Tactics

- Persistence: 255
- Defense Evasion: 250
- Initial Access: 245
- Privilege Escalation: 245
- Impact: 26

Compliance

PCI DSS

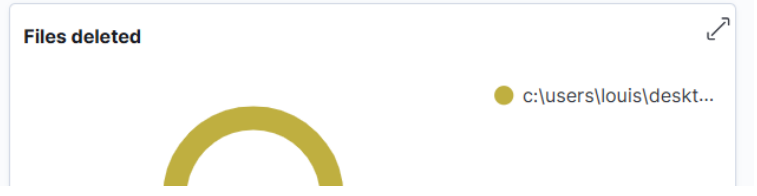
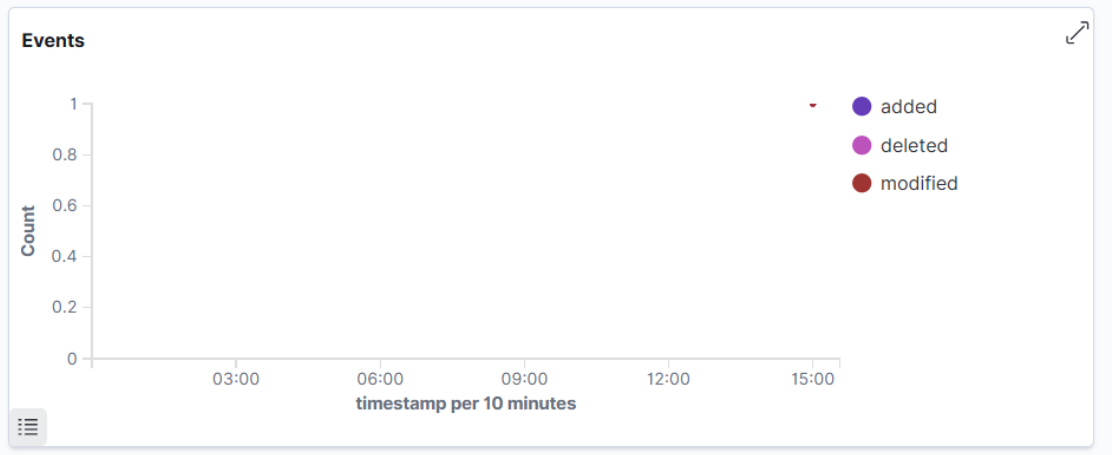
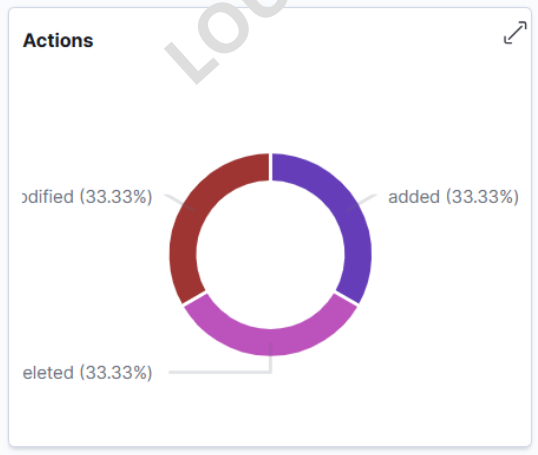
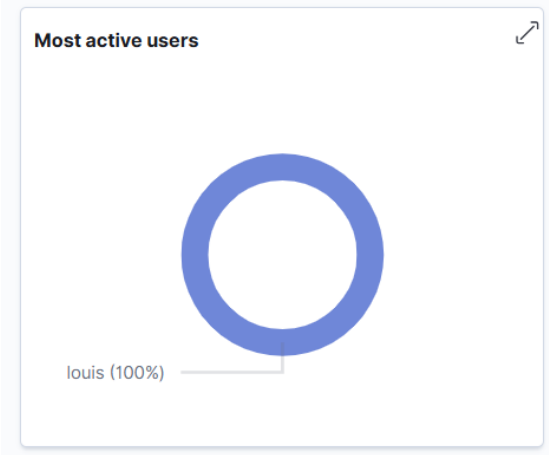
- 10.2.5 (275)
- 10.2.4 (24)
- 10.6 (11)
- 10.6.1 (10)
- 8.1.2 (10)

FIM: Recent events

Time ↓	Path	Action	Rule descrip...	Rule Level	Rule Id
Nov 2, 2025 @ 15:09:25.791	c:\users\lo...	modified	Integrity c...	7	550
Nov 2, 2025 @ 15:08:58.992	c:\users\lo...	added	File adde...	5	554
Nov 2, 2025 @ 15:08:58.992	c:\users\lo...	deleted	File delet...	7	553

Search [] DQL [] ~ 16 hours ago → ~ a few seconds ago Refresh

manager.name: wazuh-server rule.groups: syscheck agent.id: 001 + Add filter



manager.name: wazuh-server | rule.groups: syscheck | agent.id: 001 | + Add filter

wazuh-alerts-*

Search field names

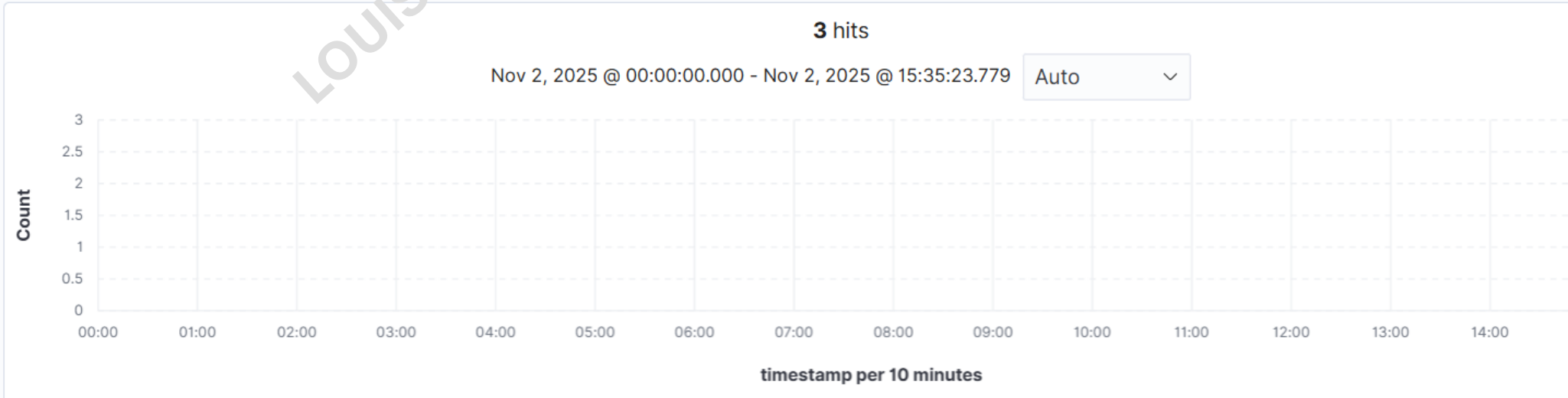
Filter by type 0

Selected fields

- rule.description
- rule.id
- rule.level
- syscheck.event
- syscheck.path

Available fields

- agent.id
- agent.ip
- agent.name
- data.aws.accountId
- data.aws.region



Time	syscheck.path	syscheck.event	rule.description	rule.level
> Nov 2, 2025 @ 15:09:25.791	c:\users\louis\desktop\wazuh file testing\test.txt	modified	Integrity checksum change detected.	7
	is\desktop\wazuh file testing\yes1.txt	deleted	File deleted.	7
> Nov 2, 2025 @ 15:08:58.992	c:\users\louis\desktop\wazuh file testing\yes1.txt	added	File added to the system.	5

File Modification

Wazuh - Wazuh | VirusTotal integration - M | VirusTotal integration - M | (179) File Integrity Monit | Download Anti Malware | +

Not secure https://192.168.149.130/app/wazuh#/overview/?tab=fim&tabView=panels&_g=(filters:!,refreshInterval:(pause:!t,value:0),t... | Introduction to clou... | SOC Types and Role... | QuillBot AI | EndPoint Security -... | Log Management -... | The Hacker News |... | Cyber Security Webi... | BrightTALK Cyber

Modules | Louis-Machine | Integrity monitoring ⓘ

- data.aws.region
- decoder.name
- full_log
- id
- input.type
- location
- manager.name
- # rule.firetimes
- rule.gdpr
- rule.gpg13
- rule.groups
- rule.hipaa
- rule.mail
- rule.mitre.id
- rule.mitre.tactic
- rule.mitre.technique
- rule.nist_800_53
- rule.pci_dss
- rule.tsc
- syscheck.attrs_after

Table JSON

_index	wazuh-alerts-4.x-2025.11.02
agent.id	001
agent.ip	192.168.149.1
agent.name	Louis-Machine
data.aws.accountId	
data.aws.region	
decoder.name	syscheck_integrity_changed
full_log	> File 'c:\users\louis\desktop\wazuh file testing\test.txt' modified Mode: whodata Changed attributes: size,mtime,md5,sha1,sha256 Size changed from '421' to '636' Old modification time was: '1762076741', now it is '1762092564' Old md5sum was: '4bdb8f63957e05196aace3d4ad21fd42' New md5sum is: '257c fbd4e0ffdf56cf5e073db7e724c12'
id	1762092565.3841790
input.type	log
location	syscheck

File Deletion

Wazuh - Wazuh | VirusTotal integration - M | VirusTotal integration - M | (179) File Integrity Monit | Download Anti Malware | +

Not secure https://192.168.149.130/app/wazuh#/overview/?tab=fim&tabView=panels&_g=(filters:!,refreshInterval:(pause:!t,value:0),time:(f...)

