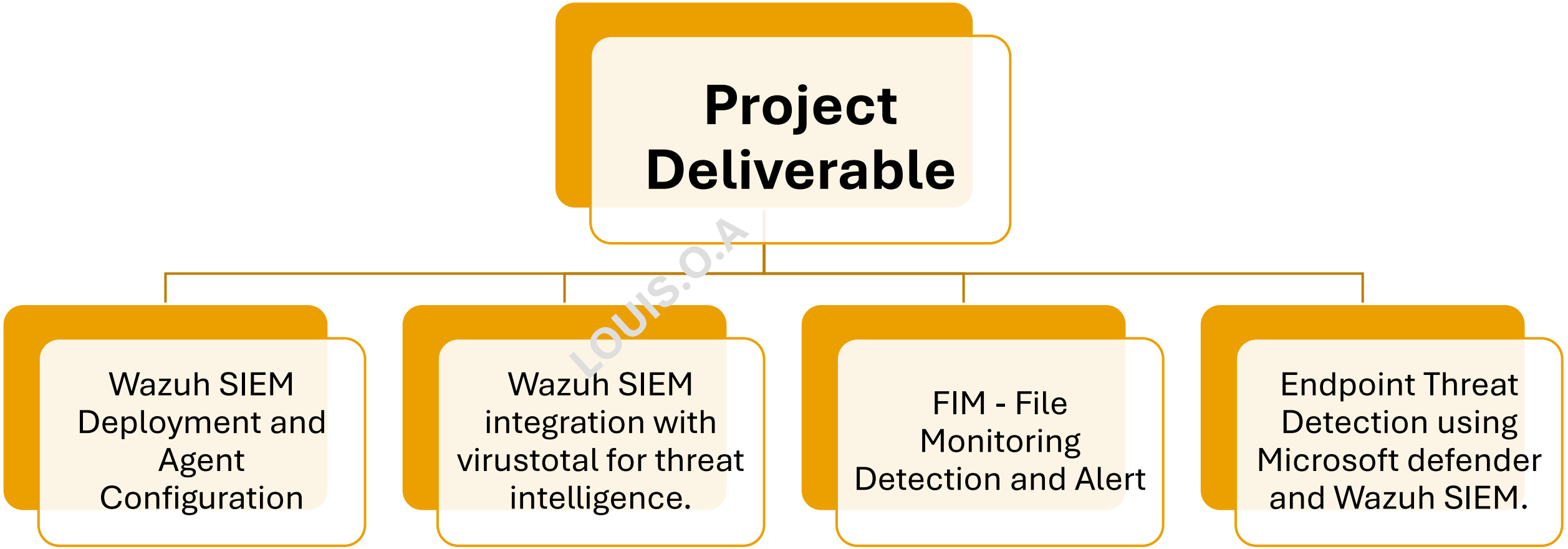
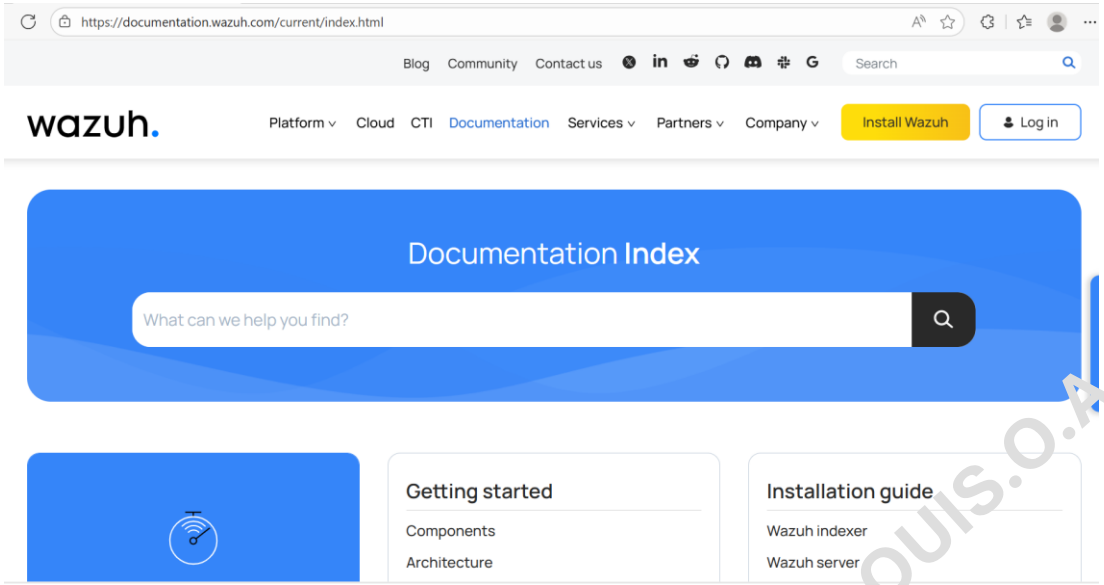
Deployment and Configuration of Security Information & Event Management (SIEM) solution for SMEs using **WAZUH** SIEM.

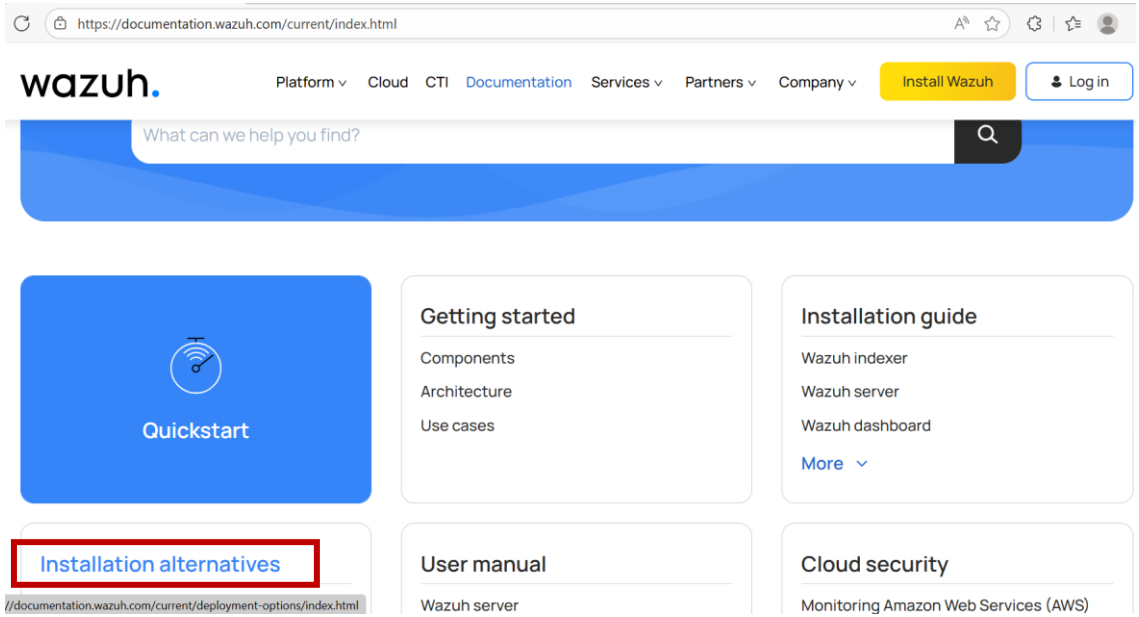
Presented By Okperiruisi Louis

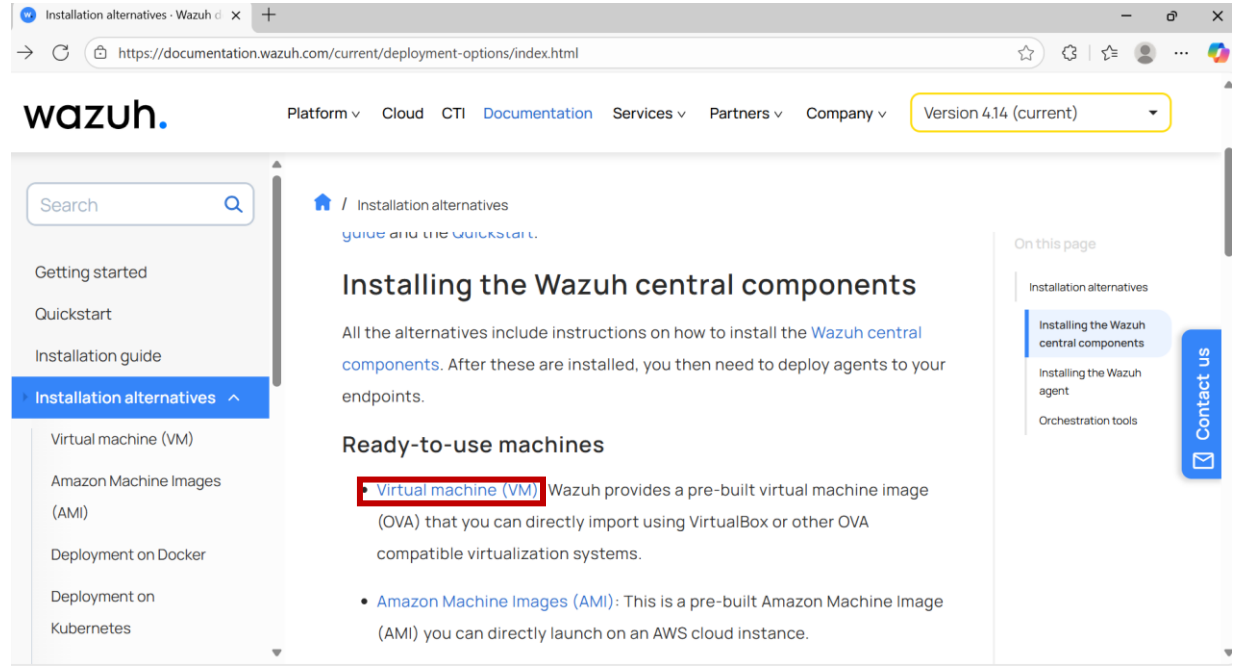
1st November 2025


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







Search

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

/ Installation alternatives / Virtual machine (VM)

Virtual machine (VM)

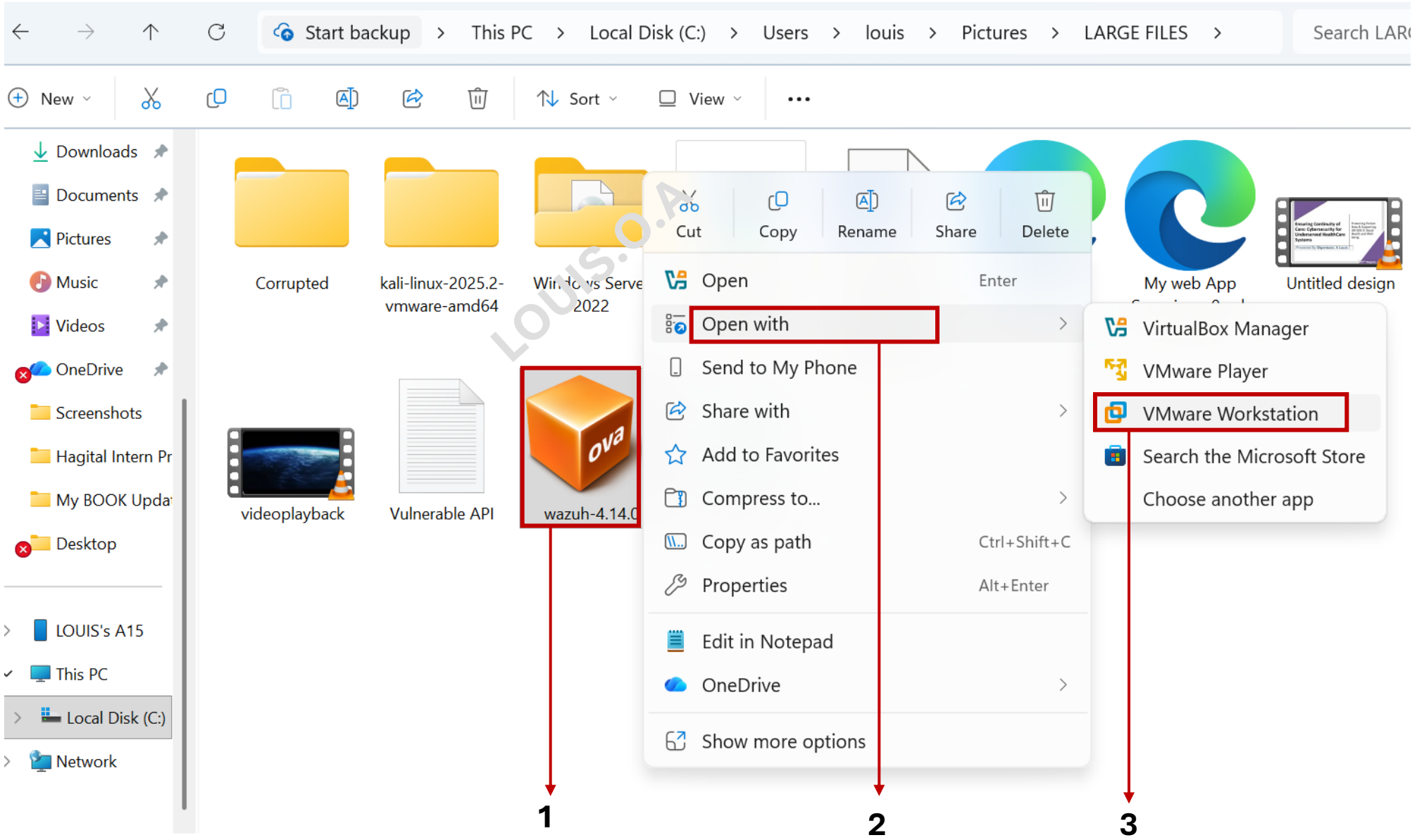
Wazuh provides a pre-built virtual machine image in Open Virtual Appliance (OVA) format. It includes the Amazon Linux 2023 operating system and the Wazuh central components.

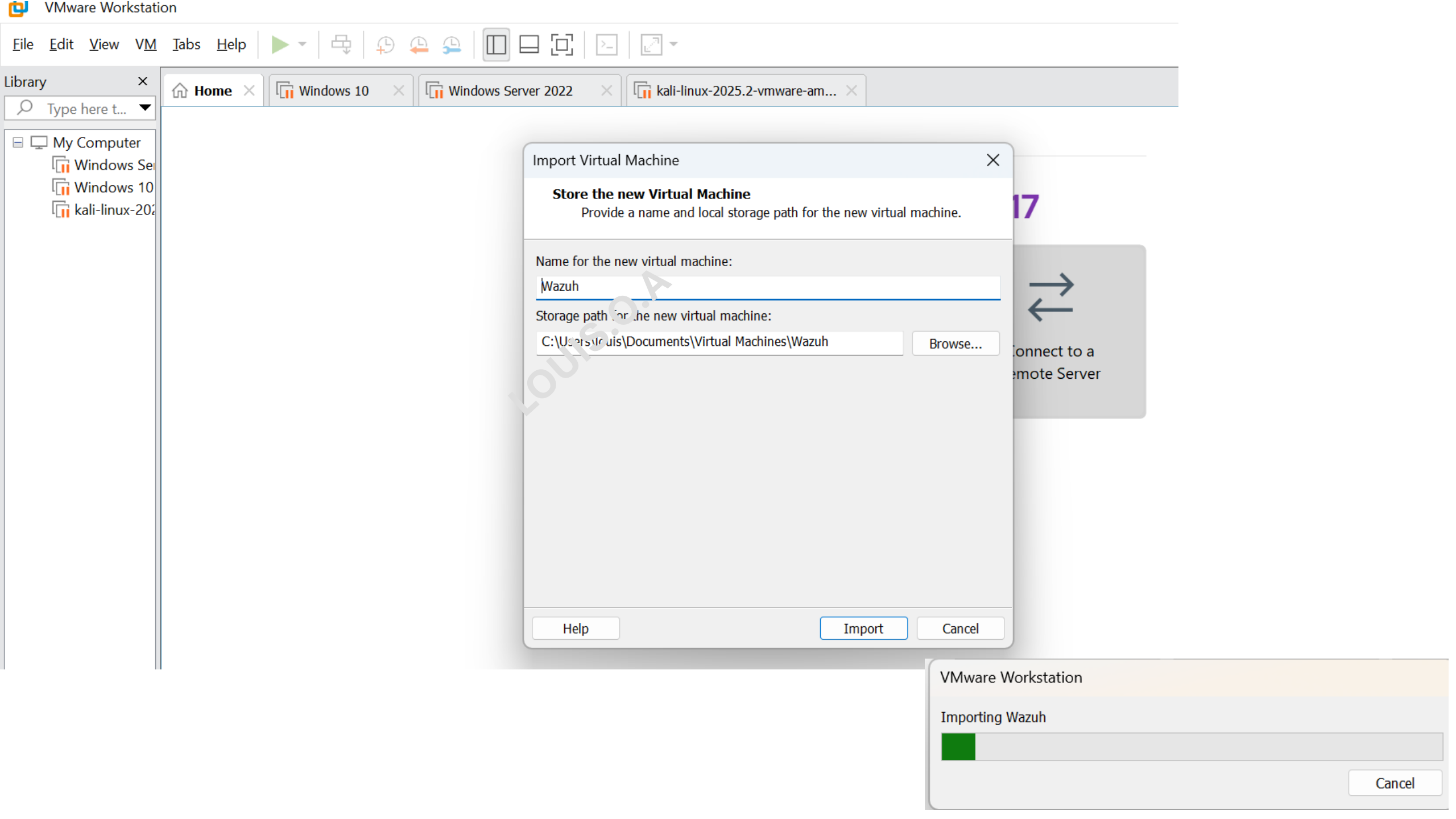
- Wazuh manager 4.14.0
- Filebeat-OSS 7.10.2
- Wazuh indexer 4.14.0
- Wazuh dashboard 4.14.0

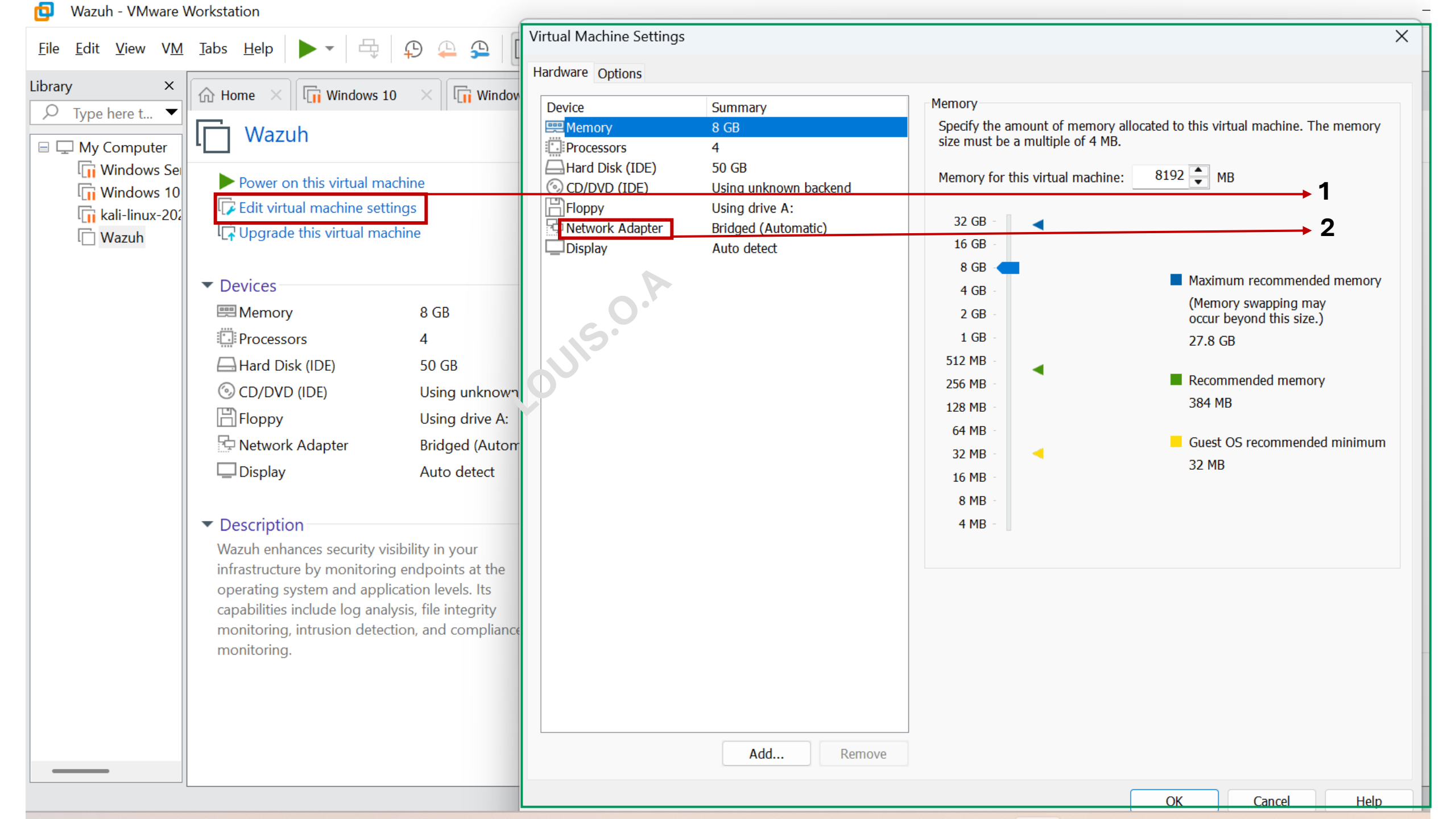
You can import the Wazuh virtual machine image to VirtualBox or other OVA-compatible virtualization systems. This VM runs only on 64-bit systems with x86_64/AMD64 architecture. It does not provide high availability or scalability out of the box. However, you can implement these using distributed deployment.

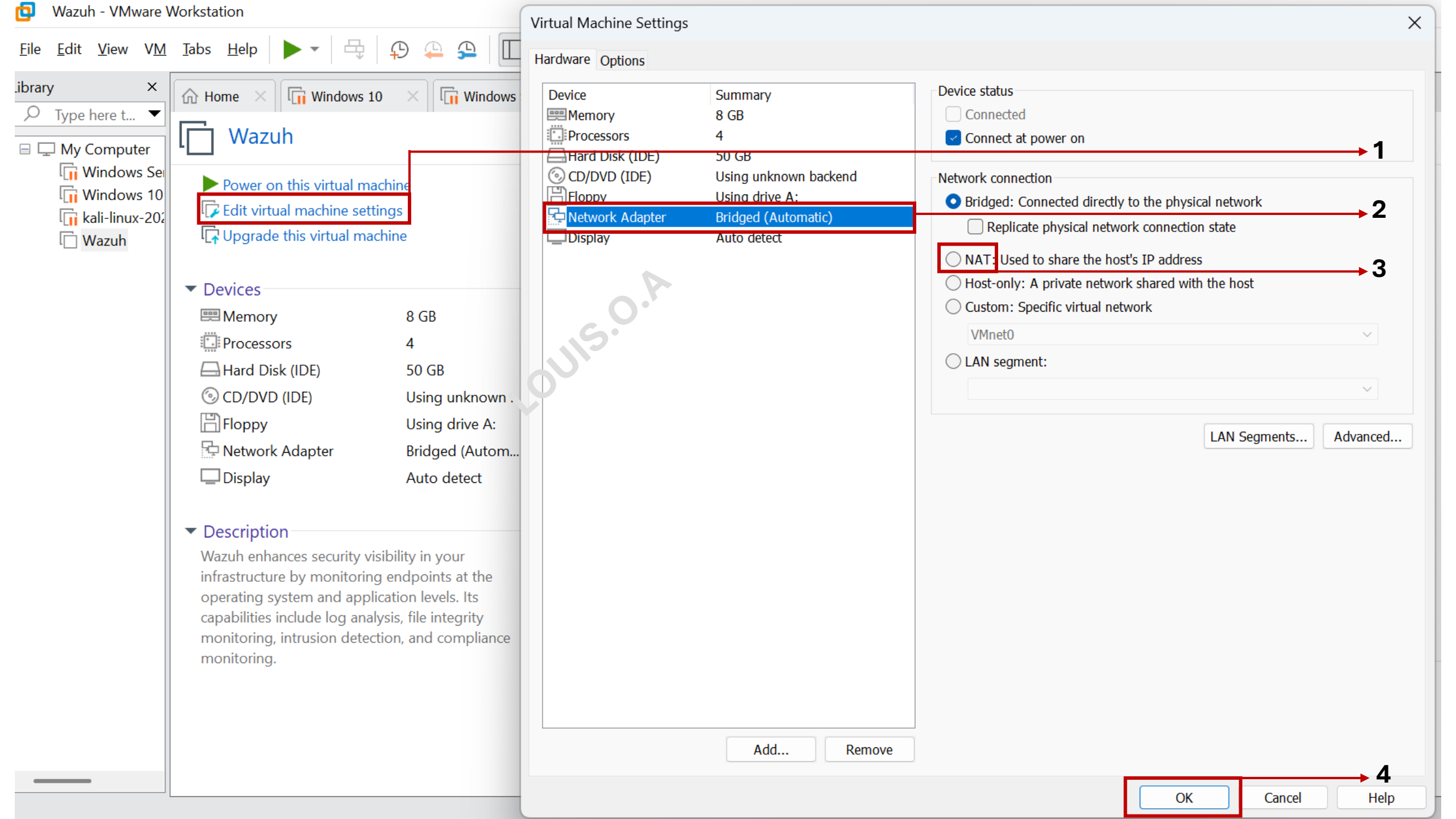
Download the virtual appliance (OVA).

Right click on the wazuh OVA file for installation




VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Windows Se
Windows 10
kali-linux-202
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
Connect to a
emote Server
VMware Workstation
Importing Wazuh
Cancel


Wazuh - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Windows Se
Windows 10
kali-linux-20
Wazuh
Home
Windows 10
Windov
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 unknow
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
Add... Remove
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: 8192 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
1
2
OK Cancel Help


Wazuh - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Windows Se
Windows 10
kali-linux-202
Wazuh
Home
Windows 10
Windows
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
Add... Remove
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...
4
OK Cancel Help
LOUIS.O.A

Wazuh - VMware Workstation

File Edit View VM Tabs Help

Library

Type here t...

My Computer
- Windows Se
- Windows 10
- kali-linux-202
- 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

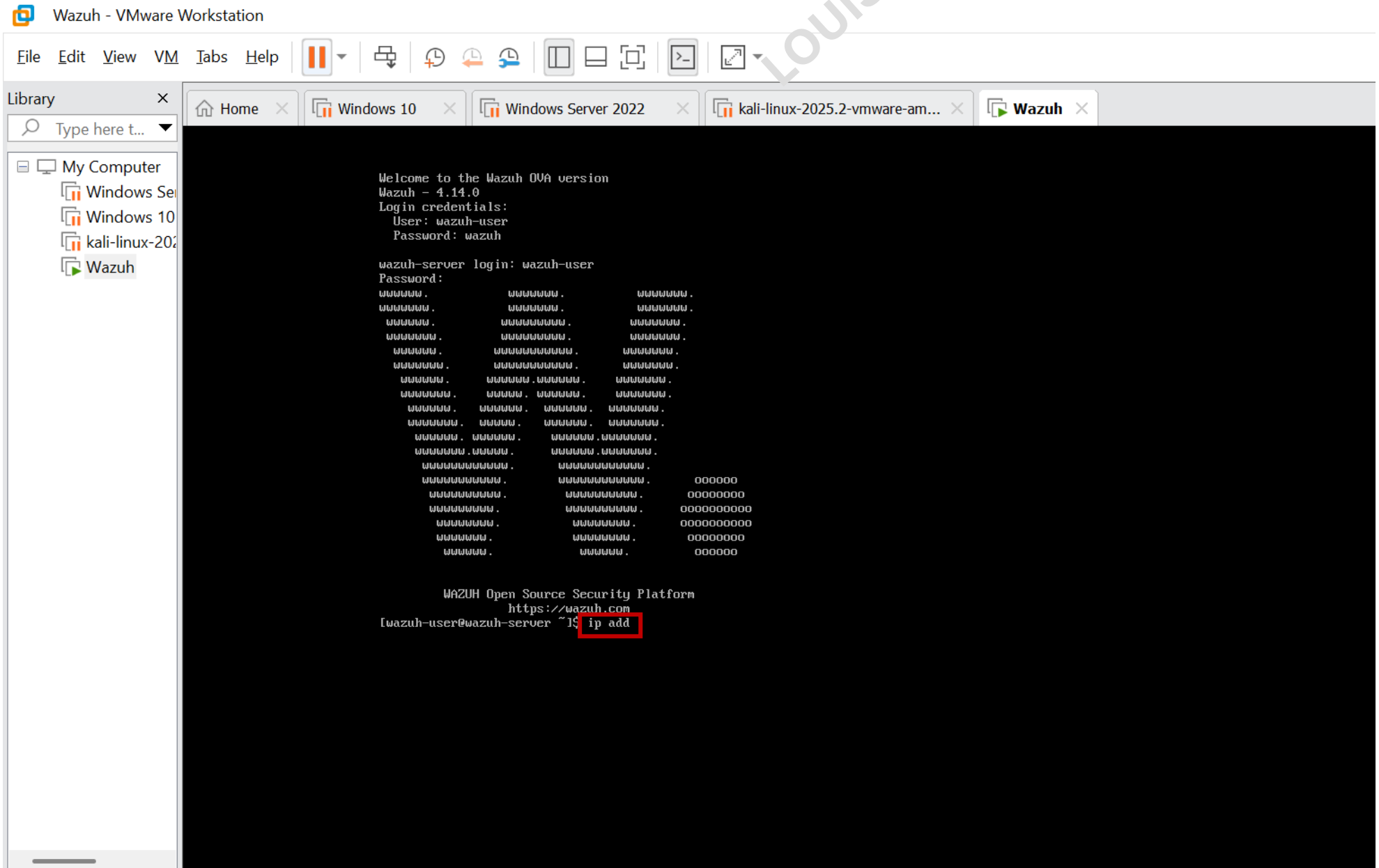
Description

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.

