Ransomware Protection on Windows Server

Introduction

Ransomware attacks encrypt or lock user files and demand ransom for recovery. These attacks spread very quickly and can cause serious data loss and service downtime.
In this project, I implemented a ransomware detection and mitigation setup using **Wazuh**. The goal was to detect suspicious file activity on a Windows Server system and automatically respond before major damage occurs.

What I Achieved

Using Wazuh, I successfully:

- Monitored critical user folders for ransomware-like behavior
- Detected suspicious file changes in near real time
- Removed malicious files automatically using Active Response
- Built a base for blocking attacker IPs and isolating compromised systems

Environment Setup

- **Wazuh Manager:** Ubuntu Desktop
- **Wazuh Agent:** Windows Server 2022

Pre-requisites

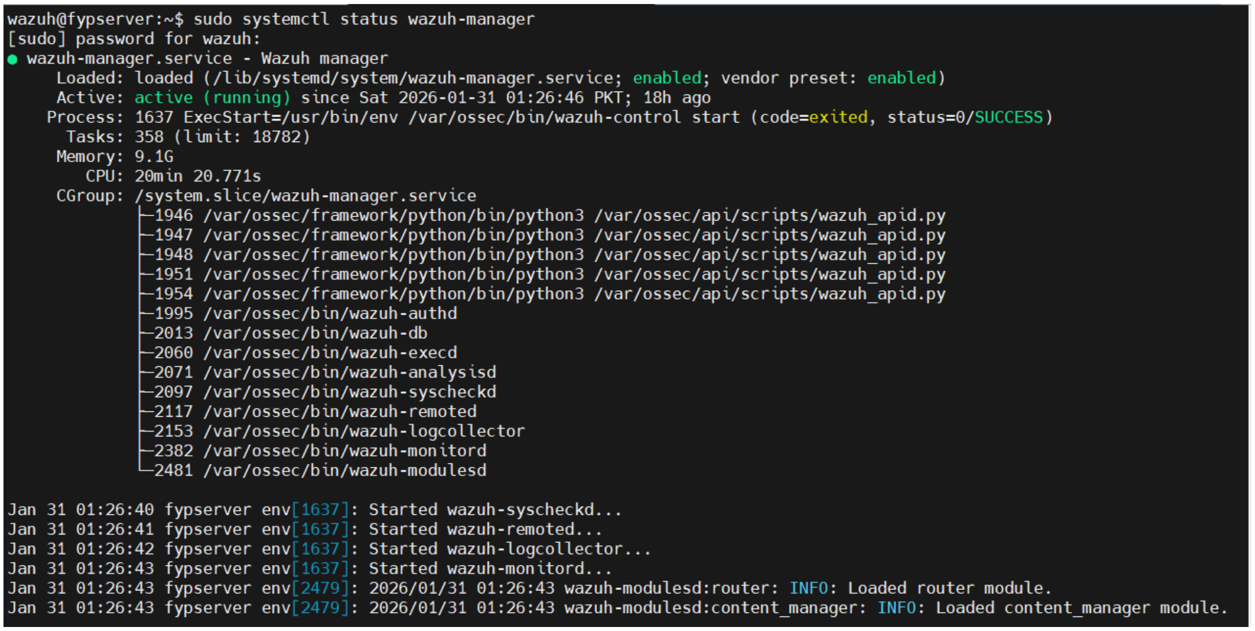
Before starting, I ensured:

- Wazuh Manager was installed and running on Ubuntu
- Wazuh Agent was installed on Windows Server 2022
- Agent was successfully registered with the manager

- Required ports were open:
  - UDP 1514 (log communication)
  - TCP 1515 (agent registration)

To confirm manager status, I ran:

sudo systemctl status wazuh-manager

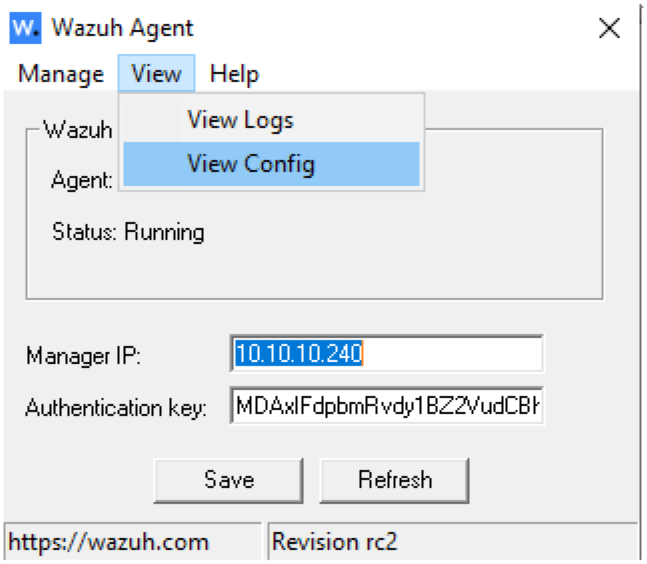


```
wazuh@fypserver:~$ sudo systemctl status wazuh-manager
[sudo] password for wazuh:
● wazuh-manager.service - Wazuh manager
     Loaded: loaded (/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2026-01-31 01:26:46 PKT; 18h ago
    Process: 1637 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
      Tasks: 358 (limit: 18782)
     Memory: 9.1G
        CPU: 20min 20.771s
     CGroup: /system.slice/wazuh-manager.service
             ├─1946 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
             ├─1947 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
             ├─1948 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
             ├─1951 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
             ├─1954 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
             ├─1995 /var/ossec/bin/wazuh-authd
             ├─2013 /var/ossec/bin/wazuh-db
             ├─2060 /var/ossec/bin/wazuh-execd
             ├─2071 /var/ossec/bin/wazuh-analysisd
             ├─2097 /var/ossec/bin/wazuh-syscheckd
             ├─2117 /var/ossec/bin/wazuh-remoted
             ├─2153 /var/ossec/bin/wazuh-logcollector
             ├─2382 /var/ossec/bin/wazuh-monitord
             └─2481 /var/ossec/bin/wazuh-modulesd

Jan 31 01:26:40 fypserver env[1637]: Started wazuh-syscheckd...
Jan 31 01:26:41 fypserver env[1637]: Started wazuh-remoted...
Jan 31 01:26:42 fypserver env[1637]: Started wazuh-logcollector...
Jan 31 01:26:43 fypserver env[1637]: Started wazuh-monitord...
Jan 31 01:26:43 fypserver env[2479]: 2026/01/31 01:26:43 wazuh-modulesd:router: INFO: Loaded router module.
Jan 31 01:26:43 fypserver env[2479]: 2026/01/31 01:26:43 wazuh-modulesd:content_manager: INFO: Loaded content_manager module.
```

Configure File Integrity Monitoring (FIM) on Windows Agent

First, I configured Wazuh to monitor user directories that are commonly targeted by ransomware.

1. On the Windows Server, I opened the Wazuh agent configuration file:



Agent:

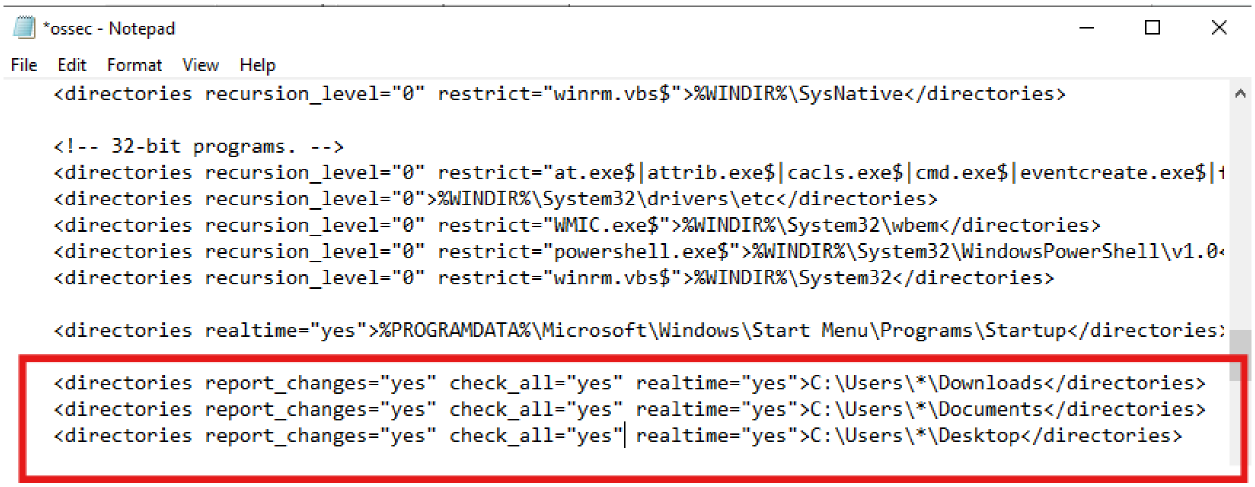
Status: Running

Manager IP: 10.10.10.240

Authentication key: MDAxlFdpbmRvdy1BZ2VudCBI

2. Inside the <syscheck> block, I added the following entries:

```
<directories realtime="yes">C:\Users\*\Downloads</directories>
<directories realtime="yes">C:\Users\*\Documents</directories>
<directories realtime="yes">C:\Users\*\Desktop</directories>
```



```
    <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\SysNative</directories>

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

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

    <directories report_changes="yes" check_all="yes" realtime="yes">C:\Users\*\Downloads</directories>
    <directories report_changes="yes" check_all="yes" realtime="yes">C:\Users\*\Documents</directories>
    <directories report_changes="yes" check_all="yes" realtime="yes">C:\Users\*\Desktop</directories>
```

This enabled real-time monitoring for file creation, modification, deletion, and renaming.

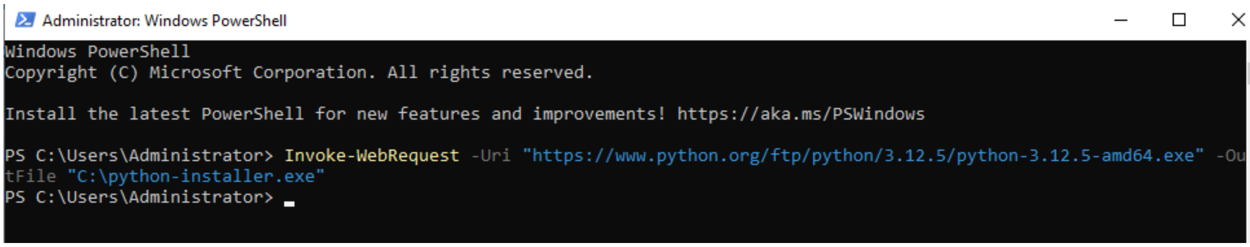
3. I saved the file and closed Notepad.

Step 2: Install Python on Windows Server

Next, I installed Python because the Active Response script depends on it.

1. I downloaded the Python installer using PowerShell:

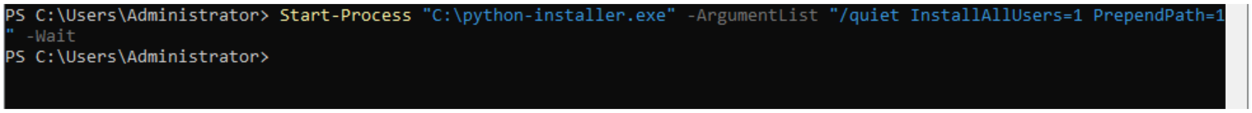
```
Invoke-WebRequest -Uri
"https://www.python.org/ftp/python/3.12.5/python-3.12.5-amd64.exe" -OutFile
"C:\python-installer.exe"
```



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> Invoke-WebRequest -Uri "https://www.python.org/ftp/python/3.12.5/python-3.12.5-amd64.exe" -Ou
tFile "C:\python-installer.exe"
PS C:\Users\Administrator> _
```

2. I installed Python silently for all users:

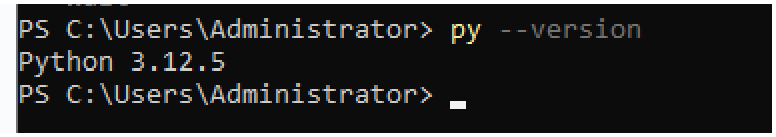
```
Start-Process "C:\python-installer.exe" -ArgumentList "/quiet InstallAllUsers=1
PrependPath=1" -Wait
```



```
PS C:\Users\Administrator> Start-Process "C:\python-installer.exe" -ArgumentList "/quiet InstallAllUsers=1 PrependPath=1
" -Wait
PS C:\Users\Administrator>
```

3. I verified the installation:

```
py --version
```



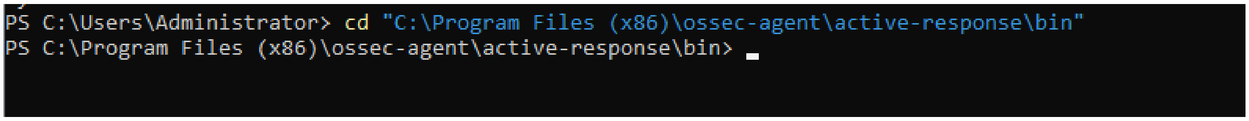
```
PS C:\Users\Administrator> py --version
Python 3.12.5
PS C:\Users\Administrator> _
```

Step 3: Create Wazuh Active Response Script

After Python installation, I created the Active Response script that removes malicious files detected via VirusTotal.

1. I navigated to the Active Response directory:

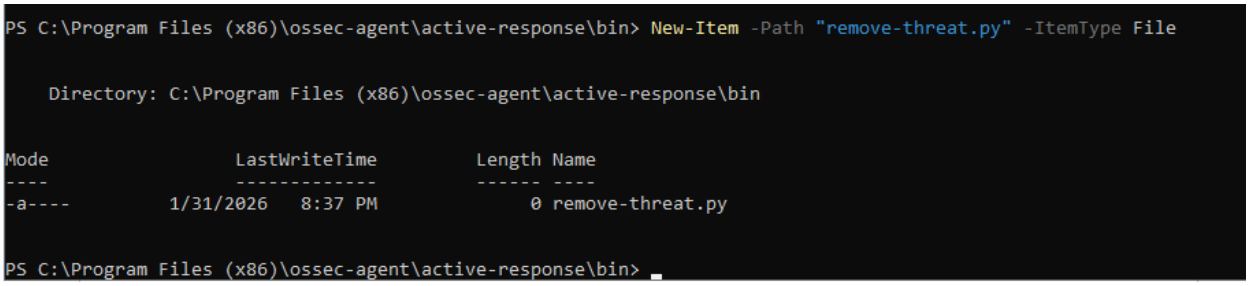
```
cd "C:\Program Files (x86)\ossec-agent\active-response\bin"
```



```
PS C:\Users\Administrator> cd "C:\Program Files (x86)\ossec-agent\active-response\bin"
PS C:\Program Files (x86)\ossec-agent\active-response\bin>
```

2. I created a new Python file:

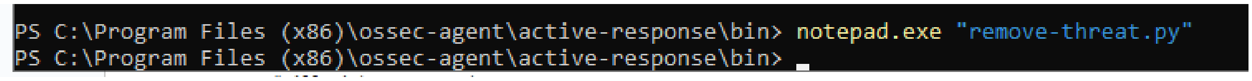
```
New-Item -Path "remove-threat.py" -ItemType File
```



```
PS C:\Program Files (x86)\ossec-agent\active-response\bin> New-Item -Path "remove-threat.py" -ItemType File


    Directory: C:\Program Files (x86)\ossec-agent\active-response\bin


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         1/31/2026   8:37 PM              0 remove-threat.py


PS C:\Program Files (x86)\ossec-agent\active-response\bin>
```

3. I opened the file in Notepad:

```
notepad.exe "remove-threat.py"
```



```
PS C:\Program Files (x86)\ossec-agent\active-response\bin> notepad.exe "remove-threat.py"
PS C:\Program Files (x86)\ossec-agent\active-response\bin>
```

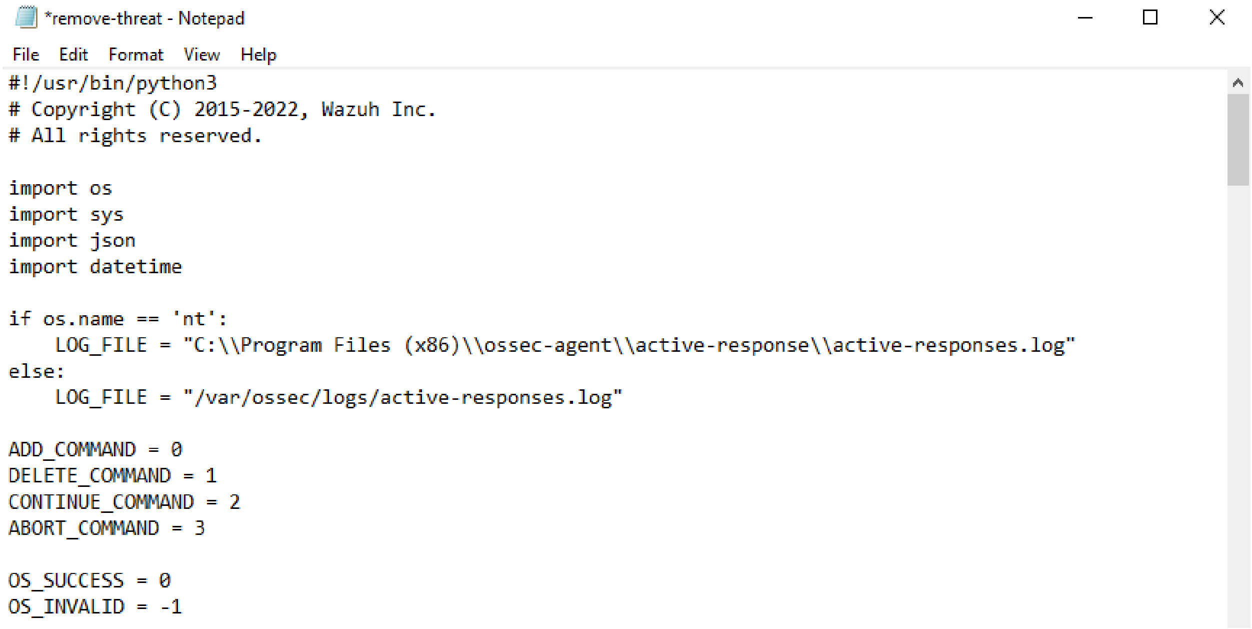
4. I pasted the following remove-threat.py code into the file and saved it.