Introduction to clou... | SOC Types and Role... | QuillBot AI | EndPoint Security -... | Log Management -... | The Hacker News |... | Cyber Security Webi... | BrightTALK Cyberse...

wazuh. Modules Louis-Machine Integrity monitoring

agent.ip	NOV 2, 2025 @ 15:09:25.791	c:\users\louis\desktop\wazuh file testing\test.txt	modified	integrity checksum changed.	7	550
agent.name	Nov 2, 2025 @ 15:08:58.992	c:\users\louis\desktop\wazuh file testing\yes1.txt	deleted	File deleted.	7	553

Expanded document

View surrounding documents View single document

Table JSON

_index	wazuh-alerts-4.x-2025.11.02
agent.id	001
agent.ip	192.168.149.1
agent.name	Louis-Machine
data.aws.accountId	
data.aws.region	
decoder.name	syscheck_deleted
full_log	File 'c:\users\louis\desktop\wazuh file testing\yes1.txt' deleted Mode: whodata
id	1762092538.3840437
input.type	log
location	syscheck
manager.name	wazuh-server
rule.description	File deleted.

File Addition

- Available fields
- agent.id
- agent.ip
- agent.name
- data.aws.accountId
- data.aws.region
- decoder.name
- full_log
- id
- input.type
- location
- manager.name
- rule.firetimes
- rule.gdpr
- rule.gpg13
- rule.groups
- rule.hipaa
- rule.mail
- rule.mitre.id
- rule.mitre.tactic
- rule.mitre.technique
- rule.nist_800_53
- rule.pci_dss
- rule.tsc
- syscheck.attrs_after
- syscheck.audit.process.id
- syscheck.audit.process.name
- syscheck.audit.user.id

Time	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
> Nov 2, 2025 @ 15:09:25.791	c:\users\louis\desktop\wazuh file testing\test.txt	modified	Integrity checksum changed.	7	550
> Nov 2, 2025 @ 15:08:58.992	c:\users\louis\desktop\wazuh file testing\yes1.txt	deleted	File deleted.	7	553
✓ Nov 2, 2025 @ 15:08:58.992	c:\users\louis\desktop\wazuh file testing\yes112.txt	added	File added to the system.	5	554

Expanded document [View surrounding documents](#) [View single document](#)

Table JSON

† _index	wazuh-alerts-4.x-2025.11.02
† agent.id	001
† agent.ip	192.168.149.1
† agent.name	Louis-Machine
† data.aws.accountId	
† data.aws.region	
† decoder.name	syscheck_new_entry
† full_log	File 'c:\users\louis\desktop\wazuh file testing\yes112.txt' added Mode: whodata
† id	1762092538.3839074
† input.type	log
† location	syscheck
† manager.name	wazuh-server
† rule.description	File added to the system.

File Monitoring alert message sent to slack channel

The screenshot shows the Microsoft Teams interface. On the left is a navigation pane with icons for Home, DMs (53), Activity, Files, and More. The main area displays a direct message conversation with 'louis (you)'. The message content is:

Alert_security: File deleted.

Below the message, a 'WAZUH Alert' is expanded, showing the following details:

- File deleted.**
- File:** 'c:\users\louis\desktop\wazuh file testing\3rd.txt' deleted
- Mode:** whodata
- Agent:** (001) - Louis-Machine
- Location:** syscheck
- Rule ID:** 553 (Level 7)

The message was received 'Today at 7:22 AM'. At the bottom of the chat, there is a text input field with the text 'Jot something down' and a rich text editor toolbar.

The screenshot shows the Wazuh web interface. At the top, there is a navigation bar with 'wazuh.' and 'Integrity monitoring' selected. Below the navigation bar is a graph showing the count of events over time, with a significant spike at 09:00. Below the graph is a table of events:

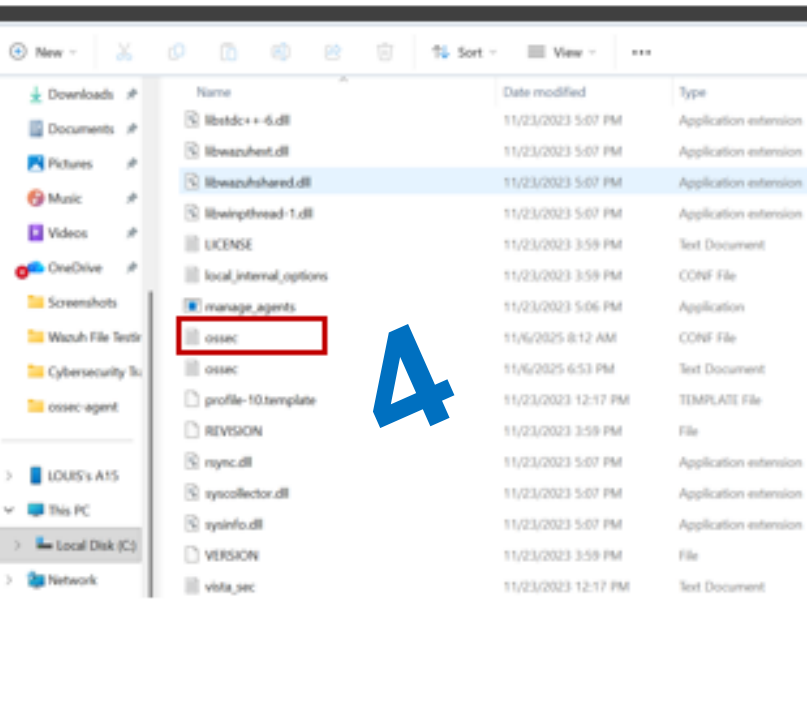
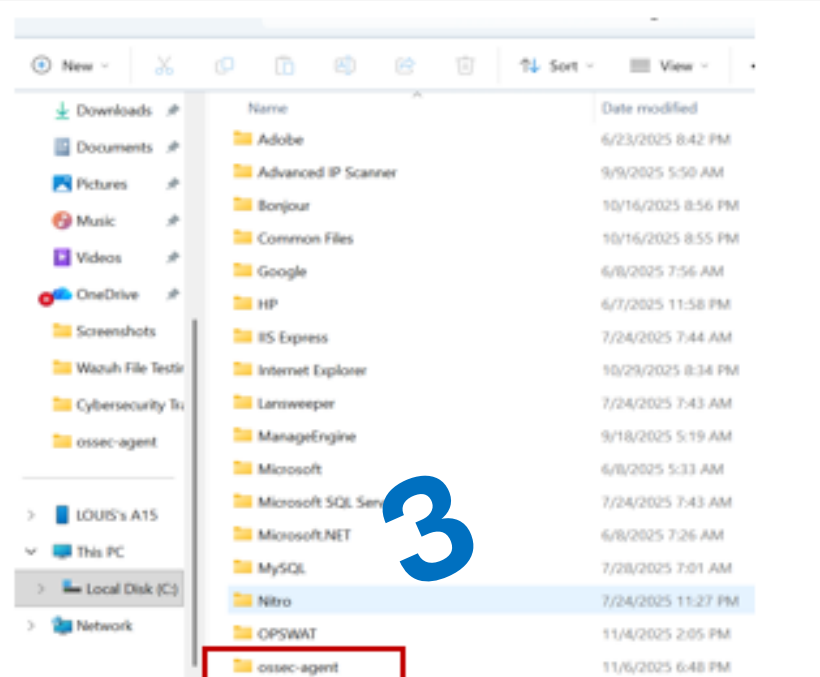
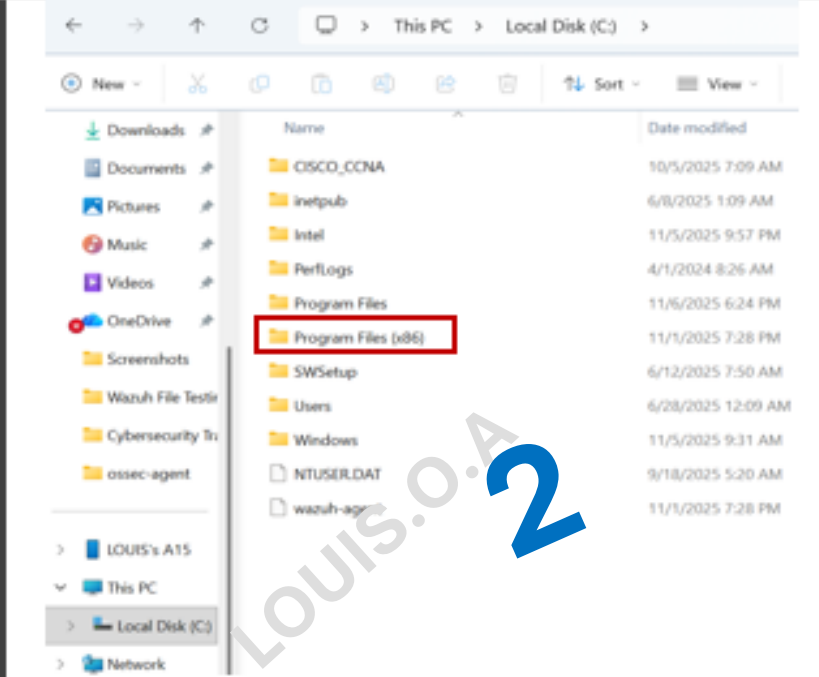
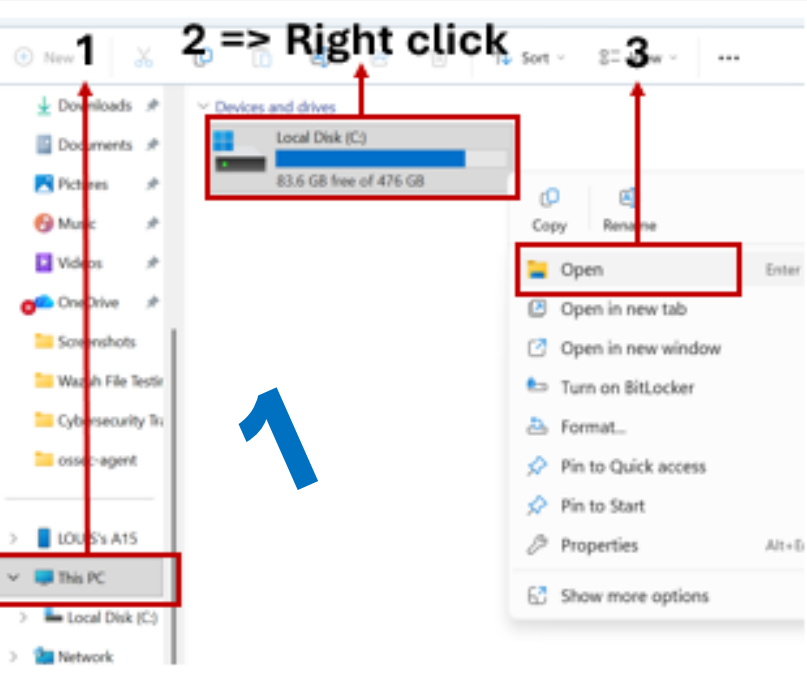
Time	syscheck.path	syscheck.event	rule.description
> Nov 6, 2025 @ 07:22:06.031	c:\users\louis\desktop\wazuh file testing\3rd.txt	deleted	File deleted.
> Nov 6, 2025 @ 07:22:01.336	c:\users\louis\desktop\wazuh file testing\new text document.txt	deleted	File deleted.
> Nov 6, 2025 @ 07:22:01.332	c:\users\louis\desktop\wazuh file testing\6th nov.txt	added	File added to the system.
> Nov 6, 2025 @ 07:21:52.598	c:\users\louis\desktop\wazuh file testing\new text document.txt	added	File added to the system.
> Nov 5, 2025 @ 20:10:45.245	c:\users\louis\desktop\wazuh file testing\2nd.txt	deleted	File deleted.
> Nov 5, 2025 @ 20:10:41.414	c:\users\louis\desktop\wazuh file testing\forth	added	File added to the system.