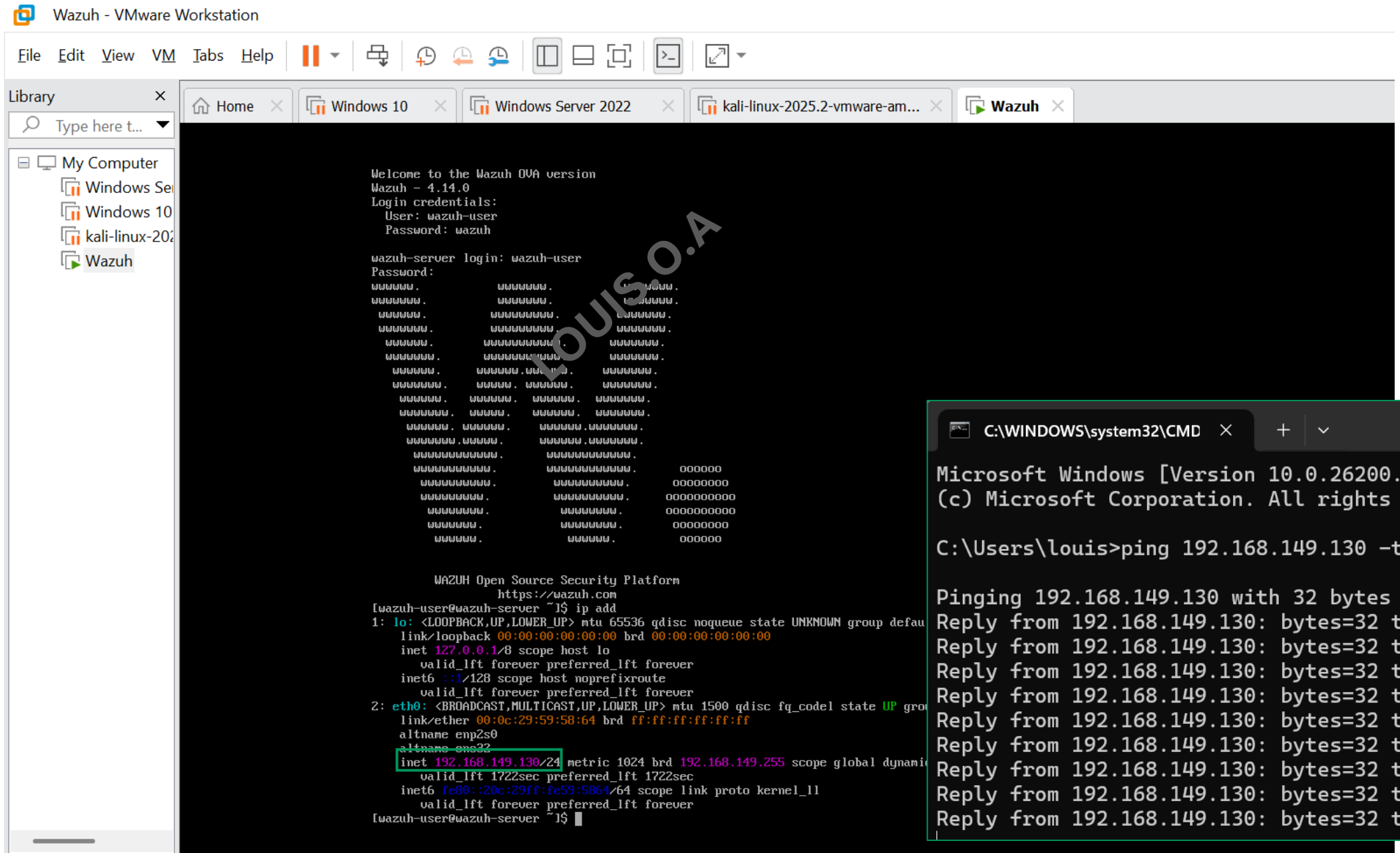
Virtual Machine Details

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

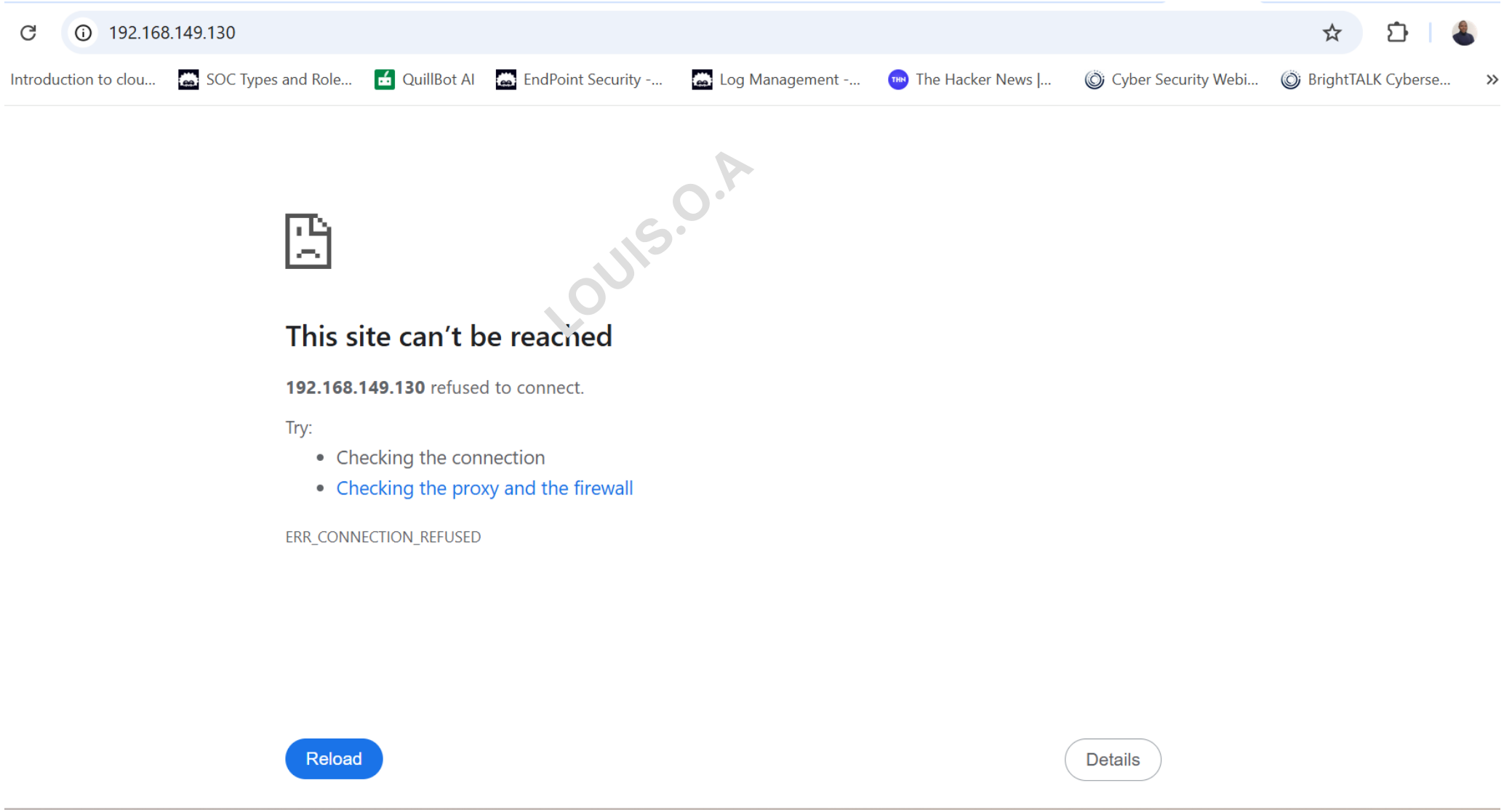
Type “ip add” and click enter, to check the ip address of the VMware.



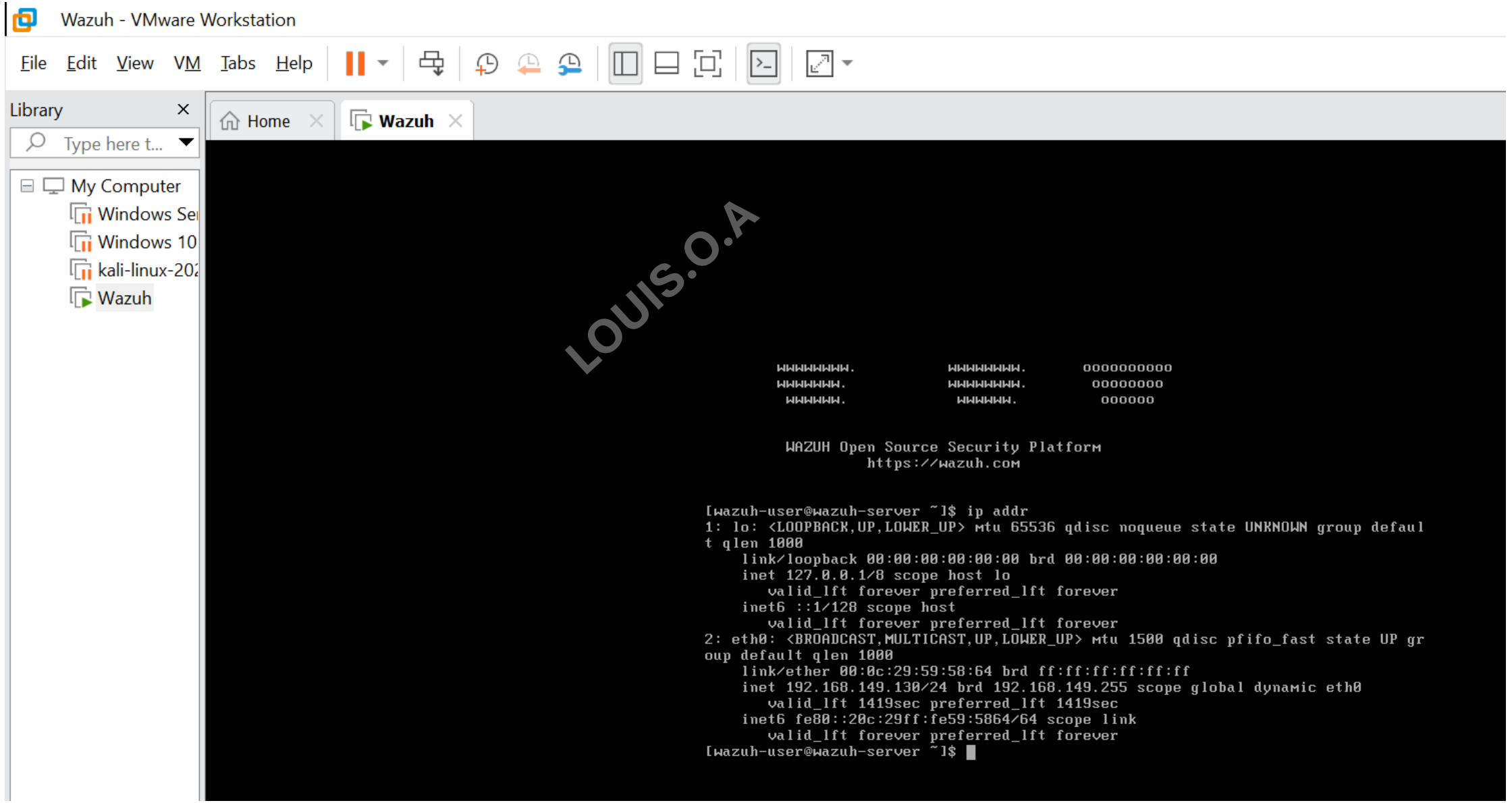
This is the ip address (192.168.149.130) of the Vmware. Go to your host PC & ping the ip to confirm its pinging. Enter the ip address on your host PC browser to open wazuh dashboard



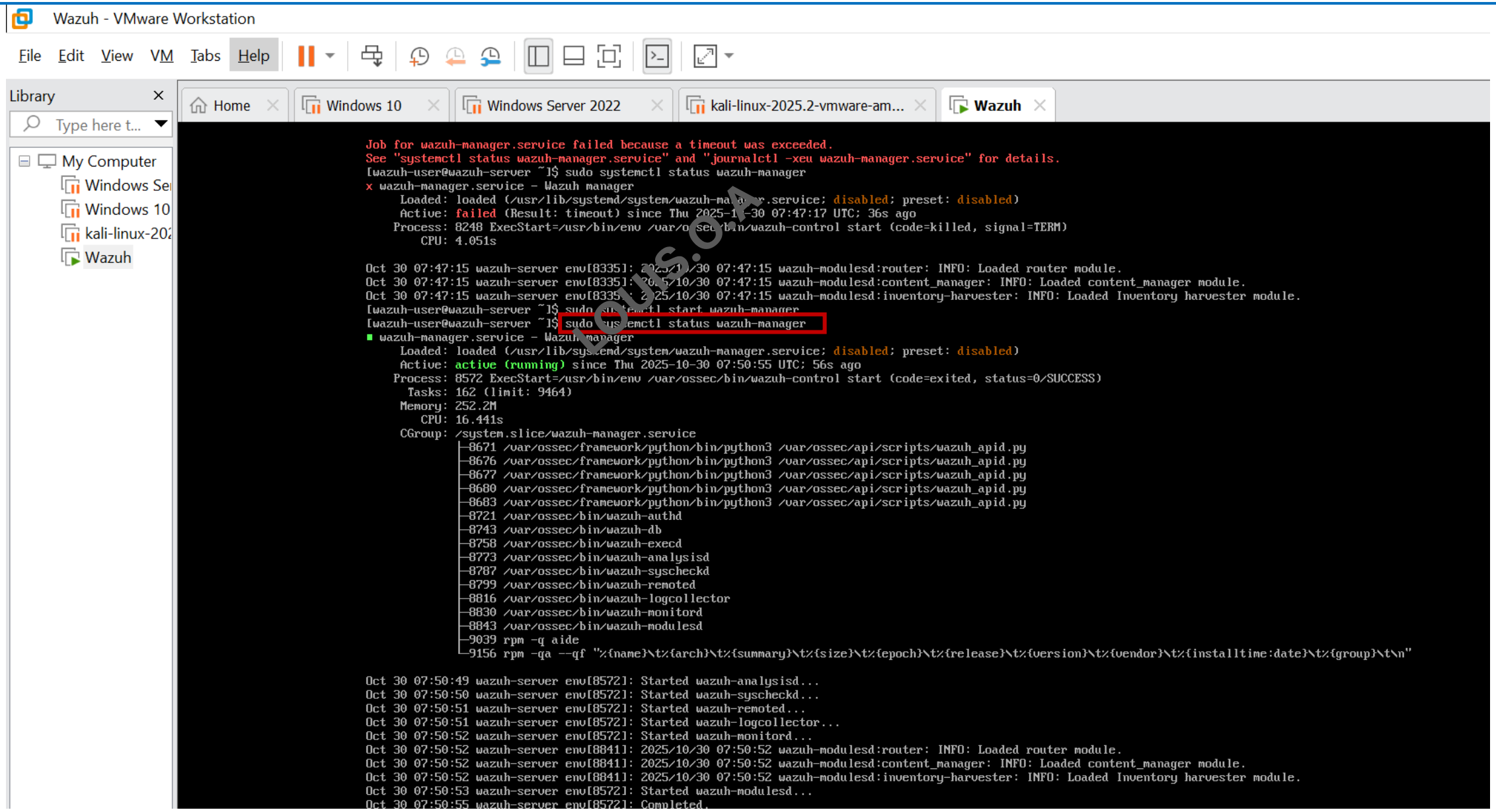
If you cannot access the wazuh dashboard using the ip address, kindly manually start wazuh dashboard server, wazuh manager, and wazuh indexer.



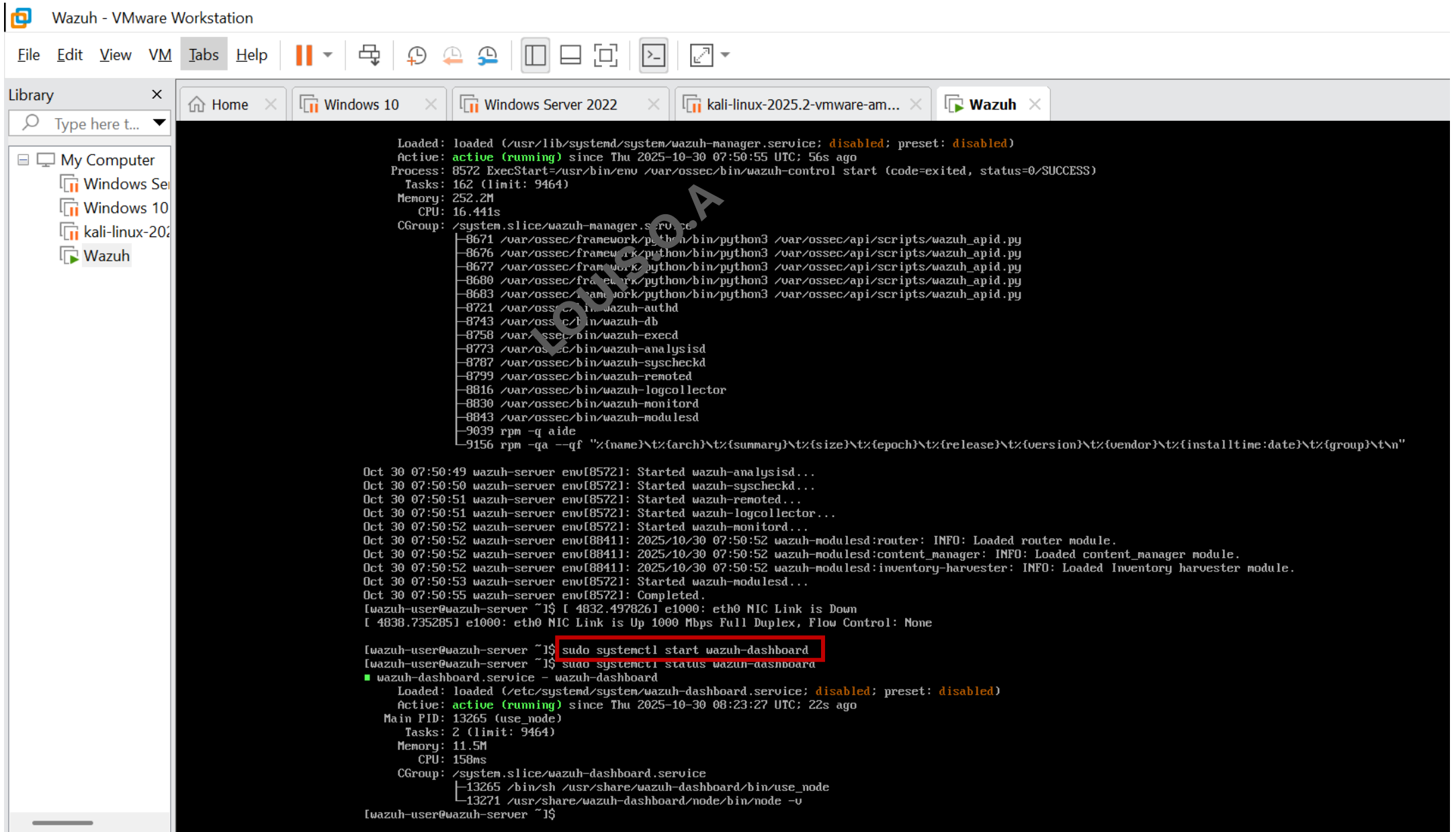
Firstly, let us start wazuh manager by typing-in “sudo systemctl start wazuh-manager”



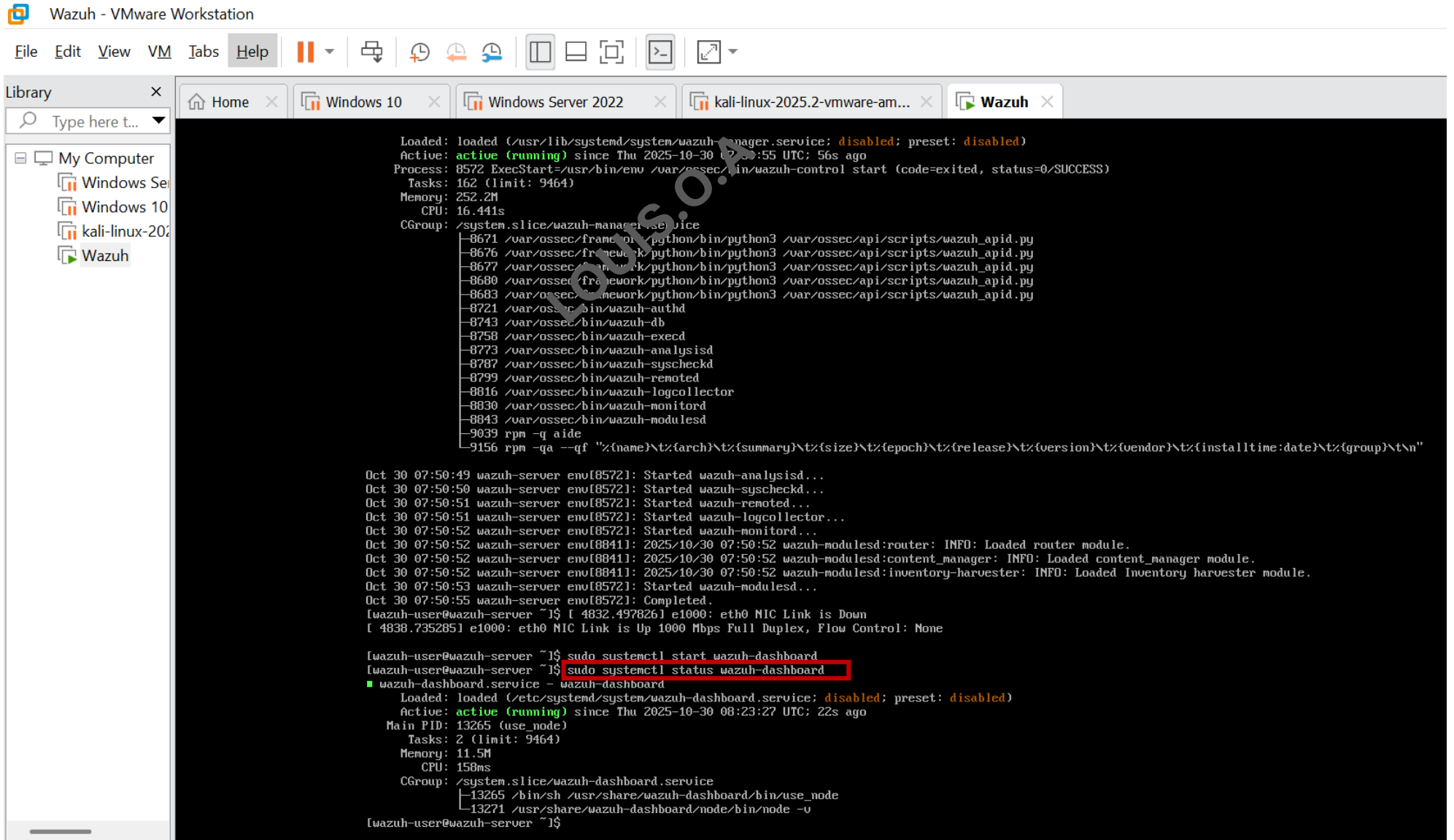
To check if the wazuh manager has started type this command "sudo systemctl status wazuh-manager" and hit enter key. Once you see these write up, it shows the wazuh is running now.



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.



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.

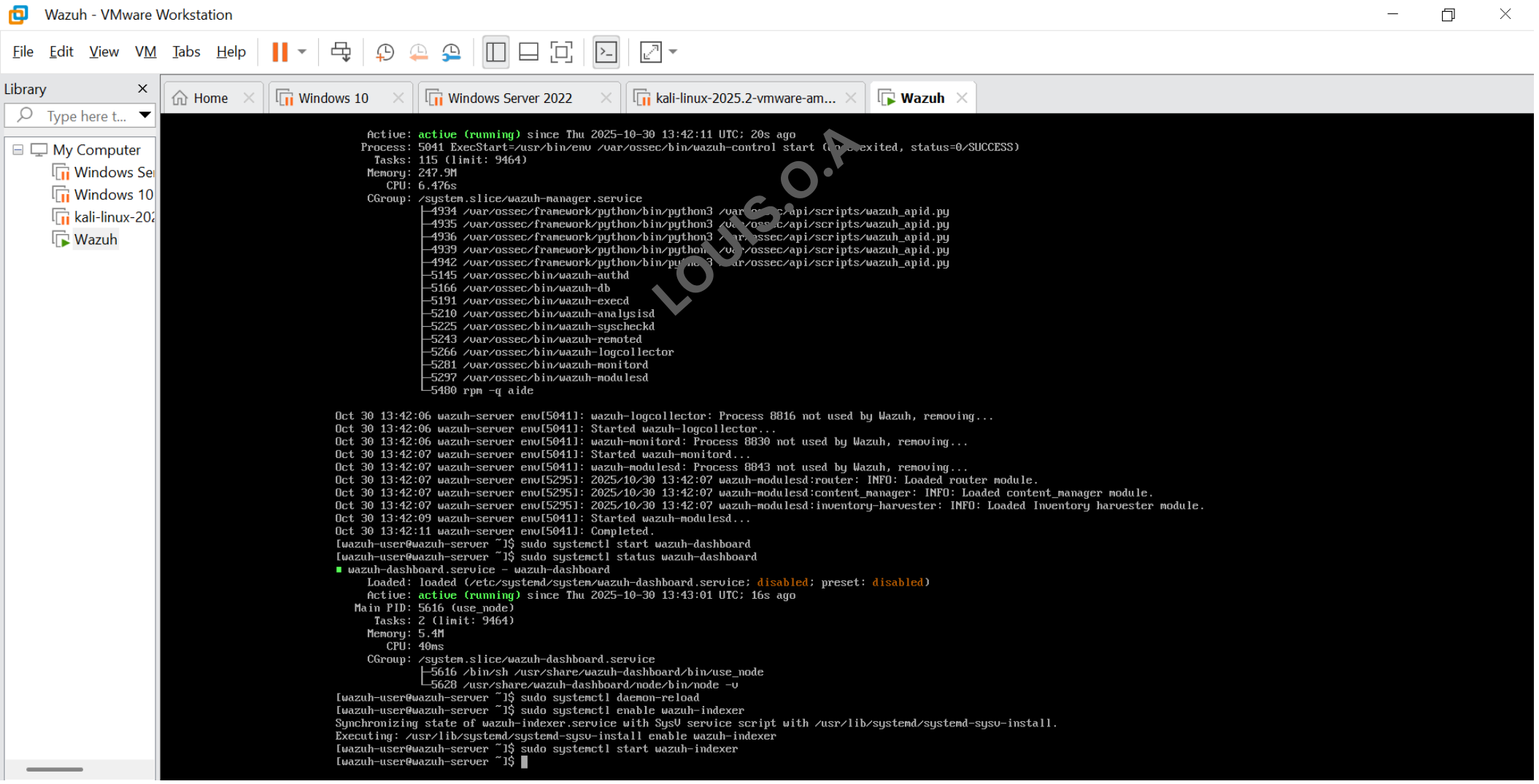


To start the indexer, firstly, enter

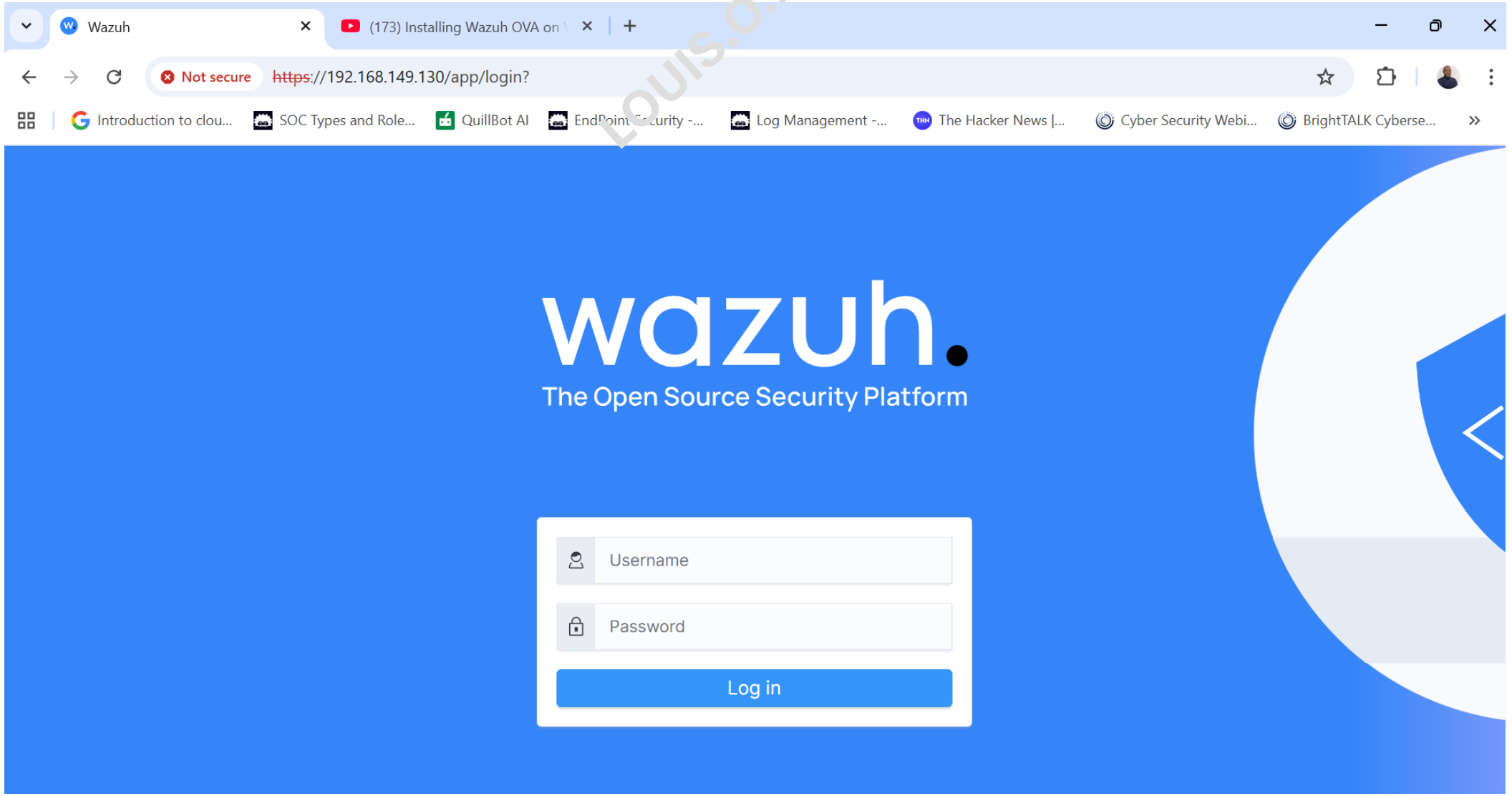
"sudo systemctl daemon-reload"