```
// remove-threat.py

#!/usr/bin/python3

# Copyright (C) 2015-2022, Wazuh Inc.

# All rights reserved.


import os
import sys
import json
import datetime

if os.name == 'nt':
    LOG_FILE = "C:\\Program Files (x86)\\ossec-agent\\active-response\\active-responses.log"
else:
    LOG_FILE = "/var/ossec/logs/active-responses.log"

ADD_COMMAND = 0
DELETE_COMMAND = 1
CONTINUE_COMMAND = 2
ABORT_COMMAND = 3

OS_SUCCESS = 0
OS_INVALID = -1

class message:
    def __init__(self):
        self.alert = ""
        self.command = 0

def write_debug_file(ar_name, msg):
    with open(LOG_FILE, mode="a") as log_file:
        log_file.write(str(datetime.datetime.now().strftime('%Y/%m/%d %H:%M:%S')) + " "
+ ar_name + ": " + msg +"\n")


def setup_and_check_message(argv):


    # get alert from stdin
    input_str = ""
    for line in sys.stdin:
        input_str = line
        break



    try:
        data = json.loads(input_str)
    except ValueError:
        write_debug_file(argv[0], 'Decoding JSON has failed, invalid input format')
        message.command = OS_INVALID
        return message

    message.alert = data

    command = data.get("command")
    if command == "add":
        message.command = ADD_COMMAND
    elif command == "delete":
        message.command = DELETE_COMMAND
    else:
        message.command = OS_INVALID
        write_debug_file(argv[0], 'Not valid command: ' + command)

    return message


def send_keys_and_check_message(argv, keys):

    # build and send message with keys
    keys_msg = json.dumps({"version": 1,"origin":{"name": argv[0],"module":"active-response"},"command":"check_keys","parameters":{"keys":keys}})

    write_debug_file(argv[0], keys_msg)

    print(keys_msg)
    sys.stdout.flush()

    # read the response of previous message
```

```
input_str = ""
while True:
    line = sys.stdin.readline()
    if line:
        input_str = line
        break

# write_debug_file(argv[0], input_str)

try:
    data = json.loads(input_str)
except ValueError:
    write_debug_file(argv[0], 'Decoding JSON has failed, invalid input format')
    return message

action = data.get("command")

if "continue" == action:
    ret = CONTINUE_COMMAND
elif "abort" == action:
    ret = ABORT_COMMAND
else:
    ret = OS_INVALID
```

```
        write_debug_file(argv[0], "Invalid value of 'command'")

    return ret

def main(argv):

    write_debug_file(argv[0], "Started")

    # validate json and get command
    msg = setup_and_check_message(argv)

    if msg.command < 0:
        sys.exit(OS_INVALID)

    if msg.command == ADD_COMMAND:
        alert = msg.alert["parameters"]["alert"]
        keys = [alert["rule"]["id"]]
        action = send_keys_and_check_message(argv, keys)

        # if necessary, abort execution
        if action != CONTINUE_COMMAND:

            if action == ABORT_COMMAND:
                write_debug_file(argv[0], "Aborted")
                sys.exit(OS_SUCCESS)
            else:
                write_debug_file(argv[0], "Invalid command")
                sys.exit(OS_INVALID)

        try:
            file_path = msg.alert["parameters"]["alert"]["data"]["virustotal"]["source"]["file"]
            if os.path.exists(file_path):
                os.remove(file_path)
            write_debug_file(argv[0], json.dumps(msg.alert) + " Successfully removed threat")
        except OSError as error:
            write_debug_file(argv[0], json.dumps(msg.alert) + "Error removing threat")



    else:
        write_debug_file(argv[0], "Invalid command")

    write_debug_file(argv[0], "Ended")

    sys.exit(OS_SUCCESS)

if __name__ == "__main__":
```

main(sys.argv)



```
#!/usr/bin/python3
# Copyright (C) 2015-2022, Wazuh Inc.
# All rights reserved.

import os
import sys
import json
import datetime

if os.name == 'nt':
    LOG_FILE = "C:\\Program Files (x86)\\ossec-agent\\active-response\\active-responses.log"
else:
    LOG_FILE = "/var/ossec/logs/active-responses.log"

ADD_COMMAND = 0
DELETE_COMMAND = 1
CONTINUE_COMMAND = 2
ABORT_COMMAND = 3

OS_SUCCESS = 0
OS_INVALID = -1
```

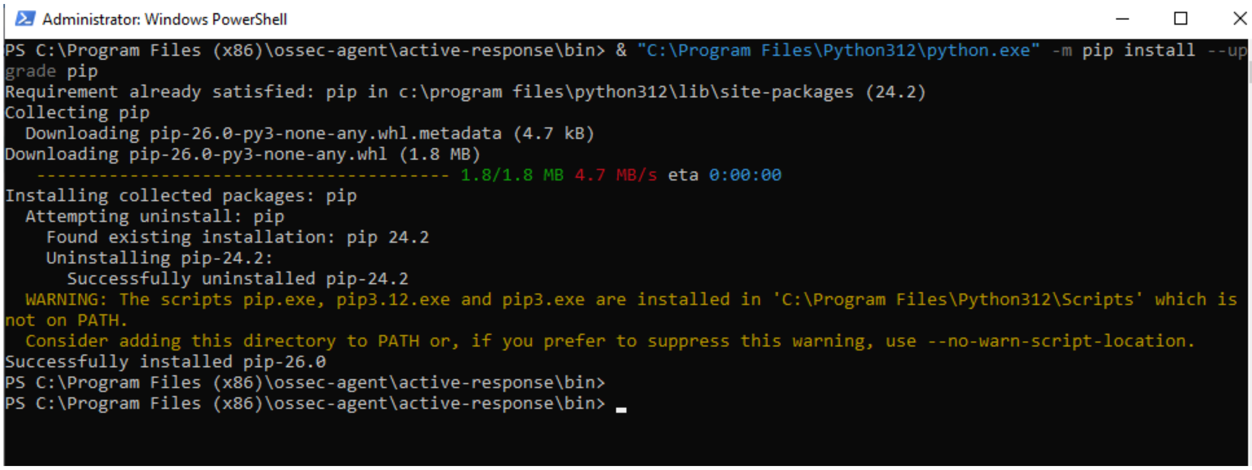
This script automatically deletes files flagged as malicious by Wazuh's VirusTotal integration.

Convert Python Script to Windows Executable

Since Wazuh Active Response works best with executables on Windows, I converted the script into an .exe file.

1. I upgraded pip:

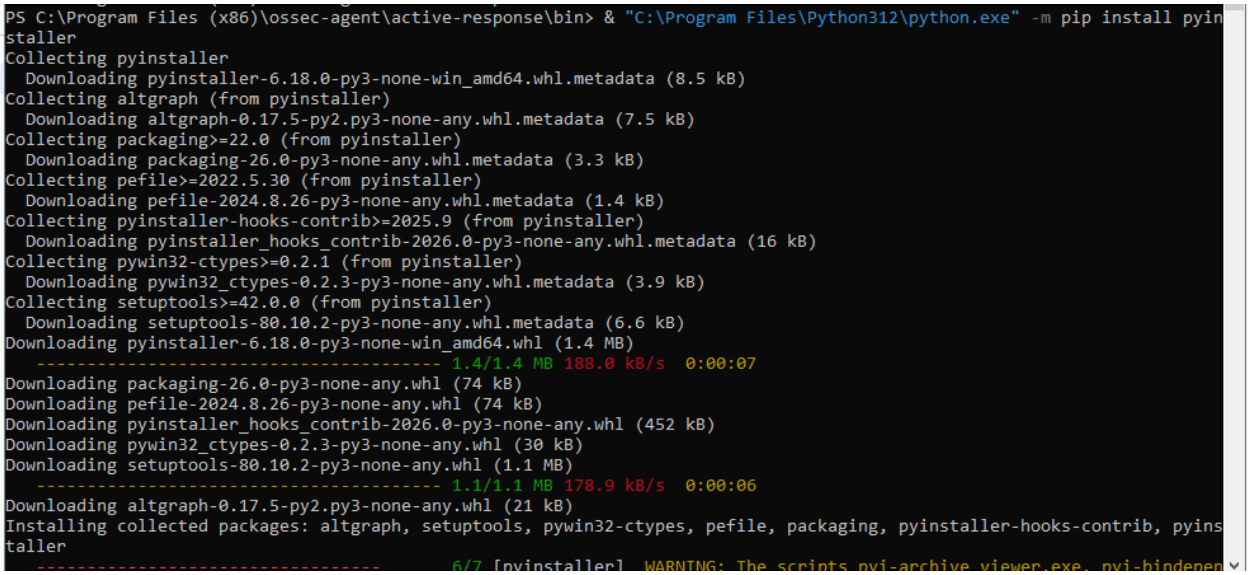
```
& "C:\Program Files\Python312\python.exe" -m pip install --upgrade pip
```



```
PS C:\Program Files (x86)\ossec-agent\active-response\bin> & "C:\Program Files\Python312\python.exe" -m pip install --up
grade pip
Requirement already satisfied: pip in c:\program files\python312\lib\site-packages (24.2)
Collecting pip
  Downloading pip-26.0-py3-none-any.whl.metadata (4.7 kB)
Downloading pip-26.0-py3-none-any.whl (1.8 MB)
   ---------------------------------------- 1.8/1.8 MB 4.7 MB/s eta 0:00:00
Installing collected packages: pip
  Attempting uninstall: pip
    Found existing installation: pip 24.2
    Uninstalling pip-24.2:
      Successfully uninstalled pip-24.2
  WARNING: The scripts pip.exe, pip3.12.exe and pip3.exe are installed in 'C:\Program Files\Python312\Scripts' which is
not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
Successfully installed pip-26.0
PS C:\Program Files (x86)\ossec-agent\active-response\bin>
PS C:\Program Files (x86)\ossec-agent\active-response\bin> _
```

2. I installed PyInstaller:

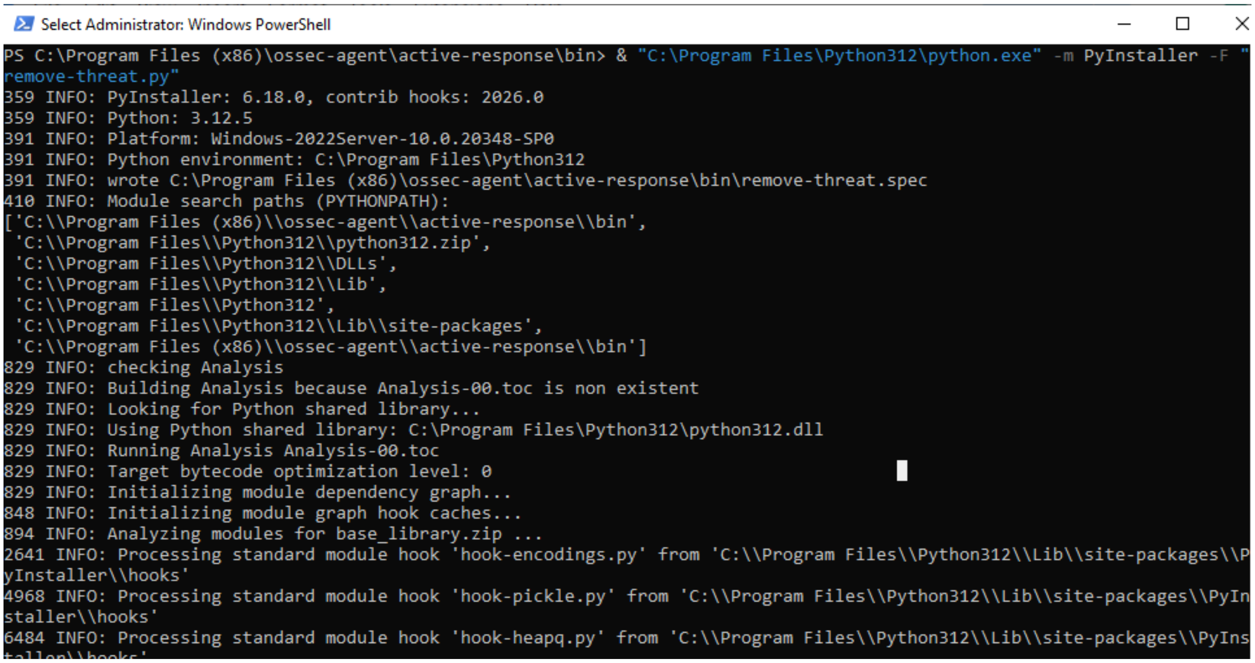
& "C:\Program Files\Python312\python.exe" -m pip install pyinstaller



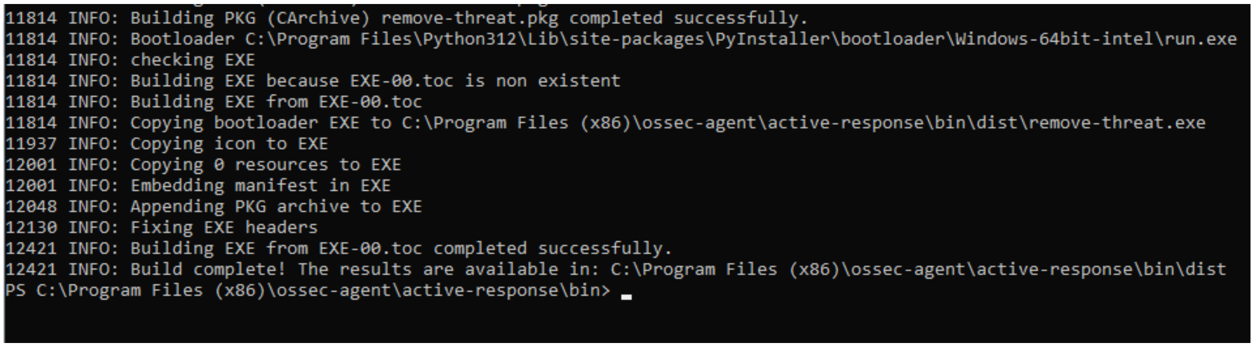
```
PS C:\Program Files (x86)\ossec-agent\active-response\bin> & "C:\Program Files\Python312\python.exe" -m pip install pyin
staller
Collecting pyinstaller
  Downloading pyinstaller-6.18.0-py3-none-win_amd64.whl.metadata (8.5 kB)
Collecting altgraph (from pyinstaller)
  Downloading altgraph-0.17.5-py2.py3-none-any.whl.metadata (7.5 kB)
Collecting packaging>=22.0 (from pyinstaller)
  Downloading packaging-26.0-py3-none-any.whl.metadata (3.3 kB)
Collecting pefile>=2022.5.30 (from pyinstaller)
  Downloading pefile-2024.8.26-py3-none-any.whl.metadata (1.4 kB)
Collecting pyinstaller-hooks-contrib>=2025.9 (from pyinstaller)
  Downloading pyinstaller_hooks_contrib-2026.0-py3-none-any.whl.metadata (16 kB)
Collecting pywin32-ctypes>=0.2.1 (from pyinstaller)
  Downloading pywin32_ctypes-0.2.3-py3-none-any.whl.metadata (3.9 kB)
Collecting setuptools>=42.0.0 (from pyinstaller)
  Downloading setuptools-80.10.2-py3-none-any.whl.metadata (6.6 kB)
Downloading pyinstaller-6.18.0-py3-none-win_amd64.whl (1.4 MB)
   ---------------------------------------- 1.4/1.4 MB 188.0 kB/s  0:00:07
Downloading packaging-26.0-py3-none-any.whl (74 kB)
Downloading pefile-2024.8.26-py3-none-any.whl (74 kB)
Downloading pyinstaller_hooks_contrib-2026.0-py3-none-any.whl (452 kB)
Downloading pywin32_ctypes-0.2.3-py3-none-any.whl (30 kB)
Downloading setuptools-80.10.2-py3-none-any.whl (1.1 MB)
   ---------------------------------------- 1.1/1.1 MB 178.9 kB/s  0:00:06
Downloading altgraph-0.17.5-py2.py3-none-any.whl (21 kB)
Installing collected packages: altgraph, setuptools, pywin32-ctypes, pefile, packaging, pyinstaller-hooks-contrib, pyins
taller
   ----------------------------------       6/7 [pyinstaller]  WARNING: The scripts pyi-archive_viewer.exe, pyi-bindepen
```

3. I created the executable:

& "C:\Program Files\Python312\python.exe" -m PyInstaller -F "remove-threat.py"

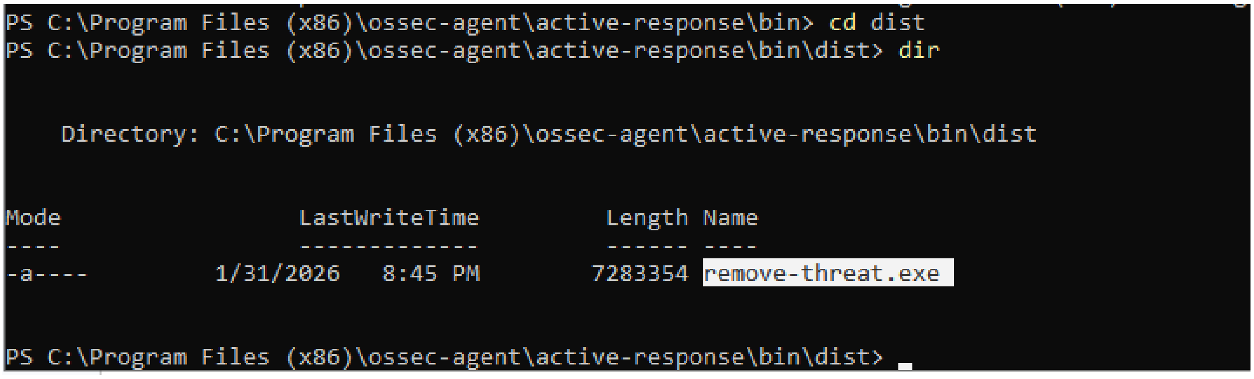


```
PS C:\Program Files (x86)\ossec-agent\active-response\bin> & "C:\Program Files\Python312\python.exe" -m PyInstaller -F "
remove-threat.py"
359 INFO: PyInstaller: 6.18.0, contrib hooks: 2026.0
359 INFO: Python: 3.12.5
391 INFO: Platform: Windows-2022Server-10.0.20348-SP0
391 INFO: Python environment: C:\Program Files\Python312
391 INFO: wrote C:\Program Files (x86)\ossec-agent\active-response\bin\remove-threat.spec
410 INFO: Module search paths (PYTHONPATH):
['C:\\Program Files (x86)\\ossec-agent\\active-response\\bin',
 'C:\\Program Files\\Python312\\python312.zip',
 'C:\\Program Files\\Python312\\DLLs',
 'C:\\Program Files\\Python312\\Lib',
 'C:\\Program Files\\Python312',
 'C:\\Program Files\\Python312\\Lib\\site-packages',
 'C:\\Program Files (x86)\\ossec-agent\\active-response\\bin']
829 INFO: checking Analysis
829 INFO: Building Analysis because Analysis-00.toc is non existent
829 INFO: Looking for Python shared library...
829 INFO: Using Python shared library: C:\Program Files\Python312\python312.dll
829 INFO: Running Analysis Analysis-00.toc
829 INFO: Target bytecode optimization level: 0
829 INFO: Initializing module dependency graph...
848 INFO: Initializing module graph hook caches...
894 INFO: Analyzing modules for base_library.zip ...
2641 INFO: Processing standard module hook 'hook-encodings.py' from 'C:\\Program Files\\Python312\\Lib\\site-packages\\P
yInstaller\\hooks'
4968 INFO: Processing standard module hook 'hook-pickle.py' from 'C:\\Program Files\\Python312\\Lib\\site-packages\\PyIn
staller\\hooks'
6484 INFO: Processing standard module hook 'hook-heapq.py' from 'C:\\Program Files\\Python312\\Lib\\site-packages\\PyIns
taller\\hooks'
```



```
11814 INFO: Building PKG (CArchive) remove-threat.pkg completed successfully.
11814 INFO: Bootloader C:\Program Files\Python312\Lib\site-packages\PyInstaller\bootloader\Windows-64bit-intel\run.exe
11814 INFO: checking EXE
11814 INFO: Building EXE because EXE-00.toc is non existent
11814 INFO: Building EXE from EXE-00.toc
11814 INFO: Copying bootloader EXE to C:\Program Files (x86)\ossec-agent\active-response\bin\dist\remove-threat.exe
11937 INFO: Copying icon to EXE
12001 INFO: Copying 0 resources to EXE
12001 INFO: Embedding manifest in EXE
12048 INFO: Appending PKG archive to EXE
12130 INFO: Fixing EXE headers
12421 INFO: Building EXE from EXE-00.toc completed successfully.
12421 INFO: Build complete! The results are available in: C:\Program Files (x86)\ossec-agent\active-response\bin\dist
PS C:\Program Files (x86)\ossec-agent\active-response\bin> _
```

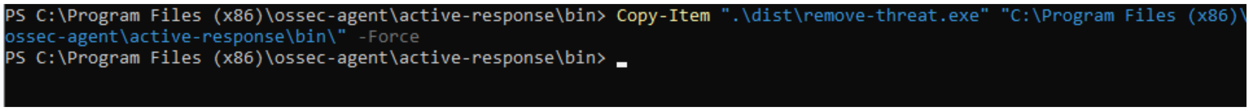
This generated remove-threat.exe inside the dist folder.