Microsoft-Windows Windows Defender Configuration

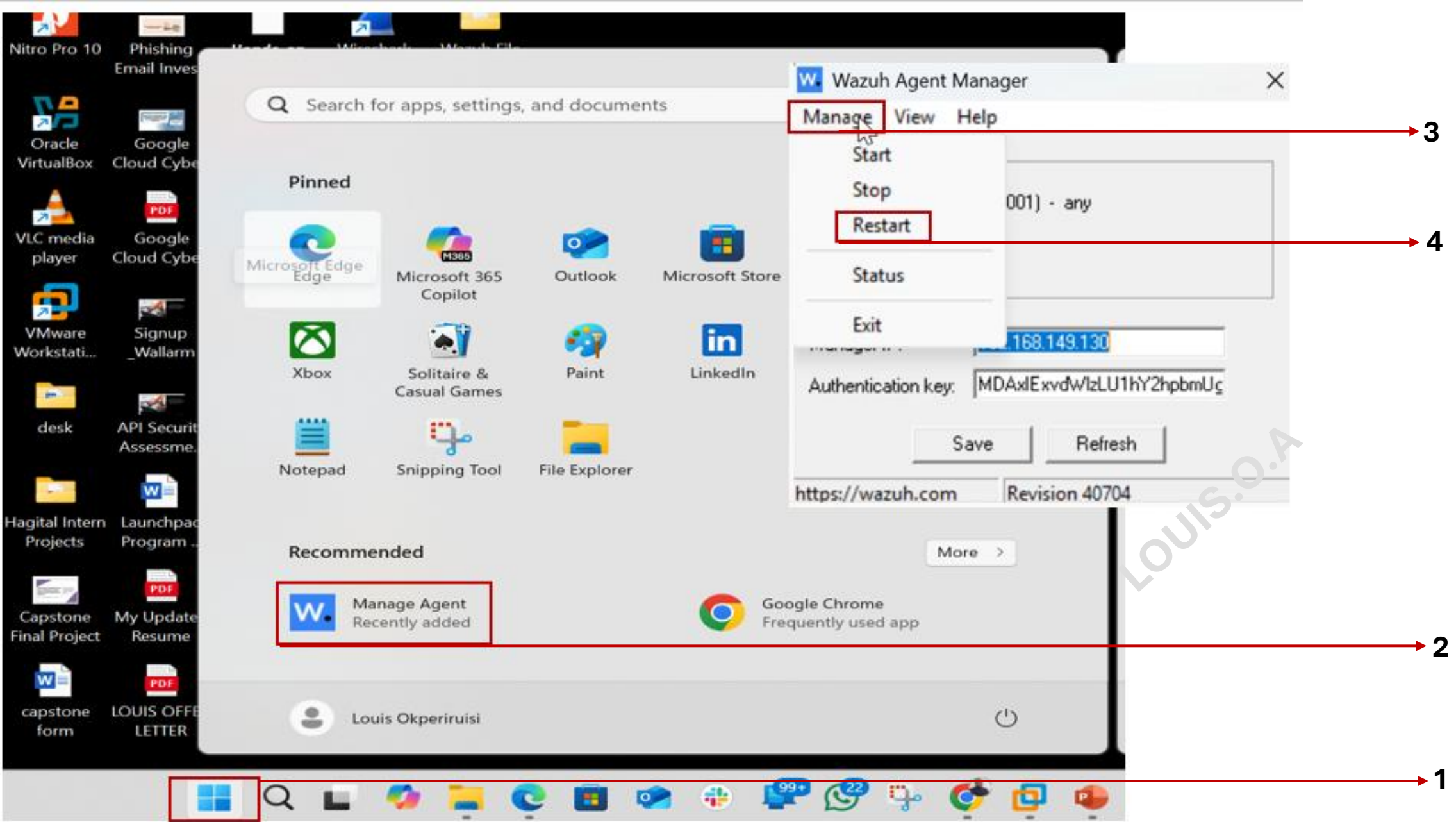
[On Windows-Agent in ossec.conf file]

LOUIS.O.A





Restart Wazuh-Server after windows agent configuration



**Linking Wazuh to my
Slack account, for
possible alert.**

LOUIS.O.A

wazuh.



slack



Signup on Slack and create a new workspace

The image shows a Slack interface with a dark purple theme. On the left sidebar, the 'Mentor Me Collective' workspace is selected. A red box highlights a '+' icon in the sidebar, which has opened a dropdown menu. The menu contains three options: 'Sign in to another workspace', 'Create a new workspace' (highlighted in blue), and 'Find workspaces'. The main area shows the workspace name 'Mentor Me Collective' and a list of channels including '# community-networking', '# events', '# job-board', and '# pets-of-mmc'. On the right, a user profile for 'Okperiruisi Louis' is displayed, showing their name, title 'gclp cloud cybersecurity, Track_Lead', and status 'Active'. The profile also includes contact information such as an email address 'louistinteds2001@gmail.com' and an option to '+ Add Phone'. The interface includes a search bar at the top and various navigation icons.

Search Mentor Me Collective

Mentor Me Collective

Home

Threads

Huddles

+

Sign in to another workspace

Create a new workspace

Find workspaces

Drag and drop important stuff here

Files

More

Channels

community-networking

emeia_cloud_cs_sm25

events

gclp-support

introductions

job-board

pets-of-mmc

sm25_gclp_community

sm25_gclp_cs_trackleads

sm25_gclp_trackleads

Browse all channels

Profile

Okperiruisi Louis

gclp cloud cybersecurity, Track_Lead

Edit

+ Add name pronunciation

+ Add pronouns

Active

9:54 PM local time

Set a status

View as

Contact information

Edit

Email address

louistinteds2001@gmail.com

+ Add Phone

About me

Edit

+ Add Start Date

Visit <https://docs.slack.dev/messaging/sending-messages-using-incoming-webhooks/> to generate Webhook Url

The screenshot shows a web browser displaying the Slack Developers documentation page. The URL in the address bar is <https://docs.slack.dev/messaging/sending-messages-using-incoming-webhooks/>. The page title is "Getting started with incoming webhooks". The main content area is divided into two steps:

- 1. Create a Slack app (if you don't already have one)**
 - A red box highlights the "Create an app" button.
 - A red arrow points from the "From scratch" option in the modal to the "Create an app" button.
- 2. Enable incoming webhooks**

A modal titled "Create an app" is open, showing two options:

- From a manifest**: Use a manifest file to add your app's basic info, scopes, settings & features to your app.
- From scratch**: Use our configuration UI to manually add basic info, scopes, settings, & features to your app.

At the bottom of the modal, there is a link: "Need help? Check our [documentation](#), or [see an example](#)".

Your Apps

Use our APIs to build an app or create a public app

Your App Configuration
[Learn about tokens](#)

Name app & choose workspace

App Name

 35

Don't worry - you'll be able to change this later.

Pick a workspace to develop your app in:

Keep in mind that you can't change this app's workspace later. If you leave the workspace, you won't be able to manage any apps you've built for it. The workspace will control the app even if you leave the workspace.

[Sign into a different workspace](#)

By creating a **Web API Application**, you agree to the [Slack API Terms of Service](#).

Cancel



Wazuh | Centra | resum | (198) | Down | integr | Linkin | Linkin | Login | new-cl | (28) In | slack |

https://api.slack.com/apps/A09R6GP561X?created=1

slack api

Alert_security ▾

Basic Information

Settings

- Basic Information
- Collaborators
- Socket Mode
- Install App
- Manage Distribution

Features

- App Home
- Agents & AI Apps NEW
- Work Object Previews...
- Workflow Steps NEW
- Org Level Apps
- Incoming Webhooks**
- Interactivity & Shortcuts
- Slash Commands

App Credentials

These credentials allow your app to access the Slack API. They are a secret. Please don't share your app credentials with anyone, include them in public code repositories, or store them in insecure ways.

