

**Kịch bản:** Không sử dụng máy attacker. Trong trường hợp này chúng ta sẽ giám sát tính toàn vẹn của tệp và dùng API VirusTotal để quét các tệp đó. Sau đó, ta sẽ cấu hình Wazuh Server để kích hoạt lệnh phản hồi và xóa các tệp mà VirusTotal phát hiện là độc hại. Để sử dụng VirusTotal, chúng ta cần khóa API VirusTotal. Trong trường hợp sử dụng này để xác thực Wazuh Server với API VirusTotal.

## 1.Kịch bản tải malware ở máy Agent Ubuntu

- Ở máy Agent Ubuntu

**B1: Cấu hình file ossec.conf. Cấu hình trong khối <syscheck> để thay đổi định dạng giám sát thư mục root theo thời gian thực.**

nano /var/ossec/etc/ossec.conf

Thêm:

<directories realtime="yes">/root</directories>

```
<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>
  <directories realtime="yes">/root</directories>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>

  <scan_on_start>yes</scan_on_start>

  <!-- Directories to check (perform all possible verifications) -->
  <directories>/etc,/usr/bin,/usr/sbin</directories>
  <directories>/bin,/sbin,/boot</directories>
```

**B2: Để xử lý đầu vào json từ tập lệnh active response, ta cần cài đặt jq cho máy Agent**

apt install jq

**B3: Tạo file** `/var/ossec/active-response/bin/remove-threat.sh`

Để kích hoạt phản hồi xóa file độc hại từ endpoint

Thêm đoạn script sau:

#!/bin/bash

```
LOCAL=`dirname $0`;
```

```
cd $LOCAL
```

```
cd ../
```

```
PWD=`pwd`
```

```
read INPUT_JSON
```

```
FILENAME=$(echo $INPUT_JSON | jq -r  
.parameters.alert.data.virustotal.source.file)
```

```
COMMAND=$(echo $INPUT_JSON | jq -r .command)
```

```
LOG_FILE="${PWD}/../logs/active-responses.log"
```

```
#----- Analyze command -----#
```

```
if [ ${COMMAND} = "add" ]
```

```
then
```

```
# Send control message to execd
```

```
printf '{"version":1,"origin":{"name":"remove-threat","module":"active-  
response"},"command":"check_keys", "parameters":{"keys":[]}}\n'
```

```
read RESPONSE
```

```
COMMAND2=$(echo $RESPONSE | jq -r .command)
```

```
if [ ${COMMAND2} != "continue" ]
```

```
then
```

```
echo "`date '+%Y/%m/%d %H:%M:%S'` $0: $INPUT_JSON Remove threat active  
response aborted" >> ${LOG_FILE}
```

```
exit 0;
```

fi

fi

# Removing file

rm -f \$FILENAME

if [ \$? -eq 0 ]; then

echo "`date '+%Y/%m/%d %H:%M:%S'` \$0: \$INPUT\_JSON Successfully removed threat" >> \${LOG\_FILE}

else

echo "`date '+%Y/%m/%d %H:%M:%S'` \$0: \$INPUT\_JSON Error removing threat" >> \${LOG\_FILE}

fi

exit 0;

```
GNU nano 6.2 /var/ossec/active-response/bin/remove-threat.sh *
#!/bin/bash

LOCAL=`dirname $0`;
cd $LOCAL
cd ../

PWD=`pwd`

read INPUT_JSON
FILENAME=$(echo $INPUT_JSON | jq -r .parameters.alert.data.virustotal.source.file)
COMMAND=$(echo $INPUT_JSON | jq -r .command)
LOG_FILE="${PWD}/../logs/active-responses.log"

----- Analyze command -----#
if [ ${COMMAND} = "add" ]
then
# Send control message to execd
printf '{"version":1,"origin":{"name":"remove-threat","module":"active-response"},"command":"c

read RESPONSE
COMMAND2=$(echo $RESPONSE | jq -r .command)
if [ ${COMMAND2} != "continue" ]
then
echo "`date '+%Y/%m/%d %H:%M:%S'` $0: $INPUT_JSON Remove threat active response aborted" >> $
exit 0;
fi
fi

Removing file
rm -f $FILENAME
if [ $? -eq 0 ]; then
echo "`date '+%Y/%m/%d %H:%M:%S'` $0: $INPUT_JSON Successfully removed threat" >> ${LOG_FILE}
else
echo "`date '+%Y/%m/%d %H:%M:%S'` $0: $INPUT_JSON Error removing threat" >> ${LOG_FILE}
fi

exit 0;else
```