"sudo systemctl enable wazuh-indexer"

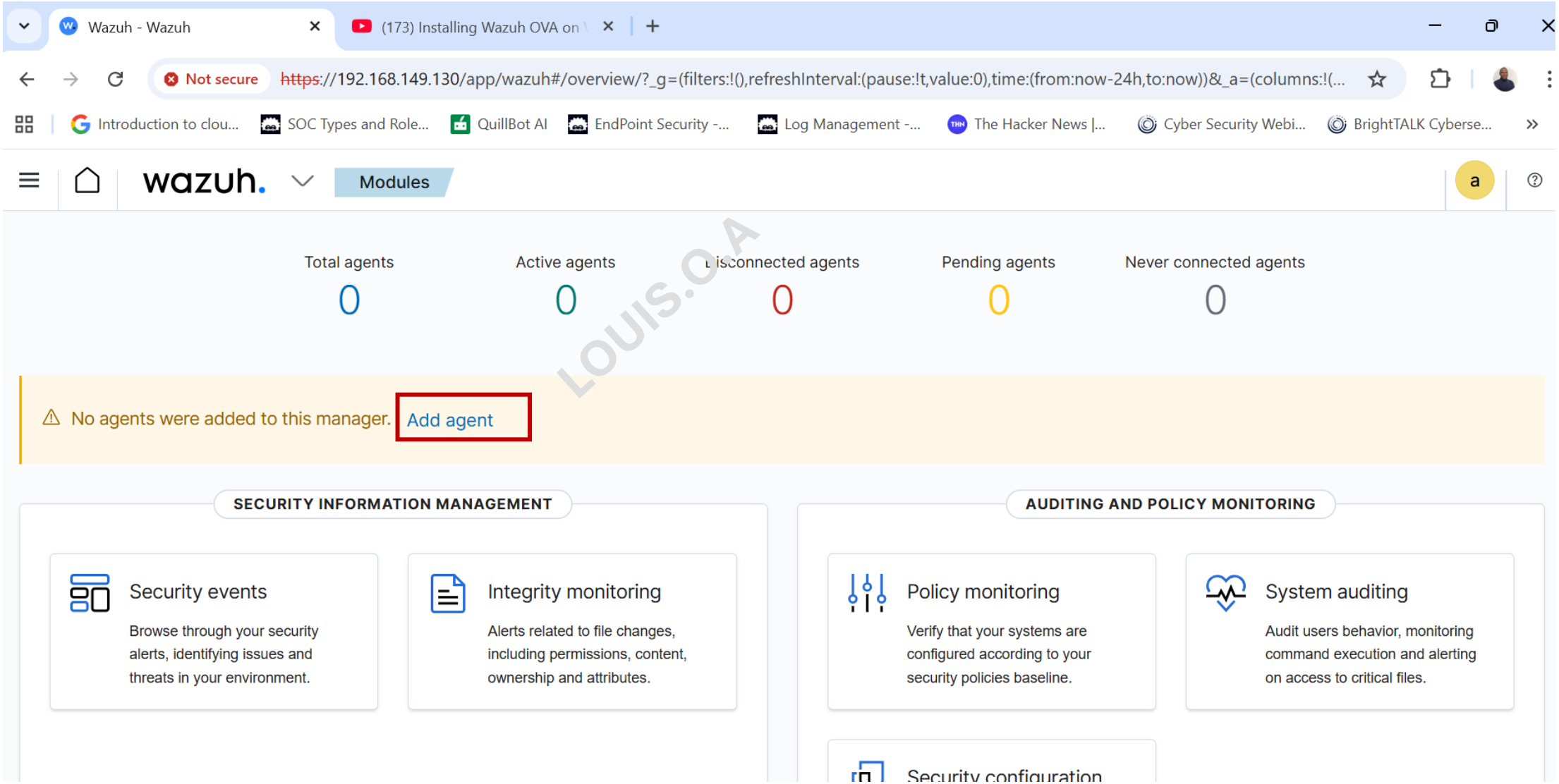
"sudo systemctl start wazuh-indexer"



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)



Close

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

1

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

2

Optional settings

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

Assign an agent name

Louis-Machine

3

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

Select one or more existing groups

Default

4 **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; msiexec.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'
```

4

5 **Start the Wazuh agent:**