App ID Date of App Creation

A09R6GP561X November 4, 2025

Client ID

9841271153926.9856567176065

Client Secret

..... Show Regenerate

You'll need to send this secret along with your client ID when making your [oauth.v2.access](#) request.

Signing Secret

Discard C...

resum | (198) | Down | integr | Linkin | Linkin | Login | new-cl | (28) In | slack | w | Extern

api.slack.com/apps/A09R6HE7917/incoming-webhooks?

Alert_security ▾

Incoming Webhooks

Settings

- Basic Information
- Collaborators
- Socket Mode
- Install App
- Manage Distribution

Features

- App Home
- Agents & AI Apps NEW
- Work Object Previews NEW
- Workflow Steps NEW
- Org Level Apps
- Incoming Webhooks**
- Interactivity & Shortcuts
- Slash Commands
- Steps from Apps LEGACY
- OAuth & Permissions
- Event Subscriptions
- User ID Translation
- App Manifest NEW
- Beta Features

Submit to Slack Marketplace

- Review & Submit

Give feedback

Slack ♥

Activate Incoming Webhooks

On **1**

Incoming webhooks are a simple way to post messages from external sources into Slack. They make use of normal HTTP requests with a JSON payload, which includes the message and a few other optional details. You can include [message attachments](#) to display richly-formatted messages.

Adding incoming webhooks requires a bot user. If your app doesn't have a [bot user](#), we'll add one for you.

Each time your app is installed, a new Webhook URL will be generated.

If you deactivate incoming webhooks, new Webhook URLs will not be generated when your app is installed to your team. If you'd like to remove access to existing Webhook URLs, you will need to [Revoke All OAuth Tokens](#).

Webhook URLs for Your Workspace

To dispatch messages with your webhook URL, send your [message](#) in JSON as the body of an [application/json](#) POST request.

Add this webhook to your workspace below to activate this curl example.

Sample curl request to post to a channel:

```
curl -X POST -H 'Content-type: application/json' --data '{"text": "Hello, World!"}' YOUR_WEBHOOK_URL_HERE
```

Webhook URL	Channel	Added By
No webhooks have been added yet.		

Add New Webhook **2**



Install the "Alert_security" app in Slack

This app was created by a member of your workspace, Security Analyst.

Workspace

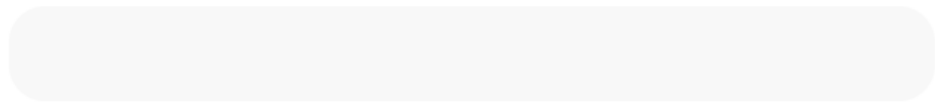
Security Analyst

Channel for webhook

Search for a channel...

"Alert_security" requires a channel to post as an app.

Review app permissions



Cancel

Install Alert_security

LOUIS.O.A

1

2

3

Chose the channel you created earlier

Alert_security

Settings

- Basic Information
- Collaborators
- Socket Mode
- Install App
- Manage Distribution

Features

- App Home
- Agents & AI Apps NEW
- Work Object Previews NEW
- Workflow Steps NEW
- Org Level Apps

Incoming Webhooks

- Interactivity & Shortcuts
- Slash Commands
- Steps from Apps LEGACY
- OAuth & Permissions
- Event Subscriptions
- User ID Translation
- App Manifest NEW
- Beta Features

Submit to Slack Marketplace

- Review & Submit
- Give feedback

Incoming Webhooks

Activate Incoming Webhooks

On

Incoming webhooks are a simple way to post messages from external sources into Slack. They make use of normal HTTP requests with a JSON payload, which includes the message and a few other optional details. You can include [message attachments](#) to display richly-formatted messages.

Adding incoming webhooks requires a bot user. If your app doesn't have a [bot user](#), we'll add one for you.

Each time your app is installed, a new Webhook URL will be generated.

If you deactivate incoming webhooks, new Webhook URLs will not be generated when your app is installed to your team. If you'd like to remove access to existing Webhook URLs, you will need to [Revoke All OAuth Tokens](#).

Webhook URLs for Your Workspace

To dispatch messages with your webhook URL, send your [message](#) in JSON as the body of an `application/json` POST request.

Add this webhook to your workspace below to activate this curl example.

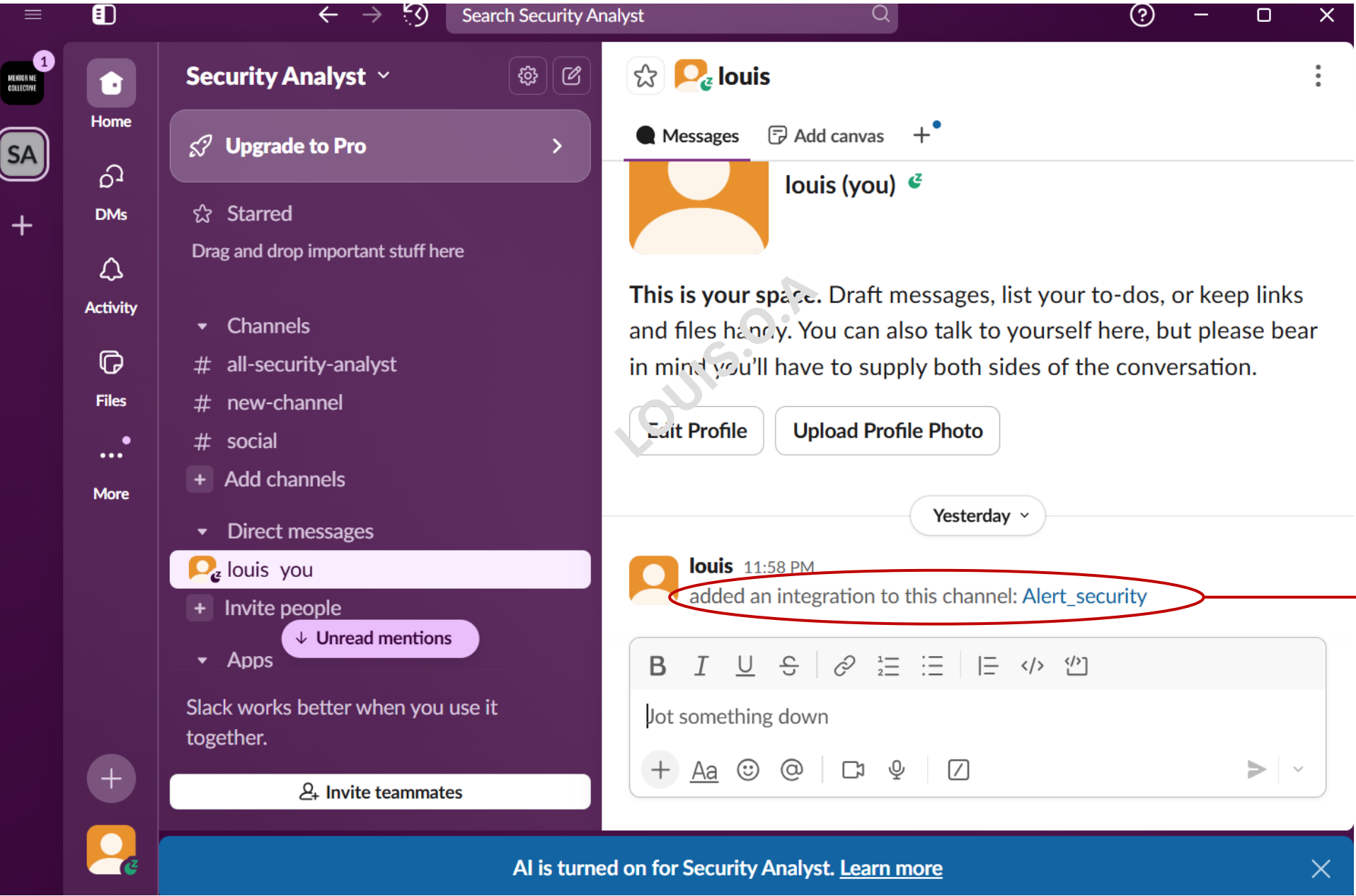
Sample curl request to post to a channel:

```
curl -X POST -H 'Content-type: application/json' --data '{"text":"Hello, World!"}' https://hooks.slack.com/services/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
```

Copy

Webhook URL	Channel	Added By
https://hooks.slack.com/services/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 Copy	louis	louis Nov 4, 2025 🗑️

Copy the Webhook URL to be used in ossec.conf



This shows it has been created

Wazuh Server configuration: Copy code from the Wazuh website into ossec.conf in wazuh-server

The screenshot shows a web browser at the URL `https://documentation.wazuh.com/current/user-manual/manager/integration-with-external-apis.html`. The page title is "wazuh." and the version is "Version 4.14 (current)". The navigation menu includes "Platform", "Cloud", "CTI", "Documentation", "Services", "Partners", and "Company". The left sidebar shows the "User manual" section expanded, with "External API integration" selected. The main content area shows step 2: "Append the configuration below to the `/var/ossec/etc/ossec.conf` file on the Wazuh server. Replace `<WEBHOOK_URL>` with your incoming webhook." Below this is a code block for the configuration, which is highlighted with a red box. The code is:

```
<ossec_config>
  <integration>
    <name>slack</name>
    <hook_url><SLACK_WEBHOOK_URL></hook_url> <!-- Replace with your Slack hook URL -->
    <alert_format>json</alert_format>
  </integration>
</ossec_config>
```

Below the code block is a note: "Note You can set a JSON object with customization fields using the `options` tag. Visit the [Slack API reference](#) for information about available customization fields." Step 3 is: "Restart the Wazuh manager to apply the changes:"

Open Wazuh-Server to configure slack alert

The screenshot shows the Wazuh web interface with the following navigation steps highlighted by red boxes and arrows:

- 1**: Click on the **Modules** menu item in the top navigation bar.
- 2**: Click on the **Management** sub-menu item in the left sidebar.
- 3**: Click on the **Configuration** sub-menu item under the **Administration** section in the central menu.