```
PS C:\Program Files (x86)\ossec-agent\active-response\bin> cd dist
PS C:\Program Files (x86)\ossec-agent\active-response\bin\dist> dir


    Directory: C:\Program Files (x86)\ossec-agent\active-response\bin\dist


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         1/31/2026   8:45 PM        7283354 remove-threat.exe


PS C:\Program Files (x86)\ossec-agent\active-response\bin\dist> _
```

4. I copied the executable to the Wazuh Active Response directory:

```
Copy-Item ".\dist\remove-threat.exe" "C:\Program Files
(x86)\ossec-agent\active-response\bin\" -Force
```

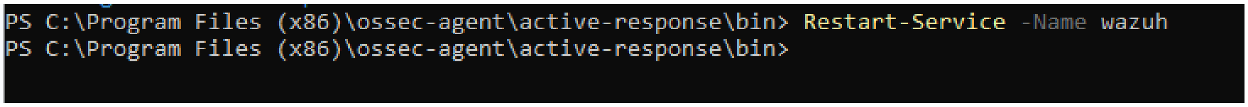


```
PS C:\Program Files (x86)\ossec-agent\active-response\bin> Copy-Item ".\dist\remove-threat.exe" "C:\Program Files (x86)\
ossec-agent\active-response\bin\" -Force
PS C:\Program Files (x86)\ossec-agent\active-response\bin>
```

Step 5: Restart Wazuh Agent

Finally, I restarted the Wazuh agent to apply all changes:

```
Restart-Service -Name wazuh
```



```
PS C:\Program Files (x86)\ossec-agent\active-response\bin> Restart-Service -Name wazuh
PS C:\Program Files (x86)\ossec-agent\active-response\bin>
```

Wazuh Server Configuration

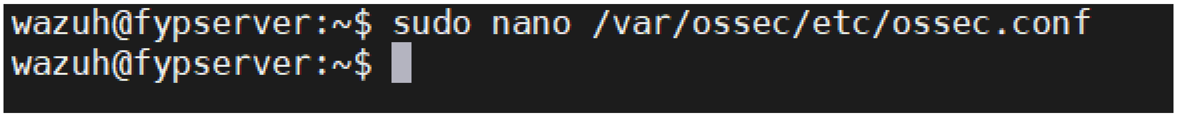
In this phase, I configured the Wazuh server to scan modified or newly added files using VirusTotal and to automatically remove malicious files using the Wazuh Active Response mechanism.

Step 1: Configure VirusTotal Integration on Wazuh Server

First, I enabled the VirusTotal integration on the Wazuh Manager so that any newly created or modified file detected by File Integrity Monitoring (FIM) can be scanned automatically.

1. On the Wazuh server (Ubuntu Desktop), I opened the Wazuh configuration file:

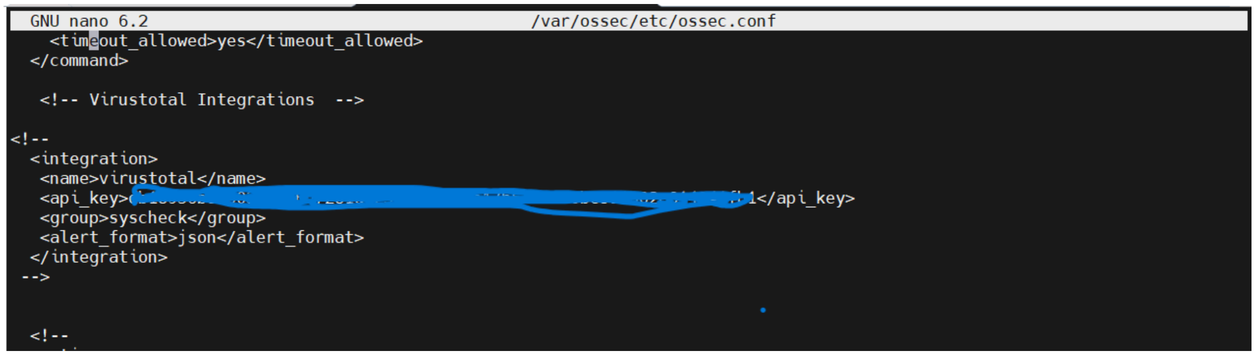
```
sudo nano /var/ossec/etc/ossec.conf
```



```
wazuh@fypserver:~$ sudo nano /var/ossec/etc/ossec.conf
wazuh@fypserver:~$
```

2. Inside the <ossec> block, I added the following configuration:

```
<integration>
  <name>virustotal</name>
  <api_key>MY_API_KEY</api_key>
  <group>syscheck</group>
  <alert_format>json</alert_format>
</integration>
```



```
GNU nano 6.2                                  /var/ossec/etc/ossec.conf
    <timeout_allowed>yes</timeout_allowed>
  </command>

   <!-- Virustotal Integrations  -->

<!--
  <integration>
   <name>virustotal</name>
   <api_key>[redacted]</api_key>
   <group>syscheck</group>
   <alert_format>json</alert_format>
  </integration>
 -->


  <!--
```

3. I replaced MY_API_KEY with my own VirusTotal API key and saved the file.

This configuration ensures that whenever a file is added or modified on the Windows endpoint, Wazuh automatically queries VirusTotal for file reputation.

Note:
The free VirusTotal API allows only four requests per minute. Due to this limitation, monitoring was restricted to important user directories such as Desktop, Documents, and Downloads.

Configure Wazuh Active Response on the Server

After enabling VirusTotal, I configured the Wazuh Active Response module to execute the remove-threat.exe file on the Windows agent whenever malware is detected.

1. On the Wazuh server, I again edited the configuration file:

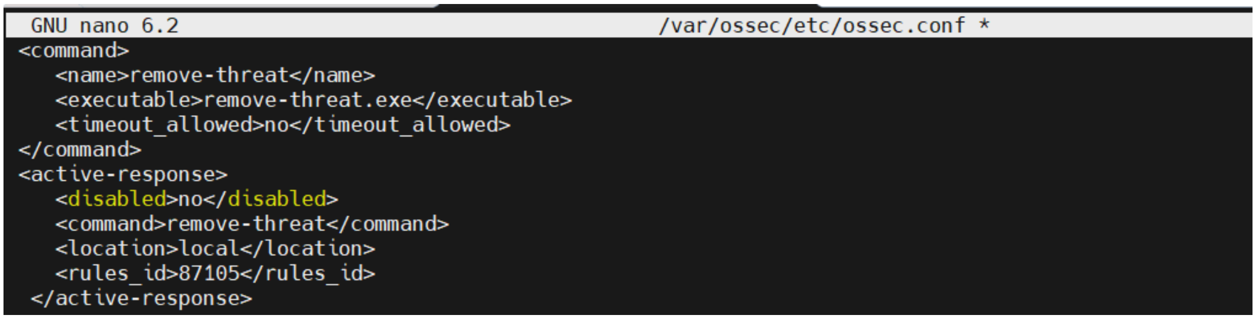
```
sudo nano /var/ossec/etc/ossec.conf
```

2. Inside the <ossec> block, I added the following command definition:

```
<command>
  <name>remove-threat</name>
  <executable>remove-threat.exe</executable>
  <timeout_allowed>no</timeout_allowed>
</command>
```

3. Then, I configured the Active Response rule:

```
<active-response>
  <disabled>no</disabled>
  <command>remove-threat</command>
  <location>local</location>
  <rules_id>87105</rules_id>
</active-response>
```



```
  GNU nano 6.2                                    /var/ossec/etc/ossec.conf *
 <command>
    <name>remove-threat</name>
    <executable>remove-threat.exe</executable>
    <timeout_allowed>no</timeout_allowed>
 </command>
 <active-response>
    <disabled>no</disabled>
    <command>remove-threat</command>
    <location>local</location>
    <rules_id>87105</rules_id>
  </active-response>
```

This setup ensures that when VirusTotal identifies a malicious file, the remove-threat.exe executable is triggered automatically on the Windows endpoint to remove the threat.

Create Custom VirusTotal Rules

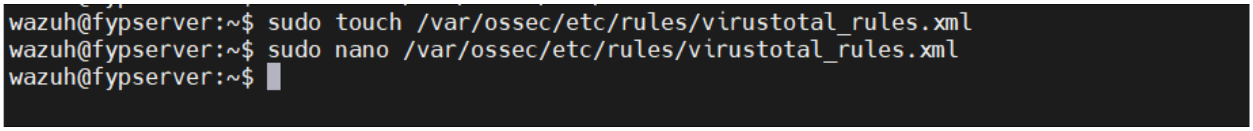
To track whether the Active Response successfully removed a threat or failed, I created custom Wazuh rules.

1. I created a new rules file:

```
touch /var/ossec/etc/rules/virustotal_rules.xml
```

2. I opened the file for editing:

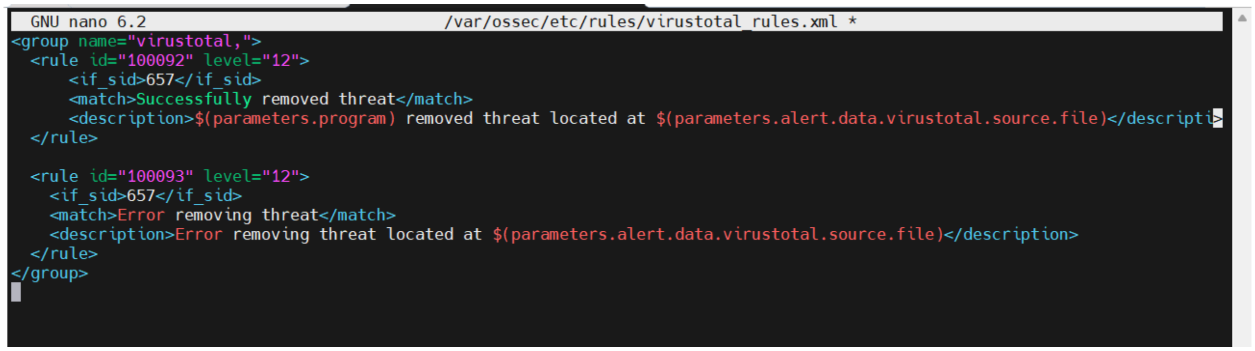
```
sudo nano /var/ossec/etc/rules/virustotal_rules.xml
```



```
wazuh@fypserver:~$ sudo touch /var/ossec/etc/rules/virustotal_rules.xml
wazuh@fypserver:~$ sudo nano /var/ossec/etc/rules/virustotal_rules.xml
wazuh@fypserver:~$ 
```

3. I added the following custom rules:

```
<group name="virustotal,">
  <rule id="100092" level="12">
      <if_sid>657</if_sid>
      <match>Successfully removed threat</match>
      <description>$(parameters.program) removed threat located at $(parameters.alert.data.virustotal.source.file)</description>
  </rule>

  <rule id="100093" level="12">
    <if_sid>657</if_sid>
    <match>Error removing threat</match>
    <description>Error removing threat located at $(parameters.alert.data.virustotal.source.file)</description>
  </rule>
</group>
```



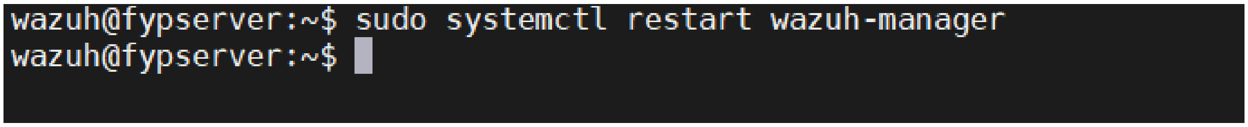
```
  GNU nano 6.2                                   /var/ossec/etc/rules/virustotal_rules.xml *
<group name="virustotal,">
  <rule id="100092" level="12">
      <if_sid>657</if_sid>
      <match>Successfully removed threat</match>
      <description>$(parameters.program) removed threat located at $(parameters.alert.data.virustotal.source.file)</descripti>
  </rule>

  <rule id="100093" level="12">
    <if_sid>657</if_sid>
    <match>Error removing threat</match>
    <description>Error removing threat located at $(parameters.alert.data.virustotal.source.file)</description>
  </rule>
</group>
```

These rules generate alerts indicating whether the malware removal process was successful or not.

Restart Wazuh Manager

After completing the configuration, I restarted the Wazuh Manager to apply all changes:

```
sudo systemctl restart wazuh-manager
```



```
wazuh@fypserver:~$ sudo systemctl restart wazuh-manager
wazuh@fypserver:~$ 
```

Ransomware Execution Detection

Apart from file-based detection, Wazuh can also detect ransomware during execution. This is done by monitoring suspicious system activities such as:

- Deleting volume shadow copies
- Disabling system recovery
- Abnormal process execution behavior

For this purpose, Sysmon logs are collected and analyzed by Wazuh.

Windows Endpoint:Sysmon Configuration

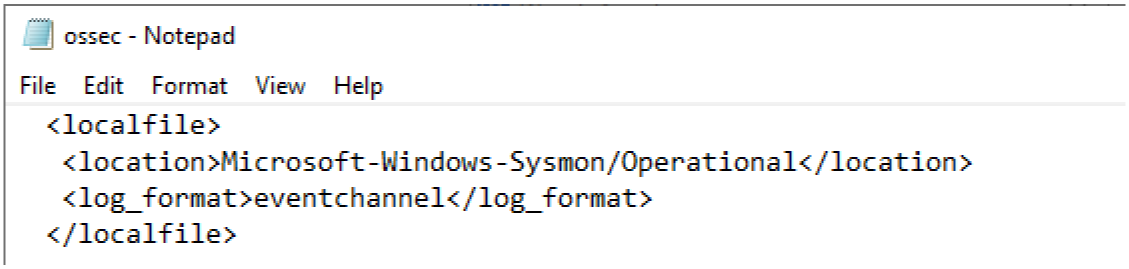
Sysmon is used to log detailed system activity such as process creation, file execution, and network connections. These logs help Wazuh detect ransomware behavior during runtime.

Note:
In my environment, Sysmon was already installed and enabled on the Windows Server 2022 system. Therefore, only log forwarding configuration was required.

Configure Sysmon Log Collection in Wazuh Agent

1. On the Windows Server, I opened the Wazuh agent configuration file:
2. Inside the <ossec_config> block, I added the following configuration to forward Sysmon logs:

```
<localfile>
  <location>Microsoft-Windows-Sysmon/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>
```

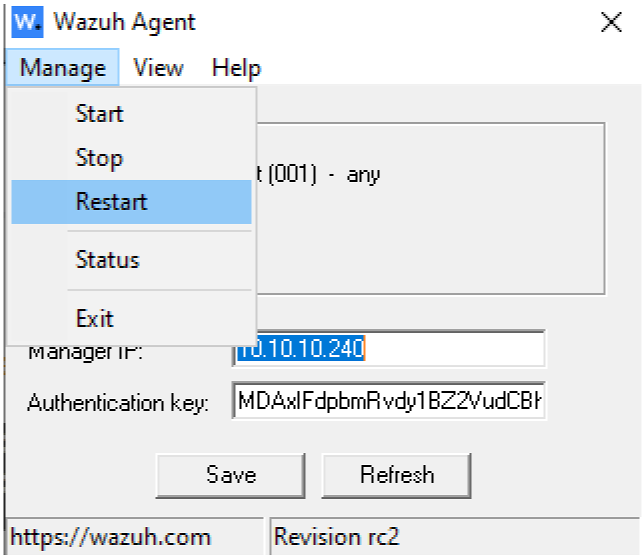


```
<localfile>
 <location>Microsoft-Windows-Sysmon/Operational</location>
 <log_format>eventchannel</log_format>
</localfile>
```

3. I saved the file and closed it.

Restart Wazuh Agent

Finally, I restarted the Wazuh agent to apply the Sysmon log configuration:



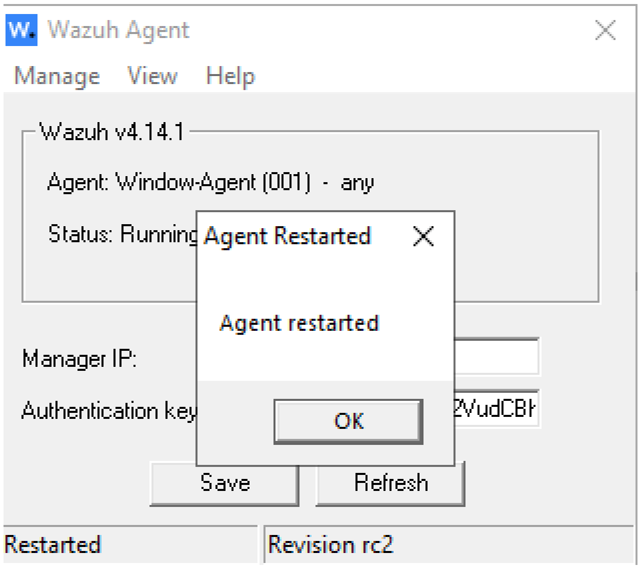
t (001) - any

Manager IP: 10.10.10.240

Authentication key: MDAxlFdpbmRvdy1BZ2VudCBh

https://wazuh.com

Revision rc2



Wazuh v4.14.1

Agent: Window-Agent (001) - any

Status: Running

Agent Restarted

Agent restarted

Manager IP:

Authentication key 2VudCBh

Restarted

Revision rc2

Wazuh Server: Ransomware Execution Detection Rules

In this step, I configured custom Wazuh rules on the Wazuh server to detect ransomware execution activities. These rules focus on common behaviors observed during ransomware attacks, such as disabling security services, deleting shadow copies, modifying system recovery settings, and mass file changes.

Create Custom Ransomware Rules File

First, I created a new rule file on the Wazuh server to store ransomware detection rules.

1. On the Wazuh server (Ubuntu Desktop), I ran the following command:

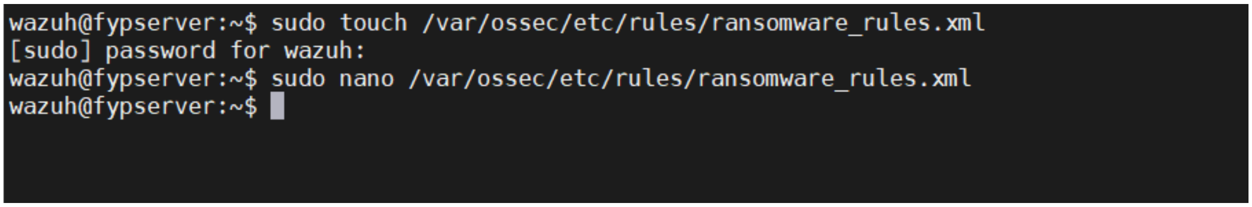
```
sudo touch /var/ossec/etc/rules/ransomware_rules.xml
```

Step 2: Add Ransomware Detection Rules

After creating the file, I added the ransomware execution detection rules.

1. I opened the rule file for editing:

```
sudo nano /var/ossec/etc/rules/ransomware_rules.xml
```



```
wazuh@fypserver:~$ sudo touch /var/ossec/etc/rules/ransomware_rules.xml
[sudo] password for wazuh:
wazuh@fypserver:~$ sudo nano /var/ossec/etc/rules/ransomware_rules.xml
wazuh@fypserver:~$ 
```

2. I added the complete ransomware rule set inside the file:

```
<group name="malware,ransomware,ransomware_pre_detection">

<!-- Rules to detect Ransomware attack -->


 <!-- Suspicious command execution -->

 <rule id="100600" level="12">

   <if_sid>61603</if_sid>

   <field name="win.eventdata.parentCommandLine" type="pcre2">(?i)[c-z]:\\\\Windows\\\\System32\\\\svchost\.exe\s-k\sWerSvcGroup</field>
```

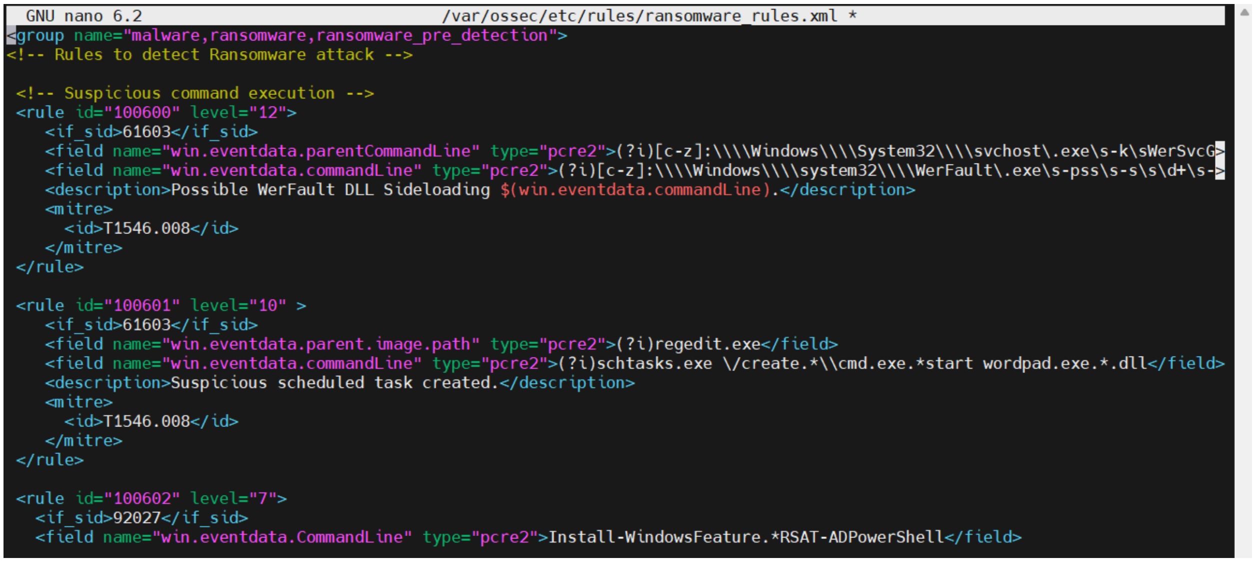
```
    <field name="win.eventdata.commandLine" type="pcre2">(?i)[c-z]:\\\\Windows\\\\system32\\\\WerFault\.exe\s-pss\s-s\s\d+\s-p\s\d+\s-ip\s\d+</field>
    <description>Possible WerFault DLL Sideloading $(win.eventdata.commandLine).</description>
    <mitre>
      <id>T1546.008</id>
    </mitre>
 </rule>

 <rule id="100601" level="10" >
    <if_sid>61603</if_sid>
    <field name="win.eventdata.parent.image.path" type="pcre2">(?i)regedit.exe</field>
    <field name="win.eventdata.commandLine" type="pcre2">(?i)schtasks.exe \/create.*\\cmd.exe.*start wordpad.exe.*.dll</field>
    <description>Suspicious scheduled task created.</description>
    <mitre>
      <id>T1546.008</id>
    </mitre>
 </rule>

 <rule id="100602" level="7">
   <if_sid>92027</if_sid>
   <field name="win.eventdata.CommandLine" type="pcre2">Install-WindowsFeature.*RSAT-ADPowerShell</field>
   <description>Remote Server Administration Tools installed.</description>
   <mitre>
     <id>T1562</id>
   </mitre>
  </rule>

<!-- Impair defenses -->
  <rule id="100603" level="10">
    <if_sid>92042</if_sid>
    <field name="win.eventdata.CommandLine" type="pcre2">netsh advfirewall set currentprofile state off</field>
    <description>Windows firewall disabled.</description>
    <mitre>
      <id>T1562</id>
    </mitre>
  </rule>

  <rule id="100604" level="10">
    <if_sid>61614</if_sid>
    <field name="win.eventdata.targetObject" type="pcre2" >HKLM\\\\System\\\\CurrentControlSet\\\\Services\\\\WinDefend</field>
    <field name="win.eventdata.eventType" type="pcre2">^DeleteKey$</field>
    <field name="win.eventdata.user" type="pcre2" >NT AUTHORITY\\\\SYSTEM</field>
    <description>Windows defender service $(win.eventdata.user) has been deleted on $(win.system.computer). Possible malicious activity.</description>
    <mitre>
      <id>T1562.001</id>
    </mitre>
  </rule>

  <rule id="100605" level="10">
    <if_sid>92027,92021</if_sid>
    <field name="win.eventdata.CommandLine" type="pcre2">(?i)powershell.*New-ItemProperty.*Windows Defender.*DisableAntiSpyware.*-Value 1.*</field>
    <description>Windows defender service has been deleted on $(win.system.computer). Possible malicious activity.</description>
    <mitre>
      <id>T1562.001</id>
    </mitre>
  </rule>

  <rule id="100606" level="10">
    <if_sid>92008,92027</if_sid>
    <field name="win.eventdata.CommandLine" type="pcre2">(?i)powershell.*Set-MpPreference.*-DisableRealTimeMonitoring.*true</field>
    <description>Windows defender realtime protection has been disabled on $(win.system.computer). Possible malicious activity.</description>
    <mitre>
      <id>T1562.001</id>
    </mitre>
  </rule>


  <rule id="100607" level="10">
    <if_sid>92042</if_sid>
    <field name="win.eventdata.CommandLine" type="pcre2">reg.exe .*Windows
Defender\\Real-Time Protection.*Disable|\/d</field>
    <description>Windows defender realtime protection has been disabled on
$(win.system.computer). Possible malicious activity.</description>
    <mitre>
      <id>T1562</id>
    </mitre>
  </rule>


  <rule id="100608" level="10">
    <if_sid>92042</if_sid>
    <field name="win.eventdata.ruleName" type="pcre2">(?i)Disabling Security
Tools</field>
    <field name="win.eventdata.targetObject" type="pcre2">(?i)Windows
Defender</field>
    <description>Windows Defender feature disabled on $(win.system.computer).
Possible malicious activity</description>
    <mitre>
      <id>T1562</id>
    </mitre>
  </rule>

  <rule id="100609" level="10">
    <if_sid>92042</if_sid>
    <field name="win.eventdata.CommandLine" type="pcre2">dism .* \/Disable-feature \/FeatureName:Windows-Defender</field>
    <description>Windows Defender disabled.</description>
    <mitre>
      <id>T1562</id>
    </mitre>
  </rule>

  <rule id="100610" level="10">
    <field name="win.system.providerName" type="pcre2">(?i)SecurityCenter</field>
    <field name="win.eventdata.data" type="pcre2">(?i)Windows Defender, SECURITY_PRODUCT_STATE_SNOOZED</field>
    <description>Windows Defender snoozed on $(win.system.computer). Possible malicious activity</description>
    <mitre>
      <id>T1562</id>
    </mitre>
  </rule>

<!-- System recovery inhibition -->
  <rule id="100611" level="10">
```

```
    <if_sid>61603</if_sid>
    <field name="win.eventdata.CommandLine" type="pcre2">(?i)bcdedit\s\s\/set\s{default}\sbootstatuspolicy\signoreallfailures</field>
    <description>Boot configuration data edited.</description>
    <mitre>
      <id>T1059</id>
    </mitre>
  </rule>


<!-- Persistence detection -->
  <rule id="100612" level="10">
    <if_sid>92300</if_sid>
    <field name="win.eventdata.image" type="pcre2">(?i)\.exe</field>
    <field name="win.eventdata.eventType" type="pcre2">(?i)SetValue</field>
    <field name="win.eventdata.targetObject" type="pcre2">(?i)HKLM\\\\SOFTWARE\\\\Microsoft\\\\Windows\\\\CurrentVersion\\\\Run\\\\[A-Za-z0-9]+</field>
    <description>New run key added to registry by $(win.eventdata.image).</description>
    <mitre>
      <id>T1547.001</id>
    </mitre>
  </rule>
```

```
 <rule id="100613" level="10">
    <if_sid>61613</if_sid>
    <field name="win.eventdata.image" type="pcre2">\.exe</field>
    <field name="win.eventdata.targetFilename" type="pcre2">(?i)ProgramData\\\\Microsoft\\\\Windows\\\\Start Menu\\\\Programs\\\\Startup\\\\.+\.exe</field>
    <description>$(win.eventdata.targetFilename) added to Startup programs by $(win.eventdata.image).</description>
    <mitre>
      <id>T1547.001</id>
    </mitre>
  </rule>


  <rule id="100614" level="10">
    <field name="win.eventdata.ruleName" type="pcre2">(?i)Credential Dumping</field>
    <field name="win.eventdata.sourceImage" type="pcre2">WerFault.exe</field>
    <description>WerFault abused to dump credentials.</description>
    <mitre>
      <id>T1003</id>
    </mitre>
  </rule>


<!-- System recovery inhibition -->
  <rule id="100615" level="12">
    <if_sid>61603</if_sid>
    <field name="win.eventdata.CommandLine" type="pcre2">(?i)vssadmin\s\sdelete\sshadows\s\/all\s\/quiet</field>
    <description>Volume shadow copy deleted using $(win.eventdata.originalFileName). Potential ransomware activity detected.</description>
    <mitre>
      <id>T1490</id>
      <id>T1059.003</id>
    </mitre>
  </rule>


  <rule id="100616" level="12">
    <if_sid>92032</if_sid>
    <field name="win.eventdata.parentCommandLine" type="pcre2">(?i)vssadmin.*delete.*shadow</field>
    <description>Volume shadow copy deleted using $(win.eventdata.originalFileName). Potential ransomware activity detected.</description>
    <mitre>
      <id>T1490</id>
      <id>T1059.003</id>
    </mitre>
  </rule>


  <rule id="100617" level="12">
    <if_sid>61603</if_sid>
    <field name="win.eventdata.CommandLine" type="pcre2">(?i).*Shadowcopy
.*Delete</field>

    <description>Volume shadow copy deleted using $(win.eventdata.originalFileName).
Potential ransomware activity detected.</description>

    <mitre>

      <id>T1490</id>

      <id>T1059.003</id>

    </mitre>

  </rule>



  <rule id="100618" level="12">

    <if_sid>61603</if_sid>

    <field name="win.eventdata.CommandLine" type="pcre2">wmic shadowcopy
delete</field>

    <description>$(win.eventdata.originalFileName) invoked to delete shadow copies.
Potential ransomware activity detected.</description>

    <mitre>

      <id>T1490</id>

      <id>T1059.003</id>

    </mitre>

  </rule>



  <rule id="100619" level="12">

    <field name="win.system.providerName"
type="pcre2">(?i)Microsoft-Windows-Sysmon</field>
```

```
    <field name="win.eventdata.CommandLine" type="pcre2">(?i)delete shadows</field>
    <description>Volume Shadow copy deleted on $(win.system.computer). Potential ransomware activity detected.</description>
    <mitre>
      <id>T1490</id>
      <id>T1059.003</id>
    </mitre>
  </rule>

  <rule id="100620" level="12">
    <if_sid>61603</if_sid>
    <field name="win.eventdata.CommandLine" type="pcre2">(?i)bcdedit\s\s\/set\s{default}\srecoveryenabled\sNo</field>
    <description>System recovery disabled. Possible ransomware activity detected.</description>
    <mitre>
      <id>T1059</id>
    </mitre>
  </rule>

  <rule id="100621" level="12">
    <if_sid>61603</if_sid>
    <field name="win.eventdata.CommandLine" type="pcre2">(?i)wbadmin\s\sdelete\scatalog\s-quiet</field>
    <description>System catalog deleted. Possible ransomware activity detected.</description>
    <mitre>
      <id>T1059</id>
    </mitre>
  </rule>

  <rule id="100622" level="12">
    <if_sid>61603</if_sid>
    <field name="win.eventdata.CommandLine" type="pcre2">(?i)bcdedit\s\s\/set\s{default}\srecoveryenabled\sNo</field>
    <description>System recovery disabled. Possible ransomware activity detected.</description>
    <mitre>
      <id>T1059</id>
    </mitre>
  </rule>

  <rule id="100623" level="12">
    <if_sid>92032</if_sid>
    <field name="win.eventdata.CommandLine" type="pcre2">(?i)wevtutil.*cl</field>
    <description>Windows event logs deleted. Possible malicious activity detected.</description>
    <mitre>
      <id>T1070.001</id>
    </mitre>
  </rule>

<!-- Ransom note file creation -->


  <rule id="100626" level="10" timeframe="50" frequency="3" ignore="300">
    <if_matched_sid>554</if_matched_sid>
    <same_field>md5</same_field>
    <different_field>file</different_field>
    <description>The file $(file) has been created in multiple directories in a short time. Possible ransomware activity.</description>
  </rule>

  <rule id="100627" level="7" timeframe="30" frequency="10" ignore="300">
    <if_matched_sid>550</if_matched_sid>
    <field name="file" type="pcre2">(?i)C:\\Users</field>
    <description>Multiple Files modified in the User directory in a short time.</description>
  </rule>

  <rule id="100629" level="7" timeframe="300" frequency="2" ignore="300">
    <if_matched_sid>63104</if_matched_sid>
    <field name="win.system.message" type="pcre2">(?i)log file was cleared</field>
```

```xml
    <description>Windows Log File Cleared.</description>
    <mitre>
      <id>T1070.001</id>
    </mitre>

  </rule>
<!-- Detect creation of typical ransom note files -->
  <rule id="100630" level="10">
    <if_group>syscheck</if_group>
    <field name="filename" type="pcre2">(?i)(README\.txt|HOW_TO_DECRYPT\.txt|RECOVER_FILES\.html)</field>
    <description>Possible ransomware ransom note detected: $(filename)</description>
    <group>ransomware,file_monitoring</group>
    <mitre>
      <id>T1486</id> <!-- Data Encrypted for Impact -->
    </mitre>
  </rule>

  <!-- Detect suspicious ransomware-related file extensions -->
  <rule id="100631" level="10">
    <if_group>syscheck</if_group>
    <field name="filename" type="pcre2">(?i)\.(locked|encrypted|crypt|cry)$</field>
    <description>Suspicious ransomware-related file extension detected: $(filename)</description>
    <group>ransomware,file_monitoring</group>
    <mitre>
      <id>T1486</id> <!-- Data Encrypted for Impact -->
    </mitre>
  </rule>

</group>

<group name="ransomware,ransomware_detection">
  <rule id="100628" level="12" timeframe="300" frequency="2" ignore="300">
    <if_matched_group>ransomware_pre_detection</if_matched_group>

<if_sid>100626,100627,100615,100616,100617,100618,100619,100630,100631</if_sid>
    <description>Ransomware activity detected.</description>
  </rule>
</group>
```



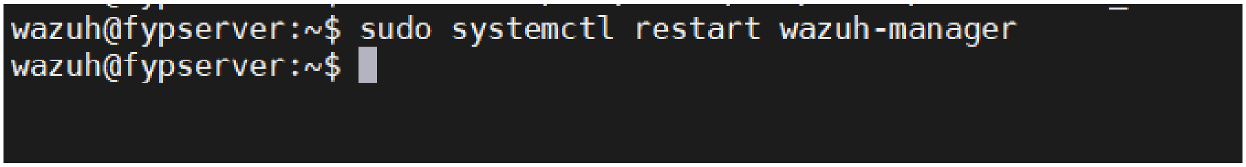
```
  GNU nano 6.2                                    /var/ossec/etc/rules/ransomware_rules.xml *
<group name="malware,ransomware,ransomware_pre_detection">
<!-- Rules to detect Ransomware attack -->

 <!-- Suspicious command execution -->
 <rule id="100600" level="12">
    <if_sid>61603</if_sid>
    <field name="win.eventdata.parentCommandLine" type="pcre2">(?i)[c-z]:\\\\Windows\\\\System32\\\\svchost\.exe\s-k\sWerSvcG>
    <field name="win.eventdata.commandLine" type="pcre2">(?i)[c-z]:\\\\Windows\\\\system32\\\\WerFault\.exe\s-pss\s-s\s\d+\s->
    <description>Possible WerFault DLL Sideloading $(win.eventdata.commandLine).</description>
    <mitre>
      <id>T1546.008</id>
    </mitre>
 </rule>

 <rule id="100601" level="10" >
    <if_sid>61603</if_sid>
    <field name="win.eventdata.parent.image.path" type="pcre2">(?i)regedit.exe</field>
    <field name="win.eventdata.commandLine" type="pcre2">(?i)schtasks.exe \/create.*\\cmd.exe.*start wordpad.exe.*.dll</field>
    <description>Suspicious scheduled task created.</description>
    <mitre>
      <id>T1546.008</id>
    </mitre>
 </rule>

 <rule id="100602" level="7">
   <if_sid>92027</if_sid>
   <field name="win.eventdata.CommandLine" type="pcre2">Install-WindowsFeature.*RSAT-ADPowerShell</field>
```

3. I saved the file and closed the editor.

Restart Wazuh Manager

To apply the newly added ransomware detection rules, I restarted the Wazuh manager service:

sudo systemctl restart wazuh-manager



```
wazuh@fypserver:~$ sudo systemctl restart wazuh-manager
wazuh@fypserver:~$ 
```

Setting Up the Test Environment

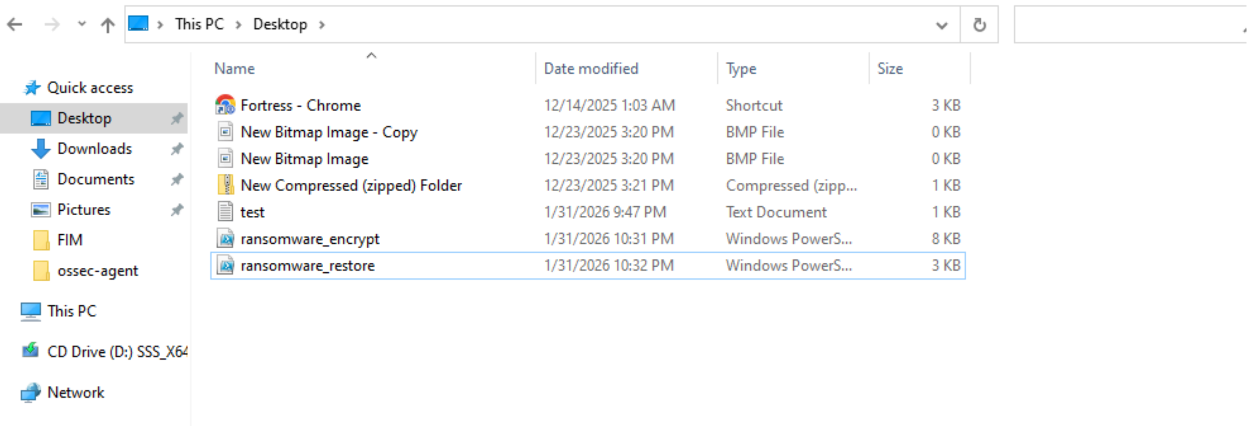
In this phase, I tested the ransomware detection capability of Wazuh by executing a controlled file encryption attack on the Windows Server. The purpose of this testing was to verify whether Wazuh can detect ransomware-like behavior such as mass file encryption, file renaming, and deletion.

Step 1: Prepare Testing Scripts on Windows Server

First, I copied the ransomware testing scripts to the Windows Server 2022 system. The following two PowerShell scripts were placed on the Desktop:

ransomware_encrypt.ps1

ransomware_restore.ps1



Name	Date modified	Type	Size
Fortress - Chrome	12/14/2025 1:03 AM	Shortcut	3 KB
New Bitmap Image - Copy	12/23/2025 3:20 PM	BMP File	0 KB
New Bitmap Image	12/23/2025 3:20 PM	BMP File	0 KB
New Compressed (zipped) Folder	12/23/2025 3:21 PM	Compressed (zipp...	1 KB
test	1/31/2026 9:47 PM	Text Document	1 KB
ransomware_encrypt	1/31/2026 10:31 PM	Windows PowerS...	8 KB
ransomware_restore	1/31/2026 10:32 PM	Windows PowerS...	3 KB

These scripts are used to simulate ransomware encryption and to restore files after testing.

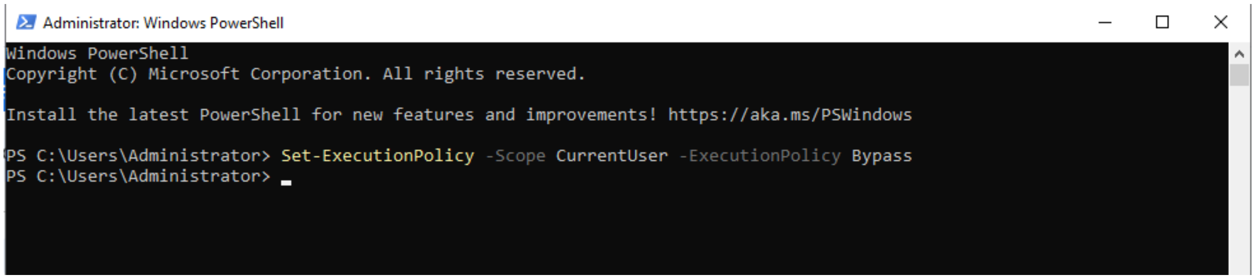
Step 2: Open PowerShell with Administrator Privileges

On Windows Server 2022, I opened **PowerShell as Administrator** to ensure the scripts could execute without permission issues.

Step 3: Enable Script Execution

Before running the scripts, I allowed PowerShell script execution for the current user by running the following command:

Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Bypass

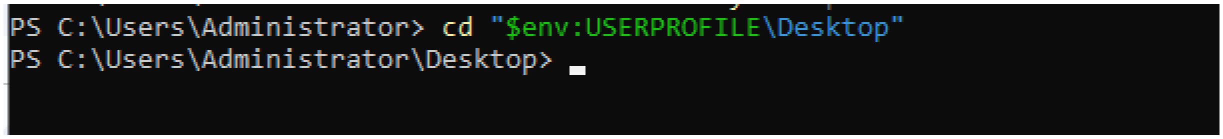


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Bypass
PS C:\Users\Administrator> _
```