```
NET START WazuhSvc
```

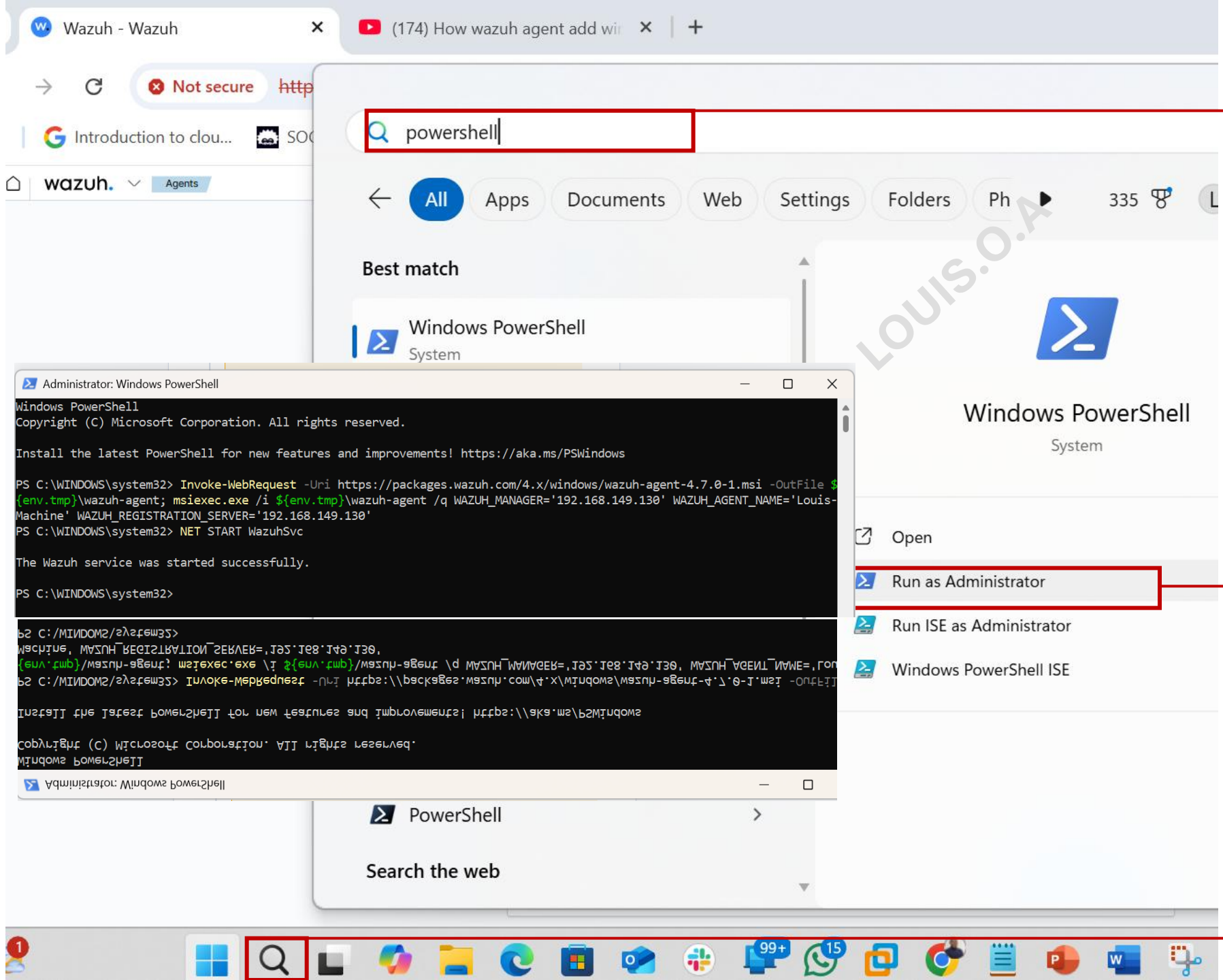
5

Close

6

READ ME

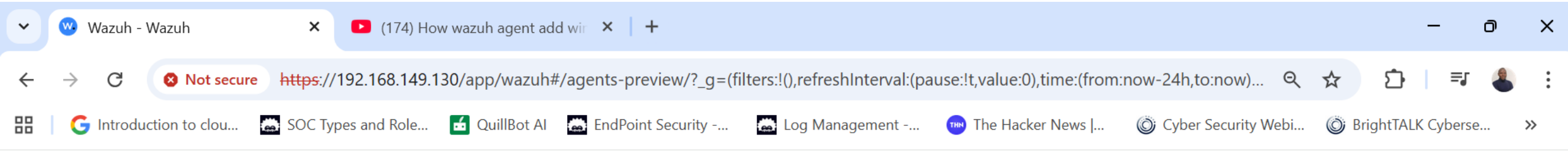
1. Chose the Agent you want to add e.g Windows PC
2. Type-in the ip address of the Wazuh Server e.g 192.168.149.130
3. Name the Agent you want to add e.g Louis-Machine
4. Open PowerShell in administrative mode as shown in the next slide to run No. 4 & 5 command.
5. Click close & go back to wazuh dashboard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

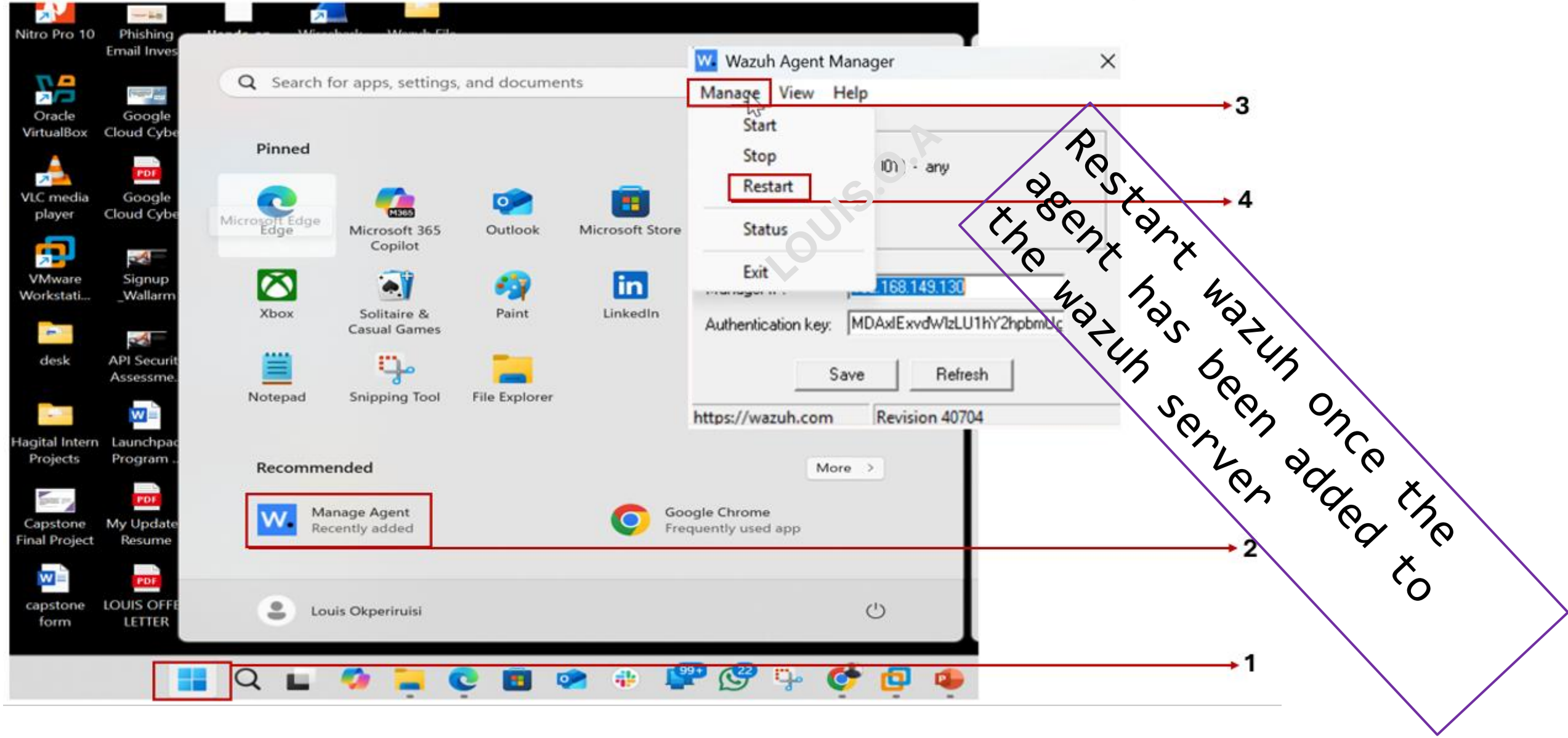


Type powershell **2**

Run as administrator **3**

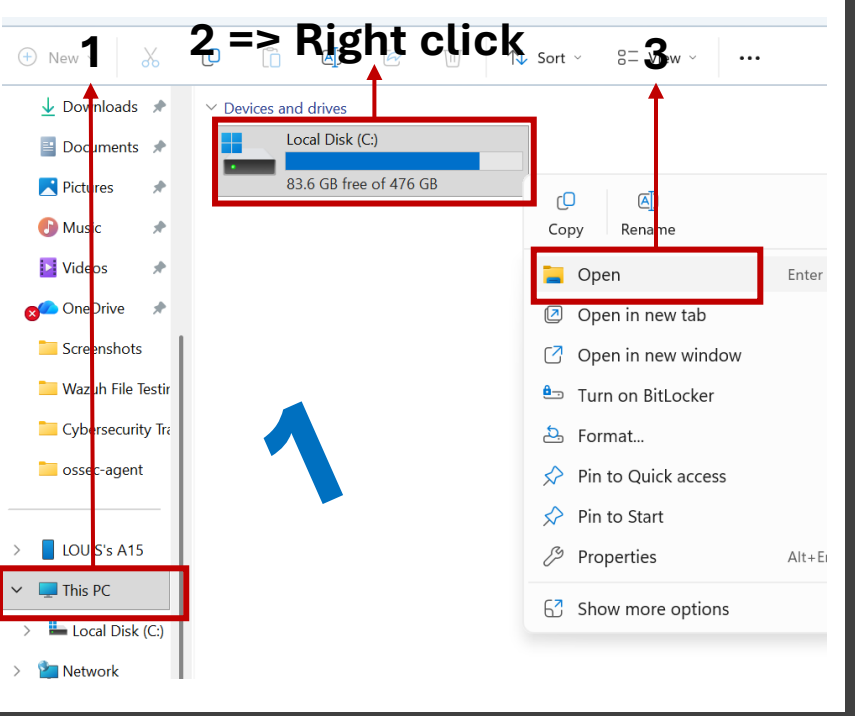
Search powershell **1**

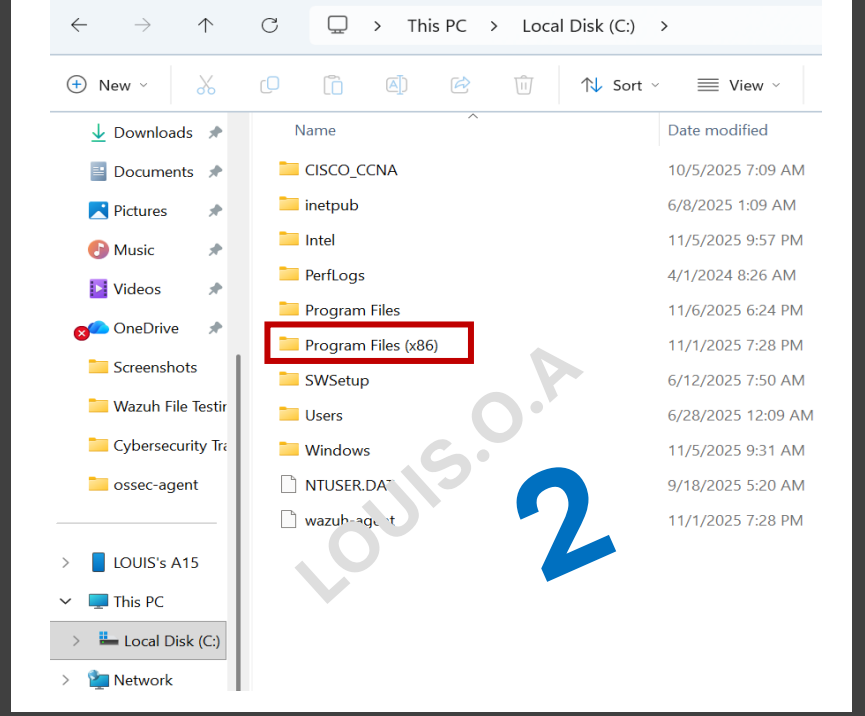

Wazuh - Wazuh
(174) How wazuh agent add wi
Not secure
https://192.168.149.130/app/wazuh#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now)...
Introduction to clou...
SOC Types and Role...
QuillBot AI
EndPoint Security -...
Log Management -...
The Hacker News |...
Cyber Security Webi...
BrightTALK Cyberse...
wazuh.
Agents
STATUS
Active (1)
Disconnected (0)
Pending (0)
Never connected (0)
DETAILS
Active
1
Disconnected
0
Pending
0
Never connected
0
Agents coverage
100.00%
Last registered agent
Louis-Machine
Most active agent
Louis-Machine
EVOLUTION
Last 24 hours
No results found
Agents (1)
Deploy new agent
Refresh
Export formatted
id!=000 and
Search
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

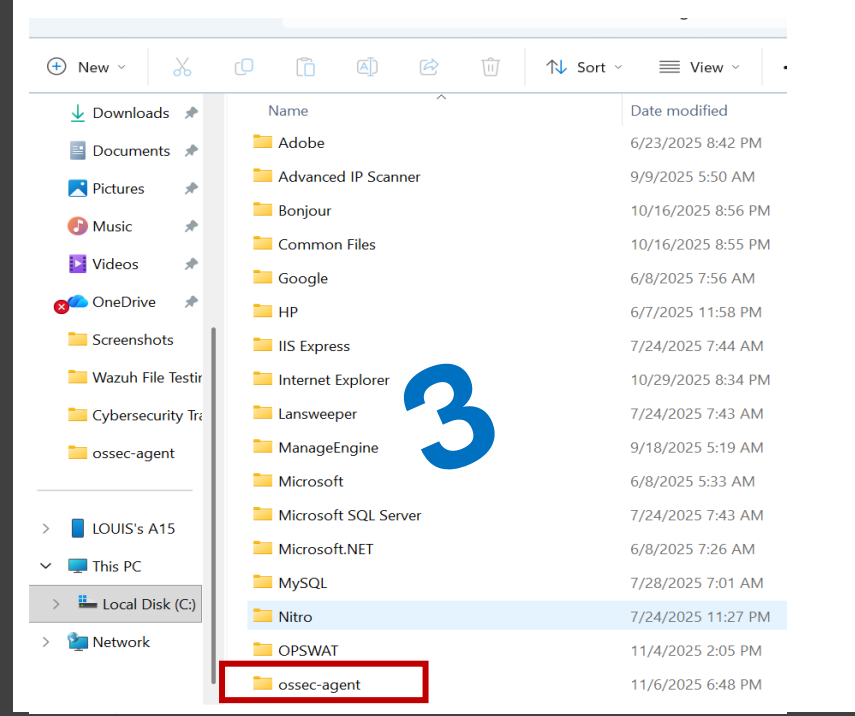

Search for apps, settings, and documents
Pinned
Microsoft Edge
Microsoft 365 Copilot
Outlook
Microsoft Store
Xbox
Solitaire & Casual Games
Paint
LinkedIn
Notepad
Snipping Tool
File Explorer
Recommended
Manage Agent
Recently added
Google Chrome
Frequently used app
More
Louis Okperiruisi
Wazuh Agent Manager
Manage
View
Help
Start
Stop
Restart
Status
Exit
Authentication key:
Save
Refresh
https://wazuh.com
Revision 40704
1
2
3
4
Restart wazuh once the agent has been added to the wazuh server

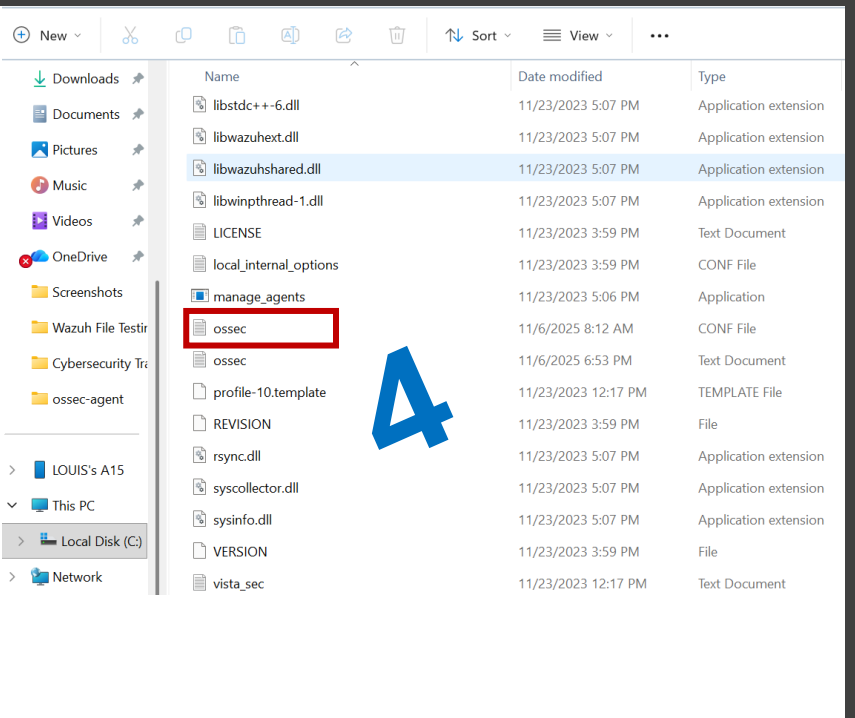
File Integrity Monitoring Configuration

[On Windows-Agent in ossec.conf file]


1
2 => Right click
3
Devices and drives
Local Disk (C:)
83.6 GB free of 476 GB
Copy
Rename
Open
Enter
Open in new tab
Open in new window
Turn on BitLocker
Format...
Pin to Quick access
Pin to Start
Properties
Alt+Enter
Show more options
This PC
Local Disk (C:)
Network
1


This PC
Local Disk (C:)
Name
Date modified
CISCO_CCNA 10/5/2025 7:09 AM
inetpub 6/8/2025 1:09 AM
Intel 11/5/2025 9:57 PM
PerfLogs 4/1/2024 8:26 AM
Program Files 11/6/2025 6:24 PM
Program Files (x86) 11/1/2025 7:28 PM
SWSetup 6/12/2025 7:50 AM
Users 6/28/2025 12:09 AM
Windows 11/5/2025 9:31 AM
NTUSER.DAT 9/18/2025 5:20 AM
2
LOUIS.O.A

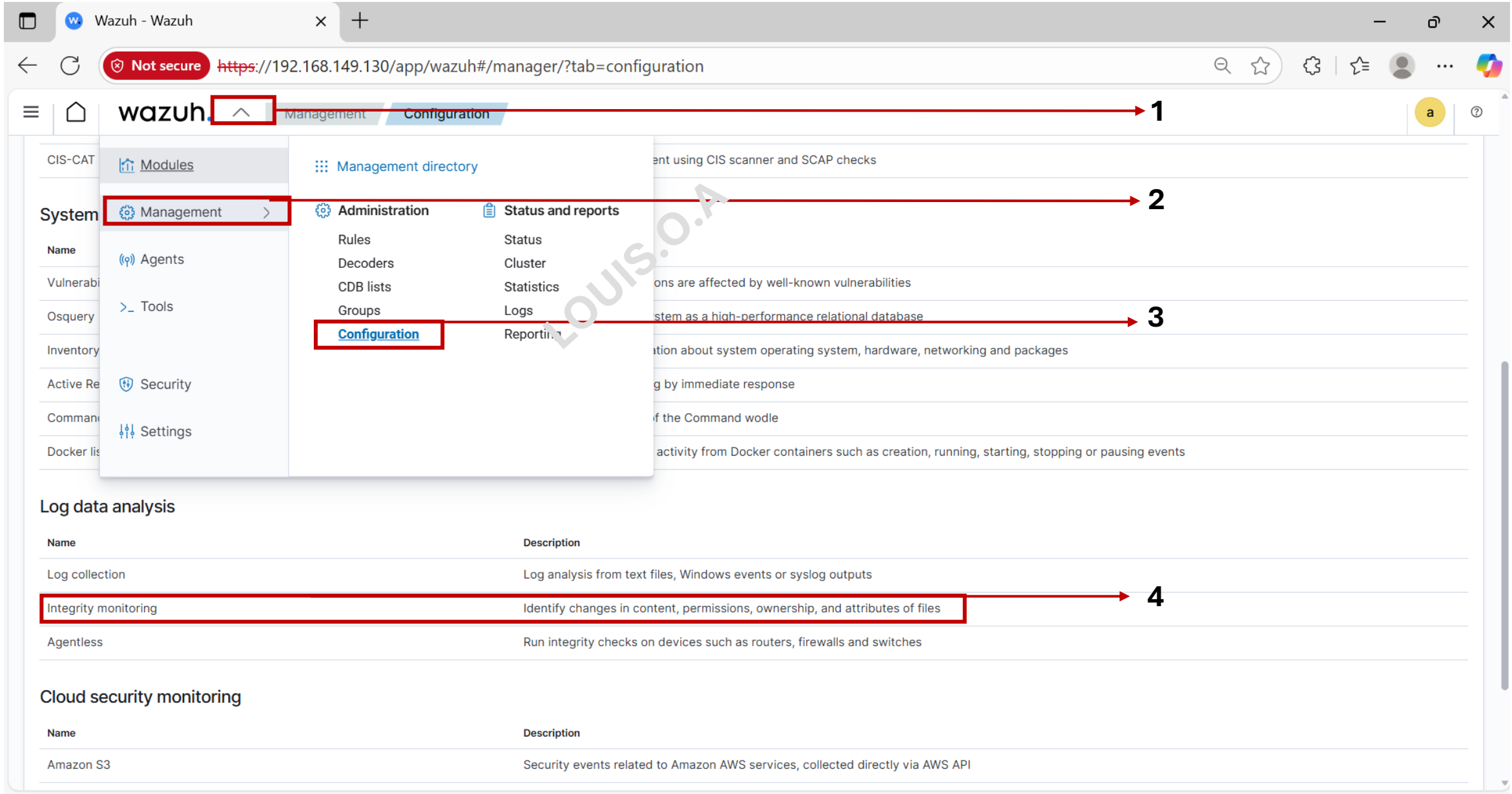

Name
Date modified
Adobe 6/23/2025 8:42 PM
Advanced IP Scanner 9/9/2025 5:50 AM
Bonjour 10/16/2025 8:56 PM
Common Files 10/16/2025 8:55 PM
Google 6/8/2025 7:56 AM
HP 6/7/2025 11:58 PM
IIS Express 7/24/2025 7:44 AM
Internet Explorer 10/29/2025 8:34 PM
Lansweeper 7/24/2025 7:43 AM
ManageEngine 9/18/2025 5:19 AM
Microsoft 6/8/2025 5:33 AM
Microsoft SQL Server 7/24/2025 7:43 AM
Microsoft.NET 6/8/2025 7:26 AM
MySQL 7/28/2025 7:01 AM
Nitro 7/24/2025 11:27 PM
OPSWAT 11/4/2025 2:05 PM
ossec-agent 11/6/2025 6:48 PM
3

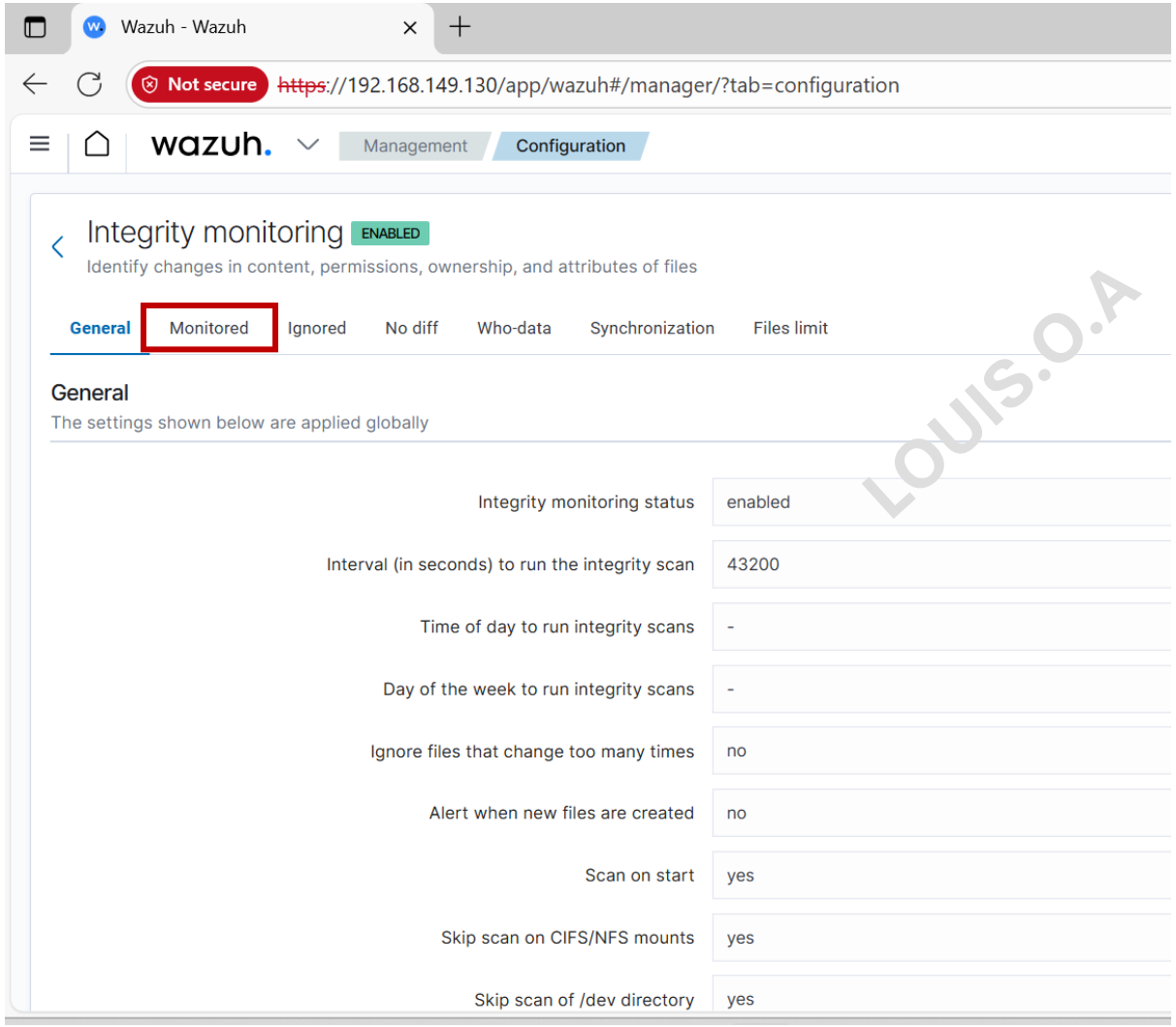

Name
Date modified
Type
libstdc++-6.dll 11/23/2023 5:07 PM Application extension
libwazuhext.dll 11/23/2023 5:07 PM Application extension
libwazuhshared.dll 11/23/2023 5:07 PM Application extension
libwinpthread-1.dll 11/23/2023 5:07 PM Application extension
LICENSE 11/23/2023 3:59 PM Text Document
local_internal_options 11/23/2023 3:59 PM CONF File
manage_agents 11/23/2023 5:06 PM Application
ossec 11/6/2025 8:12 AM CONF File
ossec 11/6/2025 6:53 PM Text Document
profile-10.template 11/23/2023 12:17 PM TEMPLATE File
REVISION 11/23/2023 3:59 PM File
rsync.dll 11/23/2023 5:07 PM Application extension
syscollector.dll 11/23/2023 5:07 PM Application extension
sysinfo.dll 11/23/2023 5:07 PM Application extension