The interface also displays the following information:

- Management directory:** Administration, Status and reports, Rules, Decoders, CDB lists, Groups, Configuration, Reporting.
- Agents:** Pending agents (0), Never connected agents (0).
- AUDITING AND POLICY MONITORING:** Policy monitoring, System auditing, Security configuration assessment.
- THREAT DETECTION AND RESPONSE** and **REGULATORY COMPLIANCE** sections are visible at the bottom.



Configuration

Refresh

[Edit configuration](#)

Main configurations

Name	Description
Global Configuration	Global and remote settings
Cluster	Master node configuration
Registration Service	Automatic agent registration service

Alerts and output management

Name	Description
Alerts	Settings related to the alerts and their format
Integrations	Slack, VirusTotal and PagerDuty integrations with external APIs

Auditing and policy monitoring

Name	Description
Policy monitoring	Configuration to ensure compliance with security policies, standards and hardening guides

Manager configuration

Refresh

Save

Restart Manager

Edit `ossec.conf` of Manager

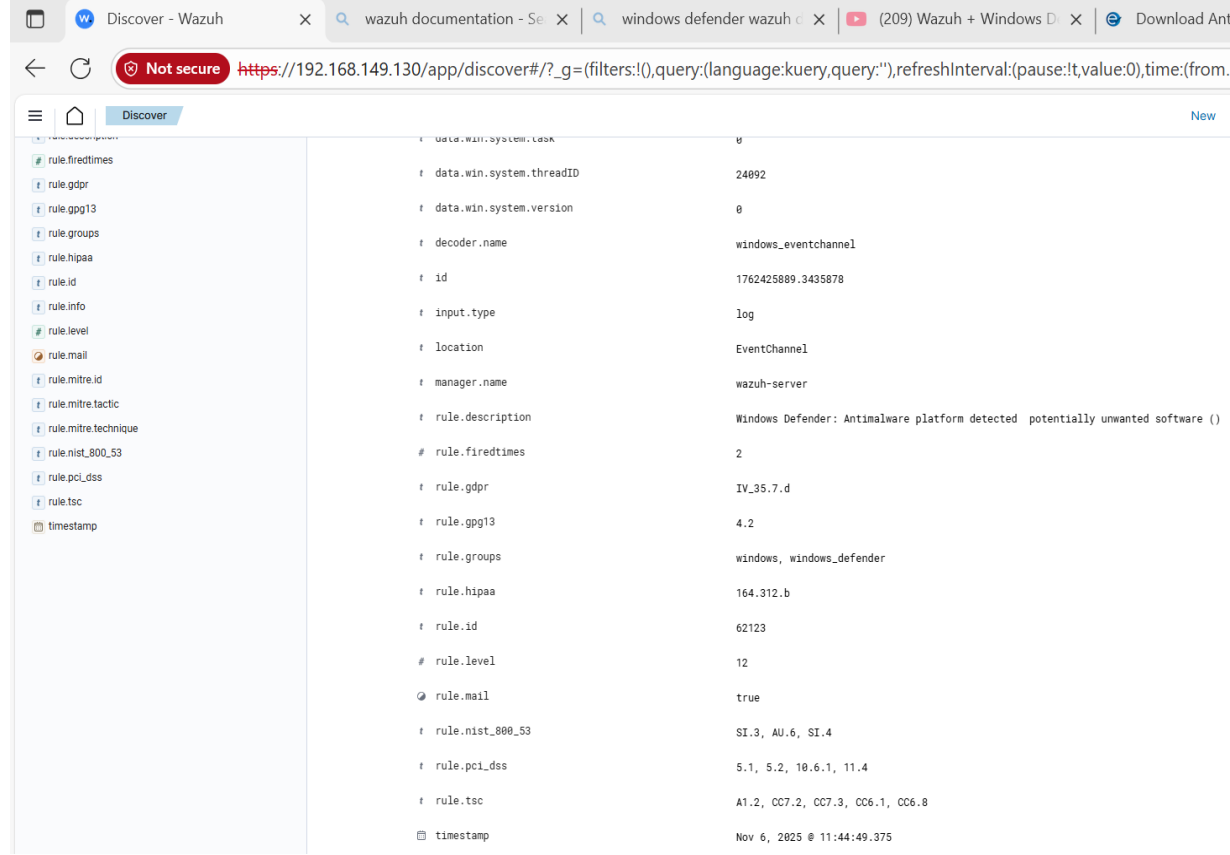
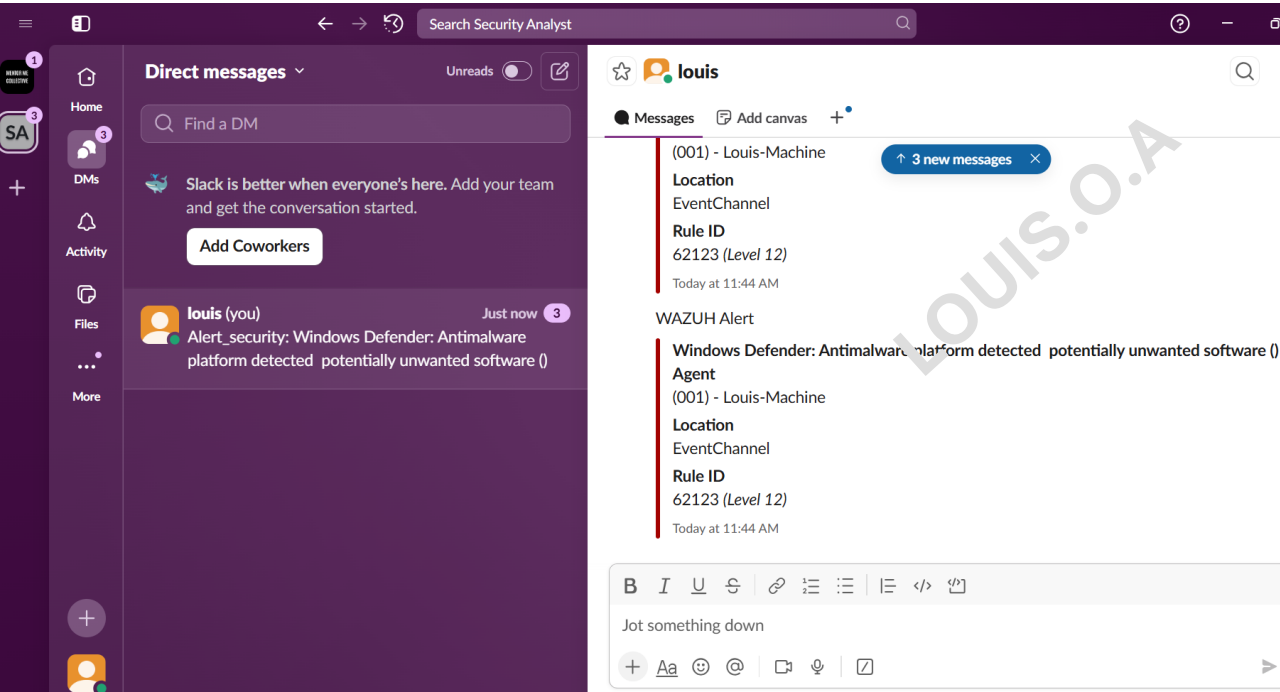
```
22
23 <alerts>
24   <log_alert_level>3</log_alert_level>
25   <email_alert_level>12</email_alert_level>
26 </alerts>
27
28 <integration>
29   <name>slack</name>
30   <hook_url>https://hooks.slack.com/services/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</hook_url>
31   <alert_format>json</alert_format>
32   <level>7</level>
33 </integration>
34
35
36 <!-- Choose between "plain", "json", or "plain,json" for the format of internal logs -->
37 <logging>
38   <log_format>plain</log_format>
39 </logging>
40
41 <remote>
42   <connection>secure</connection>
```

Visit <https://www.eicar.org/download-anti-malware-testfile/> to download Malware test file and watch Window Defender trigger alert and send message to wazuh and Slack.

The screenshot shows a web browser window with the URL <https://www.eicar.org/download-anti-malware-testfile/>. The page features the EICAR logo and a navigation bar with a contact number (+49 8194 99 84 99) and a 'CONTACT' link. The main content area is titled 'DOWNLOAD AREA' and includes the text 'using the secure, SSL enabled protocol HTTPS'. Below this, there are four download cards, each with a 'DOWNLOAD' button. The first card, 'EICAR.COM', is highlighted with a red border and contains the text 'Com-file' and '68 Bytes'. The second card, 'EICAR.COM.TXT', contains '1 Text-file' and '68 Bytes'. The third card, 'EICAR.COM.ZIP', contains '1 Zip-file' and '184 Bytes'. The fourth card, 'EICAR.COM-2.ZIP', contains '1 Zip-file' and '308 Bytes'. A watermark 'LOUIS.O.A' is visible across the page.

File Name	File Type	Size
EICAR.COM	Com-file	68 Bytes
EICAR.COM.TXT	1 Text-file	68 Bytes
EICAR.COM.ZIP	1 Zip-file	184 Bytes
EICAR.COM-2.ZIP	1 Zip-file	308 Bytes

Malware detected & triggered on wazuh, message sent to Slack Channel immediately



integration configuration of VirusTotal with wazuh



- Modules
- Management**
- Agents
- Tools
- Security
- Settings

- Management directory
 - Administration
 - Rules
 - Decoders
 - CDB lists
 - Groups
 - Configuration**
 - Status and reports
 - Status
 - Cluster
 - Statistics
 - Logs
 - Reporting

ts Pending agents Never connected agents

0 2 0

AUDITING AND POLICY MONITORING

3

- Policy monitoring**
Verify that your systems are configured according to your security policies baseline.
- System auditing**
Audit users behavior, monitoring command execution and alerting on access to critical files.
- Security configuration assessment**
Scan your assets as part of a configuration assessment audit.