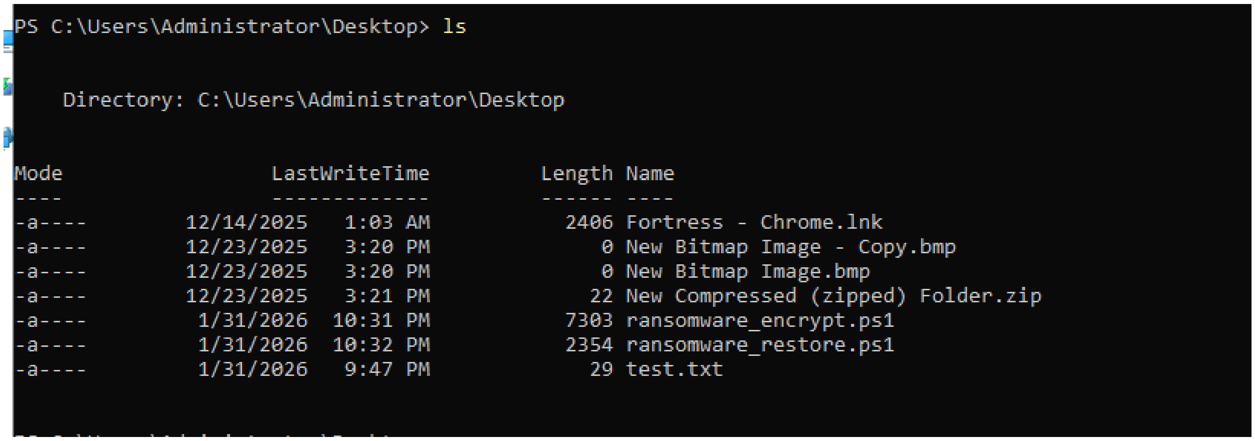
Step 4: Navigate to Script Location

Next, I navigated to the Desktop directory where the testing scripts were stored:

cd "$env:USERPROFILE\Desktop"



```
PS C:\Users\Administrator> cd "$env:USERPROFILE\Desktop"
PS C:\Users\Administrator\Desktop>
```

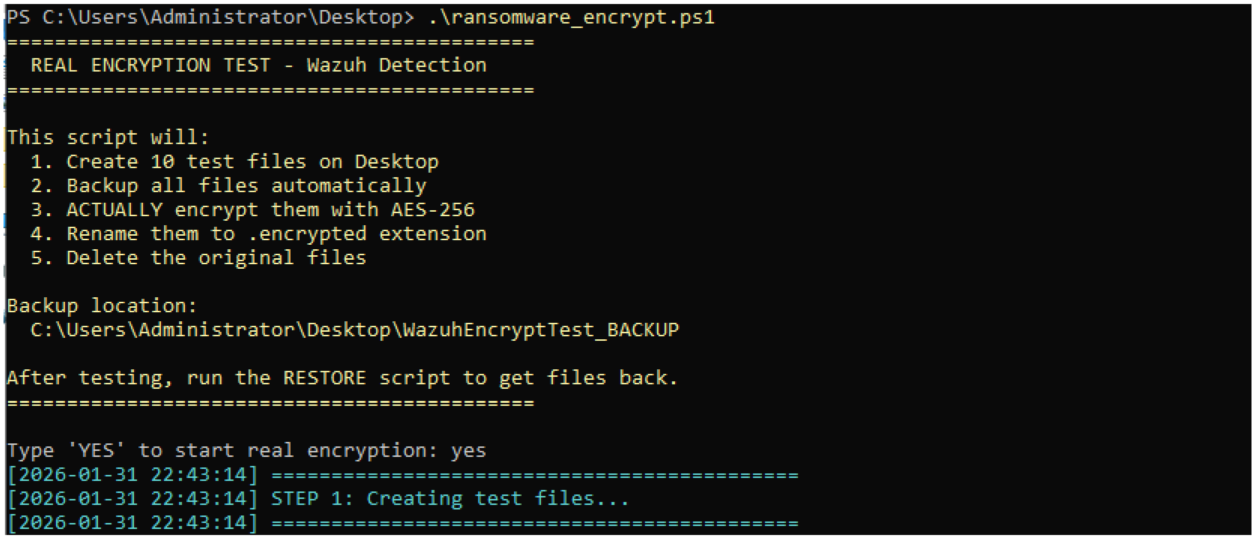


```
PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        12/14/2025   1:03 AM           2406 Fortress - Chrome.lnk
-a----        12/23/2025   3:20 PM              0 New Bitmap Image - Copy.bmp
-a----        12/23/2025   3:20 PM              0 New Bitmap Image.bmp
-a----        12/23/2025   3:21 PM             22 New Compressed (zipped) Folder.zip
-a----         1/31/2026  10:31 PM           7303 ransomware_encrypt.ps1
-a----         1/31/2026  10:32 PM           2354 ransomware_restore.ps1
-a----         1/31/2026   9:47 PM             29 test.txt
```

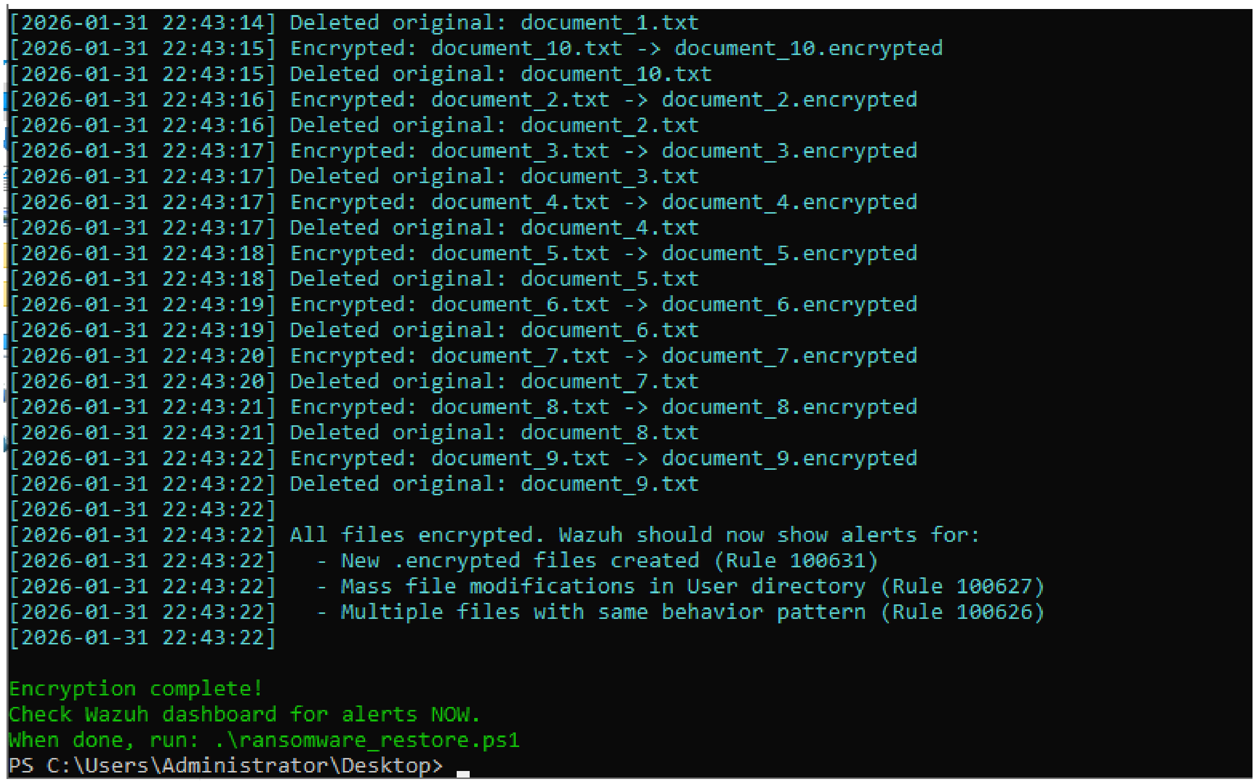
Step 5: Execute Ransomware Encryption Script

After navigating to the correct directory, I started the ransomware encryption test by running:

.\ransomware_encrypt.ps1



```
PS C:\Users\Administrator\Desktop> .\ransomware_encrypt.ps1
============================================
  REAL ENCRYPTION TEST - Wazuh Detection
============================================

This script will:
  1. Create 10 test files on Desktop
  2. Backup all files automatically
  3. ACTUALLY encrypt them with AES-256
  4. Rename them to .encrypted extension
  5. Delete the original files

Backup location:
  C:\Users\Administrator\Desktop\WazuhEncryptTest_BACKUP

After testing, run the RESTORE script to get files back.
============================================

Type 'YES' to start real encryption: yes
[2026-01-31 22:43:14] ============================================
[2026-01-31 22:43:14] STEP 1: Creating test files...
[2026-01-31 22:43:14] ============================================
```



```
[2026-01-31 22:43:14] Deleted original: document_1.txt
[2026-01-31 22:43:15] Encrypted: document_10.txt -> document_10.encrypted
[2026-01-31 22:43:15] Deleted original: document_10.txt
[2026-01-31 22:43:16] Encrypted: document_2.txt -> document_2.encrypted
[2026-01-31 22:43:16] Deleted original: document_2.txt
[2026-01-31 22:43:17] Encrypted: document_3.txt -> document_3.encrypted
[2026-01-31 22:43:17] Deleted original: document_3.txt
[2026-01-31 22:43:17] Encrypted: document_4.txt -> document_4.encrypted
[2026-01-31 22:43:17] Deleted original: document_4.txt
[2026-01-31 22:43:18] Encrypted: document_5.txt -> document_5.encrypted
[2026-01-31 22:43:18] Deleted original: document_5.txt
[2026-01-31 22:43:19] Encrypted: document_6.txt -> document_6.encrypted
[2026-01-31 22:43:19] Deleted original: document_6.txt
[2026-01-31 22:43:20] Encrypted: document_7.txt -> document_7.encrypted
[2026-01-31 22:43:20] Deleted original: document_7.txt
[2026-01-31 22:43:21] Encrypted: document_8.txt -> document_8.encrypted
[2026-01-31 22:43:21] Deleted original: document_8.txt
[2026-01-31 22:43:22] Encrypted: document_9.txt -> document_9.encrypted
[2026-01-31 22:43:22] Deleted original: document_9.txt
[2026-01-31 22:43:22]
[2026-01-31 22:43:22] All files encrypted. Wazuh should now show alerts for:
[2026-01-31 22:43:22]   - New .encrypted files created (Rule 100631)
[2026-01-31 22:43:22]   - Mass file modifications in User directory (Rule 100627)
[2026-01-31 22:43:22]   - Multiple files with same behavior pattern (Rule 100626)
[2026-01-31 22:43:22]

Encryption complete!
Check Wazuh dashboard for alerts NOW.
When done, run: .\ransomware_restore.ps1
PS C:\Users\Administrator\Desktop> _
```

Step 6: Confirm Encryption Process

The script displayed a warning message explaining the encryption process. To proceed with the test, I typed **YES** and pressed **Enter**.

Step 7: Automatic Encryption Process

Once confirmed, the script automatically performed the following actions:

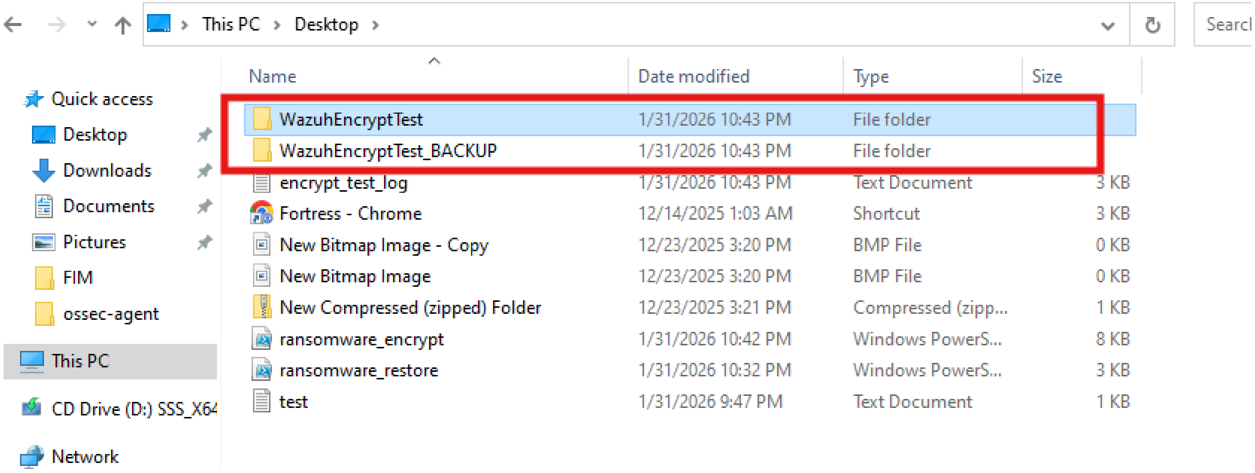
- Created a test folder named WazuhEncryptTest on the Desktop
- Generated 10 sample text files inside the folder
- Created a backup folder named WazuhEncryptTest_BACKUP
- Encrypted all text files using AES-256 encryption
- Renamed encrypted files with the .encrypted extension
- Deleted the original .txt files

Step 8: Verify Encryption Results

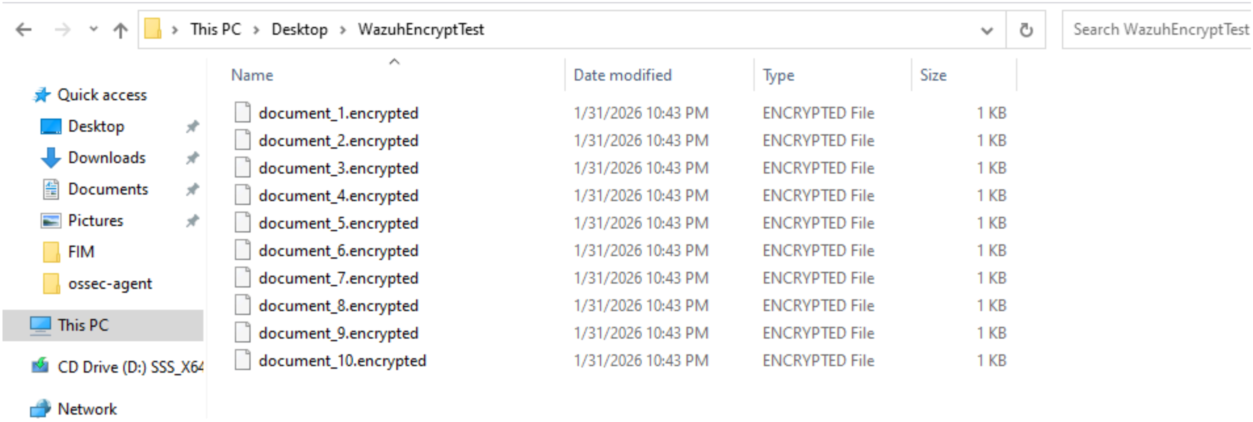
After the script finished execution, I opened **File Explorer** and verified the following:

- The WazuhEncryptTest folder contained only .encrypted files
- The WazuhEncryptTest_BACKUP folder contained the original .txt files

This confirmed that the encryption process completed successfully.

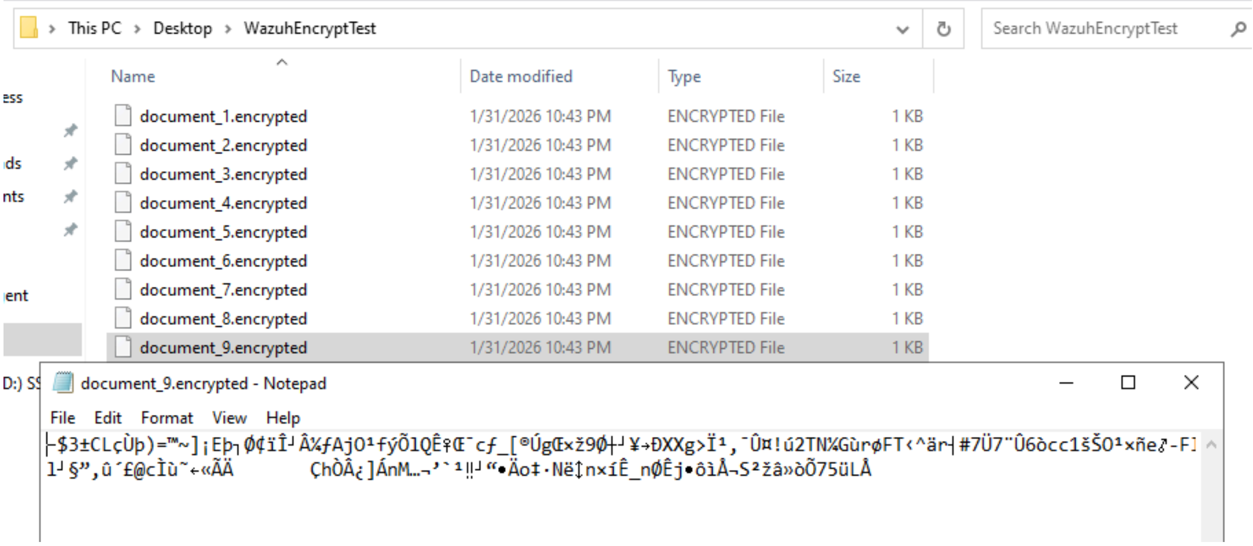


Name	Date modified	Type	Size
WazuhEncryptTest	1/31/2026 10:43 PM	File folder	
WazuhEncryptTest_BACKUP	1/31/2026 10:43 PM	File folder	
encrypt_test_log	1/31/2026 10:43 PM	Text Document	3 KB
Fortress - Chrome	12/14/2025 1:03 AM	Shortcut	3 KB
New Bitmap Image - Copy	12/23/2025 3:20 PM	BMP File	0 KB
New Bitmap Image	12/23/2025 3:20 PM	BMP File	0 KB
New Compressed (zipped) Folder	12/23/2025 3:21 PM	Compressed (zipp...	1 KB
ransomware_encrypt	1/31/2026 10:42 PM	Windows PowerS...	8 KB
ransomware_restore	1/31/2026 10:32 PM	Windows PowerS...	3 KB
test	1/31/2026 9:47 PM	Text Document	1 KB



Name	Date modified	Type	Size
document_1.encrypted	1/31/2026 10:43 PM	ENCRYPTED File	1 KB
document_2.encrypted	1/31/2026 10:43 PM	ENCRYPTED File	1 KB
document_3.encrypted	1/31/2026 10:43 PM	ENCRYPTED File	1 KB
document_4.encrypted	1/31/2026 10:43 PM	ENCRYPTED File	1 KB
document_5.encrypted	1/31/2026 10:43 PM	ENCRYPTED File	1 KB
document_6.encrypted	1/31/2026 10:43 PM	ENCRYPTED File	1 KB
document_7.encrypted	1/31/2026 10:43 PM	ENCRYPTED File	1 KB
document_8.encrypted	1/31/2026 10:43 PM	ENCRYPTED File	1 KB
document_9.encrypted	1/31/2026 10:43 PM	ENCRYPTED File	1 KB
document_10.encrypted	1/31/2026 10:43 PM	ENCRYPTED File	1 KB

I opened only one file that had encrypted content.