VERSION 11/23/2023 3:59 PM File
vista_sec 11/23/2023 12:17 PM Text Document
4

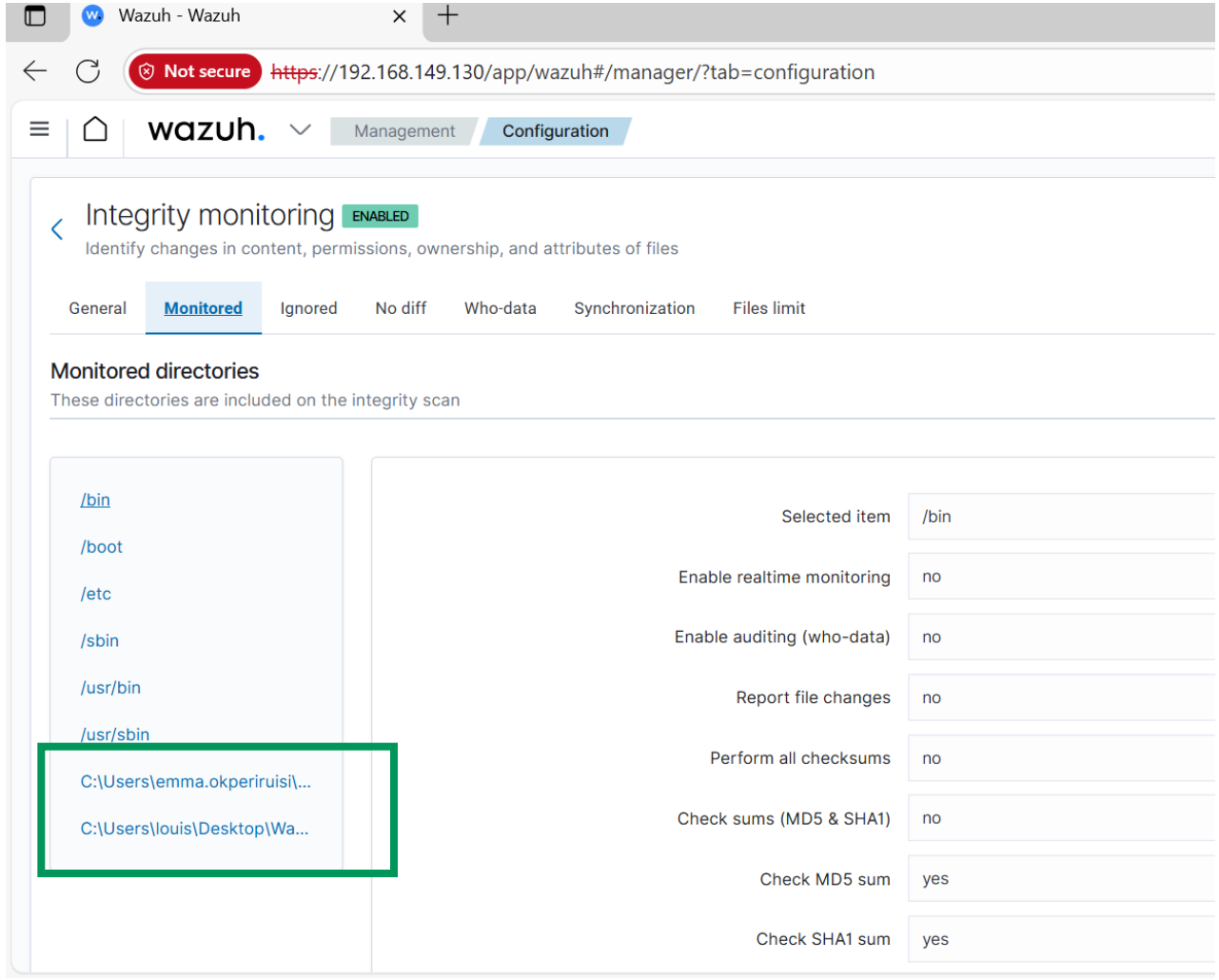

File Edit View
<!--
Wazuh - Agent - Default configuration for Windows
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->
<ossec_config>
<client>
<server>
<address>192.168.149.130</address>
<port>1514</port>
<protocol>tcp</protocol>
</server>
<config-profile>windows, windows10</config-profile>
<enrollment>
<enabled>yes</enabled>
<manager_address>192.168.149.130</manager_address>
<agent_name>Louis-Machine</agent_name>
</enrollment>
</client>
<!-- Agent buffer options -->
<client_buffer>
<disabled>no</disabled>
<queue_size>5000</queue_size>
<events_per_second>500</events_per_second>
</client_buffer>
Scroll Down
5

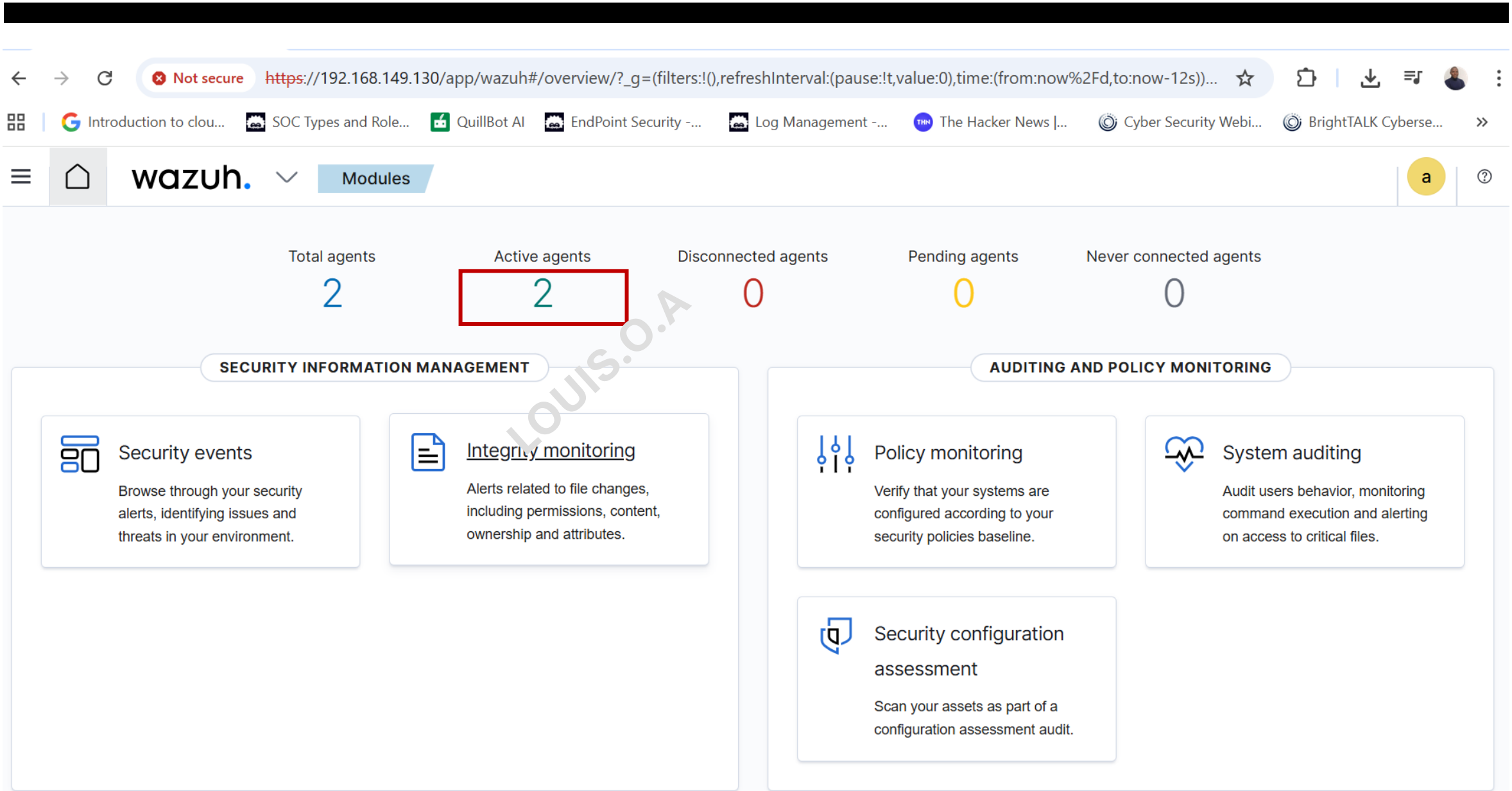

File Edit View
<!-- Policy monitoring -->
<rootcheck>
<disabled>no</disabled>
<windows_apps>./shared/win_applications_rcl.txt</windows_apps>
<windows_malware>./shared/win_malware_rcl.txt</windows_malware>
</rootcheck>
<!-- Security Configuration Assessment -->
<sca>
<enabled>yes</enabled>
<scan_on_start>yes</scan_on_start>
<interval>12h</interval>
<skip_nfs>yes</skip_nfs>
</sca>
<!-- File integrity monitoring -->
<syscheck>
<disabled>no</disabled>
<!-- Frequency that syscheck is executed default every 12 hours -->
<frequency>43200</frequency>
<!-- Default files to be monitored. -->
<directories recursion_level="0" restrict="regedit.exe$|system.ini$|win.ini$">%WINDIR%</directories>
<directories>C:\Users\louis\Desktop\Wazuh File Testing</directories>
<directories whodata="yes" report_changes="yes" check_all="yes">C:\Users\louis\Desktop\Wazuh File Testing</directories>
<directories>C:\Users\emma.okperiruisi\Desktop\Test Folder</directories>
<directories whodata="yes" report_changes="yes" check_all="yes">C:\Users\emma.okperiruisi\Desktop\Test Folder</directories>
<directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net$|reg.exe$|regedt32.exe|regsvr32.exe|runas.exe|sc.exe|schtasks.exe|sethc.exe|subst.exe$">%WINDIR%\SysNative</directories>
6

View all monitored directories by wazuh.




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

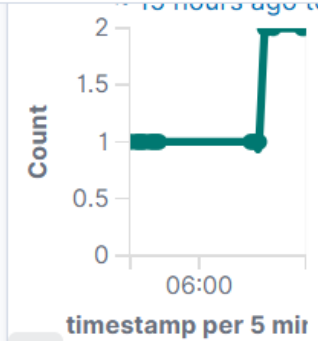

Not secure
https://192.168.149.130/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now%2Fd,to:now-12s))...
Introduction to clou...
SOC Types and Role...
QuillBot AI
EndPoint Security -...
Log Management -...
The Hacker News |...
Cyber Security Webi...
BrightTALK Cyberse...
wazuh.
Modules
a
Total agents
2
Active agents
2
Disconnected agents
0
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.

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

Active	Disconnected	Pending	Never connected	Agents coverage
2	0	0	0	100.00%

Last registered agent
virtualMachine

Most active agent
Louis-Machine



Agents (2)

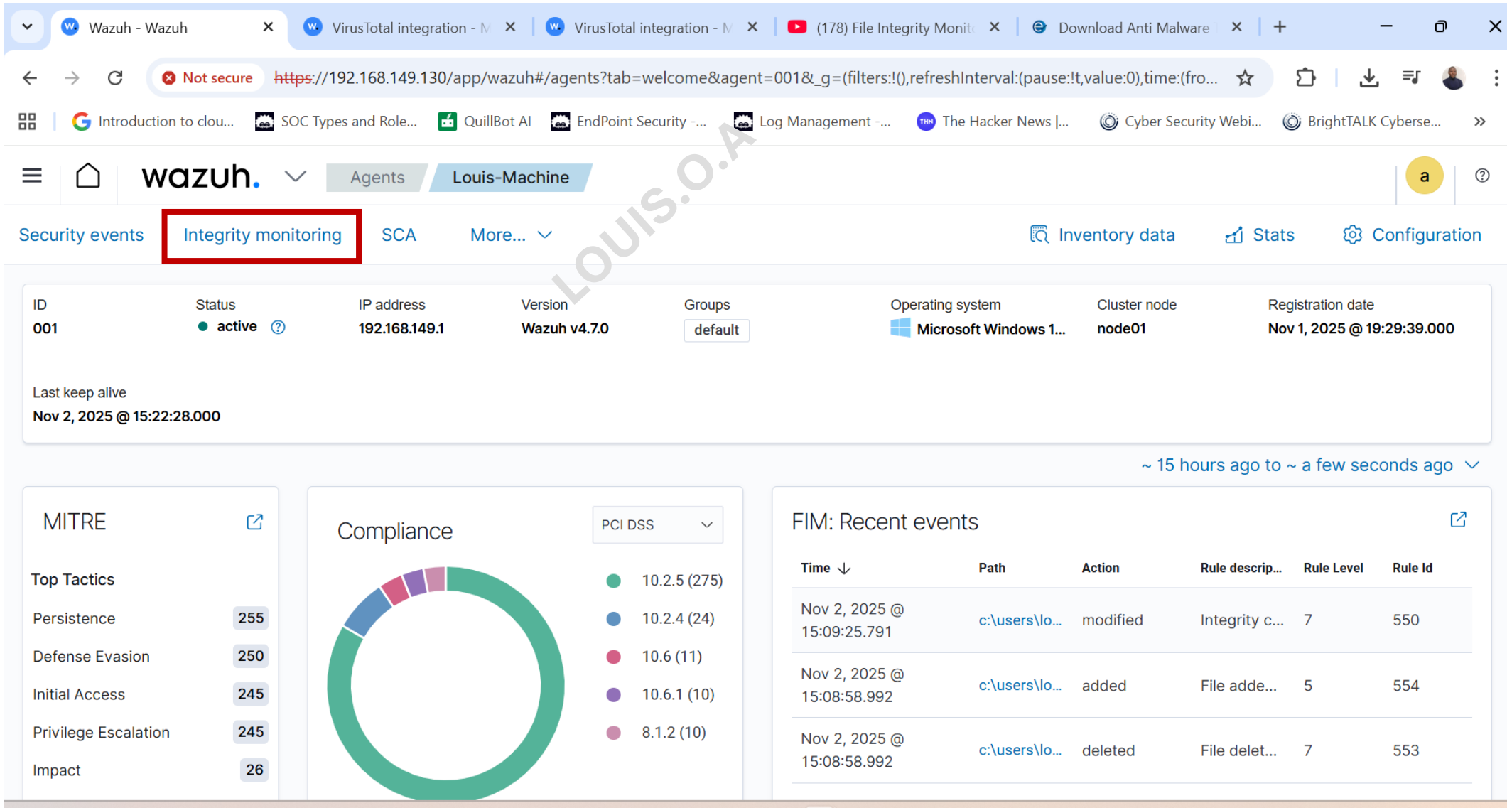
Deploy new agent | Refresh | Export for

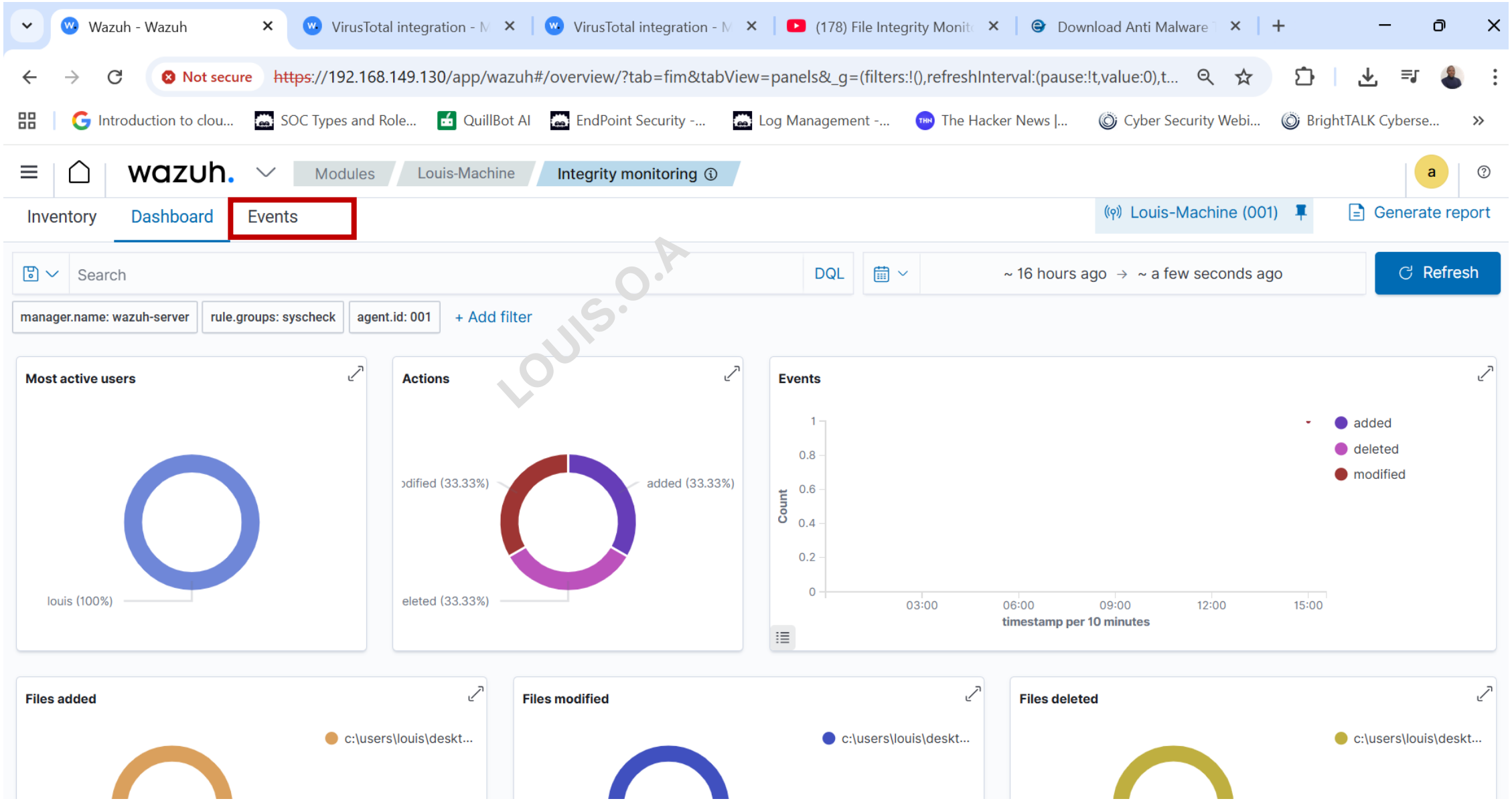
id!=000 and status=active | WQL

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#/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 Cyberse...
wazuh.
Modules
Louis-Machine
Integrity monitoring
Inventory
Dashboard
Events
Louis-Machine (001)
Generate report
Search
DQL
~ 16 hours ago → ~ a few seconds ago
Refresh
manager.name: wazuh-server
rule.groups: syscheck
agent.id: 001
+ Add filter
LOUIS.O.A
Most active users
louis (100%)
Actions
odified (33.33%)
added (33.33%)
eleted (33.33%)
Events
added
deleted
modified
Count
timestamp per 10 minutes
Files added
c:\users\louis\deskt...
Files modified
c:\users\louis\deskt...
Files deleted
c:\users\louis\deskt...

Wazuh - Wazuh | VirusTotal integration - M | VirusTotal integration - M | (178) 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 Cybers

wazuh. Modules > Louis-Machine > Integrity monitoring

Inventory | Dashboard | Events

Louis-Machine

Search | DQL | ~ 16 hours ago → ~ a few seconds ago

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

wazuh-alerts-*