Wazuh - Wazuh x VirusTotal integration x Centralized configur. x (206) Wazuh + Wind x Download Anti Malw x new-channel (Chan x +

Not secure https://192.168.149.130/app/wazuh#/manager/?tab=configuration

wazuh. Management Configuration

Configuration

Refresh Edit configuration

Main configurations

Name	Description
Global Configuration	Global and remote settings
Cluster	Master node configuration
Registration Service	Automatic agent registration service

Alerts and output management

Name	Description
Alerts	Settings related to the alerts and their format
Integrations	Slack, VirusTotal and PagerDuty integrations with external APIs

Auditing and policy monitoring

Name	Description
Policy monitoring	Configuration to ensure compliance with security policies, standards and hardening guides

Copy the code from wazuh website

Wazuh - Wazuh x VirusTotal integrati... Centralized configur... (206) Wazuh + Wind x

Not secure https://192.168.149.130/app/wazuh#/manager/?tab=configuration

wazuh. Management Configuration

Manager configuration

Edit ossec.conf of Manager

```
4 Mailing list: https://groups.google.com/forum/#!forum/wazuh
5 -->
6
7 <ossec_config>
8   <global>
9     <jsonout_output>yes</jsonout_output>
10    <alerts_log>yes</alerts_log>
11    <logall>no</logall>
12    <logall_json>no</logall_json>
13    <email_notification>no</email_notification>
14    <smtp_server>smtp.example.wazuh.com</smtp_server>
15    <email_from>wazuh@example.wazuh.com</email_from>
16    <email_to>recipient@example.wazuh.com</email_to>
17    <email_maxperhour>12</email_maxperhour>
18    <email_log_source>alerts.log</email_log_source>
19    <agents_disconnection_time>10m</agents_disconnection_time>
20    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
21  </global>
22
23  <alerts>
24    <log_alert_level>3</log_alert_level>
25    <email_alert_level>12</email_alert_level>
26  </alerts>
27
28  <integration>
29    <name>slack</name>
30    <hook_url>https://hooks.slack.com/services/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</hook_url>
31    <alert_format>json</alert_format>
32    <level>7</level>
33  </integration>
```



wazuh. Management Configuration

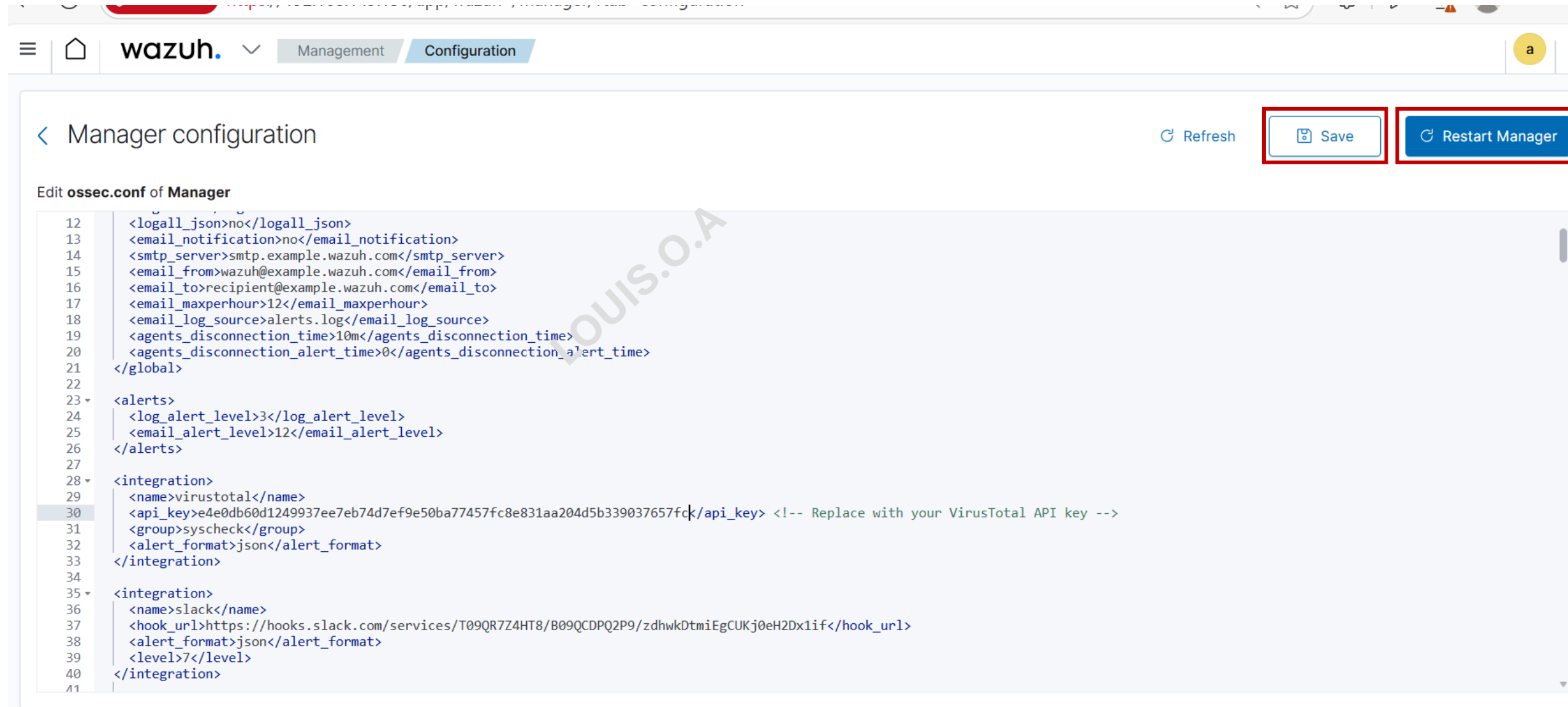
Manager configuration

Edit ossec.conf of Manager

```
13 <email_notification>no</email_notification>
14 <smtp_server>smtp.example.wazuh.com</smtp_server>
15 <email_from>wazuh@example.wazuh.com</email_from>
16 <email_to>recipient@example.wazuh.com</email_to>
17 <email_maxperhour>12</email_maxperhour>
18 <email_log_source>alerts.log</email_log_source>
19 <agents_disconnection_time>10m</agents_disconnection_time>
20 <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
21 </global>
22
23  <alerts>
24    <log_alert_level>3</log_alert_level>
25    <email_alert_level>12</email_alert_level>
26  </alerts>
27
28  <integration>
29    <name>virustotal</name>
30    <api_key>API_KEY</api_key> <!-- Replace with your VirusTotal API key -->
31    <group>syscheck</group>
32    <alert_format>json</alert_format>
33  </integration>
34
35  <integration>
36    <name>slack</name>
37    <hook_url>https://hooks.slack.com/services/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</hook_url>
38    <alert_format>json</alert_format>
39    <level>7</level>
40  </integration>
41
```



Insert the API KEY generated from VirusTotal



Management Configuration

< Manager configuration Refresh Save Restart Manager

Edit **ossec.conf** of Manager

```
12 <logall_json>no</logall_json>
13 <email_notification>no</email_notification>
14 <smtp_server>smtp.example.wazuh.com</smtp_server>
15 <email_from>wazuh@example.wazuh.com</email_from>
16 <email_to>recipient@example.wazuh.com</email_to>
17 <email_maxperhour>12</email_maxperhour>
18 <email_log_source>alerts.log</email_log_source>
19 <agents_disconnection_time>10m</agents_disconnection_time>
20 <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
21 </global>
22
23 <alerts>
24 | <log_alert_level>3</log_alert_level>
25 | <email_alert_level>12</email_alert_level>
26 </alerts>
27
28 <integration>
29 | <name>virustotal</name>
30 | <api_key>e4e0db60d1249937ee7eb74d7ef9e50ba77457fc8e831aa204d5b339037657fc</api_key> <!-- Replace with your VirusTotal API key -->
31 | <group>syscheck</group>
32 | <alert_format>json</alert_format>
33 </integration>
34
35 <integration>
36 | <name>slack</name>
37 | <hook_url>https://hooks.slack.com/services/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</hook_url>
38 | <alert_format>json</alert_format>
39 | <level>7</level>
40 </integration>
41
```

Check if VirusTotal has been integrated to wazuh

The screenshot shows the Wazuh web interface with the following navigation steps highlighted by red boxes and arrows:

- 1**: The **Management** tab in the top navigation bar.
- 2**: The **Management** menu item in the left sidebar.
- 3**: The **Configuration** menu item under the **Administration** sub-menu.
- 4**: The **Integrations** section in the main content area, specifically the link for **Slack, VirusTotal and PagerDuty integrations with external APIs**.

The browser address bar shows the URL: `https://192.168.149.130/app/wazuh#/manager/?tab=configuration`. The page title is "wazuh." and the current view is "Configuration".

VirusTotal has been integrated, We can now download/ run test malicious file

The screenshot shows the Wazuh web interface. The browser address bar displays a 'Not secure' warning and the URL `https://192.168.149.130/app/wazuh#/manager/?tab=configuration`. The navigation bar includes the Wazuh logo and tabs for 'Management' and 'Configuration'. The main content area is titled 'Integrations' and contains two sections: 'VirusTotal' and 'Slack'. The 'VirusTotal' section is active and shows three configuration fields: 'Filter alerts by this level or above' set to '0', 'Filter alerts by these rule groupst' set to 'syscheck', and 'Used format to write alerts' set to 'json'. The 'Slack' section is partially visible below, showing a 'Hook URL' field with the value `https://hooks.slack.com/services/T09QR7Z4HT8/B09QCI`, and 'Filter alerts by this level or above' set to '7' and 'Used format to write alerts' set to 'json'. A large 'LOUIS.O.A' watermark is overlaid on the page.