This PC › Desktop › WazuhEncryptTest

Search WazuhEncryptTest

Name	Date modified	Type	Size
document_1.encrypted	1/31/2026 10:43 PM	ENCRYPTED File	1 KB
document_2.encrypted	1/31/2026 10:43 PM	ENCRYPTED File	1 KB
document_3.encrypted	1/31/2026 10:43 PM	ENCRYPTED File	1 KB
document_4.encrypted	1/31/2026 10:43 PM	ENCRYPTED File	1 KB
document_5.encrypted	1/31/2026 10:43 PM	ENCRYPTED File	1 KB
document_6.encrypted	1/31/2026 10:43 PM	ENCRYPTED File	1 KB
document_7.encrypted	1/31/2026 10:43 PM	ENCRYPTED File	1 KB
document_8.encrypted	1/31/2026 10:43 PM	ENCRYPTED File	1 KB
document_9.encrypted	1/31/2026 10:43 PM	ENCRYPTED File	1 KB

document_9.encrypted - Notepad

```
├$3±CLçÙþ)=™~]¡Eþ┐Ø¢ïÎ┘Â¼ƒAjO¹fýÕ1QÊ♀Œ¯cƒ_[®ÚgŒ×ž9Ø╫┘¥→ÐXXg>Ï¹,¯Û¤!ú2TN%GùrøFT‹^är┤#7Ü7¨Û6òcc1šŠO¹×ñe♪-FI
1┘§”,û´£@cÌù˜←«ÃÄ        ÇhÒÂ¿]ÁnM…¬’`¹‼┘“•Äo‡·Në↕n×íÊ_nØÊj•ôìÅ¬S²žâ»òÕ75üLÅ
```

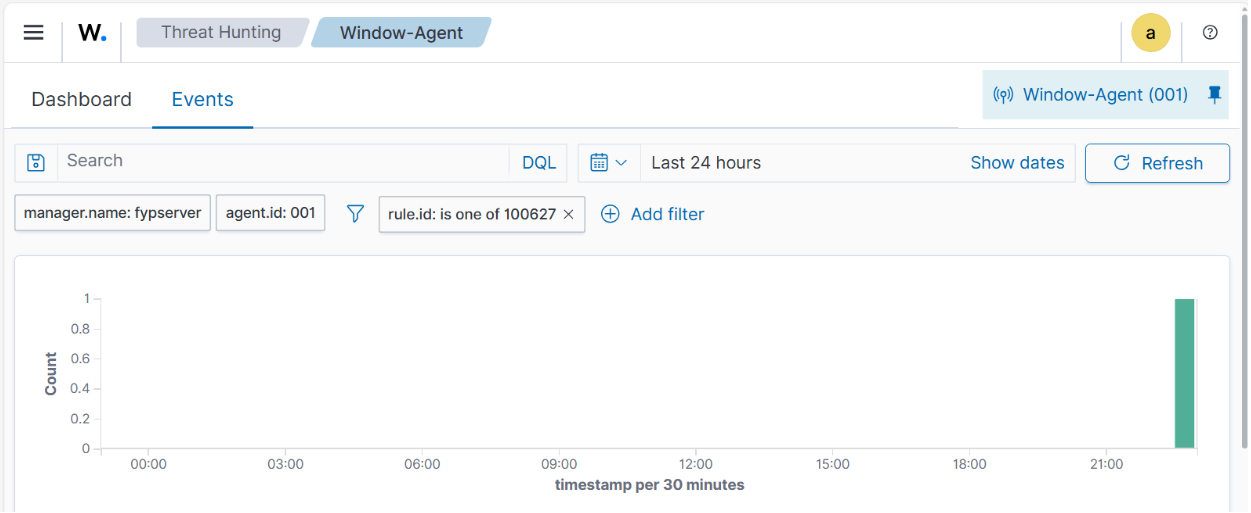
Step 9: Check Wazuh Dashboard for Alerts

After encryption I then opened the **Wazuh Dashboard** and navigated to:

Threat Hunting Section:

Step 10: Verify Ransomware Detection Alerts

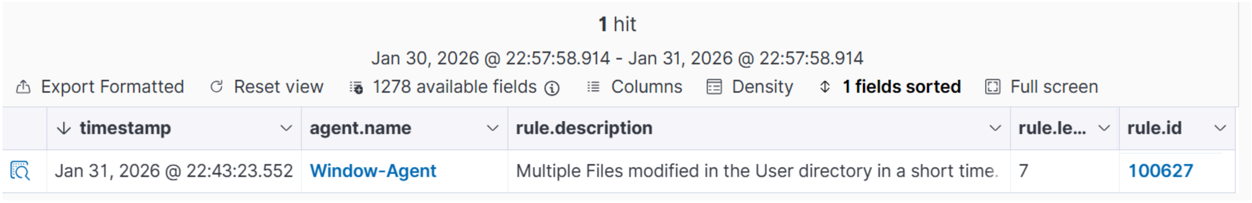
On the Events page, I confirmed that Wazuh generated alerts related to ransomware activity.



manager.name: fypserver

agent.id: 001

rule.id: is one of 100627

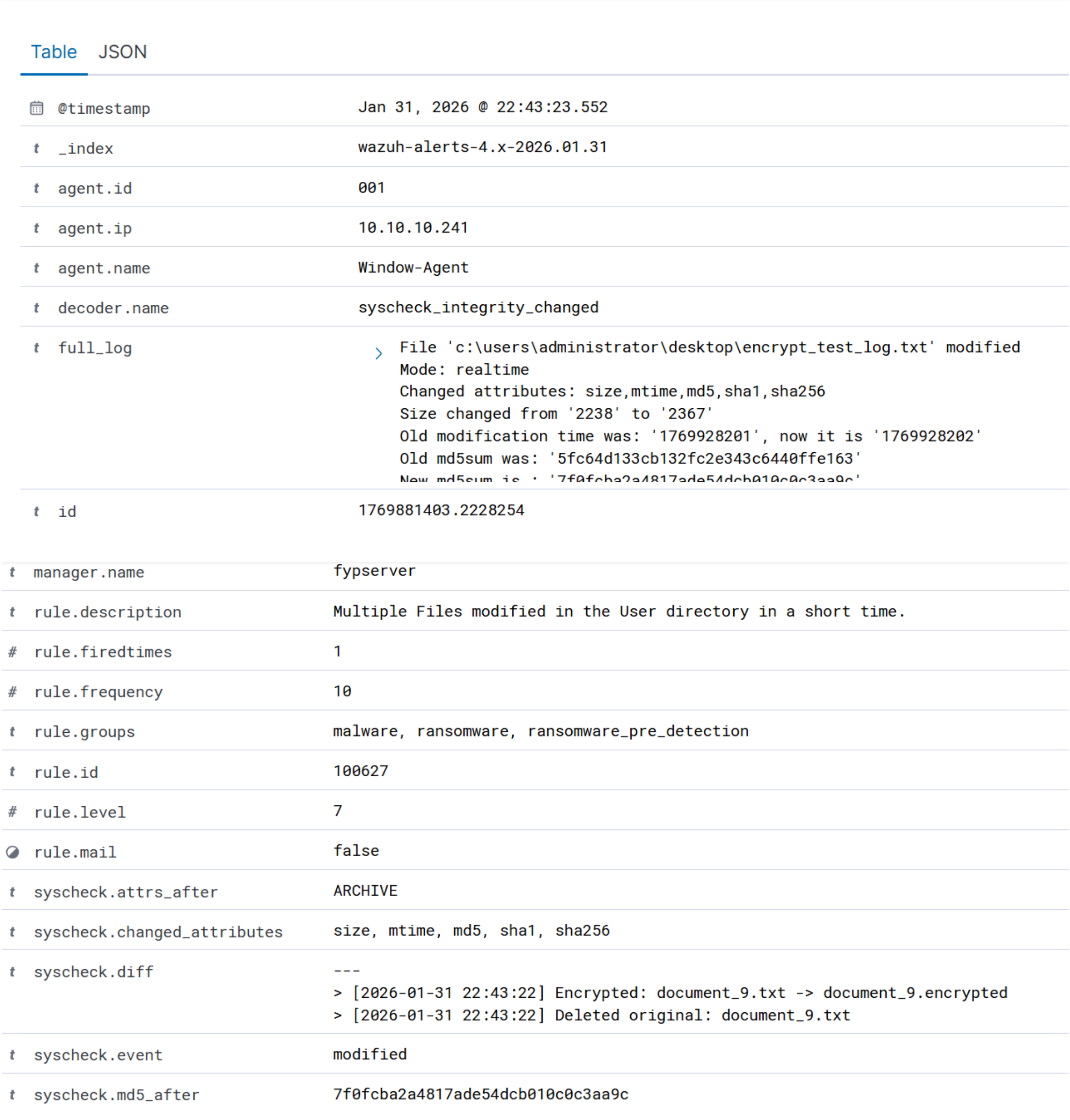


1 hit

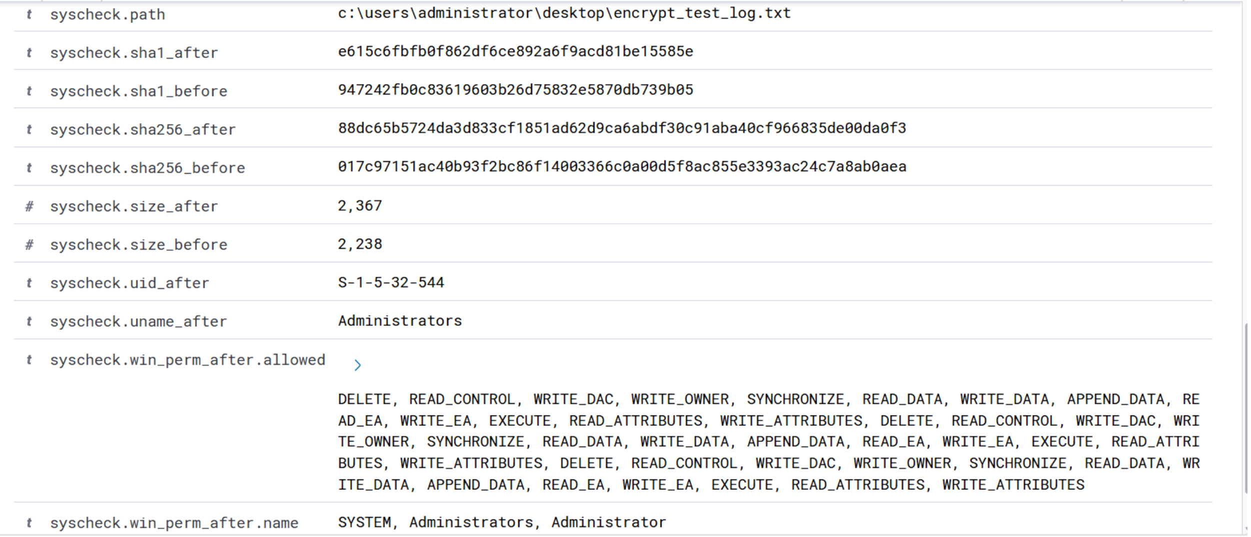
Jan 30, 2026 @ 22:57:58.914 - Jan 31, 2026 @ 22:57:58.914

timestamp	agent.name	rule.description	rule.le...	rule.id
Jan 31, 2026 @ 22:43:23.552	Window-Agent	Multiple Files modified in the User directory in a short time.	7	100627

Details:



@timestamp	Jan 31, 2026 @ 22:43:23.552
_index	wazuh-alerts-4.x-2026.01.31
agent.id	001
agent.ip	10.10.10.241
agent.name	Window-Agent
decoder.name	syscheck_integrity_changed
full_log	File 'c:\users\administrator\desktop\encrypt_test_log.txt' modified Mode: realtime Changed attributes: size,mtime,md5,sha1,sha256 Size changed from '2238' to '2367' Old modification time was: '1769928201', now it is '1769928202' Old md5sum was: '5fc64d133cb132fc2e343c6440ffe163' New md5sum is : '7f0fcba2a4817ade54dcb010c0c3aa9c'
id	1769881403.2228254
manager.name	fypserver
rule.description	Multiple Files modified in the User directory in a short time.
rule.firedtimes	1
rule.frequency	10
rule.groups	malware, ransomware, ransomware_pre_detection
rule.id	100627
rule.level	7
rule.mail	false
syscheck.attrs_after	ARCHIVE
syscheck.changed_attributes	size, mtime, md5, sha1, sha256
syscheck.diff	--- > [2026-01-31 22:43:22] Encrypted: document_9.txt -> document_9.encrypted > [2026-01-31 22:43:22] Deleted original: document_9.txt
syscheck.event	modified
syscheck.md5_after	7f0fcba2a4817ade54dcb010c0c3aa9c



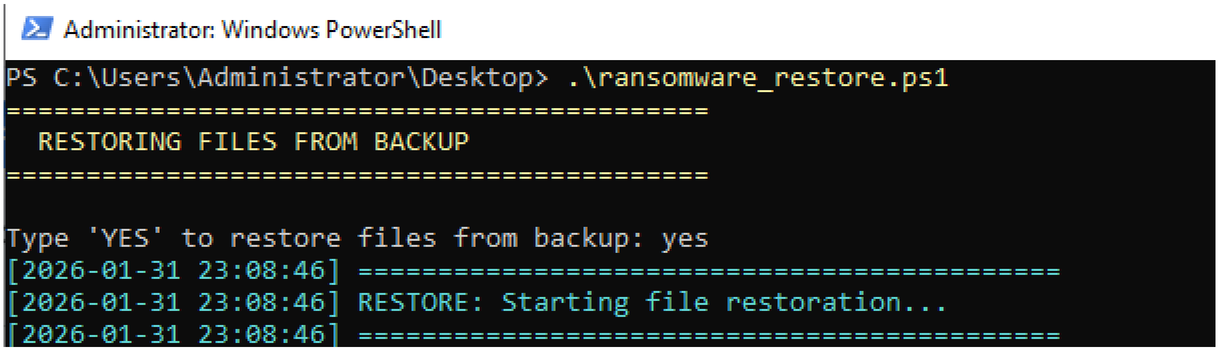
t	syscheck.path	c:\users\administrator\desktop\encrypt_test_log.txt
t	syscheck.sha1_after	e615c6fbfb0f862df6ce892a6f9acd81be15585e
t	syscheck.sha1_before	947242fb0c83619603b26d75832e5870db739b05
t	syscheck.sha256_after	88dc65b5724da3d833cf1851ad62d9ca6abdf30c91aba40cf966835de00da0f3
t	syscheck.sha256_before	017c97151ac40b93f2bc86f14003366c0a00d5f8ac855e3393ac24c7a8ab0aea
#	syscheck.size_after	2,367
#	syscheck.size_before	2,238
t	syscheck.uid_after	S-1-5-32-544
t	syscheck.uname_after	Administrators
t	syscheck.win_perm_after.allowed	DELETE, READ_CONTROL, WRITE_DAC, WRITE_OWNER, SYNCHRONIZE, READ_DATA, WRITE_DATA, APPEND_DATA, READ_EA, WRITE_EA, EXECUTE, READ_ATTRIBUTES, WRITE_ATTRIBUTES, DELETE, READ_CONTROL, WRITE_DAC, WRITE_OWNER, SYNCHRONIZE, READ_DATA, WRITE_DATA, APPEND_DATA, READ_EA, WRITE_EA, EXECUTE, READ_ATTRIBUTES, WRITE_ATTRIBUTES, DELETE, READ_CONTROL, WRITE_DAC, WRITE_OWNER, SYNCHRONIZE, READ_DATA, WRITE_DATA, APPEND_DATA, READ_EA, WRITE_EA, EXECUTE, READ_ATTRIBUTES, WRITE_ATTRIBUTES
t	syscheck.win_perm_after.name	SYSTEM, Administrators, Administrator

Step 12: Restore Original Files

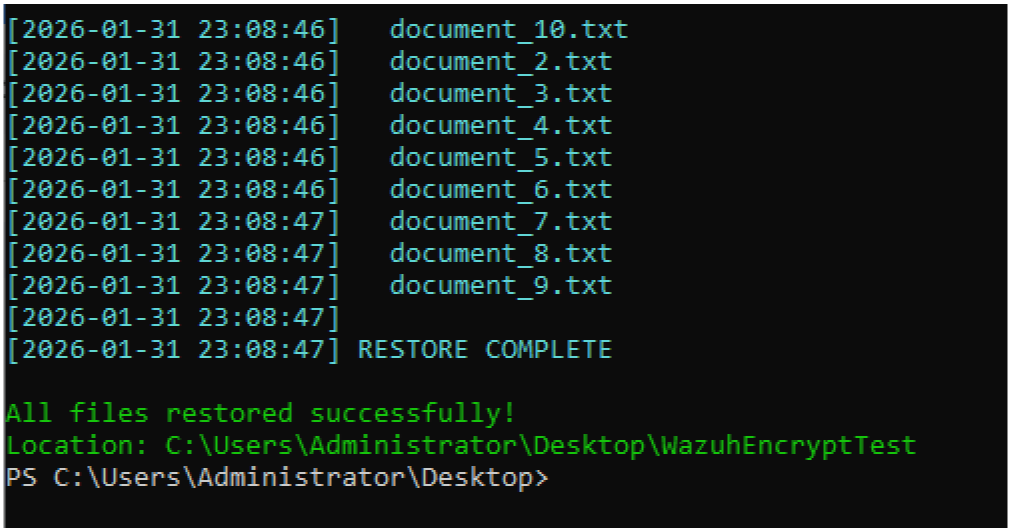
After completing the testing and verification, I restored the original files by running the restore script:

.\ransomware_restore.ps1

When prompted, I typed **YES** and pressed **Enter**.



```
PS C:\Users\Administrator\Desktop> .\ransomware_restore.ps1
============================================
  RESTORING FILES FROM BACKUP
============================================

Type 'YES' to restore files from backup: yes
[2026-01-31 23:08:46] ============================================
[2026-01-31 23:08:46] RESTORE: Starting file restoration...
[2026-01-31 23:08:46] ============================================
```



```
[2026-01-31 23:08:46]   document_10.txt
[2026-01-31 23:08:46]   document_2.txt
[2026-01-31 23:08:46]   document_3.txt
[2026-01-31 23:08:46]   document_4.txt
[2026-01-31 23:08:46]   document_5.txt
[2026-01-31 23:08:46]   document_6.txt
[2026-01-31 23:08:47]   document_7.txt
[2026-01-31 23:08:47]   document_8.txt
[2026-01-31 23:08:47]   document_9.txt
[2026-01-31 23:08:47]
[2026-01-31 23:08:47] RESTORE COMPLETE

All files restored successfully!
Location: C:\Users\Administrator\Desktop\WazuhEncryptTest
PS C:\Users\Administrator\Desktop>
```