Search field names

Filter by type 0

Selected fields

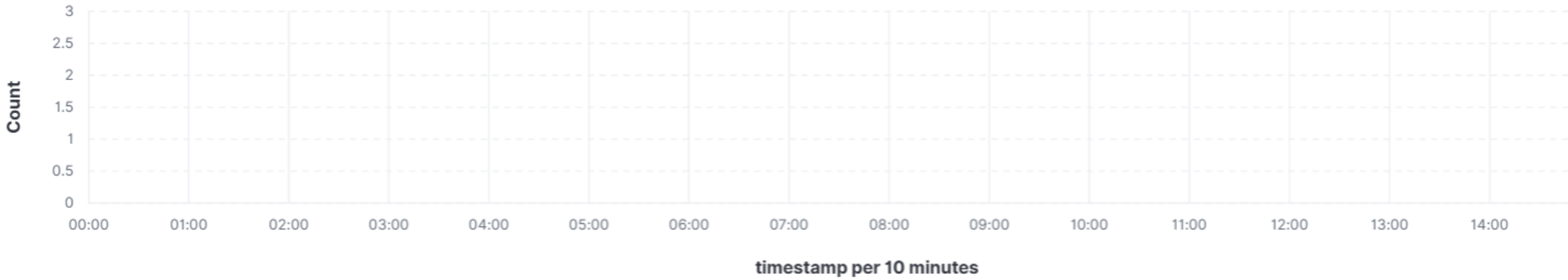
- t rule.description
- t rule.id
- # rule.level
- t syscheck.event
- t syscheck.path

Available fields

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

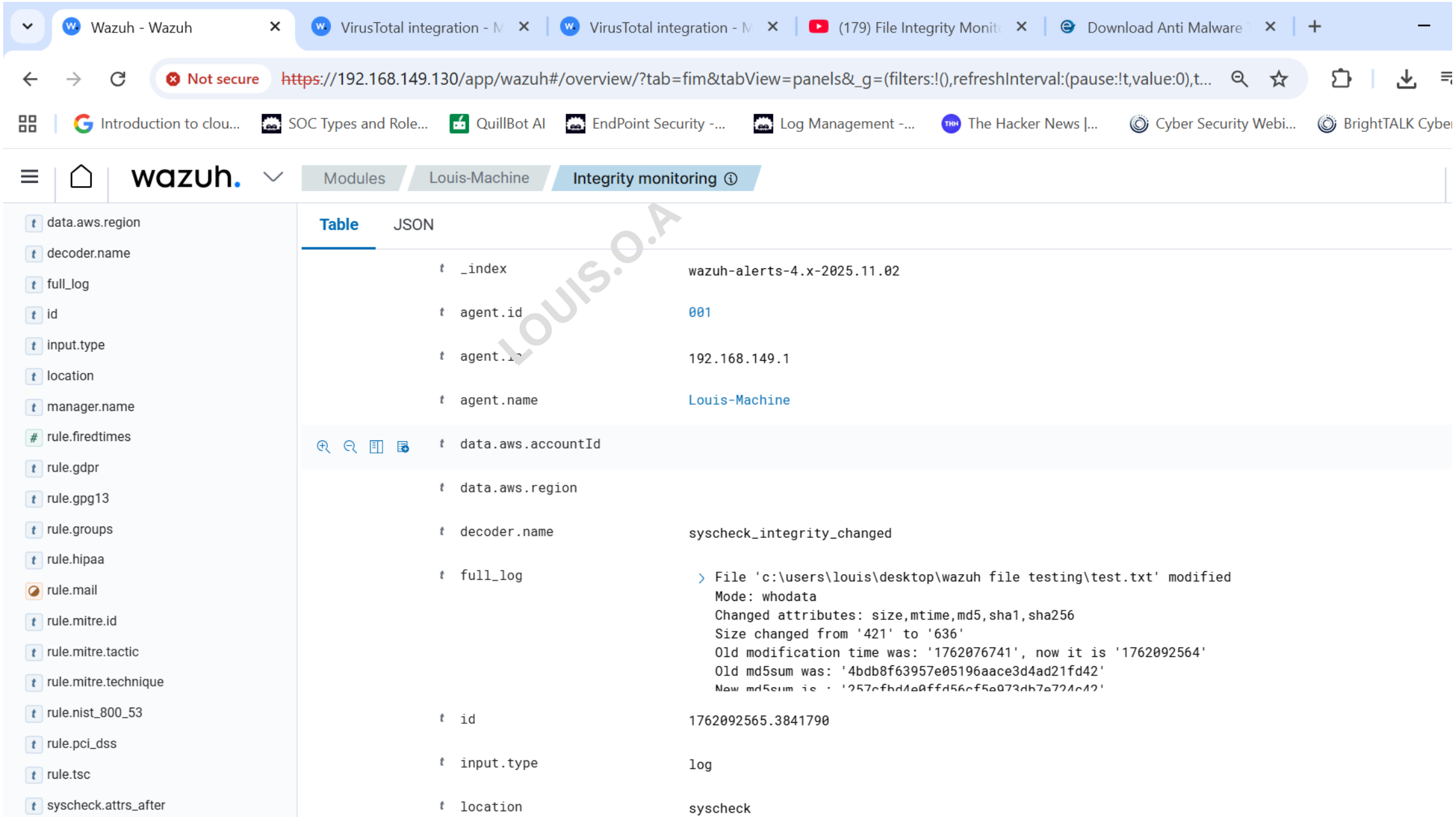
3 hits

Nov 2, 2025 @ 00:00:00.000 - Nov 2, 2025 @ 15:35:23.779 Auto

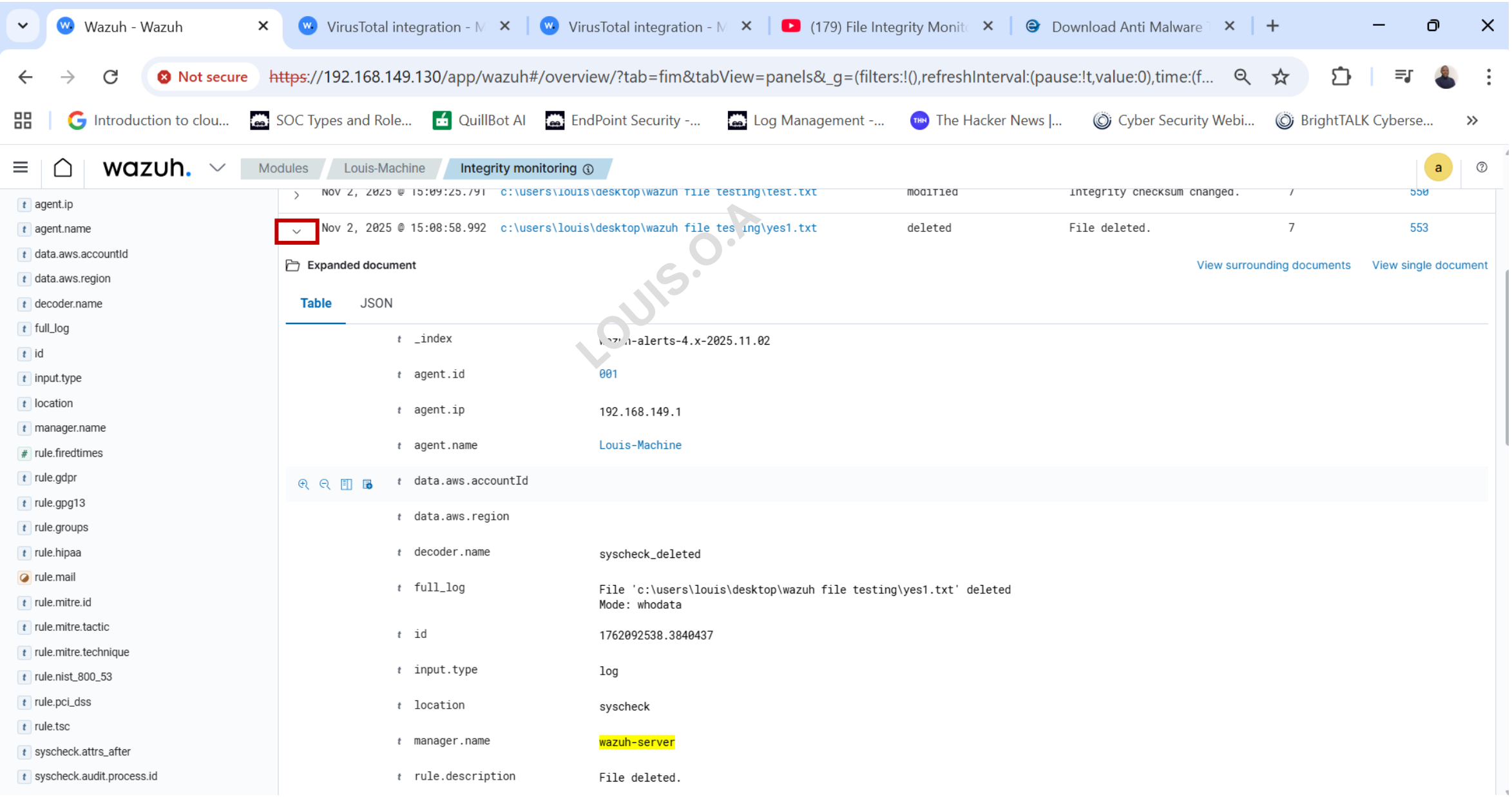


Time	syscheck.path	syscheck.event	rule.description	rule.level	r
Nov 2, 2025 @ 15:09:25.791	c:\users\louis\desktop\wazuh file testing\test.txt	modified	Integrity checksum changed.	7	5
	is\desktop\wazuh file testing\yes1.txt	deleted	File deleted.	7	5
Nov 2, 2025 @ 15:08:58.992	c:\users\louis\desktop\wazuh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

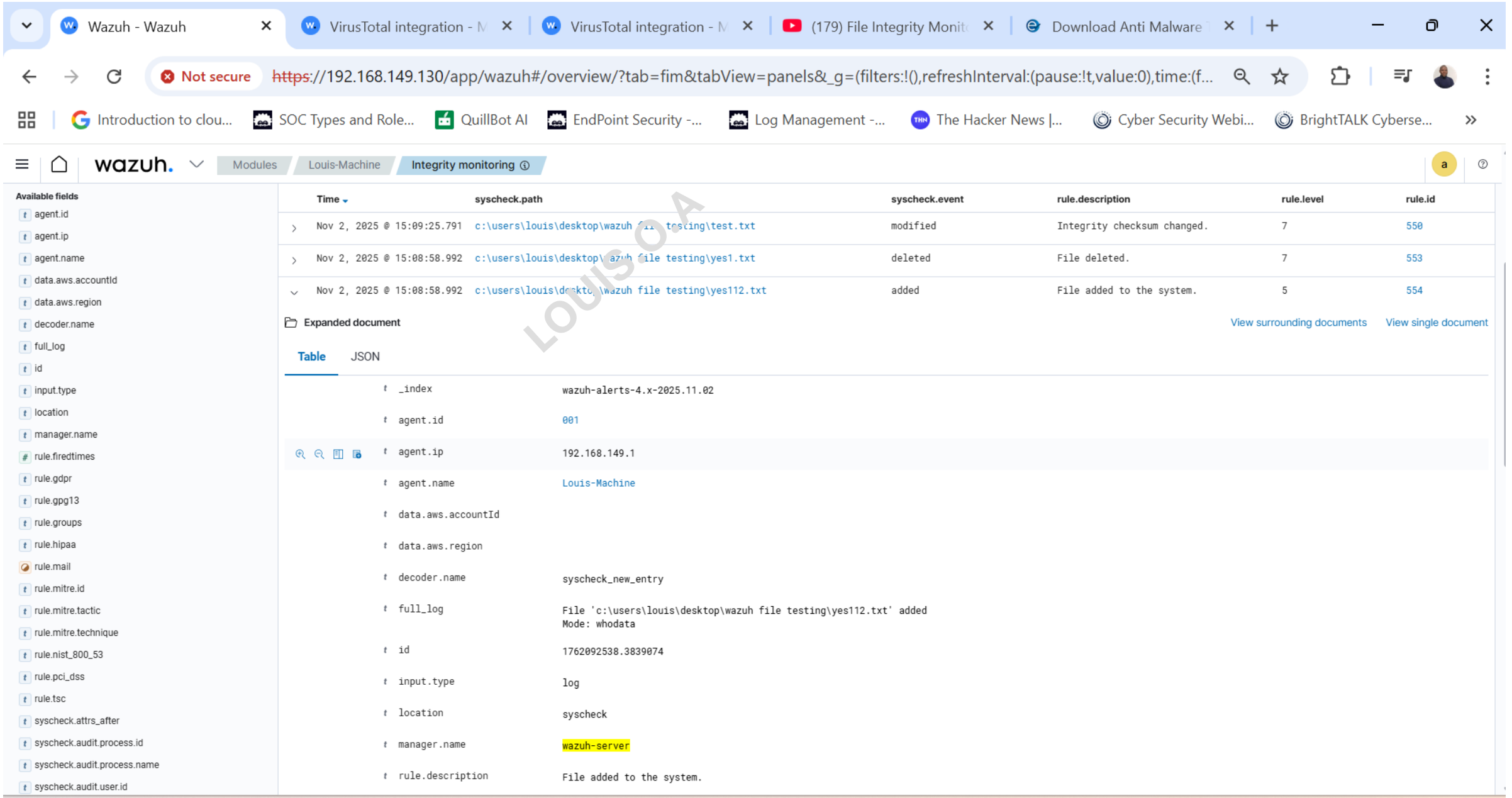
File Modification



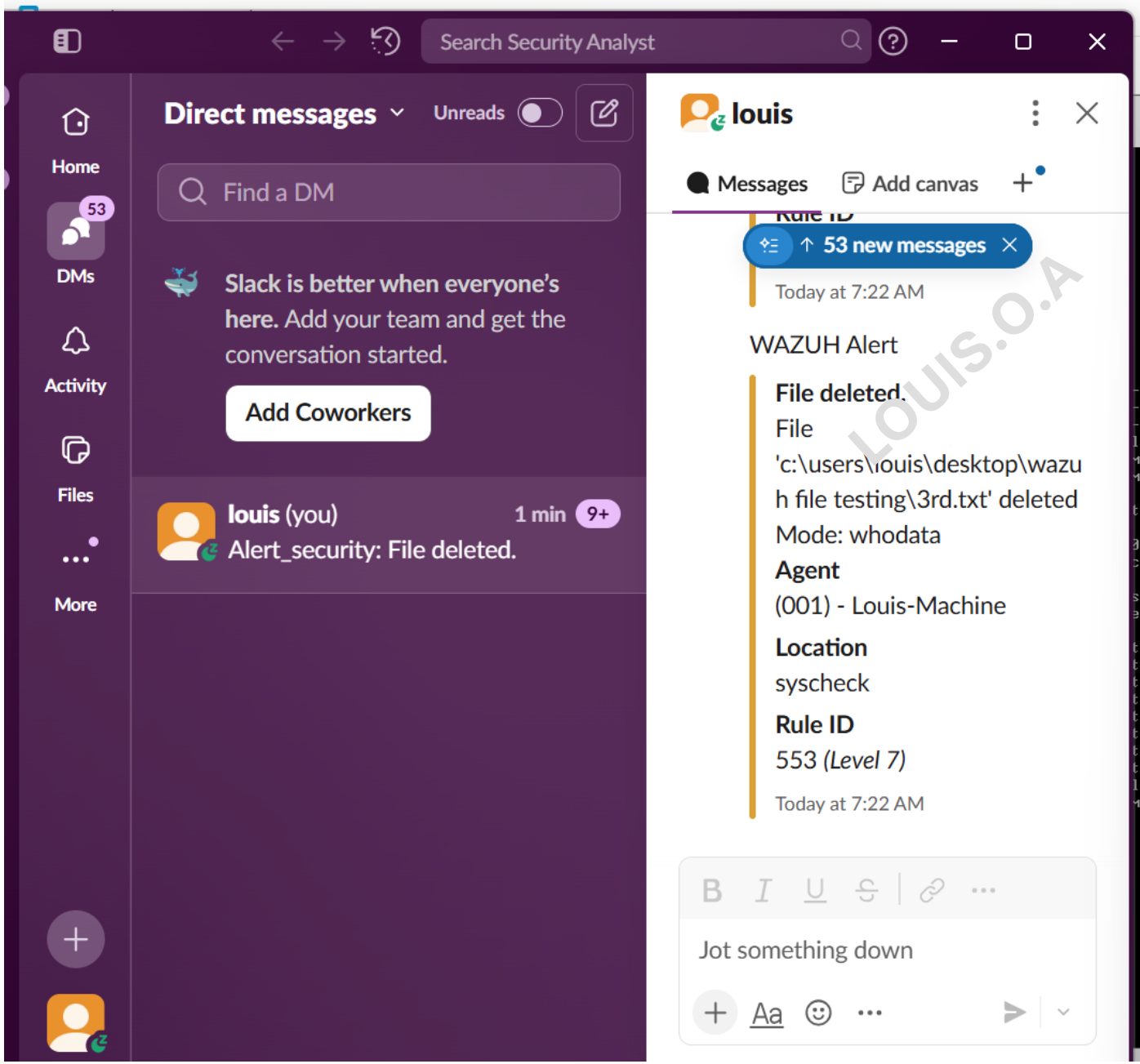
File Deletion

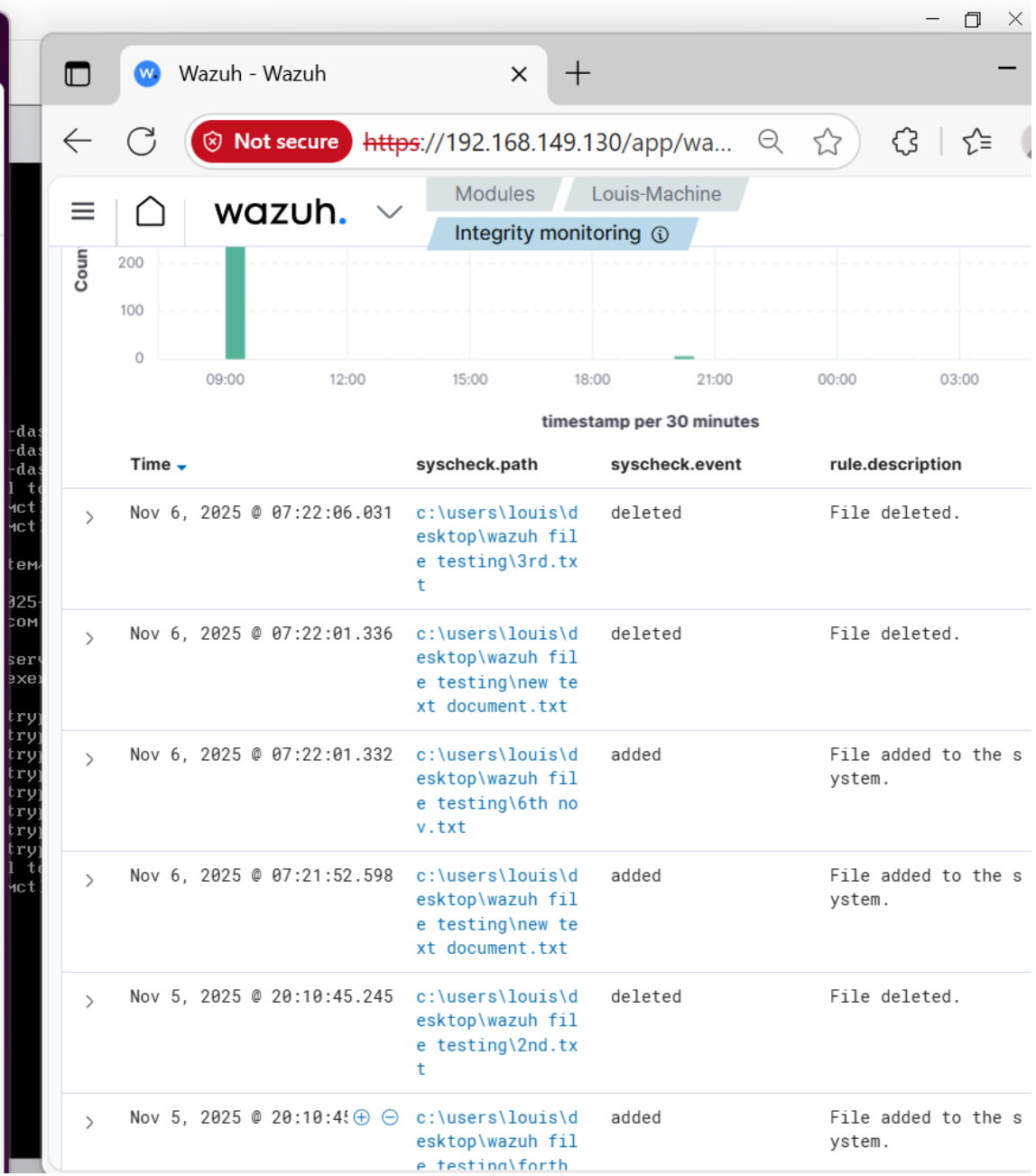


File Addition



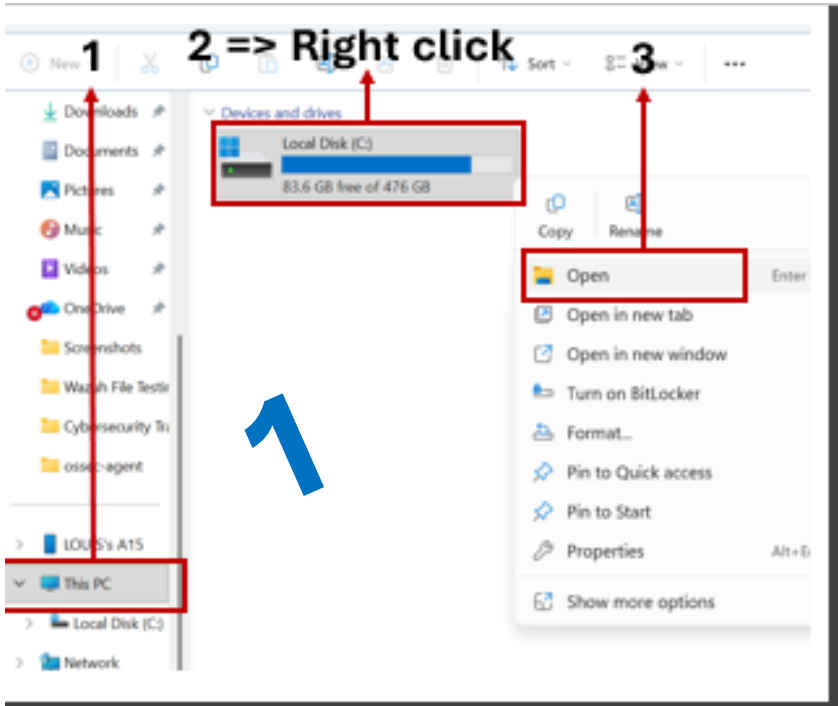
File Monitoring alert message sent to slack channel

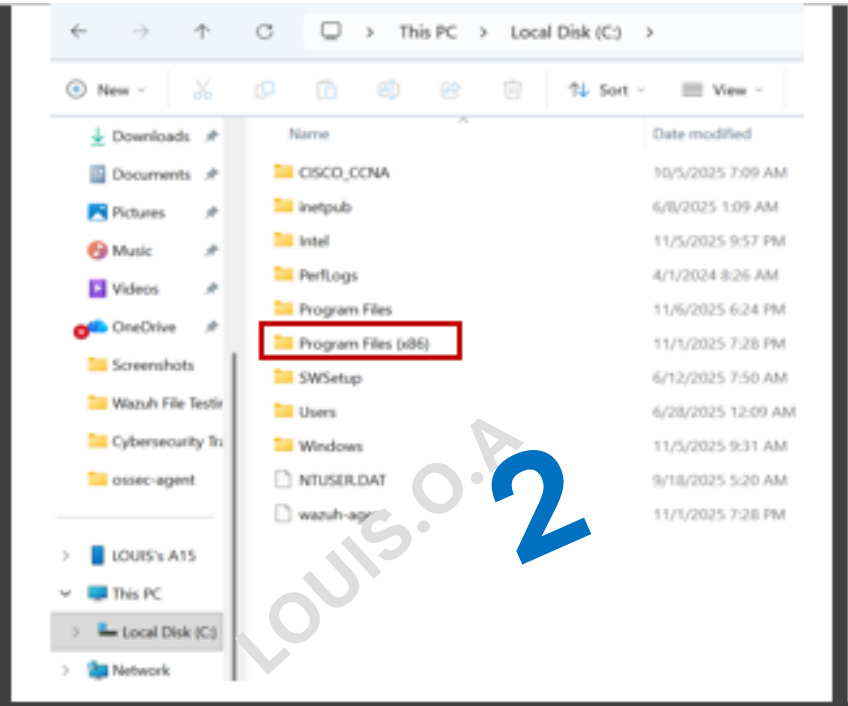


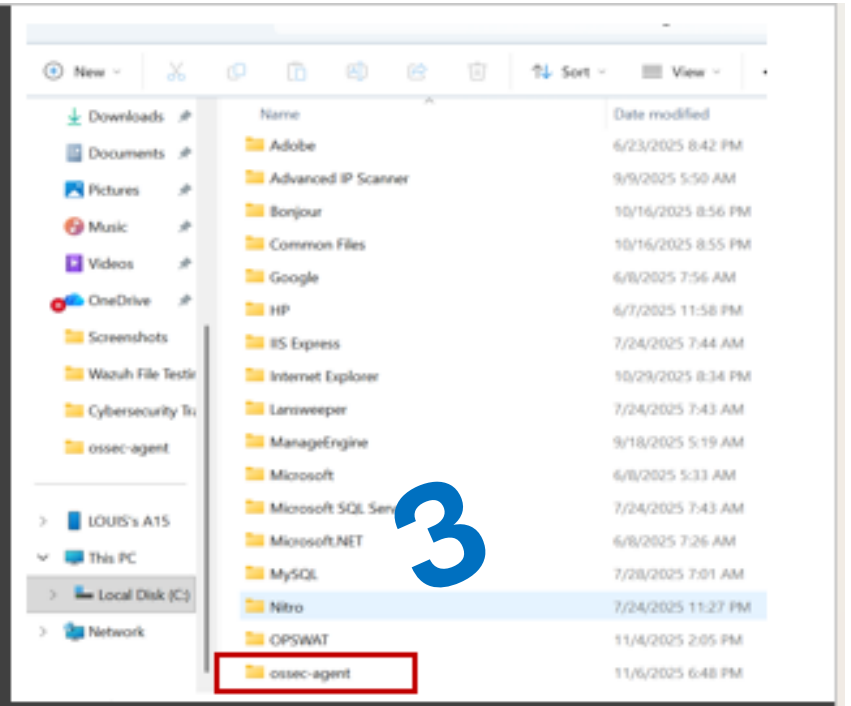


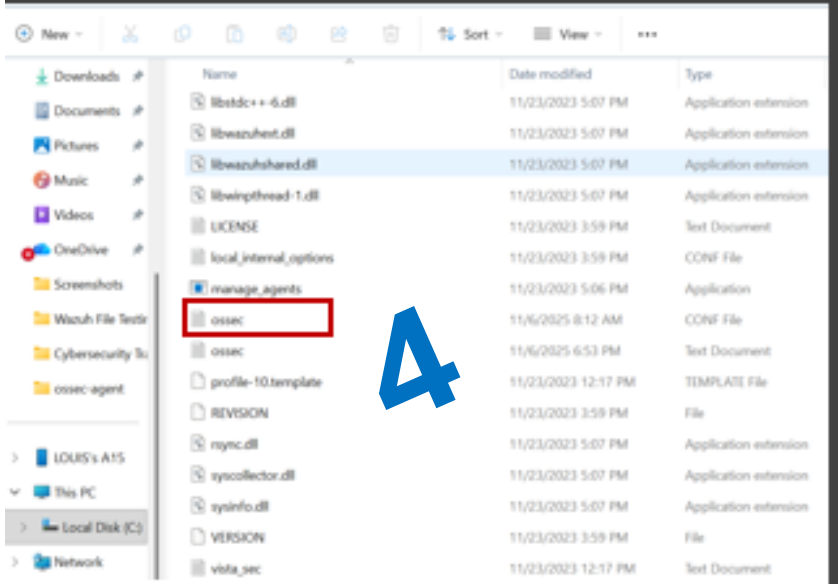
Microsoft-Windows Windows Defender Configuration

[On Windows-Agent in ossec.conf file]


1
2 => Right click
3
Local Disk (C:)
83.6 GB free of 476 GB
Copy
Rename
Open
Open in new tab
Open in new window
Turn on BitLocker
Format...
Pin to Quick access
Pin to Start
Properties
Show more options
1


This PC
Local Disk (C:)
Program Files (x86)
2
Louis.o.A

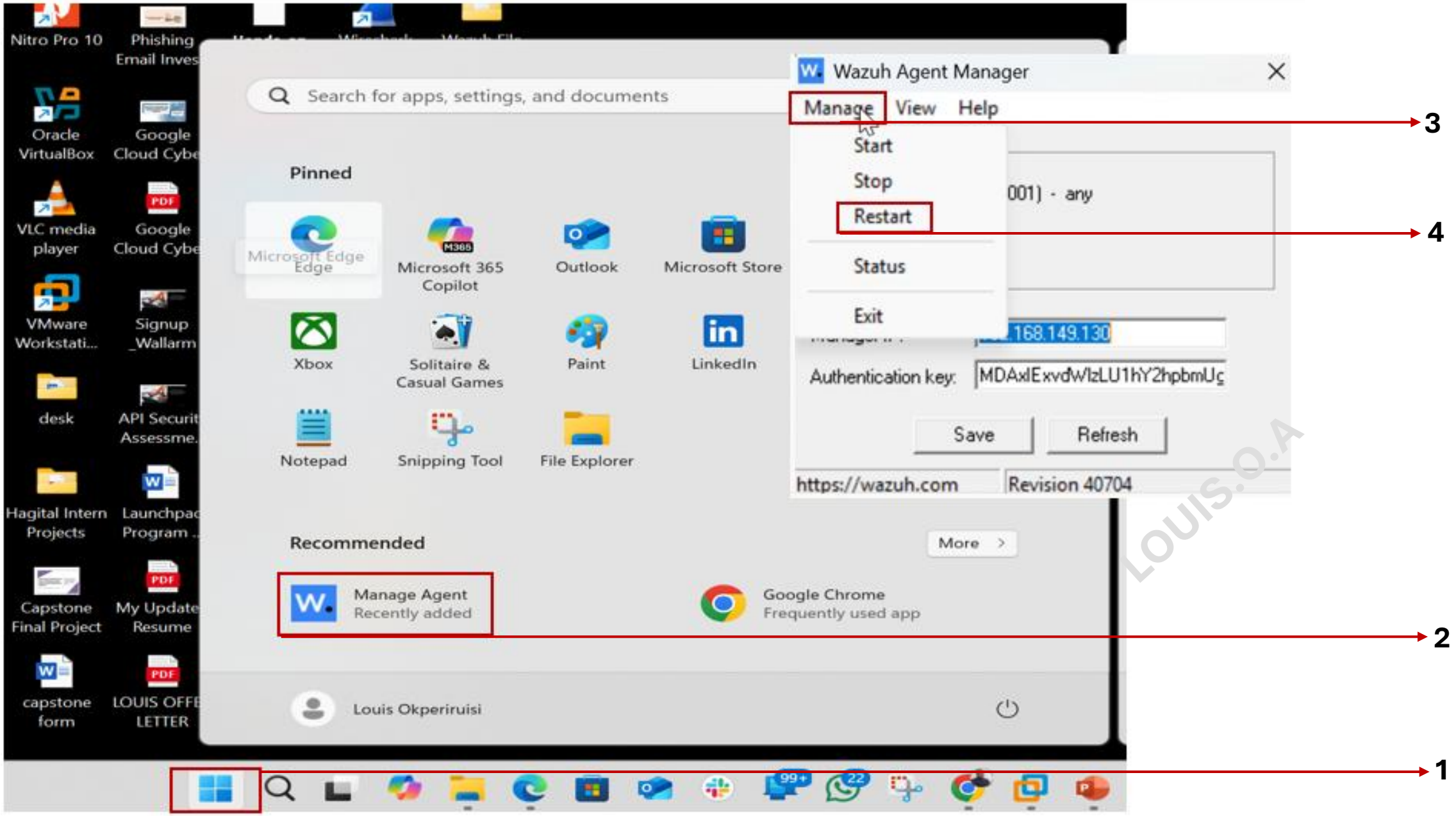

ossec-agent
3


ossec
4


Scroll Down
5
<!--
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>192.168.149.130</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>
<enrollment>
<enabled>yes</enabled>
<manager_address>192.168.149.130</manager_address>
<agent_name>Louis-Machine</agent_name>
</enrollment>
</client>
<!-- Agent buffer options -->
<client_buffer>
<disabled>no</disabled>
<queue_size>5000</queue_size>
<events_per_second>500</events_per_second>
</client_buffer>

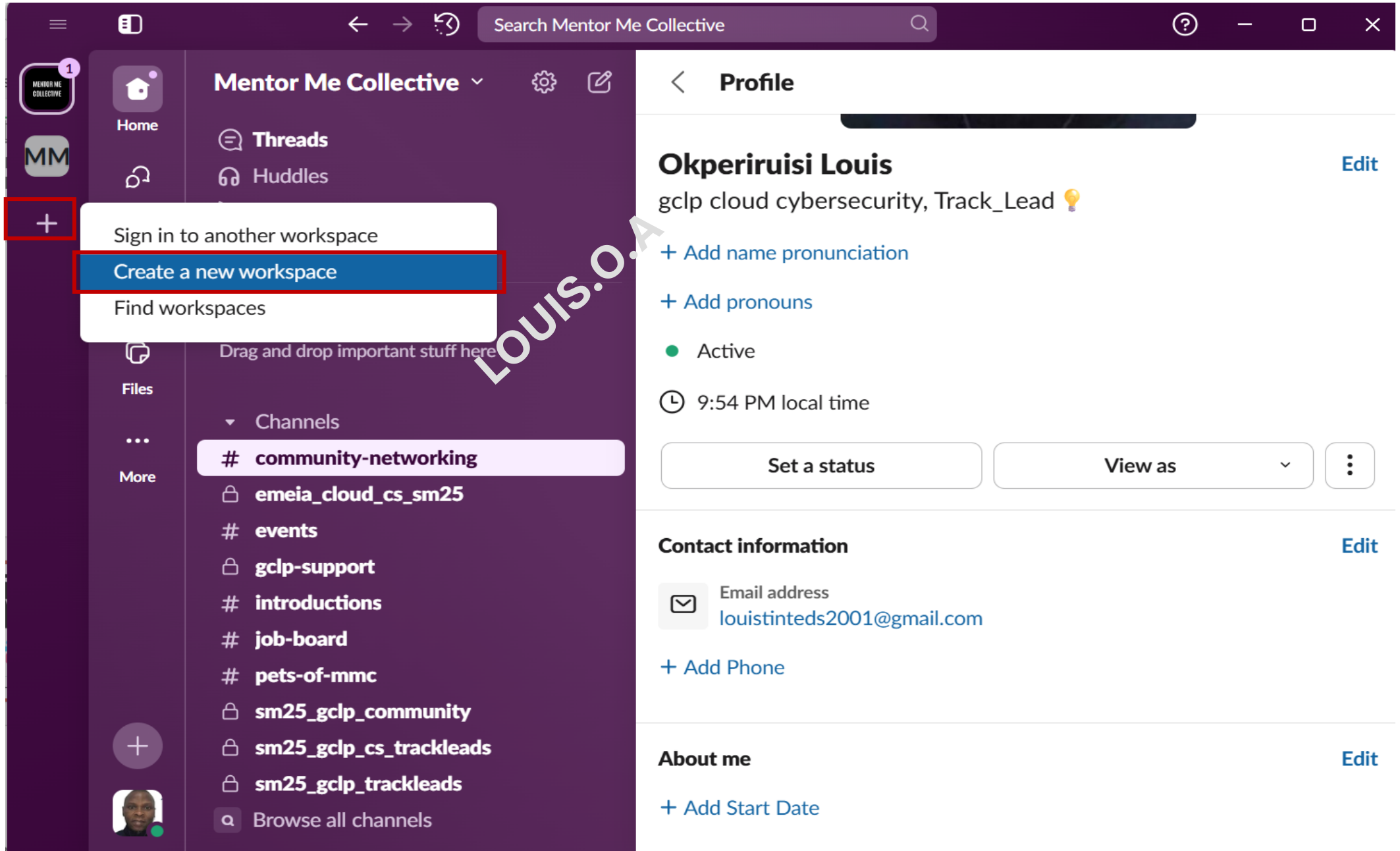

6
</localfile>
<localfile>
<location>Security</location>
<log_format>eventchannel</log_format>
<query>Event/System[EventID != 5145 and EventID != 5156 and EventID != 5447 and
EventID != 4656 and EventID != 4658 and EventID != 4663 and EventID != 4660 and
EventID != 4670 and EventID != 4690 and EventID != 4703 and EventID != 4907 and
EventID != 5152 and EventID != 5157]</query>
</localfile>
<localfile>
<location>System</location>
<log_format>eventchannel</log_format>
</localfile>
<localfile>
<log_format>syslog</log_format>
</localfile>
<localfile>
<location>Microsoft-Windows-Windows Defender/Operational</location>
<log_format>eventchannel</log_format>
</localfile>
<!-- Policy monitoring -->
<rootcheck>
<disabled>no</disabled>
<windows_apps>./shared/win_applications_rcl.txt</windows_apps>
<windows_malware>./shared/win_malware_rcl.txt</windows_malware>
</rootcheck>

Restart Wazuh-Server after windows agent configuration

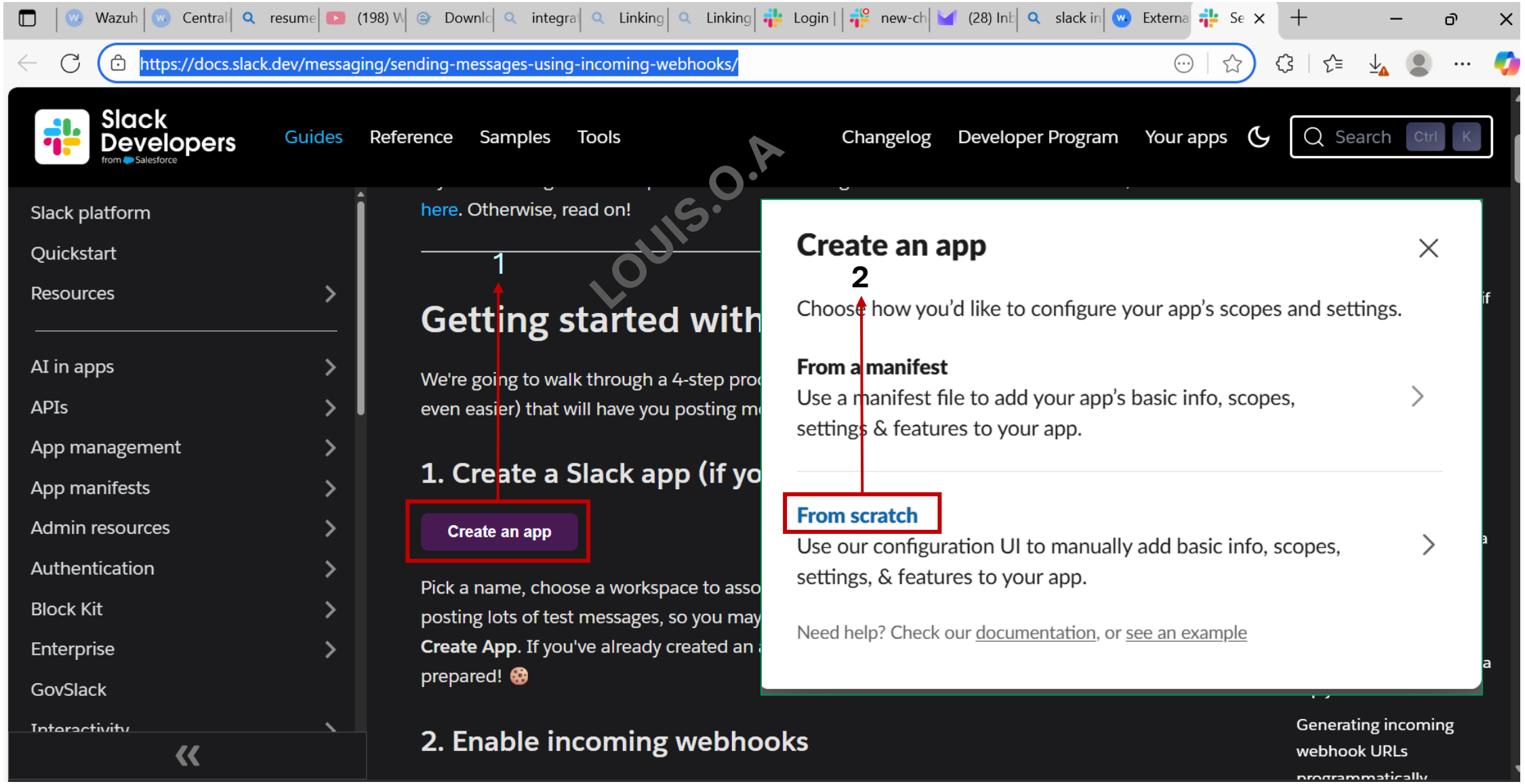


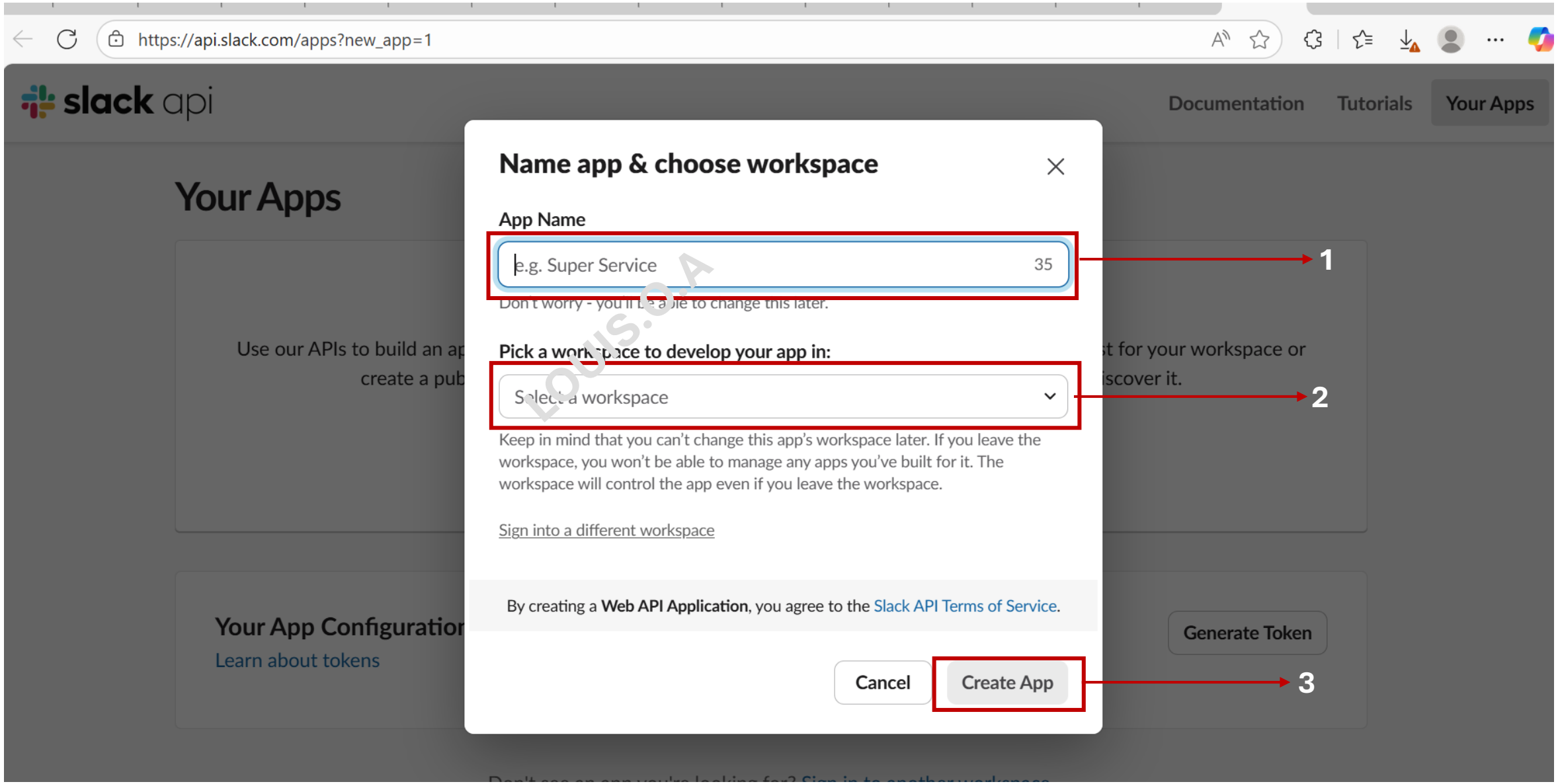
Linking Wazuh to my Slack account, for possible alert.

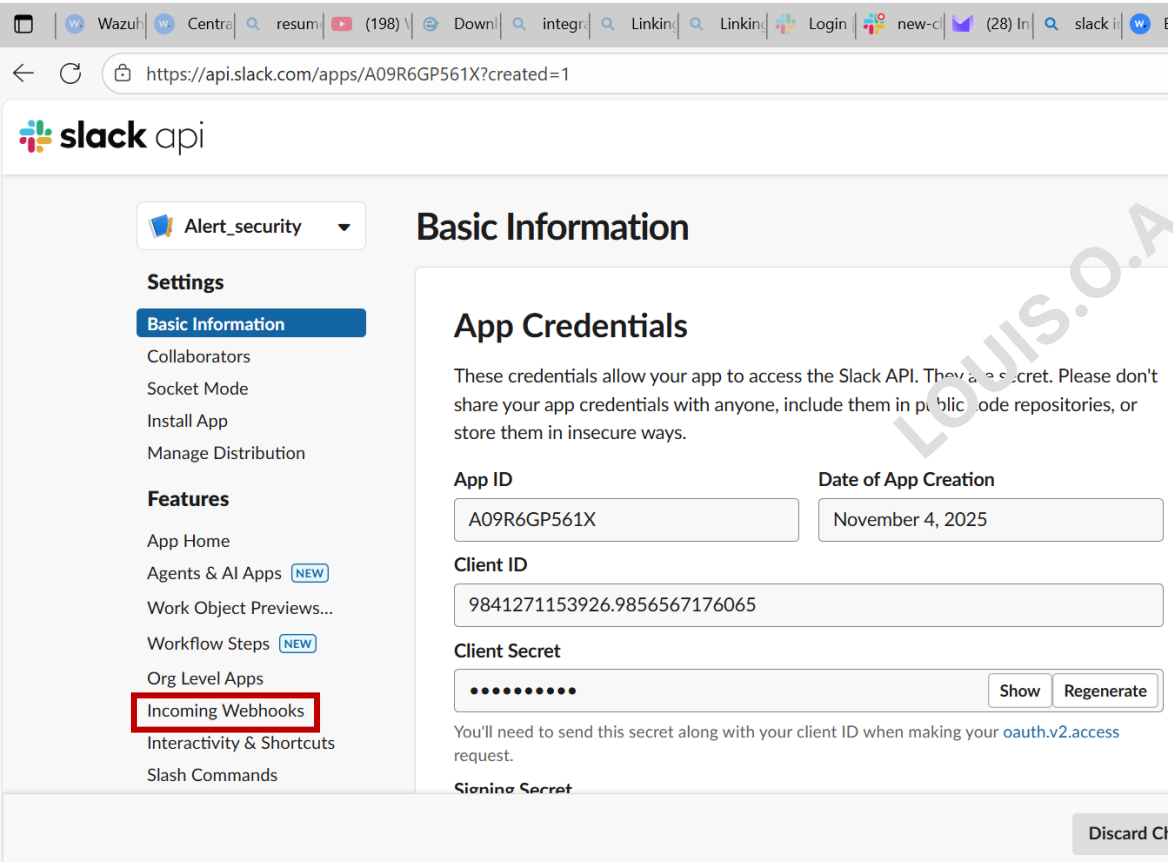
Signup on Slack and create a new workspace

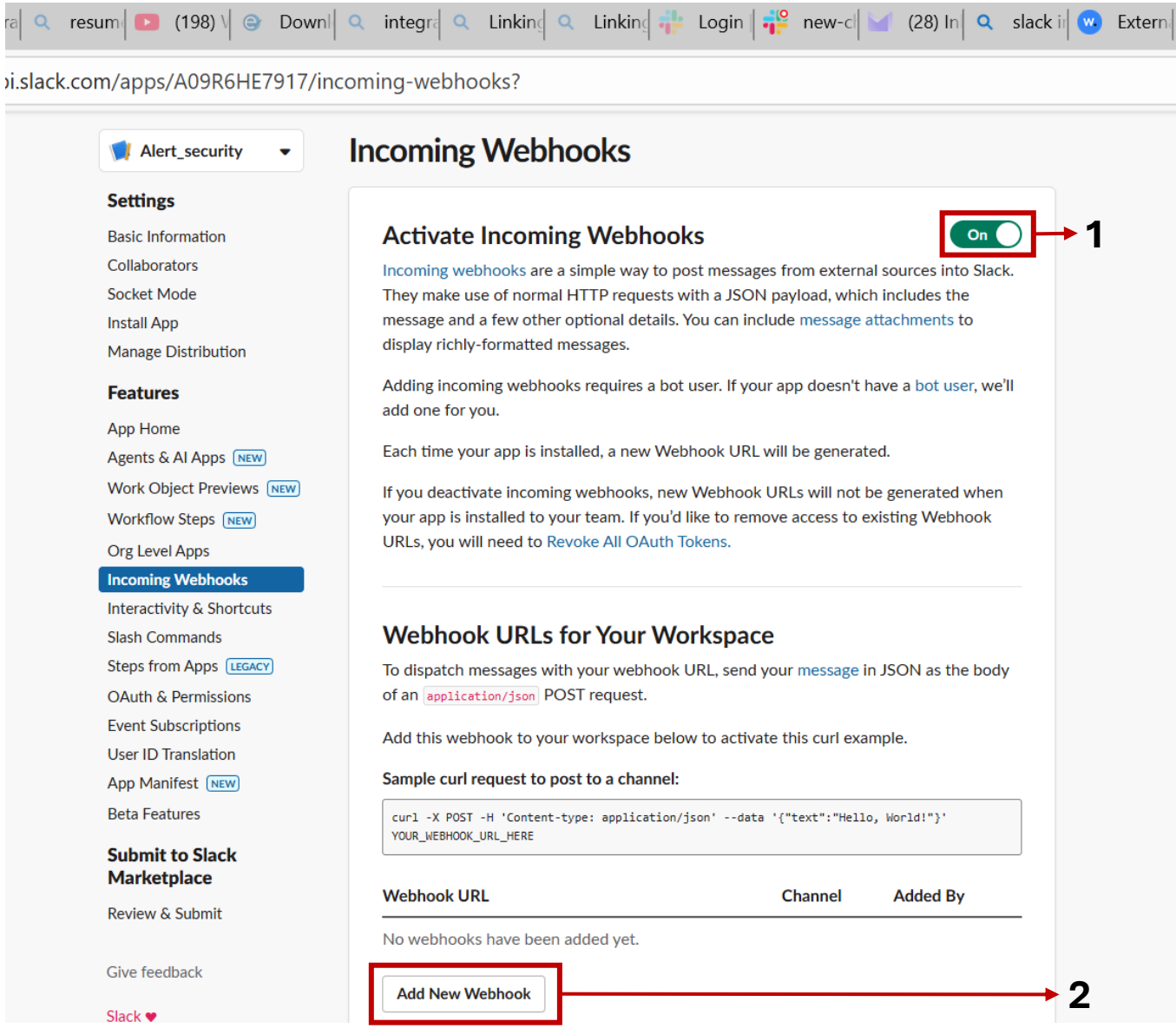


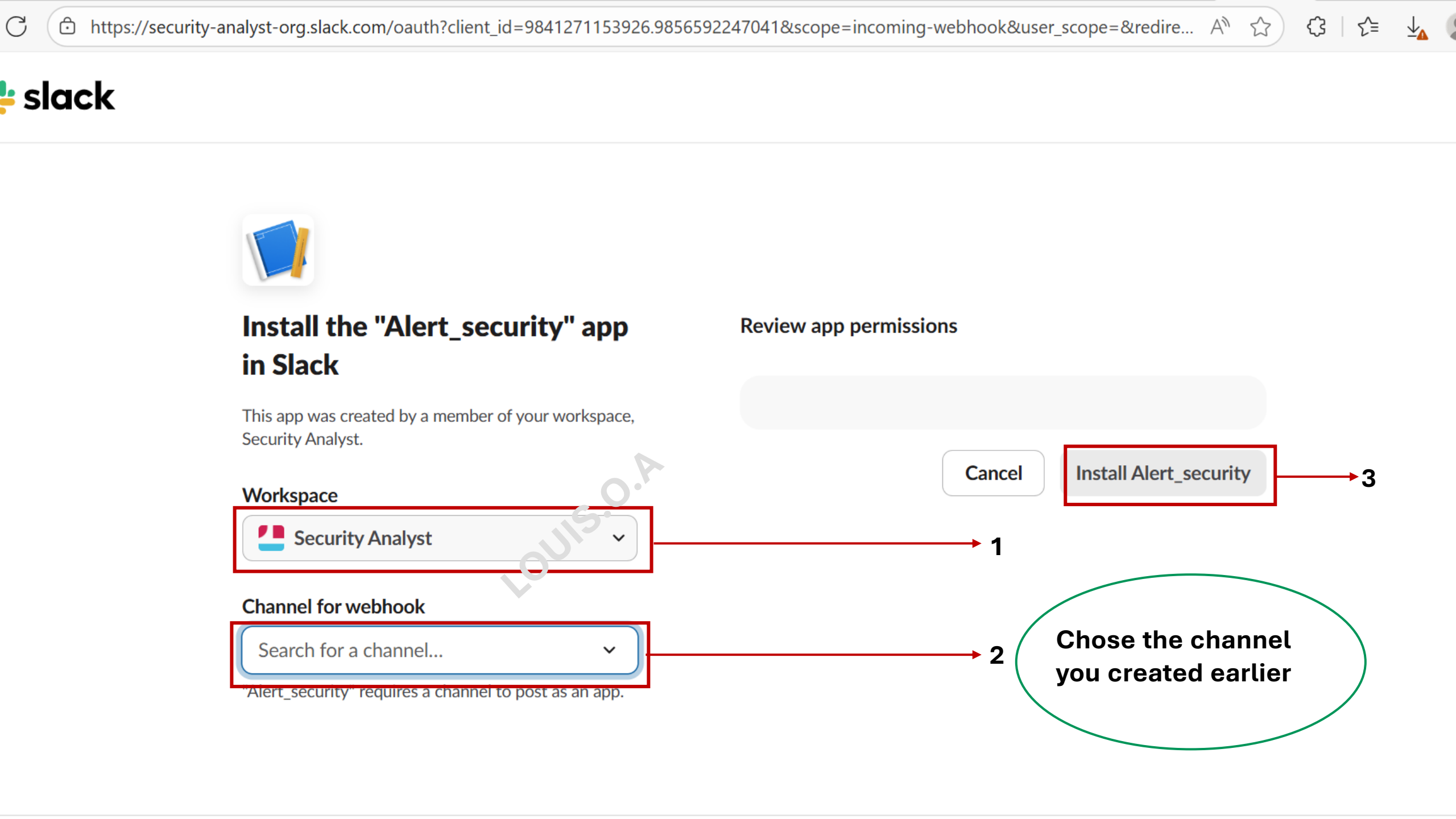
Visit https://docs.slack.dev/messaging/sending-messages-using-incoming-webhooks/ to generate Webhook Url




https://api.slack.com/apps?new_app=1
slack api
Documentation
Tutorials
Your Apps
Your Apps
Use our APIs to build an ap
create a pub
st for your workspace or
iscover it.
Your App Configuratior
Learn about tokens
Generate Token
Name app & choose workspace
App Name
e.g. Super Service
35
Don't worry - you'll be able to change this later.
Pick a workspace to develop your app in:
Select a workspace
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
Create App
1
2
3