← ↻ Not secure `https://192.168.149.130/app/wazuh#/manager/?tab=configuration` 🔍 ☆

☰ 🏠 wazuh. ▾ Management Configuration

Integrations

Slack, VirusTotal and PagerDuty integrations with external APIs

VirusTotal

Get notified when malicious software is found

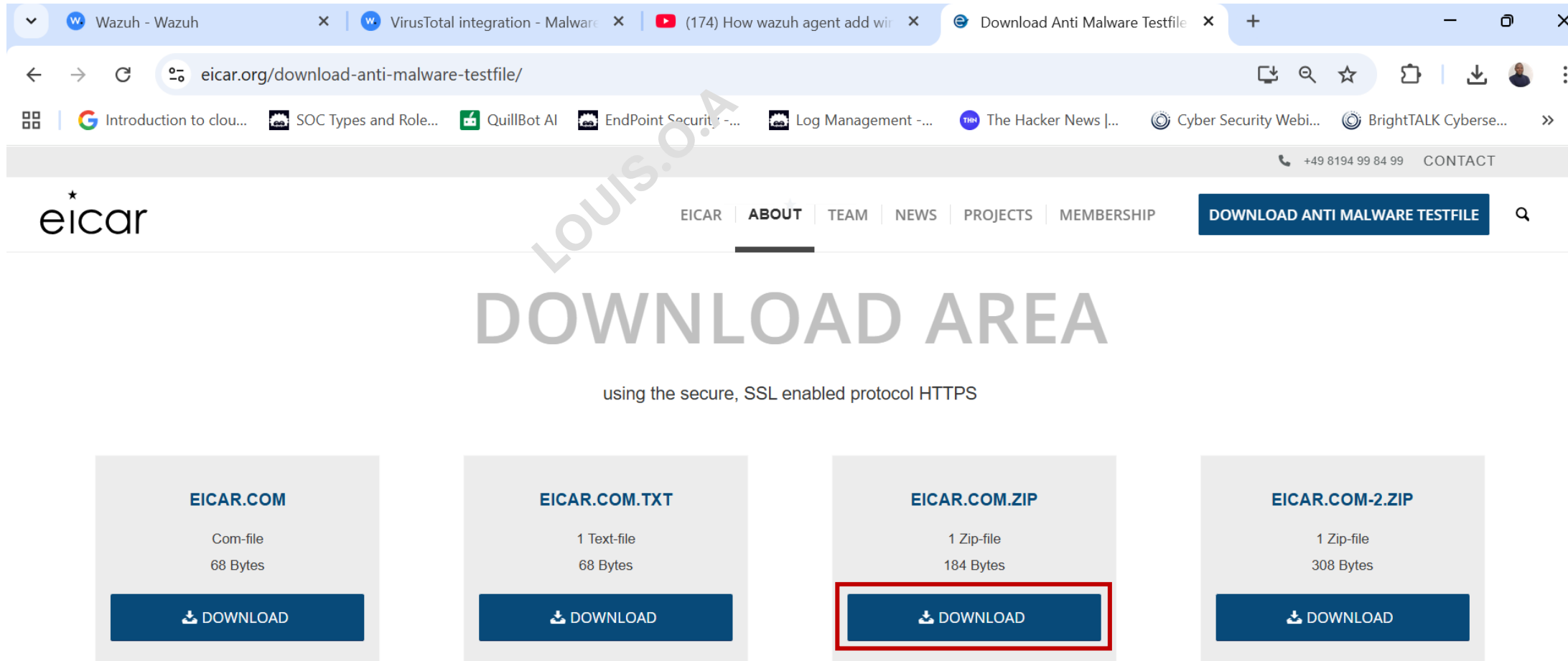
Filter alerts by this level or above	<input type="text" value="0"/>
Filter alerts by these rule groupst	<input type="text" value="syscheck"/>
Used format to write alerts	<input type="text" value="json"/>

Slack

Get alerts directly on Slack

Hook URL	<input type="text" value="https://hooks.slack.com/services/T09QR7Z4HT8/B09QCI"/>
Filter alerts by this level or above	<input type="text" value="7"/>
Used format to write alerts	<input type="text" value="json"/>

Visit <https://eicar.org/download-anti-malware-testfile/> to download and run a malicious file to see VirusTotal in action.



The screenshot shows a web browser window with the URL eicar.org/download-anti-malware-testfile/. The page features a navigation menu with links for EICAR, ABOUT, TEAM, NEWS, PROJECTS, and MEMBERSHIP. A prominent blue button labeled "DOWNLOAD ANTI MALWARE TESTFILE" is visible. The main content area is titled "DOWNLOAD AREA" and includes the text "using the secure, SSL enabled protocol HTTPS". Below this, there are four download options, each with a "DOWNLOAD" button:

File Name	Description	Size
EICAR.COM	Com-file	68 Bytes
EICAR.COM.TXT	1 Text-file	68 Bytes
EICAR.COM.ZIP	1 Zip-file	184 Bytes
EICAR.COM-2.ZIP	1 Zip-file	308 Bytes

The "EICAR.COM.ZIP" option is highlighted with a red rectangular border.



The terminal window displays system logs, including the following entries:

```
-fzero-link -gen-decls  
-Wassign-Intercept -Wno-protocol  
-Wselector  
-Wstrict-selector-match  
-Wundeclared-selector  
2017: apport: report /var/crash/_usr_bin_cma  
trix.1000.crash already exists and unseen, do  
ing nothing to avoid disk usage DoS  
ERROR: apport (pid 18485) Thu Mar 16 11:44:59  
2017: called for pid 18484, signal 8, core 1
```

A large white download icon is centered over the terminal output.

Total agents

2

Active agents

1

Disconnected agents

1

Pending agents

0

Never connected agents

0

SECURITY INFORMATION MANAGEMENT



Security events

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



Integrity monitoring

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

AUDITING AND POLICY MONITORING



Policy monitoring

Verify that your systems are configured according to your security policies baseline.



System auditing

Audit users behavior, monitoring command execution and alerting on access to critical files.



Security configuration assessment

Scan your assets as part of a configuration assessment audit.

THREAT DETECTION AND RESPONSE



Vulnerabilities

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



VirusTotal

Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.

REGULATORY COMPLIANCE



PCI DSS

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

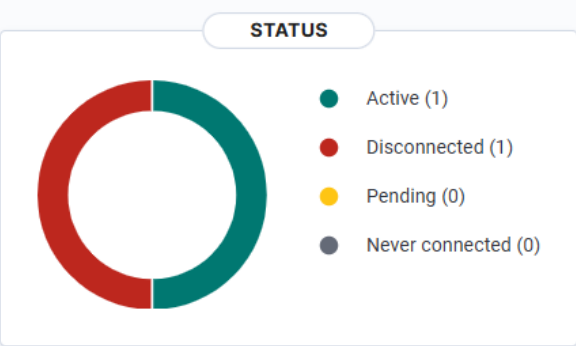


NIST 800-53

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



MITRE ATT&CK

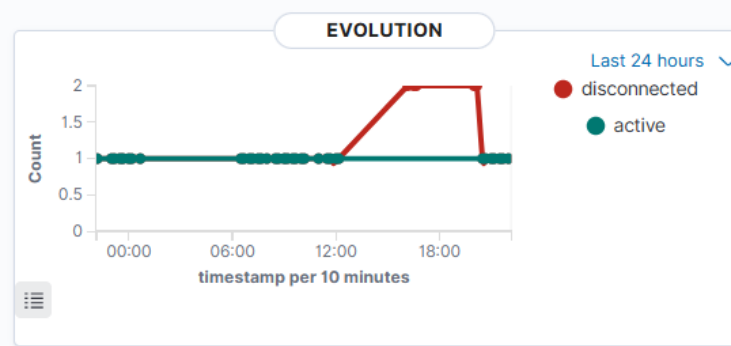


DETAILS

Active	Disconnected	Pending	Never connected	Agents coverage
1	1	0	0	50.00%

Last registered agent: **virtualMachine**

Most active agent: **Louis-Machine**



Agents (1)

id!=000 and status=active

Deploy new agent Refresh Export formatted Refresh

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	Louis-Machine	192.168.149.1	default	Microsoft Windows 11 Pro 10.0.26200.7019	node01	v4.7.0	active ?	👁️ 🔍

Rows per page: 10

☰ 🏠 **wazuh.** ▼ Agents Louis-Machine

Security events
Integrity monitoring
SCA
Vulnerabilities
MITRE ATT&CK
More... ▼

ID	Status	IP address	Version	Groups	Operati
001	● active ⓘ	192.168.149.1	Wazuh v4.7.0	default	🖱 Mic

MITRE

Top Tactics

- Persistence: 499
- Defense Evasion: 496
- Initial Access: 483
- Privilege Escalation: 483
- Impact: 47

Compliance

PCI DSS

- 0.2.5 (531)
- 0.6.1 (120)
- 5.1 (80)
- 5.2 (63)
- 11.4 (53)

FIM: Recen

Time ↓

- Nov 7, 2025 @ 21:56:04.882
- Nov 7, 2025 @ 21:55:56.088
- Nov 7, 2025 @ 06:33:10.915

Events count evolution

SCA: Lastes

CIS Microsoft

Policy

CIS Micros Benchmark

☰ 🏠 **wazuh.** ▼ Modules Louis-Machine Security events ⓘ

Dashboard Events

🔍 Search

manager.name: wazuh-server
agent.id: 001
+ Add filter

Total **835**
Level 12 or above alerts **29**
Authenticat **4**

Alert groups evolution

Alerts

Top 5 alerts

Top 5 rule groups

Search DQL Last 24 hours Show dates Refresh

manager.name: wazuh-server agent.id: 001 + Add filter

wazuh-alerts-*

Search field names

Filter by type 0

Selected fields

- rule.description
data.win.eventdata.action ID
data.win.eventdata.action Name
data.win.eventdata.additional Actions ID
data.win.eventdata.additional Actions String
data.win.eventdata.address
data.win.eventdata.addressLength
data.win.eventdata.appName
data.win.eventdata.appPath
data.win.eventdata.appTimeStamp
data.win.eventdata.appVersion
data.win.eventdata.attachedFiles
data.win.eventdata.authenticationPackageName
data.win.eventdata.binary
data.win.eventdata.bucket
data.win.eventdata.bucketId
data.win.eventdata.bucketType
data.win.eventdata.cabGuid