#### B4: Thay đổi quyền sở hữu và quyền của tệp `/var/ossec/active-response/bin/remove-threat.sh`

`sudo chmod 750 /var/ossec/active-response/bin/remove-threat.sh`

`sudo chown root:wazuh /var/ossec/active-response/bin/remove-threat.sh`

#### B5: Khởi động lại Wazuh Agent để áp dụng các thay đổi

`sudo systemctl restart wazuh-agent`

- Ở máy Wazuh Server

## **B1: Thêm các quy tắc sau vào tệp local\_rules.xml**

Các quy tắc này được thêm vào để cảnh báo về những thay đổi trong thư mục root được phát hiện khi FIM quét

```
nano /var/ossec/etc/rules/local_rules.xml
```

Thêm đoạn script:

```
<group name="syscheck,pci_dss_11.5,nist_800_53_SI.7,">
  <!-- Rules for Linux systems -->
  <rule id="100200" level="7">
    <if_sid>550</if_sid>
    <field name="file">/root</field>
    <description>File modified in /root directory.</description>
  </rule>
  <rule id="100201" level="7">
    <if_sid>554</if_sid>
    <field name="file">/root</field>
    <description>File added to /root directory.</description>
  </rule>
</group>
```

```

GNU nano 6.2 /var/ossec/etc/rules/local_rules.xml *

<!-- Example -->
<group name="local,syslog,sshd,">

  <!--
  Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 ssh2
  -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>

</group>

<group name="attack">
  <rule id="100100" level="10">
    <if_group>web|attack|attacks</if_group>
    <list field="srcip" lookup="address_match_key">etc/lists/blacklist-alienvault</list>
    <description>IP address found in Alienvault reputation database</description>
  </rule>
</group>

<group name="syscheck,pci_dss_11.5,nist_800_53_SI.7,">
  <!-- Rules for Linux systems -->
  <rule id="100200" level="7">
    <if_sid>550</if_sid>
    <field name="file">/root</field>
    <description>File modified in /root directory.</description>
  </rule>
  <rule id="100201" level="7">
    <if_sid>554</if_sid>
    <field name="file">/root</field>
    <description>File added to /root directory.</description>
  </rule>
</group>