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 secret. Please don't share your app credentials with anyone, include them in public code repositories, or store them in insecure ways.
App ID
A09R6GP561X
Date of App Creation
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 Ch
LOUIS.O.A


i.slack.com/apps/A09R6HE7917/incoming-webhooks?
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
Slack
Incoming Webhooks
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


https://security-analyst-org.slack.com/oauth?client_id=9841271153926.9856592247041&scope=incoming-webhook&user_scope=&redire...
slack
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
3
1
2
Chose the channel you created earlier
LOUIS.O.A

https://api.slack.com/apps/A09R6HE7917/incoming-webhooks?success=1

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.

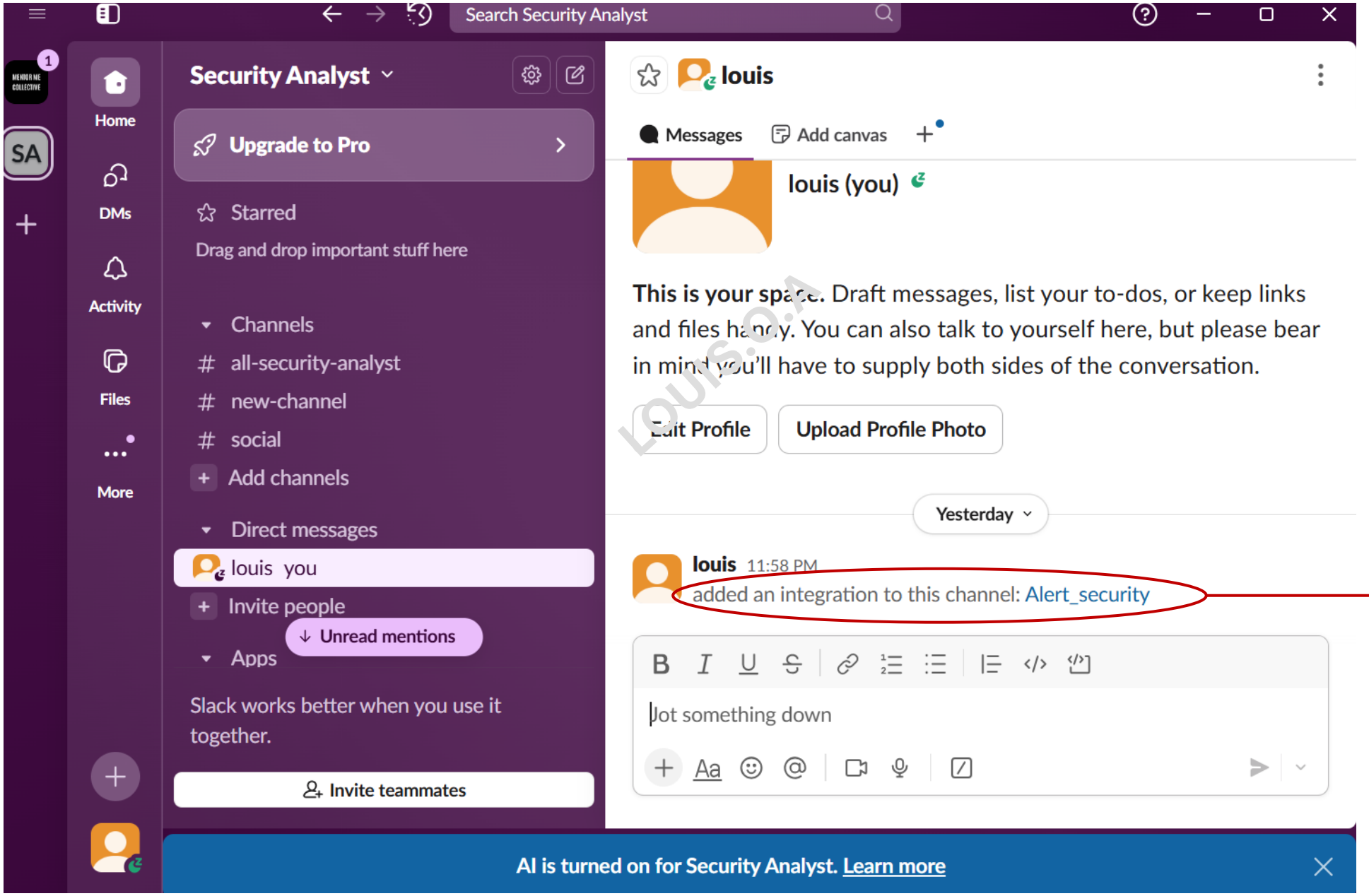
Sample curl request to post to a channel:

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

Copy

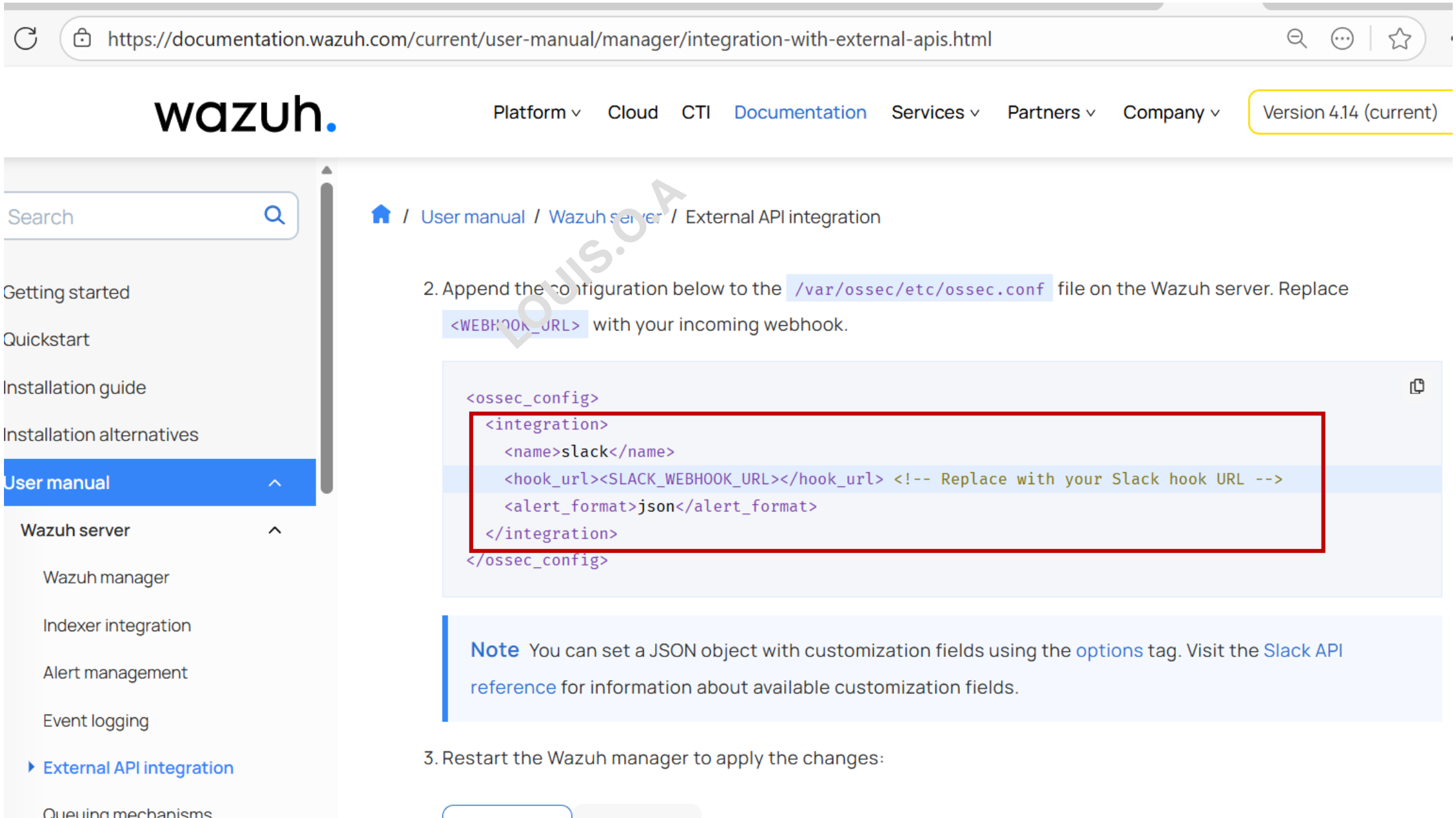
Webhook URL	Channel	Added By
https://hooks.slack.com/services/T09QR7 Copy	louis	louis Nov 4, 2025

Copy the Webhook URL to be used in ossec.conf

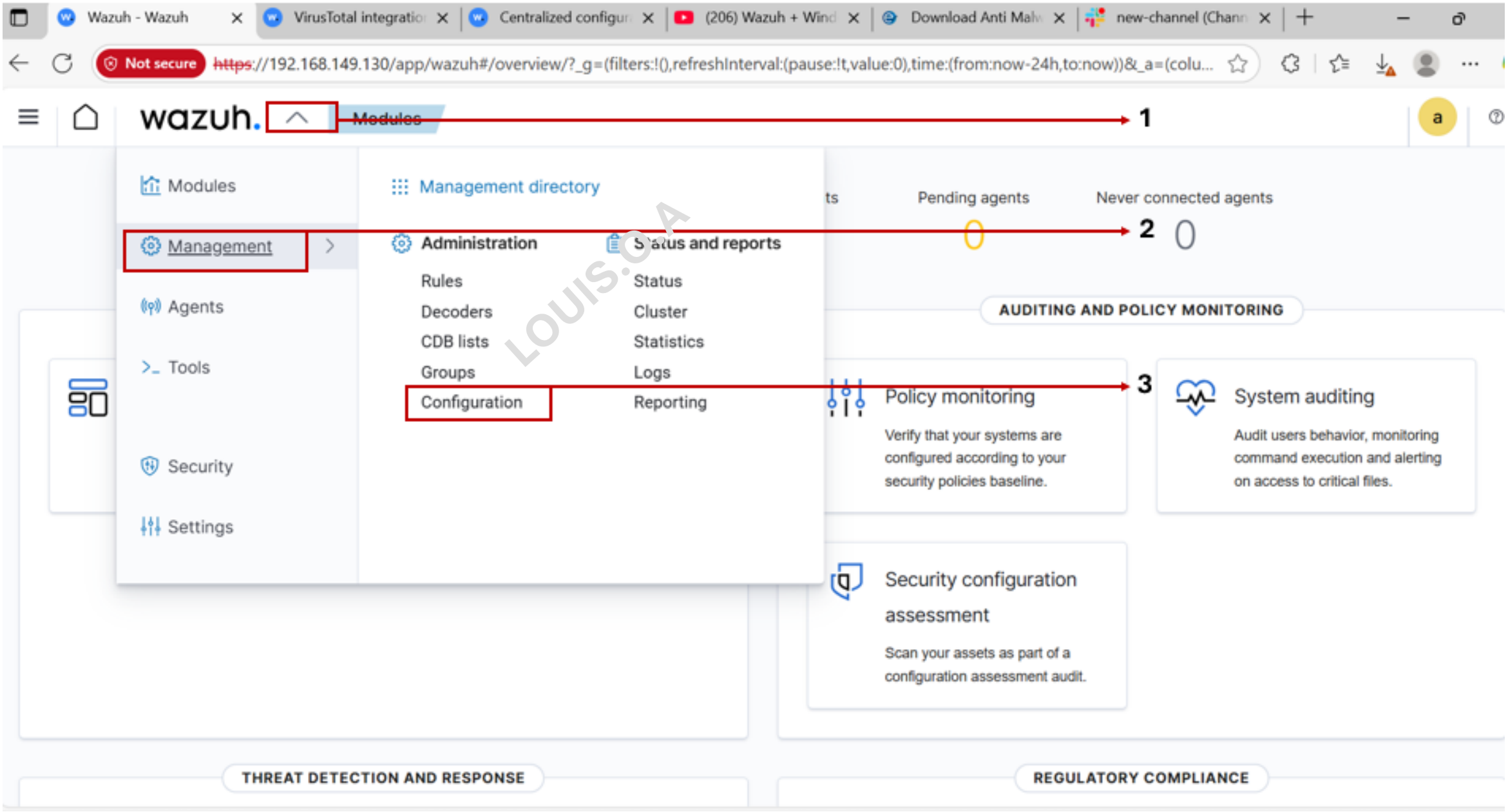


This shows it has been created

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



Open Wazuh-Server to configure slack alert



Configuration

Refresh | Edit configuration

Main configurations

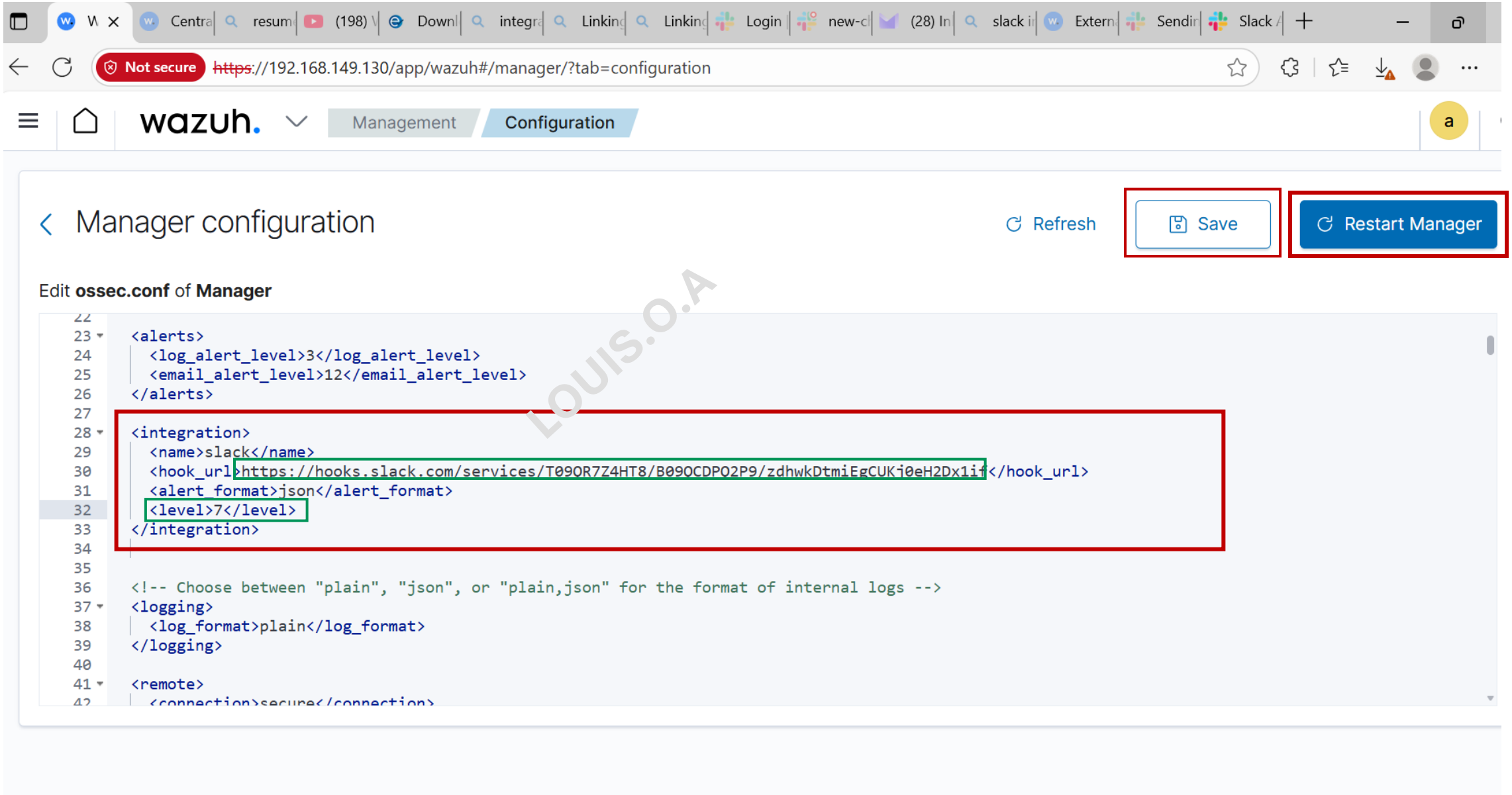
Name	Description
Global Configuration	Global and remote settings
Cluster	Master node configuration
Registration Service	Automatic agent registration service

Alerts and output management

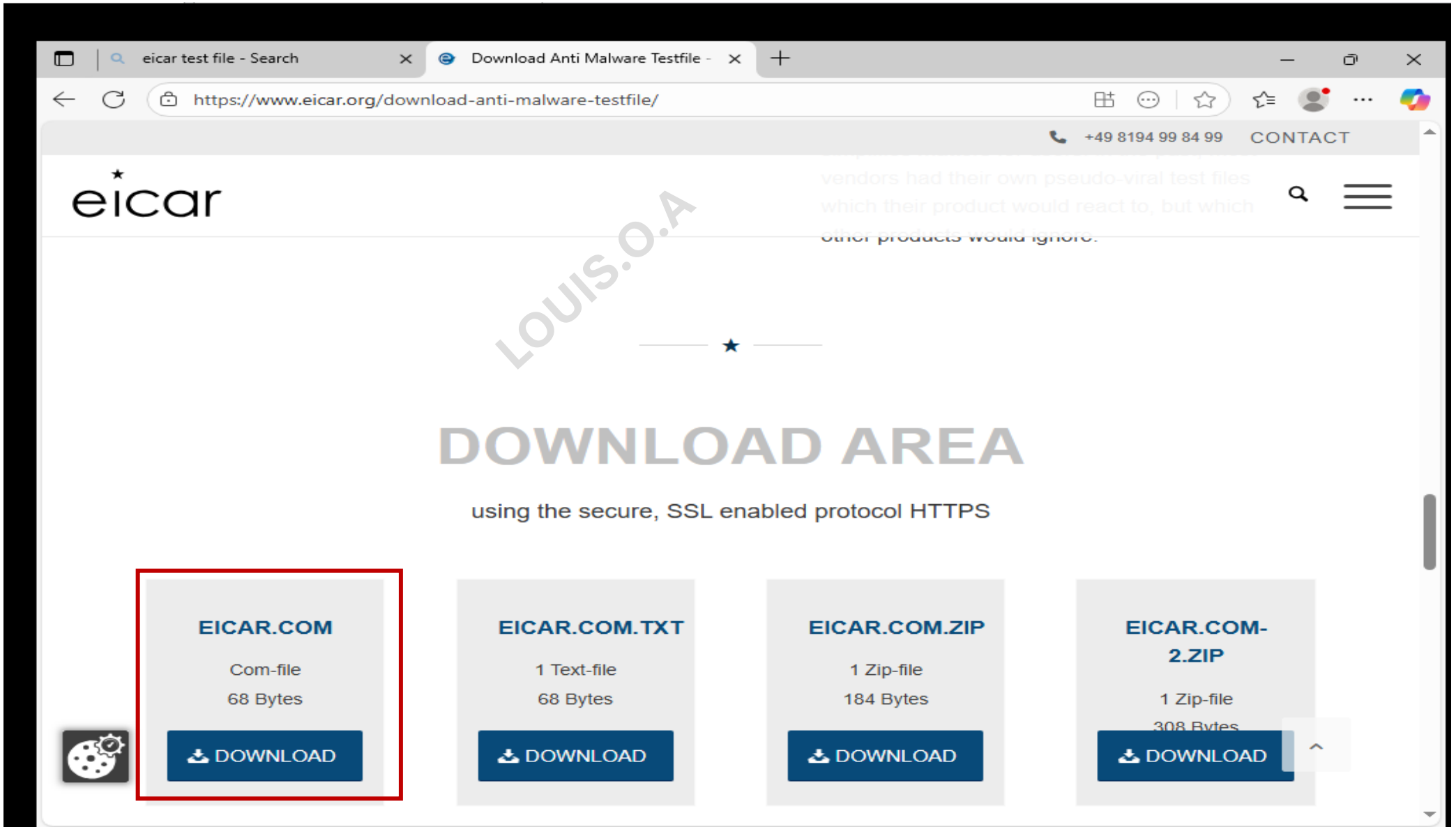
Name	Description
Alerts	Settings related to the alerts and their format
Integrations	Slack, VirusTotal and PagerDuty integrations with external APIs

Auditing and policy monitoring

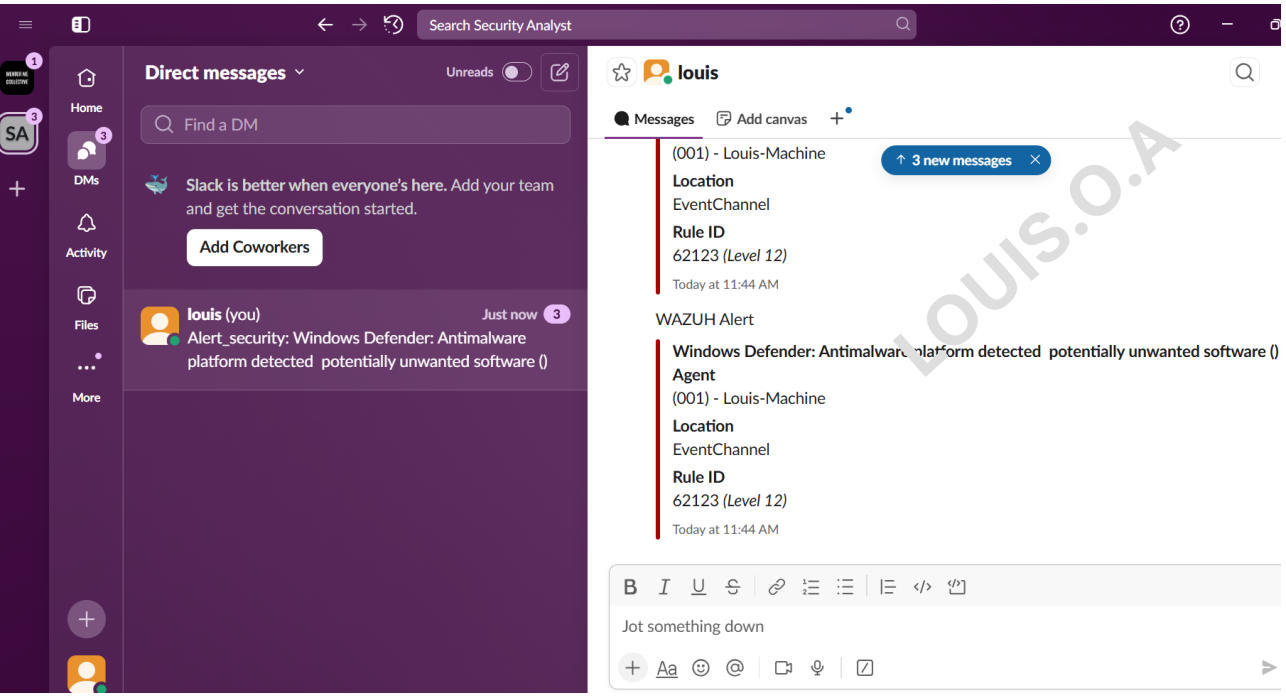
Name	Description
Policy monitoring	Configuration to ensure compliance with security policies, standards and hardening guides

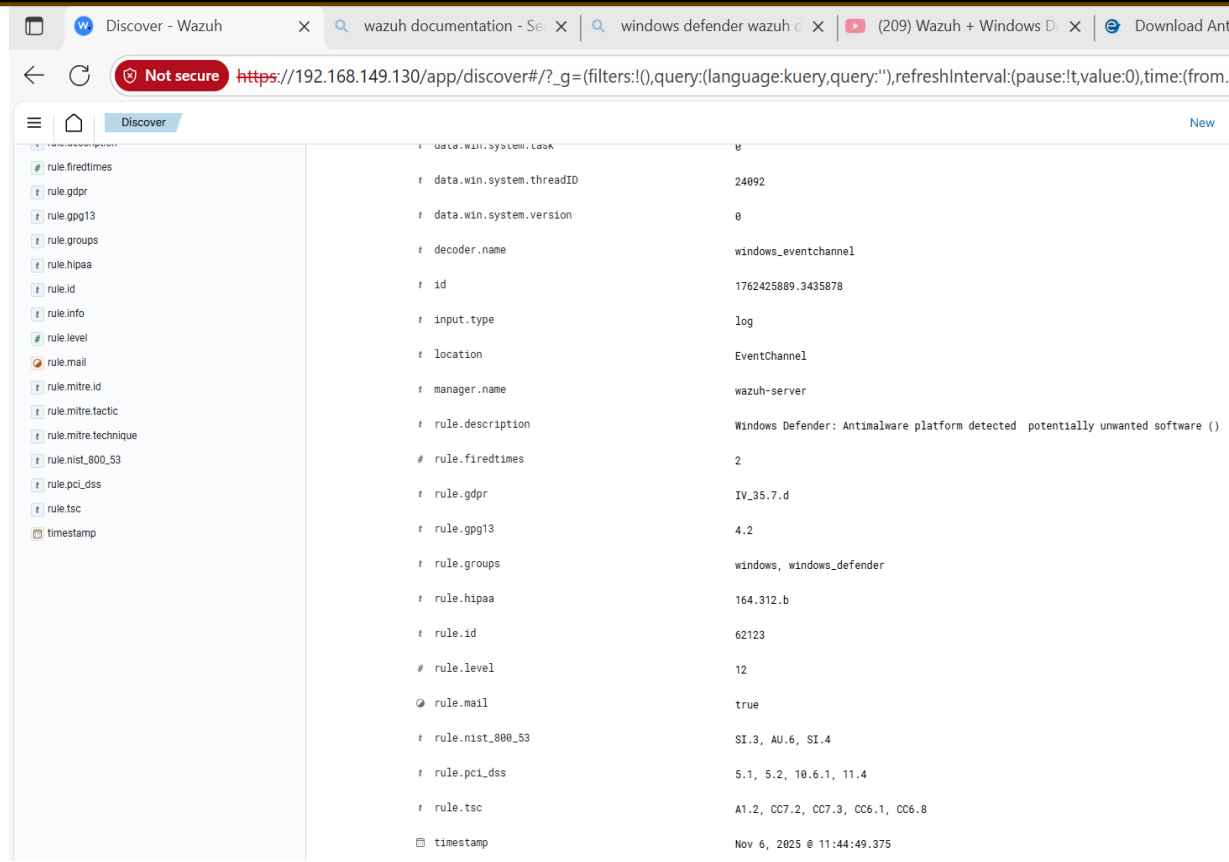

Not secure
https://192.168.149.130/app/wazuh#/manager/?tab=configuration
wazuh.
Management
Configuration
a
Manager configuration
Refresh
Save
Restart Manager
Edit ossec.conf of Manager
LOUIS.O.A
<alerts>
<log_alert_level>3</log_alert_level>
<email_alert_level>12</email_alert_level>
</alerts>
<integration>
<name>slack</name>
<hook_url>https://hooks.slack.com/services/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</hook_url>
<alert_format>json</alert_format>
<level>7</level>
</integration>
<!-- Choose between "plain", "json", or "plain,json" for the format of internal logs -->
<logging>
<log_format>plain</log_format>
</logging>
<remote>

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.

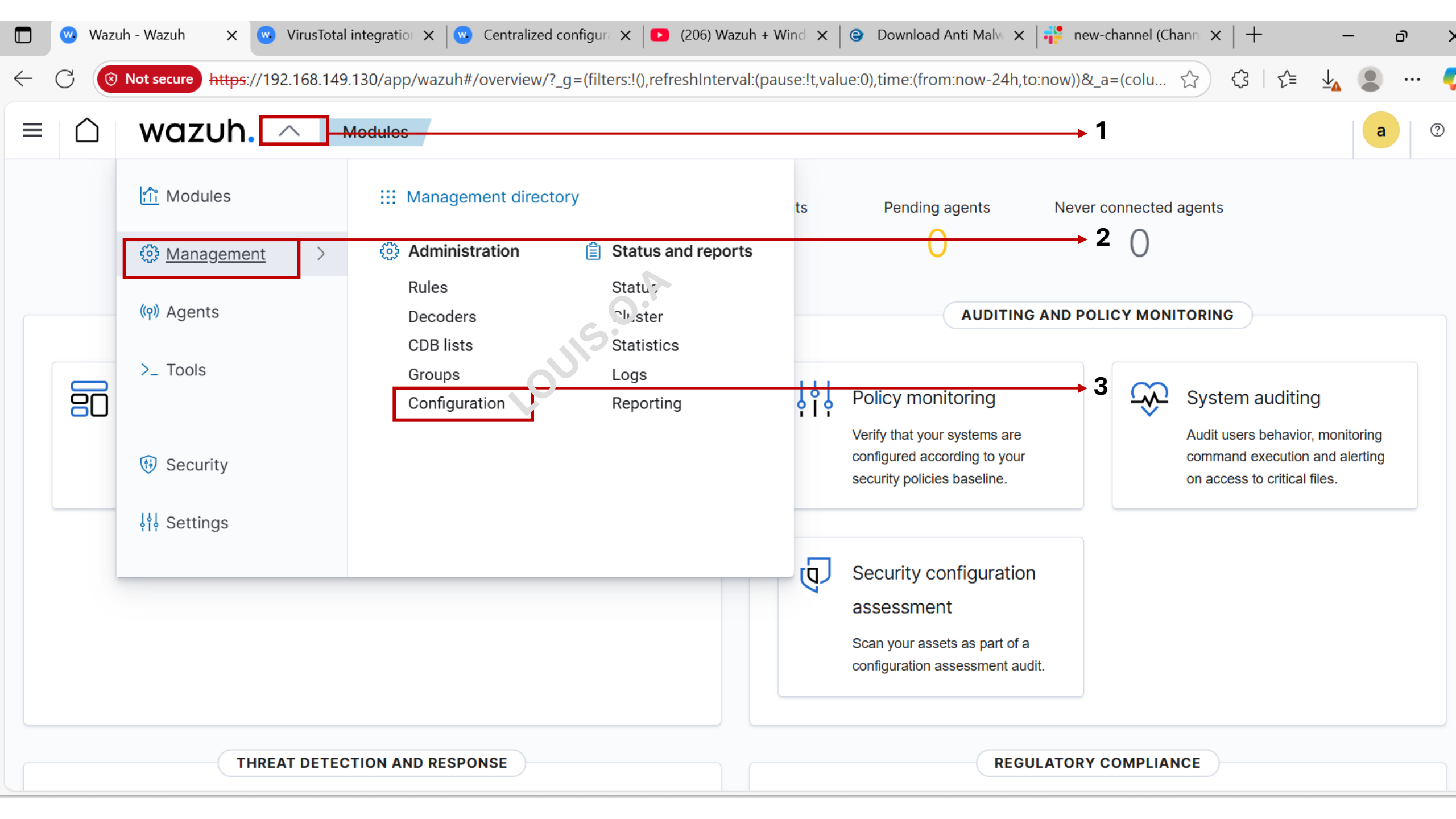


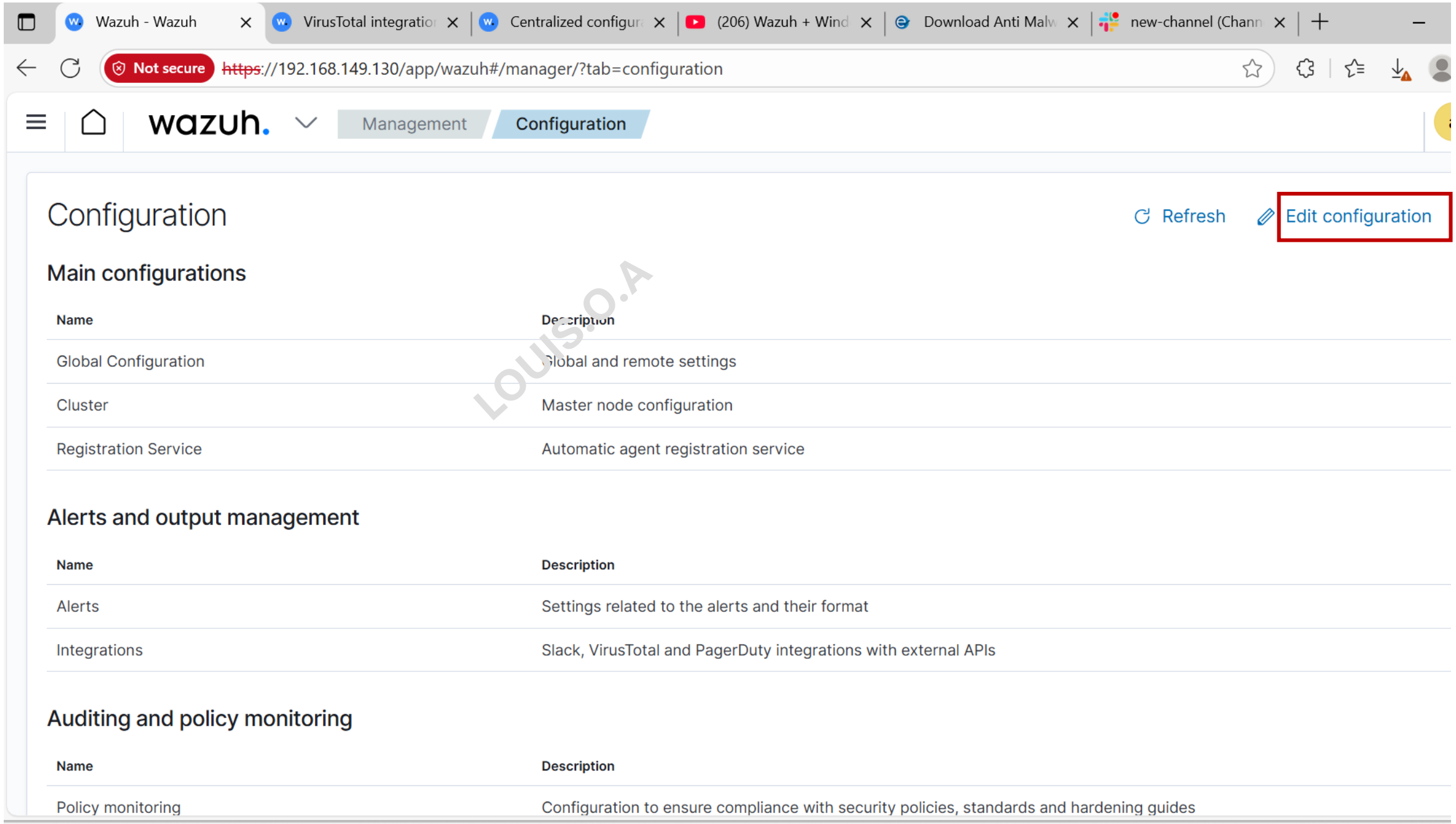
Malware detected & triggered on wazuh, message sent to Slack Channel immediately



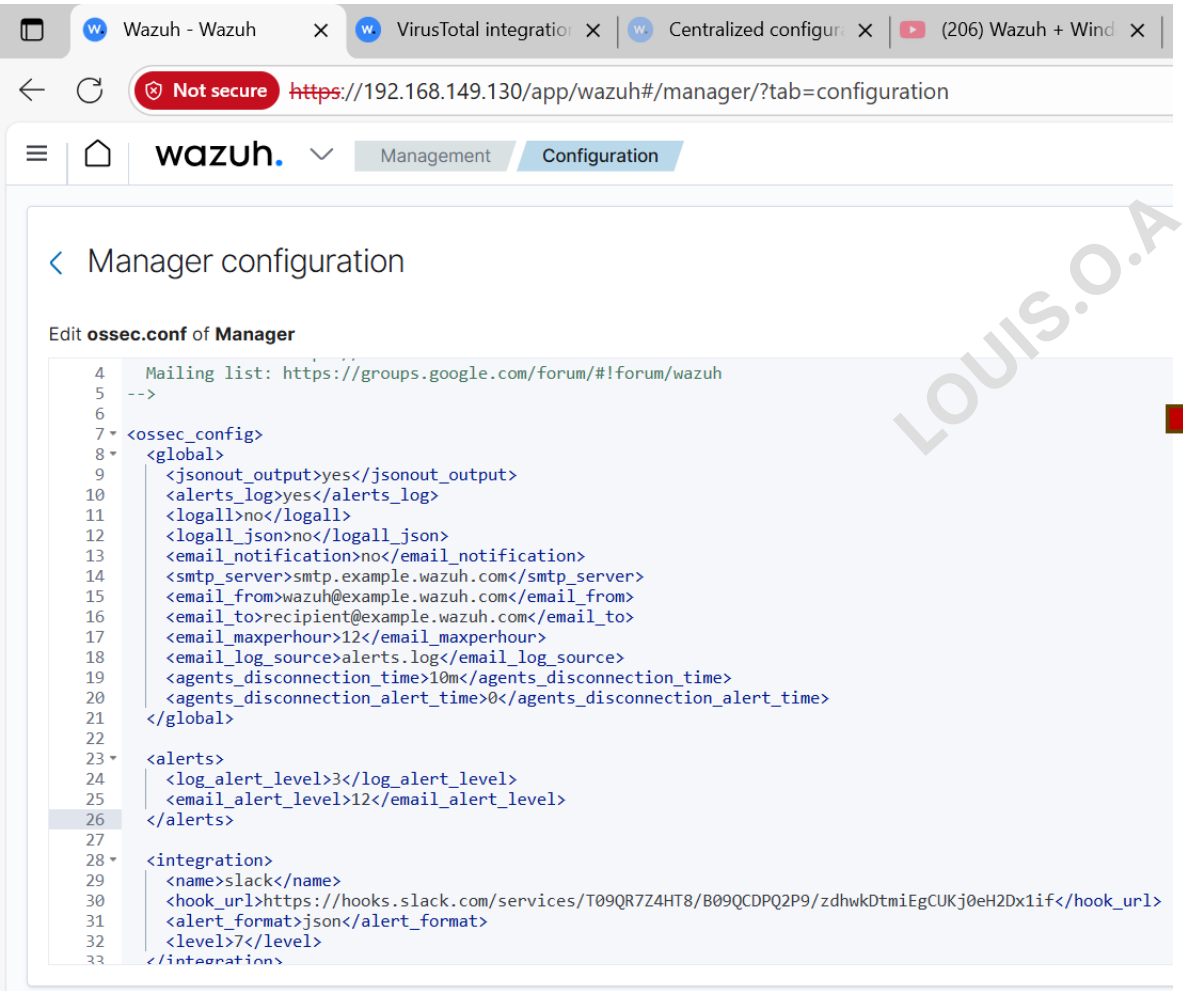


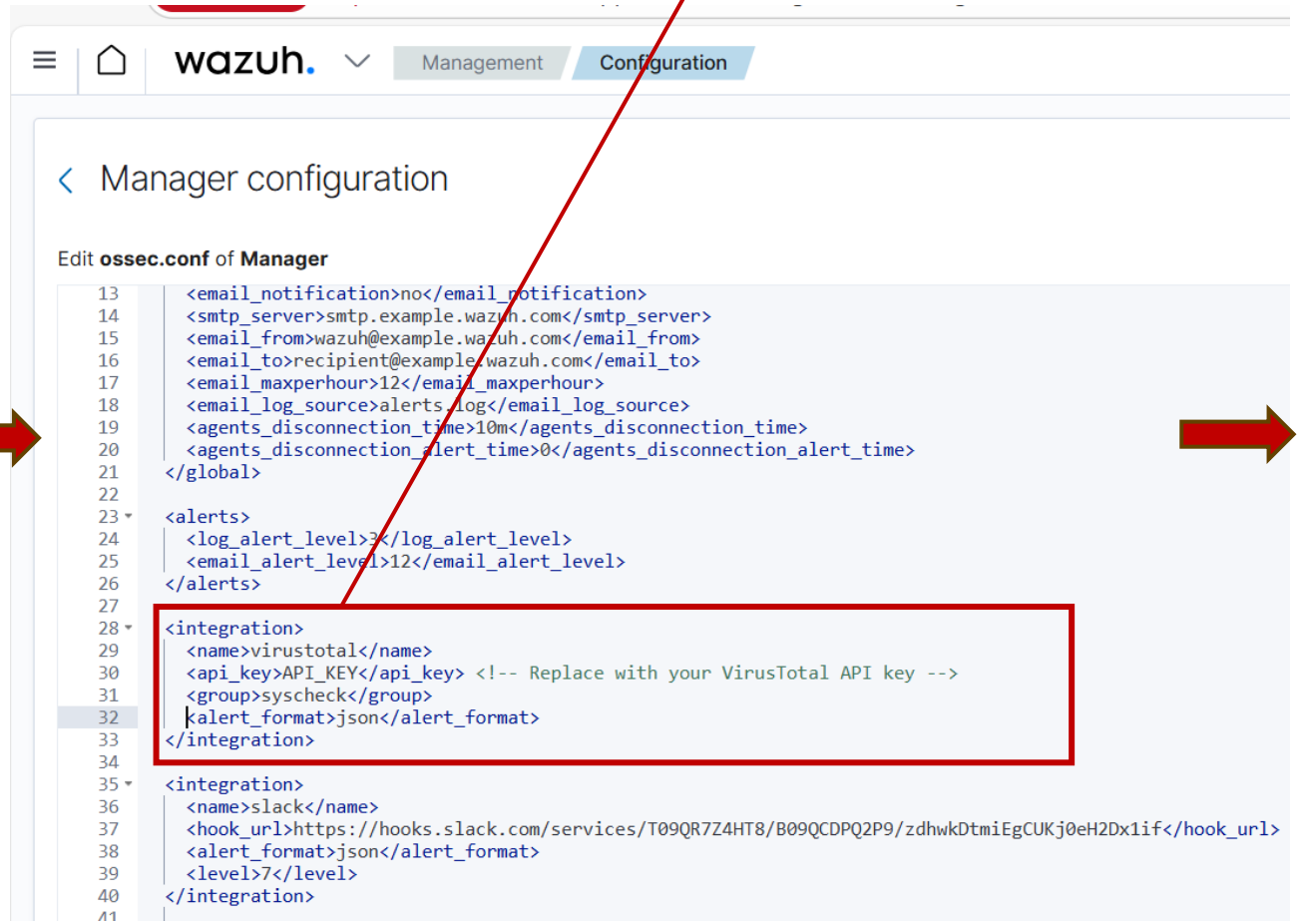
integration configuration of VirusTotal with wazuh


Wazuh - Wazuh
VirusTotal integratio
Centralized configur
(206) Wazuh + Wind
Download Anti Malw
new-channel (Chann
Not secure
https://192.168.149.130/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(colu...
wazuh.
Modules
a
1
Modules
Management
Agents
Tools
Security
Settings
Management directory
Administration
Rules
Decoders
CDB lists
Groups
Configuration
Status and reports
Statistics
Logs
Reporting
2
Pending agents
0
Never connected agents
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.
THREAT DETECTION AND RESPONSE
REGULATORY COMPLIANCE


Wazuh - Wazuh
VirusTotal integratio
Centralized configur
(206) Wazuh + Wind
Download Anti Malw
new-channel (Chann
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





Insert the API KEY generated from VirusTotal

wazuh. Management Configuration

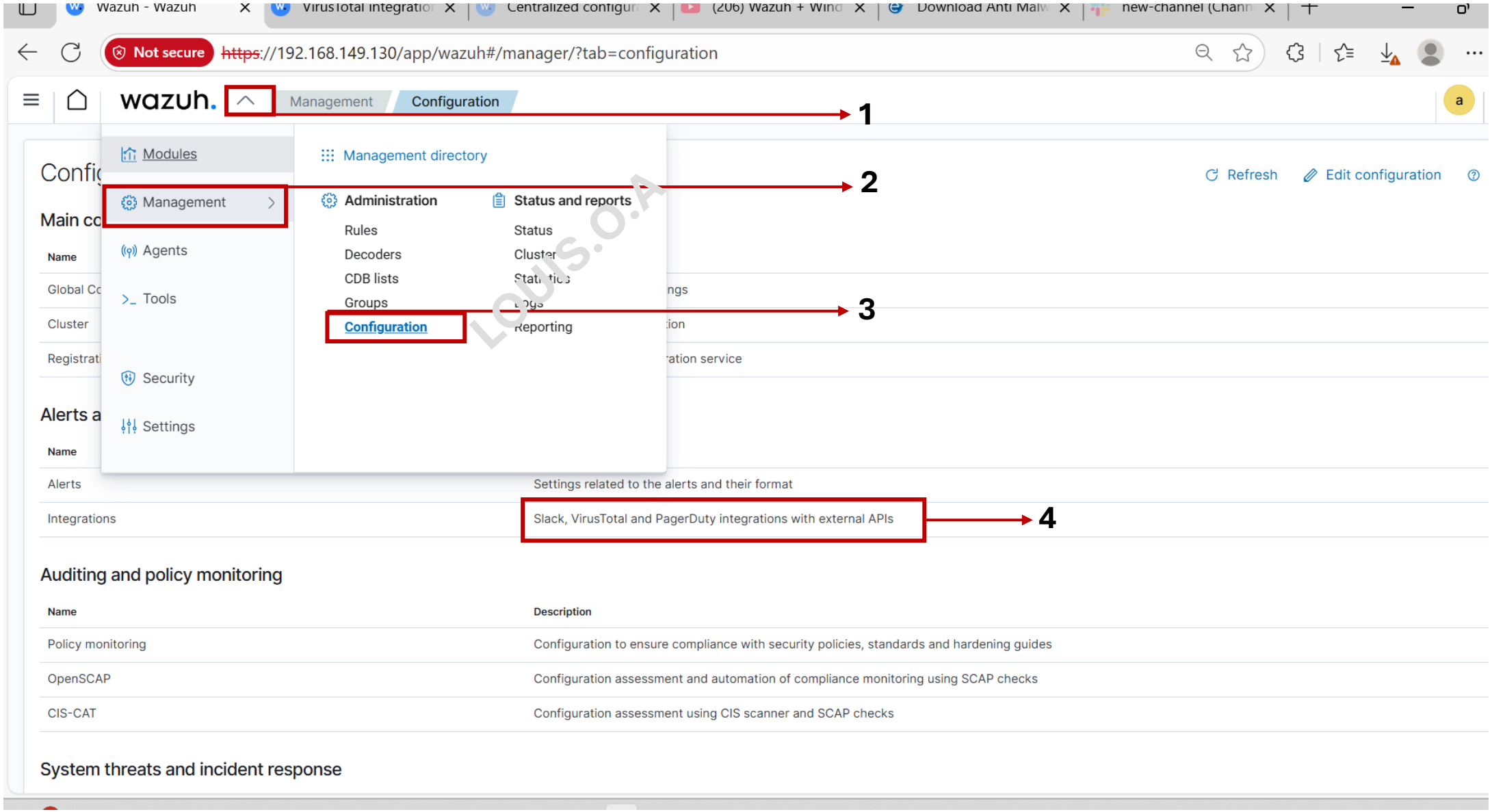
Manager configuration

Refresh | Save | Restart Manager

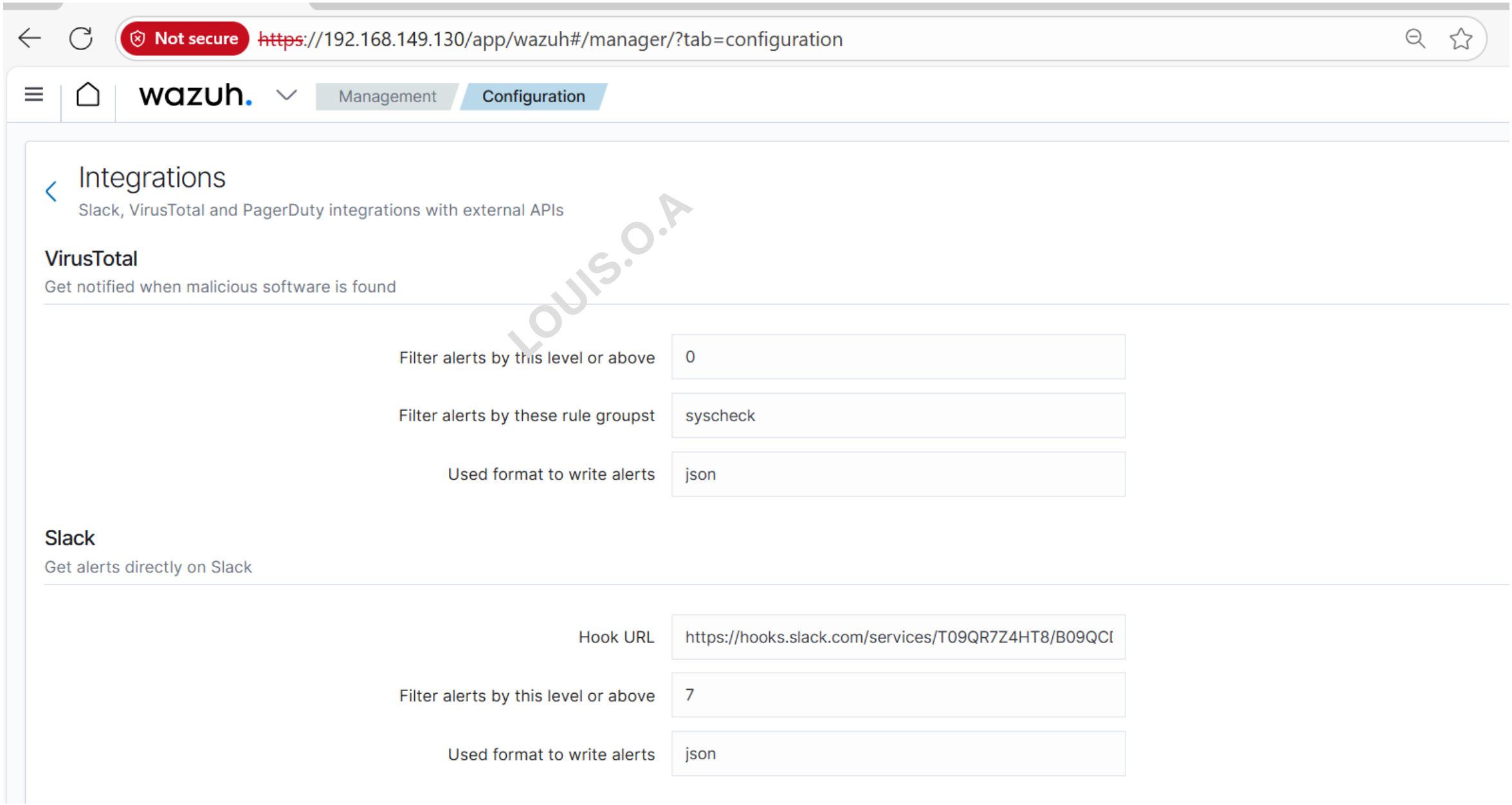
Edit **ossec.conf** of **Manager**