Another Test

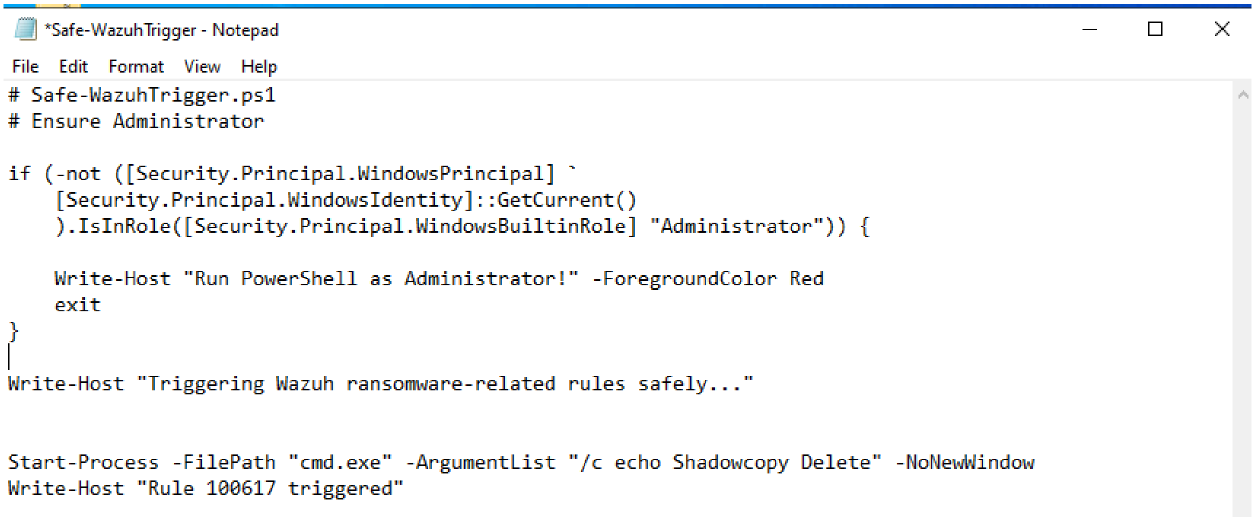
// Safe-WazuhTrigger.ps1

```
# Safe-WazuhTrigger.ps1
# Ensure Administrator

if (-not ([Security.Principal.WindowsPrincipal] `
    [Security.Principal.WindowsIdentity]::GetCurrent()
    ).IsInRole([Security.Principal.WindowsBuiltinRole] "Administrator")) {

    Write-Host "Run PowerShell as Administrator!" -ForegroundColor Red
    exit
}

Write-Host "Triggering Wazuh ransomware-related rules safely..."


Start-Process -FilePath "cmd.exe" -ArgumentList "/c echo Shadowcopy Delete"
-NoNewWindow
Write-Host "Rule 100617 triggered"
```

Step 1: Save the Script

Save the file as:

C:\Users\Administrator\Desktop\Safe-WazuhTrigger.ps1



```
# Safe-WazuhTrigger.ps1
# Ensure Administrator

if (-not ([Security.Principal.WindowsPrincipal] `
    [Security.Principal.WindowsIdentity]::GetCurrent()
    ).IsInRole([Security.Principal.WindowsBuiltinRole] "Administrator")) {

    Write-Host "Run PowerShell as Administrator!" -ForegroundColor Red
    exit
}

Write-Host "Triggering Wazuh ransomware-related rules safely..."


Start-Process -FilePath "cmd.exe" -ArgumentList "/c echo Shadowcopy Delete" -NoNewWindow
Write-Host "Rule 100617 triggered"
```

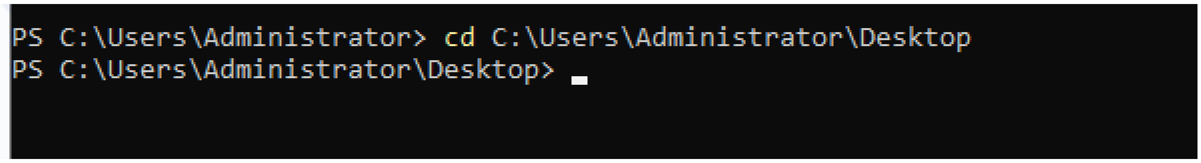
Step 2: Open PowerShell as Administrator

Open **PowerShell** using **Run as Administrator**.

Step 3: Go to Script Location

Run:

cd C:\Users\Administrator\Desktop

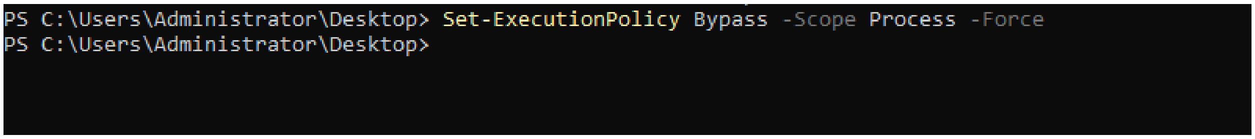


```
PS C:\Users\Administrator> cd C:\Users\Administrator\Desktop
PS C:\Users\Administrator\Desktop>
```

Step 4: Temporarily Bypass Execution Policy

Run:

Set-ExecutionPolicy Bypass -Scope Process -Force

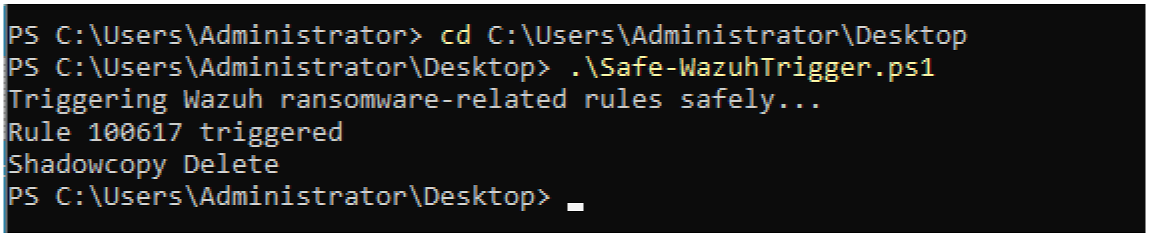


```
PS C:\Users\Administrator\Desktop> Set-ExecutionPolicy Bypass -Scope Process -Force
PS C:\Users\Administrator\Desktop>
```

Step 5: Execute the Script

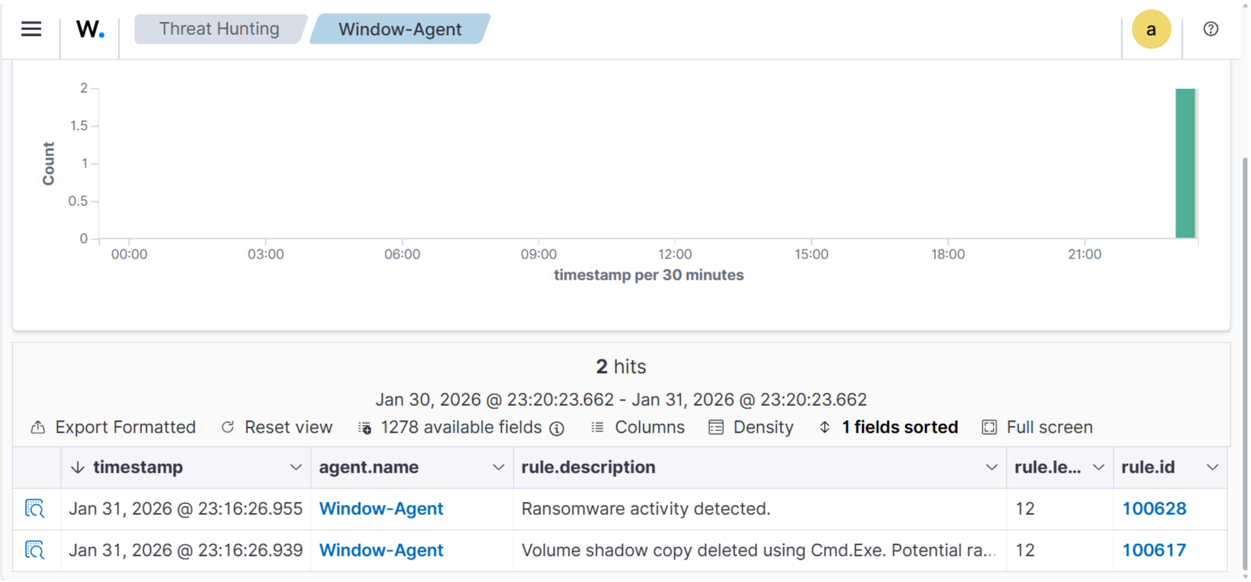
Run:

.\Safe-WazuhTrigger.ps1



```
PS C:\Users\Administrator> cd C:\Users\Administrator\Desktop
PS C:\Users\Administrator\Desktop> .\Safe-WazuhTrigger.ps1
Triggering Wazuh ransomware-related rules safely...
Rule 100617 triggered
Shadowcopy Delete
PS C:\Users\Administrator\Desktop> _
```

Now I see the alerts on the dashboard related to ransomware attacks.

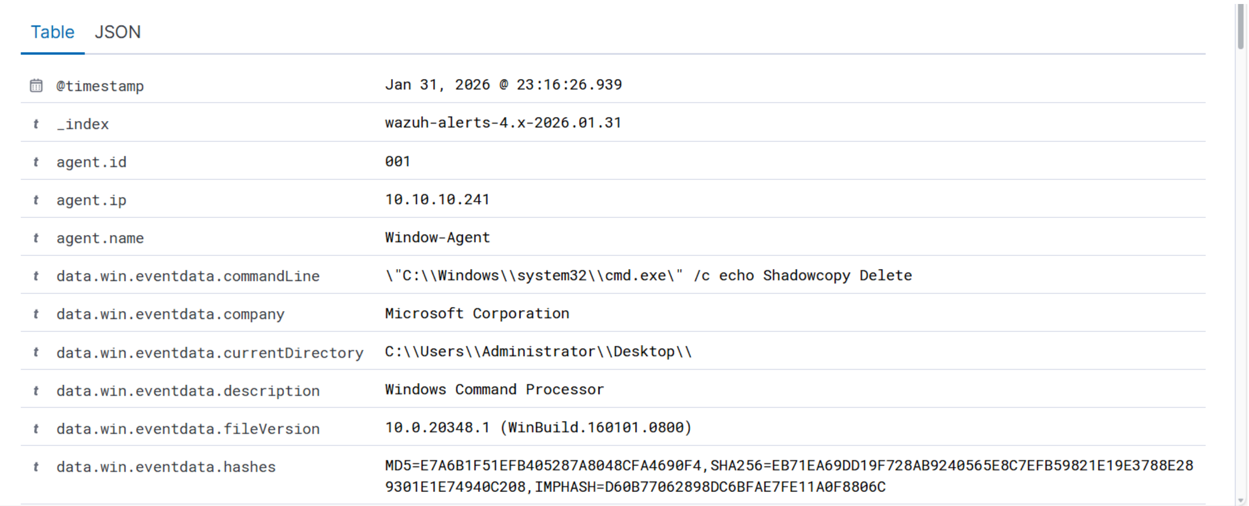


2 hits

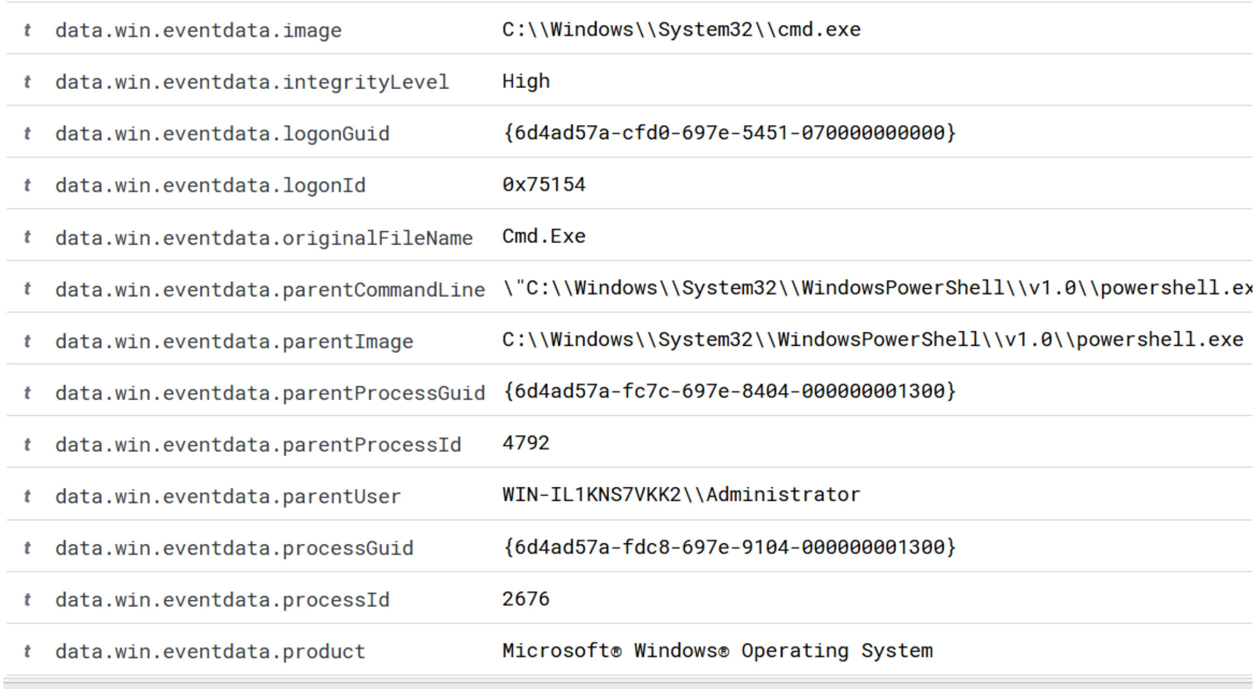
Jan 30, 2026 @ 23:20:23.662 - Jan 31, 2026 @ 23:20:23.662

timestamp	agent.name	rule.description	rule.le...	rule.id
Jan 31, 2026 @ 23:16:26.955	Window-Agent	Ransomware activity detected.	12	100628
Jan 31, 2026 @ 23:16:26.939	Window-Agent	Volume shadow copy deleted using Cmd.Exe. Potential ra...	12	100617

Details:

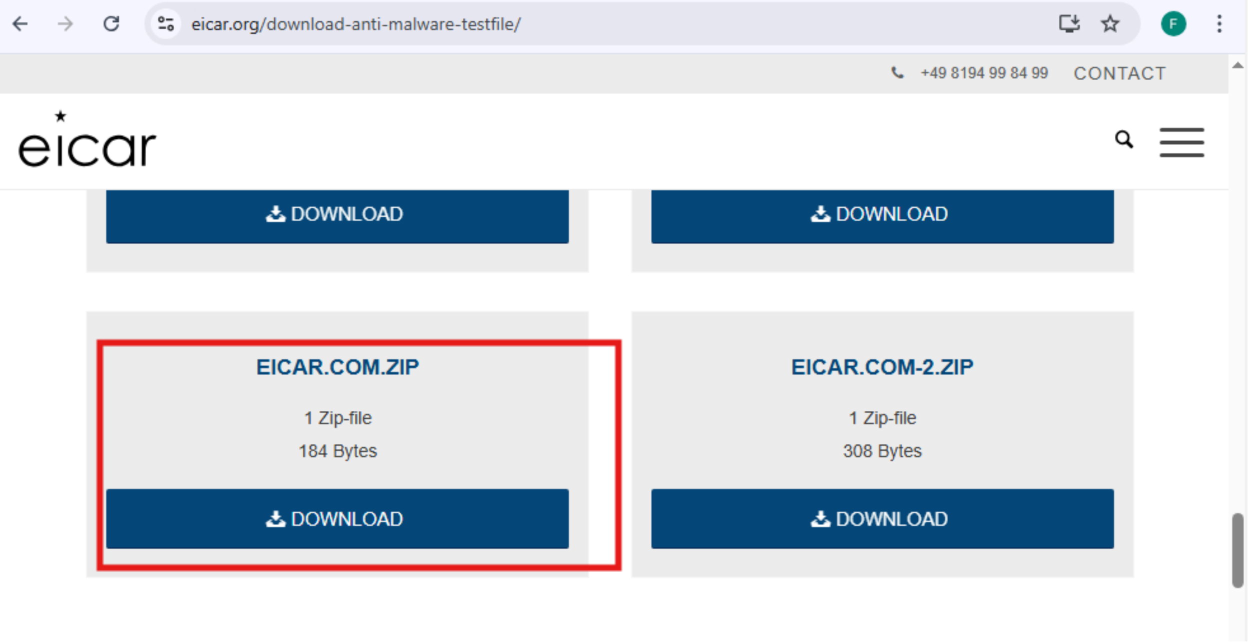


📅	@timestamp	Jan 31, 2026 @ 23:16:26.939
t	_index	wazuh-alerts-4.x-2026.01.31
t	agent.id	001
t	agent.ip	10.10.10.241
t	agent.name	Window-Agent
t	data.win.eventdata.commandLine	\\"C:\\\\Windows\\\\system32\\\\cmd.exe\\" /c echo Shadowcopy Delete
t	data.win.eventdata.company	Microsoft Corporation
t	data.win.eventdata.currentDirectory	C:\\\\Users\\\\Administrator\\\\Desktop\\\\
t	data.win.eventdata.description	Windows Command Processor
t	data.win.eventdata.fileVersion	10.0.20348.1 (WinBuild.160101.0800)
t	data.win.eventdata.hashes	MD5=E7A6B1F51EFB405287A8048CFA4690F4,SHA256=EB71EA69DD19F728AB9240565E8C7EFB59821E19E3788E289301E1E74940C208,IMPHASH=D60B77062898DC6BFAE7FE11A0F8806C



t	data.win.eventdata.image	C:\\\\Windows\\\\System32\\\\cmd.exe
t	data.win.eventdata.integrityLevel	High
t	data.win.eventdata.logonGuid	{6d4ad57a-cfd0-697e-5451-070000000000}
t	data.win.eventdata.logonId	0x75154
t	data.win.eventdata.originalFileName	Cmd.Exe
t	data.win.eventdata.parentCommandLine	\\"C:\\\\Windows\\\\System32\\\\WindowsPowerShell\\\\v1.0\\\\powershell.ex
t	data.win.eventdata.parentImage	C:\\\\Windows\\\\System32\\\\WindowsPowerShell\\\\v1.0\\\\powershell.exe
t	data.win.eventdata.parentProcessGuid	{6d4ad57a-fc7c-697e-8404-000000001300}
t	data.win.eventdata.parentProcessId	4792
t	data.win.eventdata.parentUser	WIN-IL1KNS7VKK2\\\\Administrator
t	data.win.eventdata.processGuid	{6d4ad57a-fdc8-697e-9104-000000001300}
t	data.win.eventdata.processId	2676
t	data.win.eventdata.product	Microsoft® Windows® Operating System

When I download the malicious file then the file is automatically removed from the system.