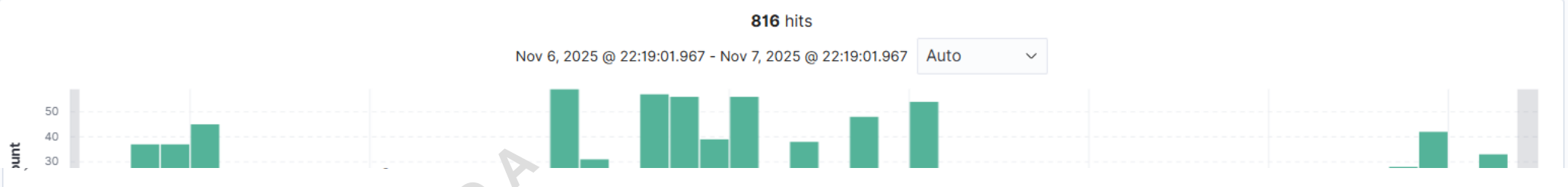


Table with 6 columns: expand icon, timestamp, message, count, and ID. The row for 'VirusTotal: Alert - c:\users\louis\desktop\wazuh file testing\new text document.txt - No positives found' is highlighted with a red box.

- data.win.eventdata.address
- data.win.eventdata.addressLength
- data.win.eventdata.appName
- data.win.eventdata.appPath
- data.win.eventdata.appTimeStamp
- data.win.eventdata.appVersion
- data.win.eventdata.attachedFiles
- data.win.eventdata.authenticationPackageName
- data.win.eventdata.binary
- data.win.eventdata.bucket
- data.win.eventdata.bucketId
- data.win.eventdata.bucketType
- data.win.eventdata.cabGuid
- data.win.eventdata.cabId
- data.win.eventdata.category ID
- data.win.eventdata.category Name
- data.win.eventdata.clientPID
- data.win.eventdata.clientProcessId
- data.win.eventdata.cloud protection intelligence Compilation Timestamp
- data.win.eventdata.cloud protection intelligence Type
- data.win.eventdata.cloud protection intelligence Type Index
- data.win.eventdata.cloud protection intelligence Version
- data.win.eventdata.

Nov 7, 2025 @ 21:56:07.823 VirusTotal: Alert - c:\users\louis\desktop\wazuh file testing\new text document.txt - No positives found 3 87104

Expanded document [View surrounding documents](#) [View single document](#)

Table JSON

🔍 🔍 📄 📄	🔑	_index	wazuh-alerts-4.x-2025.11.07
	🔑	agent.id	001
	🔑	agent.ip	192.168.149.1
	🔑	agent.name	Louis-Machine
	🔑	data.aws.accountId	
	🔑	data.aws.region	
	🔑	data.integration	virustotal
	🔑	data.virustotal.found	1
	🔑	data.virustotal.malicious	0
	🔑	data.virustotal.permalink	>
			https://www.virustotal.com/gui/file/e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855/detection/f-e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855-1762548722
	🔑	data.virustotal.positives	0
	🔑	data.virustotal.scan_date	2025-11-07 20:52:02
	🔑	data.virustotal.sha1	da39a3ee5e6b4b0d3255bfef95601890afd80709



Search: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Louis OKPERIRUISI



Community Score 1790

File distributed by Linux, Offensive Security and others.

Reanalyze
 Similar
 More

e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Size: 0 B
 Last Analysis Date: 3 minutes ago

android-cts-7.1_r6-linux_x86-arm.zip

- nsrl
- via-tor
- direct-cpu-clock-access
- legit
- known-distributor
- trusted
- zero-filled
- software-collection
- runtime-modules
- attachment

This report corresponds to an **empty file**, it can't exhibit malicious behavior by itself. [Learn more.](#)

[DETECTION](#)
[DETAILS](#)
[COMMUNITY](#) 30+

Crowdsourced Sigma Rules ⓘ

CRITICAL 0 HIGH 0 **MEDIUM 1** LOW 0

Matches rule **Suspicious History File Operations** by Mikhail Larin, oscd.community at Sigma Integrated Rule Set (GitHub)
 ↳ *Detects commandline operations on shell history files*

Crowdsourced IDS rules ⓘ



Slack also got the alert notification of the flagged malicious activity

The screenshot displays the Slack interface. On the left, the sidebar shows the 'Direct messages' section with a search bar and a list of DMs. The active DM is with 'louis (you)', showing a message from 'Alert_security' with the text 'Alert_security: Logon failure - Unknown user or bad password.' and a timestamp of '3 mins' with '9+' reactions.

The main content area shows a direct message from 'louis' with the following details:

- Message ID: 62123 (Level 12)
- Time: Today at 8:47 PM
- Notification: 34 new messages
- Alert Content:
 - 8:47 WAZUH Alert
 - Windows Defender: Antimalware platform detected potentially unwanted software ()
 - Agent (001) - Louis-Machine
 - Location EventChannel
 - Rule ID 62123 (Level 12)
 - Today at 8:47 PM
- Alert_security APP 8:56 PM
- WAZUH Alert
- Logon failure - Unknown user or bad password.
- Agent (001) - Louis-Machine

The bottom of the interface shows a rich text editor with a toolbar containing icons for bold (B), italic (I), underline (U), strikethrough (ABC), link, list, table, code, and insert. The text input field contains 'Jot something down' and the bottom bar includes a plus sign, font size (Aa), emojis, mentions (@), attachments, and a send button.

Another Alert.....

Not secure https://192.168.149.130/app/discover#/?_g=(filters:!(),query:(language:kuery,query:""),refreshInterval:(pause:!t,value:0),time:(from...

Discover

Nov 6, 2025 @ 15:59:58.638

data.virustotal.permalink: https://www.virustotal.com/gui/file/509790d92c2c8846bf4ffacfb03c4f8817ac548262c70c13b08ef5cdfba6f596/detection data.virustotal.scan_date: 2025-11-06T14:55:58.638Z @sampledata: true rule.mail: false rule.level: 9 rule.description: VirusTotal: Alert - /tmp/virus/notavirus - 17 engines detected this file

cluster.name: wazuh agent.ip: 47.204.15.21 agent.name: Ubuntu agent.id: 004 manager.name: wazuh-server data.virustotal.malicious: 0 data.virustotal.total: 017

data.virustotal.found: 1 data.virustotal.positives: 17 data.virustotal.source.sha1: 4bed69e46ba1c56da72b9700631f48d46c4face3 data.virustotal.source.file: /tmp/virus/notavirus

data.virustotal.source.alert_id: 2184926007.4694507 data.virustotal.source.md5: 30de8bcea838e7d82026e91b6e26c388

data.virustotal.permalink: https://www.virustotal.com/gui/file/509790d92c2c8846bf4ffacfb03c4f8817ac548262c70c13b08ef5cdfba6f596/detection data.virustotal.scan_date: 2025-11-06T14:55:58.638Z @sampledata: true rule.mail: false rule.level: 9 rule.description: VirusTotal: Alert - /tmp/virus/notavirus - 17 engines detected this file

Expanded document

View surrounding documents View single document

Table JSON

@sampledata	true
_index	wazuh-alerts-4.x-sample-threat-detection
agent.id	004
agent.ip	47.204.15.21
agent.name	Ubuntu
cluster.name	wazuh
data.virustotal.found	1
data.virustotal.malicious	0
data.virustotal.permalink	https://www.virustotal.com/gui/file/509790d92c2c8846bf4ffacfb03c4f8817ac548262c70c13b08ef5cdfba6f596/detection
data.virustotal.positives	17
data.virustotal.scan_date	2025-11-06T14:55:58.638Z
data.virustotal.source.alert_id	2184926007.4694507
data.virustotal.source.file	/tmp/virus/notavirus
data.virustotal.source.md5	30de8bcea838e7d82026e91b6e26c388
data.virustotal.source.sha1	4bed69e46ba1c56da72b9700631f48d46c4face3

Snipping Tool

509790d92c2c8846bf4ffacfb03c4f8817ac548262c70c13b08ef5cdfba6f596

Sign in Sign up



Community Score -42

67/72 security vendors flagged this file as malicious

Reanalyze Similar More

509790d92c2c8846bf4ffacfb03c4f8817ac548262c70c13b08ef5cdfba6f596

Size 3.12 MB

Last Analysis Date 5 months ago



AutoRun.exe

- peexe
- persistence
- checks-user-input
- spreader
- detect-debug-environment
- aspack
- overlay
- checks-usb-bus

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Join our Community and enjoy additional community insights and crowd-sourced detections, plus an API key to automate checks.

Popular threat label trojan.stone/lamer

Threat categories trojan virus worm

Family labels stone lamer stihat

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Win32/Lamer.F.X2070	Alibaba	Virus:Win32/InfectPE.ali2000007
AliCloud	Trojan:Win/Delf	ALYac	Application.Stone.A
Antiy-AVL	Virus/Win32.Lamer.cb	Arcabit	Application.Stone.A
Arctic Wolf	Unsafe	Avast	Win32:Stihat [Wrm]
AVG	Win32:Stihat [Wrm]	Avira (no cloud)	BDS/Backdoor.Gen2
Baidu	Win32.Virus.Lamer.e	BitDefender	Application.Stone.A



THANK YOU!

LOUIS.O.A