```
    <logall_json>no</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
  </global>

  <alerts>
    <log_alert_level>3</log_alert_level>
    <email_alert_level>12</email_alert_level>
  </alerts>

  <integration>
    <name>virustotal</name>
    <api_key>e4e0db60d1249937ee7eb74d7ef9e50ba77457fc8e831aa204d5b339037657fck/api_key> <!-- Replace with your VirusTotal API key -->
    <group>syscheck</group>
    <alert_format>json</alert_format>
  </integration>

  <integration>
    <name>slack</name>
    <hook_url>https://hooks.slack.com/services/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</hook_url>
    <alert_format>json</alert_format>
    <level>7</level>
  </integration>
```

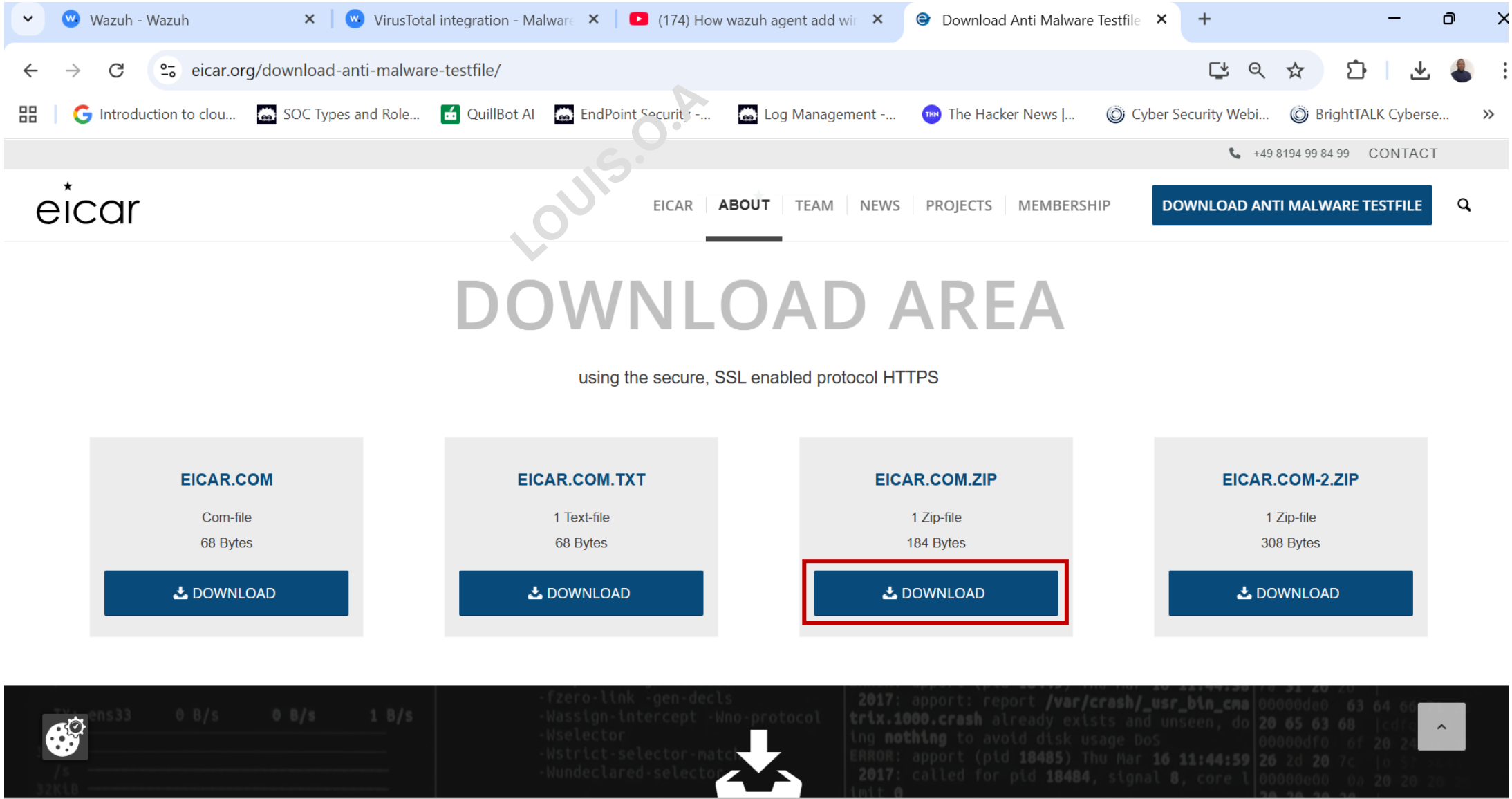
Check if VirusTotal has been integrated to wazuh



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



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



wazuh. Modules

a

Total agents	Active agents	Disconnected agents	Pending agents	Never connected agents
2	1	1	0	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.

MITRE ATT&CK

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.

Not secure https://192.168.149.130/app/wazuh#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=...

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

wazuh. Agents

a

STATUS

- Active (1)
- Disconnected (1)
- Pending (0)
- Never connected (0)

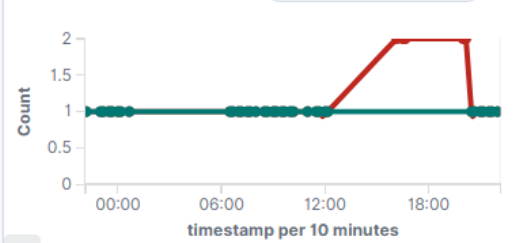
DETAILS

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

Last registered agent: virtualMachine

Most active agent: Louis-Machine

EVOLUTION



Agents (1)

Deploy new agent | Refresh | Export formatted

id!=000 and status=active | 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

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

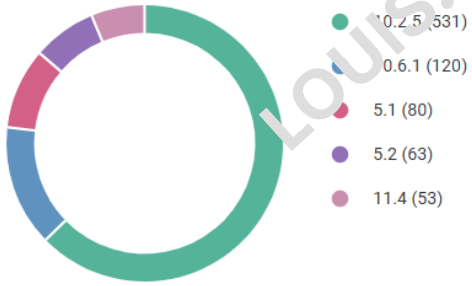
MITRE

Top Tactics

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

Compliance

PCI DSS



FIM: Recen

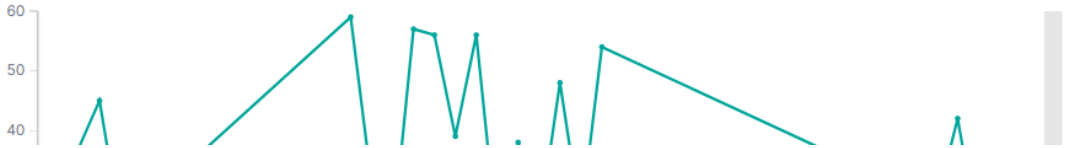
Time

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

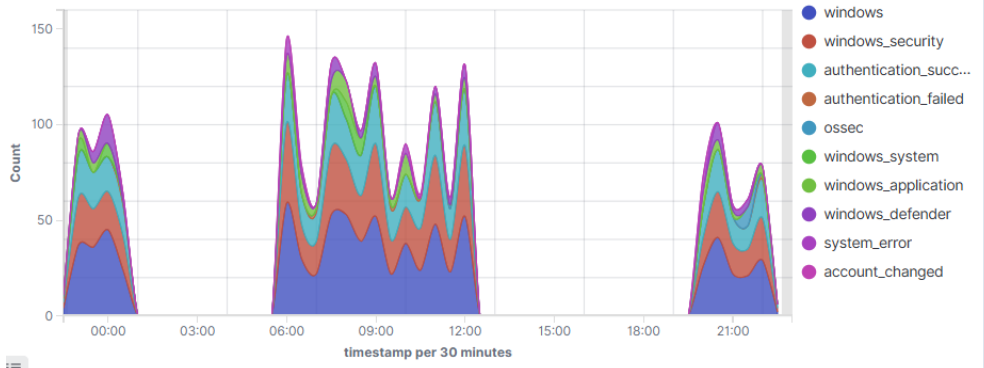
Dashboard | Events

Search

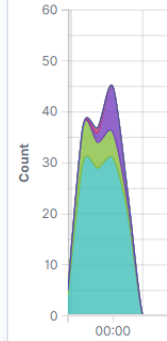
manager.name: wazuh-server | agent.id: 001 | + Add filter

Total	Level 12 or above alerts	Authentica
835	29	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

Available fields

- 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

816 hits

Nov 6, 2025 @ 22:19:01.967 - Nov 7, 2025 @ 22:19:01.967 Auto

Nov 7, 2025 @ 21:57:43.781	Logon failure - Unknown user or bad password.	5	60122
Nov 7, 2025 @ 21:57:42.619	Windows logon success.	3	60106
Nov 7, 2025 @ 21:56:15.370	Software Protection service scheduled successfully.	3	60642
Nov 7, 2025 @ 21:56:14.862	Windows logon success.	3	60106
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
Nov 7, 2025 @ 21:56:04.882	File added to the system.	5	554
Nov 7, 2025 @ 21:55:59.203	VirusTotal: Alert - c:\users\louis\desktop\wazuh file testing\6th nov.txt - No positives found	3	87104
Nov 7, 2025 @ 21:55:56.088	File deleted.	7	553
Nov 7, 2025 @ 21:55:41.833	Windows logon success.	3	60106
Nov 7, 2025 @ 21:55:37.579	Windows logon success.	3	60106
Nov 7, 2025 @ 21:48:31.185	Windows Defender: Antimalware platform performed an action to protect you from potentially unwanted software ().	3	62124
Nov 7, 2025 @ 21:48:26.179	Windows Defender: Antimalware platform detected potentially unwanted software ().	12	62123
Nov 7, 2025 @ 21:47:24.993	Windows logon success.	3	60106

- 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

0
/ 61

Community Score 1790

File distributed by Linux, Offensive Security and others.

Reanalyze Similar More

e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

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

Size
0 B

Last Analysis Date
3 minutes ago

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

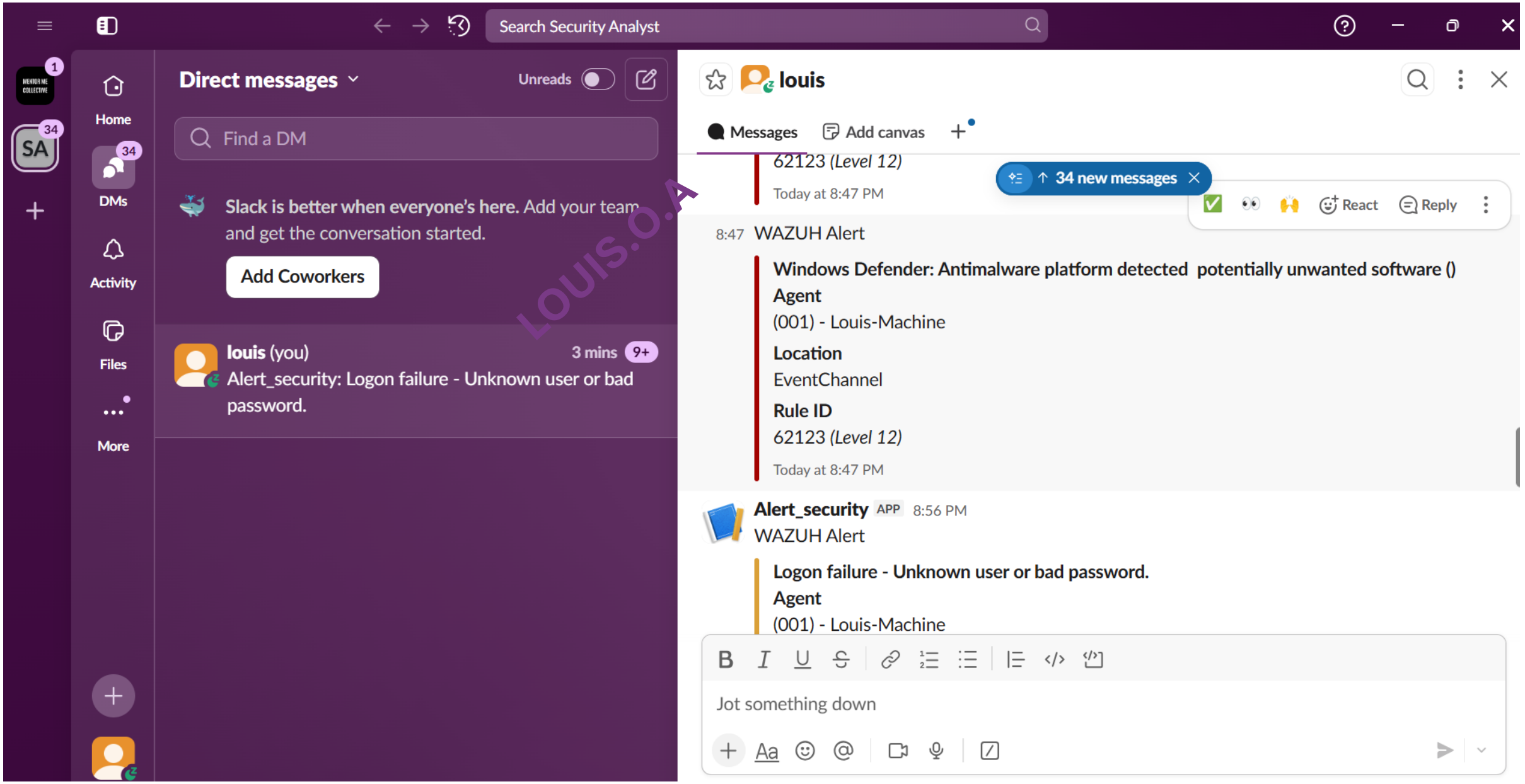
CRITICAL 0 HIGH 0 MEDIUM 1 LOW 0

⚠ Matches rule Suspicious History File Operations by Mikhail Larin, oscd.community at Sigma Integrated Rule Set (GitHub)

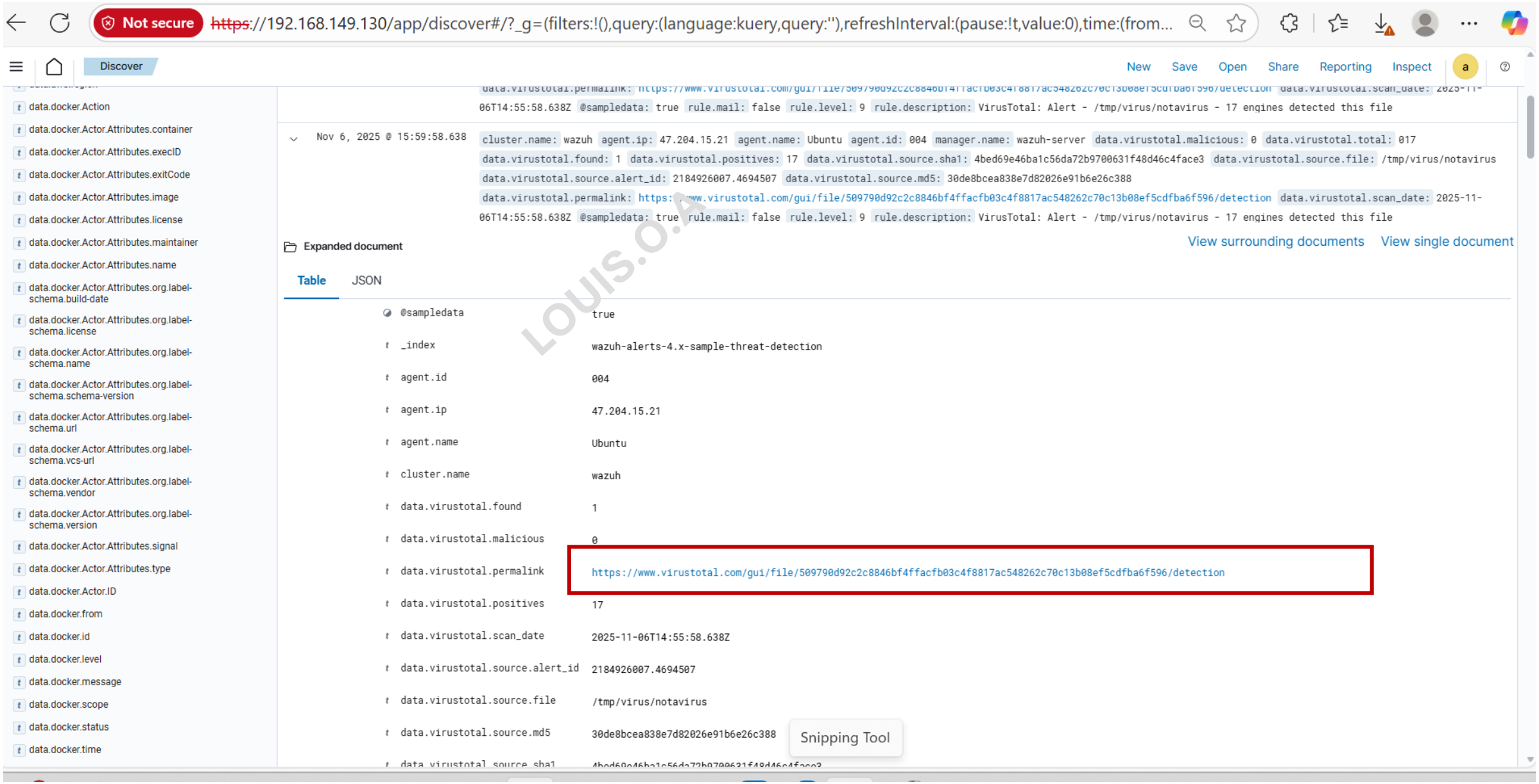
↳ *Detects commandline operations on shell history files*

Crowdsourced IDS rules

Slack also got the alert notification of the flagged malicious activity



Another Alert.....



https://www.virustotal.com/gui/file/509790d92c2c8846bf4ffacfb03c4f8817ac548262c70c13b08ef5cdfba6f596/detection

509790d92c2c8846bf4ffacfb03c4f8817ac548262c70c13b08ef5cdfba6f596

Sign in Sign up

67 / 72

Community Score -42

67/72 security vendors flagged this file as malicious

Reanalyze Similar More

509790d92c2c8846bf4ffacfb03c4f8817ac548262c70c13b08ef5cdfba6f596

AutoRun.exe

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

Size 3.12 MB

Last Analysis Date 5 months ago

EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced 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