EICAR.COM.ZIP

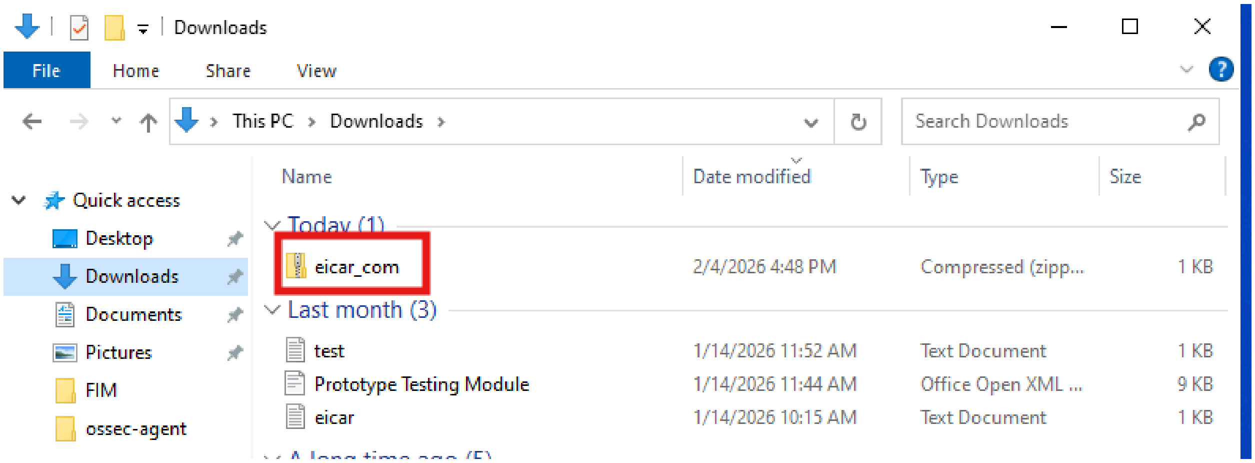
1 Zip-file

184 Bytes

EICAR.COM-2.ZIP

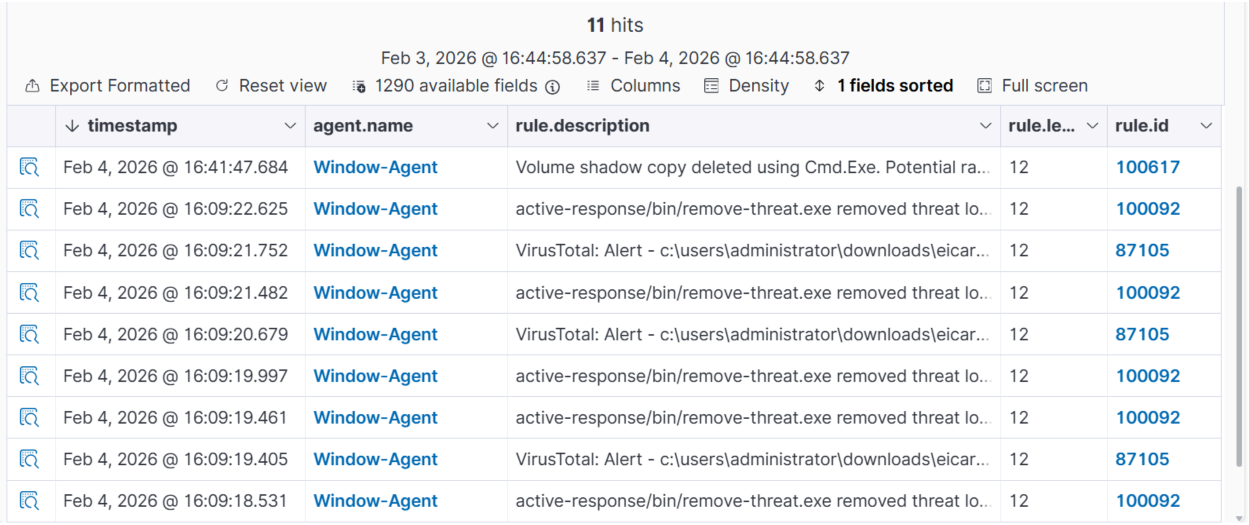
1 Zip-file

308 Bytes



Name	Date modified	Type	Size
Today (1)			
eicar_com	2/4/2026 4:48 PM	Compressed (zipp...	1 KB
Last month (3)			
test	1/14/2026 11:52 AM	Text Document	1 KB
Prototype Testing Module	1/14/2026 11:44 AM	Office Open XML ...	9 KB
eicar	1/14/2026 10:15 AM	Text Document	1 KB
A long time ago (5)			

Now file is removed and alerts are shown in the Dashboard;

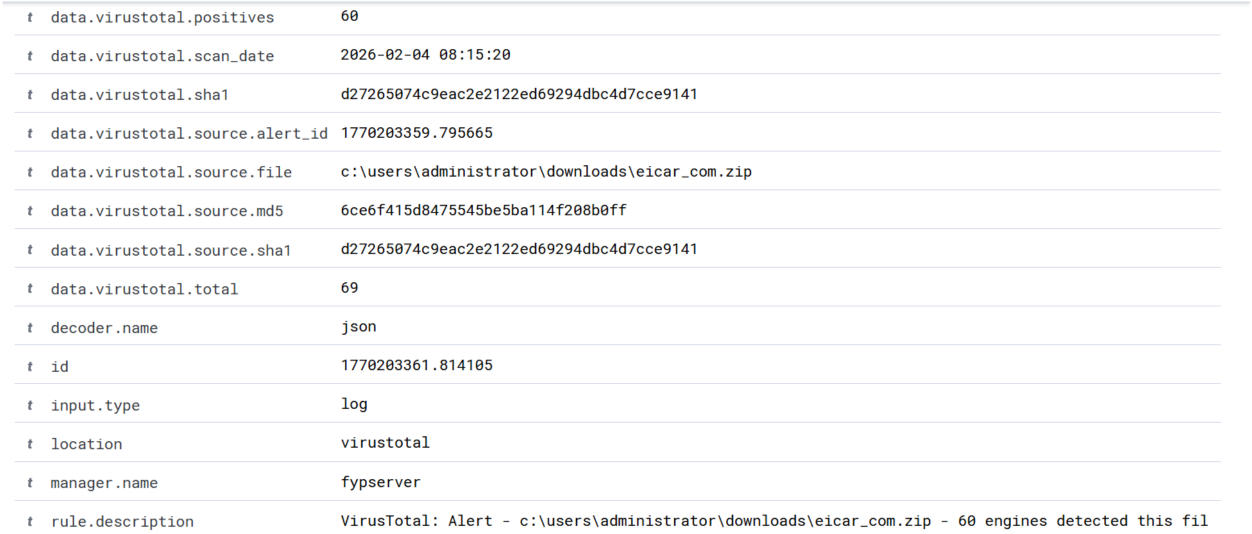


11 hits

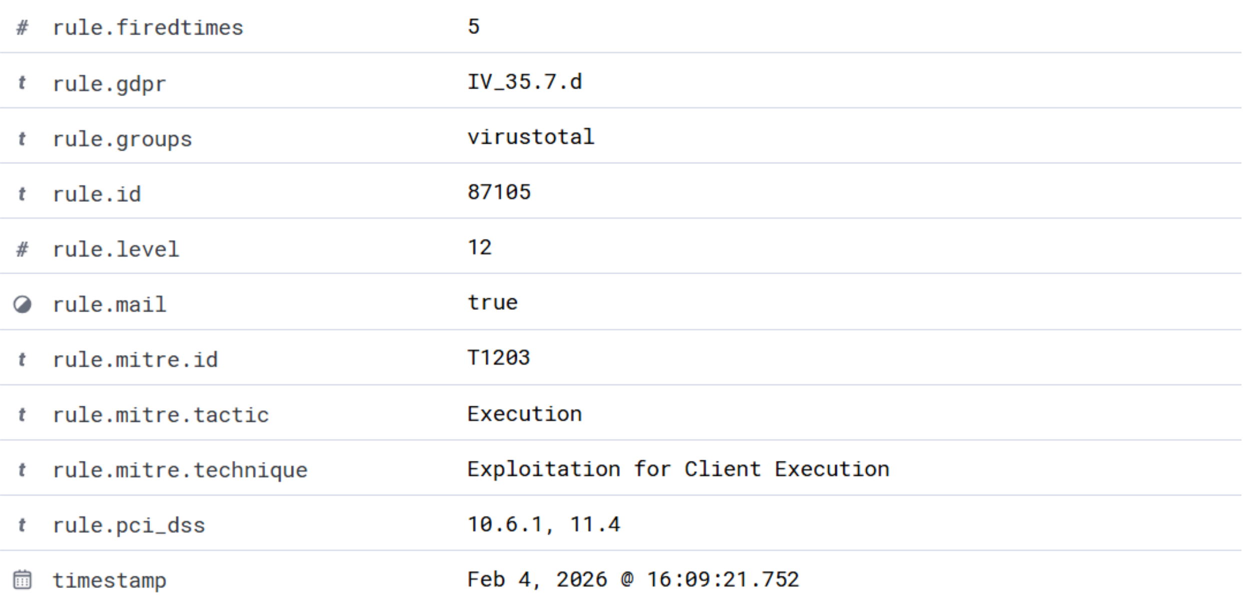
Feb 3, 2026 @ 16:44:58.637 - Feb 4, 2026 @ 16:44:58.637

timestamp	agent.name	rule.description	rule.le...	rule.id
Feb 4, 2026 @ 16:41:47.684	Window-Agent	Volume shadow copy deleted using Cmd.Exe. Potential ra...	12	100617
Feb 4, 2026 @ 16:09:22.625	Window-Agent	active-response/bin/remove-threat.exe removed threat lo...	12	100092
Feb 4, 2026 @ 16:09:21.752	Window-Agent	VirusTotal: Alert - c:\users\administrator\downloads\eicar...	12	87105
Feb 4, 2026 @ 16:09:21.482	Window-Agent	active-response/bin/remove-threat.exe removed threat lo...	12	100092
Feb 4, 2026 @ 16:09:20.679	Window-Agent	VirusTotal: Alert - c:\users\administrator\downloads\eicar...	12	87105
Feb 4, 2026 @ 16:09:19.997	Window-Agent	active-response/bin/remove-threat.exe removed threat lo...	12	100092
Feb 4, 2026 @ 16:09:19.461	Window-Agent	active-response/bin/remove-threat.exe removed threat lo...	12	100092
Feb 4, 2026 @ 16:09:19.405	Window-Agent	VirusTotal: Alert - c:\users\administrator\downloads\eicar...	12	87105
Feb 4, 2026 @ 16:09:18.531	Window-Agent	active-response/bin/remove-threat.exe removed threat lo...	12	100092

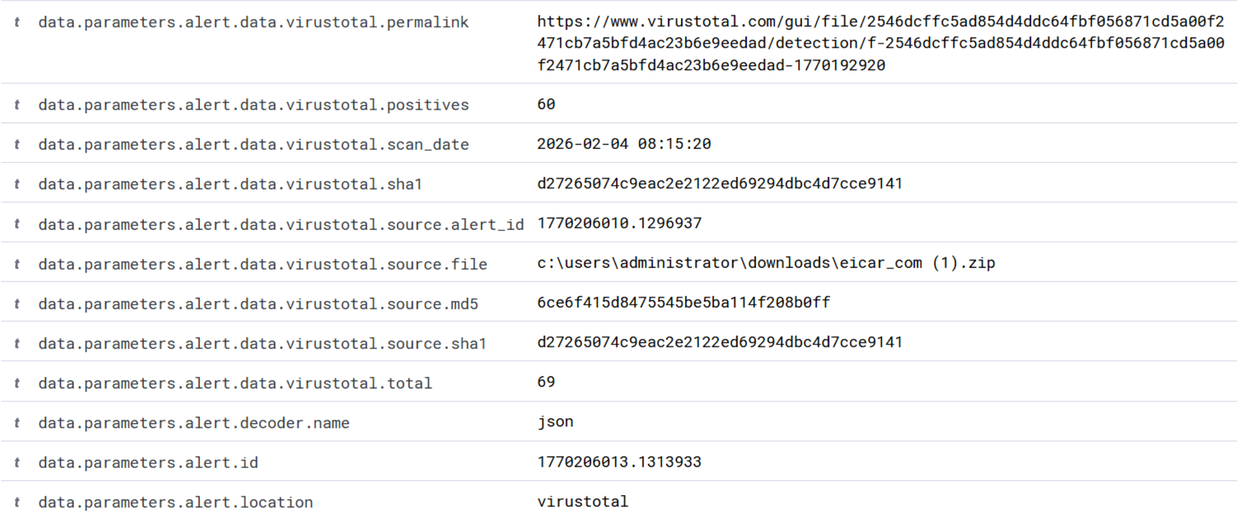
Details:



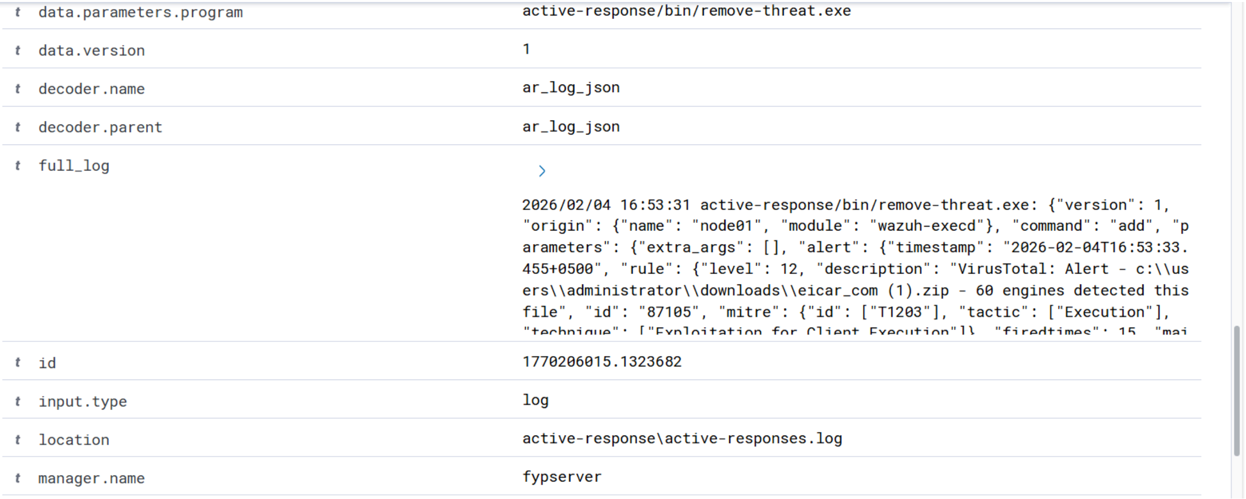
t	data.virustotal.positives	60
t	data.virustotal.scan_date	2026-02-04 08:15:20
t	data.virustotal.sha1	d27265074c9eac2e2122ed69294dbc4d7cce9141
t	data.virustotal.source.alert_id	1770203359.795665
t	data.virustotal.source.file	c:\users\administrator\downloads\eicar_com.zip
t	data.virustotal.source.md5	6ce6f415d8475545be5ba114f208b0ff
t	data.virustotal.source.sha1	d27265074c9eac2e2122ed69294dbc4d7cce9141
t	data.virustotal.total	69
t	decoder.name	json
t	id	1770203361.814105
t	input.type	log
t	location	virustotal
t	manager.name	fypserver
t	rule.description	VirusTotal: Alert - c:\users\administrator\downloads\eicar_com.zip - 60 engines detected this fil



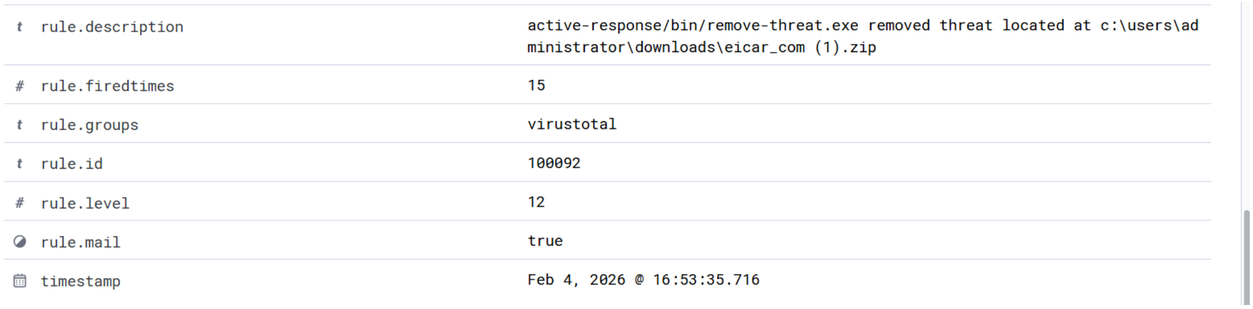
#	rule.firedtimes	5
t	rule.gdpr	IV_35.7.d
t	rule.groups	virustotal
t	rule.id	87105
#	rule.level	12
◑	rule.mail	true
t	rule.mitre.id	T1203
t	rule.mitre.tactic	Execution
t	rule.mitre.technique	Exploitation for Client Execution
t	rule.pci_dss	10.6.1, 11.4
📅	timestamp	Feb 4, 2026 @ 16:09:21.752



t	data.parameters.alert.data.virustotal.permalink	https://www.virustotal.com/gui/file/2546dcffc5ad854d4ddc64fbf056871cd5a00f2471cb7a5bfd4ac23b6e9eedad/detection/f-2546dcffc5ad854d4ddc64fbf056871cd5a00f2471cb7a5bfd4ac23b6e9eedad-1770192920
t	data.parameters.alert.data.virustotal.positives	60
t	data.parameters.alert.data.virustotal.scan_date	2026-02-04 08:15:20
t	data.parameters.alert.data.virustotal.sha1	d27265074c9eac2e2122ed69294dbc4d7cce9141
t	data.parameters.alert.data.virustotal.source.alert_id	1770206010.1296937
t	data.parameters.alert.data.virustotal.source.file	c:\users\administrator\downloads\eicar_com (1).zip
t	data.parameters.alert.data.virustotal.source.md5	6ce6f415d8475545be5ba114f208b0ff
t	data.parameters.alert.data.virustotal.source.sha1	d27265074c9eac2e2122ed69294dbc4d7cce9141
t	data.parameters.alert.data.virustotal.total	69
t	data.parameters.alert.decoder.name	json
t	data.parameters.alert.id	1770206013.1313933
t	data.parameters.alert.location	virustotal



t	data.parameters.program	active-response/bin/remove-threat.exe
t	data.version	1
t	decoder.name	ar_log_json
t	decoder.parent	ar_log_json
t	full_log	› 2026/02/04 16:53:31 active-response/bin/remove-threat.exe: {"version": 1, "origin": {"name": "node01", "module": "wazuh-execd"}, "command": "add", "parameters": {"extra_args": [], "alert": {"timestamp": "2026-02-04T16:53:33.455+0500", "rule": {"level": 12, "description": "VirusTotal: Alert - c:\\users\\administrator\\downloads\\eicar_com (1).zip - 60 engines detected this file", "id": "87105", "mitre": {"id": ["T1203"], "tactic": ["Execution"], "technique": ["Exploitation for Client Execution"]}, "firedtimes": 15, "mai
t	id	1770206015.1323682
t	input.type	log
t	location	active-response\active-responses.log
t	manager.name	fypserver



t	rule.description	active-response/bin/remove-threat.exe removed threat located at c:\users\administrator\downloads\eicar_com (1).zip
#	rule.firedtimes	15
t	rule.groups	virustotal
t	rule.id	100092
#	rule.level	12
◐	rule.mail	true
📅	timestamp	Feb 4, 2026 @ 16:53:35.716

Summary:

In this project, I implemented ransomware detection using Wazuh on a Windows machine. For testing, I created some sample files on the desktop and ran a safe encryption script that simulates real ransomware behavior. The Wazuh agent on the Windows system monitored these files and tracked all changes, such as file creation, modification, and deletion. These events were sent to the Wazuh manager for analysis.

The Wazuh manager detected suspicious activity, like multiple files being encrypted quickly and unusual file extensions appearing. When this behavior was found, alerts were generated on the Wazuh dashboard, showing details like file names, locations, and timestamps. This confirmed that Wazuh can detect ransomware activity in real time.

After the detection, I used a restore script to safely recover all original files from the backup. This ensured no data was lost and the system returned to normal. This project shows that Wazuh can automatically detect ransomware-like behavior, alert administrators, and protect data before any real damage happens.