```

## B2: Thêm script quy tắc vào file ossec.conf vào máy wazuh server

nano /var/ossec/etc/ossec.conf

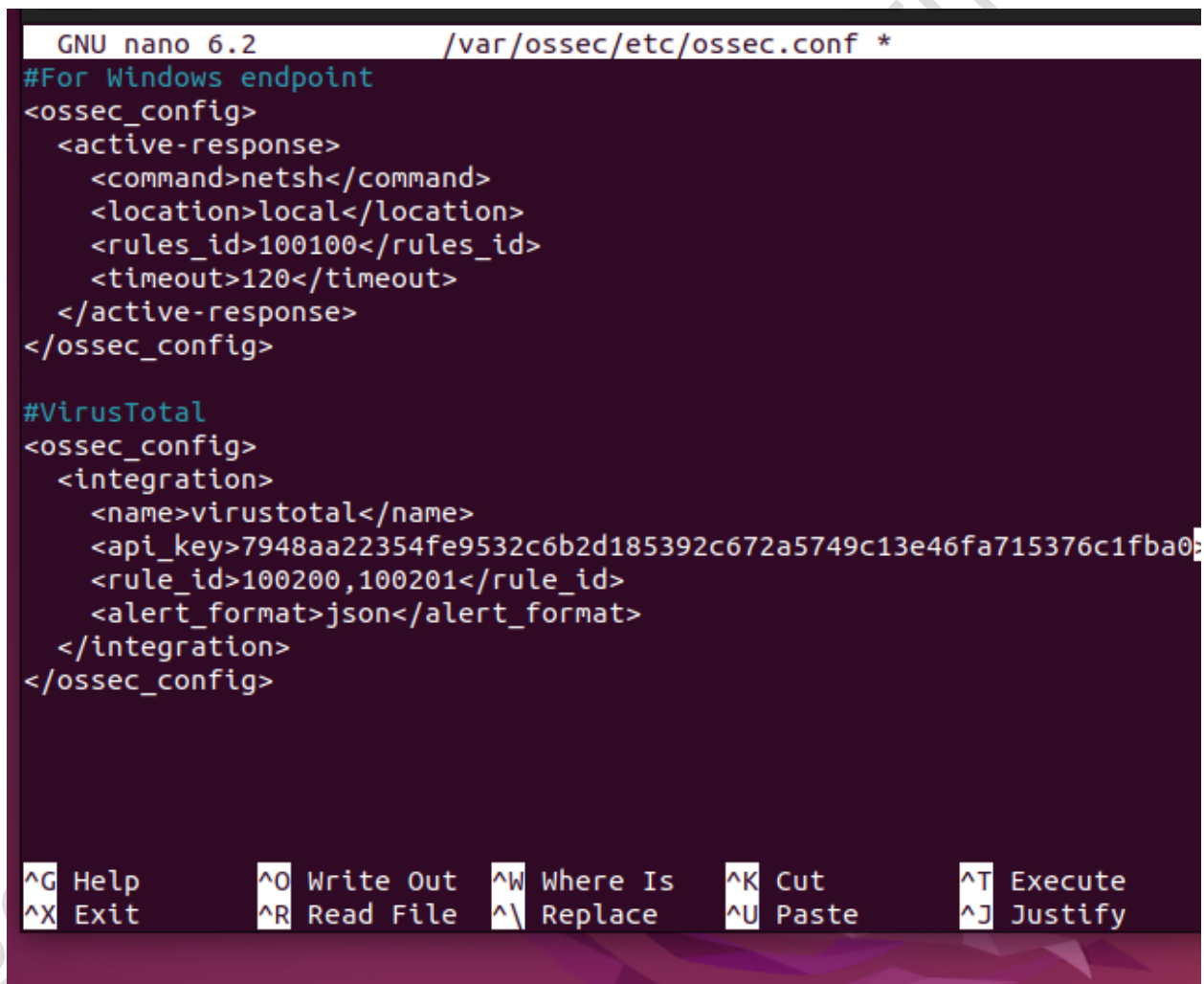
Để kích hoạt tích hợp VirusTotal, ta cần thay thế VirusTotal API Key mặc định bằng khóa API Key VirusTotal của mình. Điều này kích hoạt truy vấn VirusTotal bất cứ khi nào.

Thêm :

#VirusTotal

<ossec\_config>

```
<integration>
  <name>virustotal</name>
  <api_key>7948aa22354fe9532c6b2d1c13e46fa715376c1fba0</api_key> <!--
Replace with your VirusTotal API key ->
  <rule_id>100200,100201</rule_id>
  <alert_format>json</alert_format>
</integration>
</ossec_config>
```



```
GNU nano 6.2 /var/ossec/etc/ossec.conf *
#For Windows endpoint
<ossec_config>
  <active-response>
    <command>netsh</command>
    <location>local</location>
    <rules_id>100100</rules_id>
    <timeout>120</timeout>
  </active-response>
</ossec_config>

#VirusTotal
<ossec_config>
  <integration>
    <name>virustotal</name>
    <api_key>7948aa22354fe9532c6b2d185392c672a5749c13e46fa715376c1fba0</api_key>
    <rule_id>100200,100201</rule_id>
    <alert_format>json</alert_format>
  </integration>
</ossec_config>
```

Tiếp tục thêm:

```
<ossec_config>
  <command>
    <name>remove-threat</name>
    <executable>remove-threat.sh</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>
</ossec_config>
```

```
#VirusTotal
<ossec_config>
  <integration>
    <name>virustotal</name>
    <api_key>7948aa22354fe9532c6b2d185392c672a5</api_key>
    <rule_id>100200,100201</rule_id>
    <alert_format>json</alert_format>
  </integration>
</ossec_config>

<ossec_config>
  <command>
    <name>remove-threat</name>
    <executable>remove-threat.sh</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>
</ossec_config>
```



Điều này cho phép trực tiếp phản hồi và kích hoạt tập lệnh remove.sh khi VirusTotal gắn cờ một tệp là độc hại.

### **B3: Thêm quy tắc sau vào tệp local\_rules.xml vào máy Wazuh server**

```
nano /var/ossec/etc/rules/local_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)</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>
```

```

<!-- Rules for Linux systems -->
<rule id="100200" level="7">
  <if_sid>550</if_sid>
  <field name="file">/root</field>
  <description>File modified in /root directory.</description>
</rule>
<rule id="100201" level="7">
  <if_sid>554</if_sid>
  <field name="file">/root</field>
  <description>File added to /root directory.</description>
</rule>
</group>

<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.vir
  </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.
  </rule>
</group>

```

Khôi lệnh này cảnh báo về kết quả phản hồi đang hoạt động

#### **B4: Khởi động lại máy Wazuh server để áp dụng các thay đổi**

systemctl restart wazuh-manager.service

**Tại máy Agent Ubuntu tải xuống một tệp độc hại thử nghiệm vào thư mục root**

curl -LO <https://secure.eicar.org/eicar.com> && ls -lah eicar.com

```

root@ubuntu-agent:~# curl -LO https://secure.eicar.org/eicar.com && ls -lah eicar.com
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload  Total   Spent    Left     Speed
100    68  100    68    0     0    17      0  0:00:04  0:00:03  0:00:01   17
-rw-r--r-- 1 root root 68 0.0 1 14:46 eicar.com
root@ubuntu-agent:~#

```

**Kết quả:**

Security Alerts						
Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID	
Oct 1, 2024 > @ 16:40:10.17 6			active-response/bin/remove-threat.sh removed threat located at /root/eicar.com	12	100092	
Oct 1, 2024 > @ 16:40:08.99 1	T1070.004 T1485	Defense Evasion, Impact	File deleted.	7	553	
Oct 1, 2024 > @ 16:40:08.71 0	T1203	Execution	VirusTotal: Alert - /root/eicar.com - 63 engines detected this file	12	87105	

- Phát hiện cảnh báo file độc hại với Rule ID là 87105 và level là 12. Cấp cảnh báo 12 này cho ta biết là event rất quan trọng

Total	Level 12 or above alerts	Authentication failure	Authentication success
<b>104</b>	<b>5</b>	<b>0</b>	<b>8</b>

- Có 63 công cụ đã phát hiện ra file này là file độc hại

location	virustotal
manager.name	anh-attt
rule.description	VirusTotal: Alert - /root/eicar.com - 63 engines detected this file
rule.firedtimes	1

- Và Wazuh đã xóa file độc hại này ngay sau đó

Oct 1, 2024				
✓ @	T1070.004	T1485	Defense Evasion, Impact	File deleted.
16:40:08.99				
1				

**Table**   **JSON**   **Rule**

@timestamp	2024-10-01T09:40:08.991Z
_id	JupzR5IB9Dlp8o-apYEI
agent.id	001
agent.ip	192.168.198.148
agent.name	ubuntu-agent
decoder.name	syscheck_deleted

full_log	File '/root/eicar.com' deleted Mode: realtime
----------	--

- Cuối cùng là hiển thị phản hồi xóa threat nằm ở /root

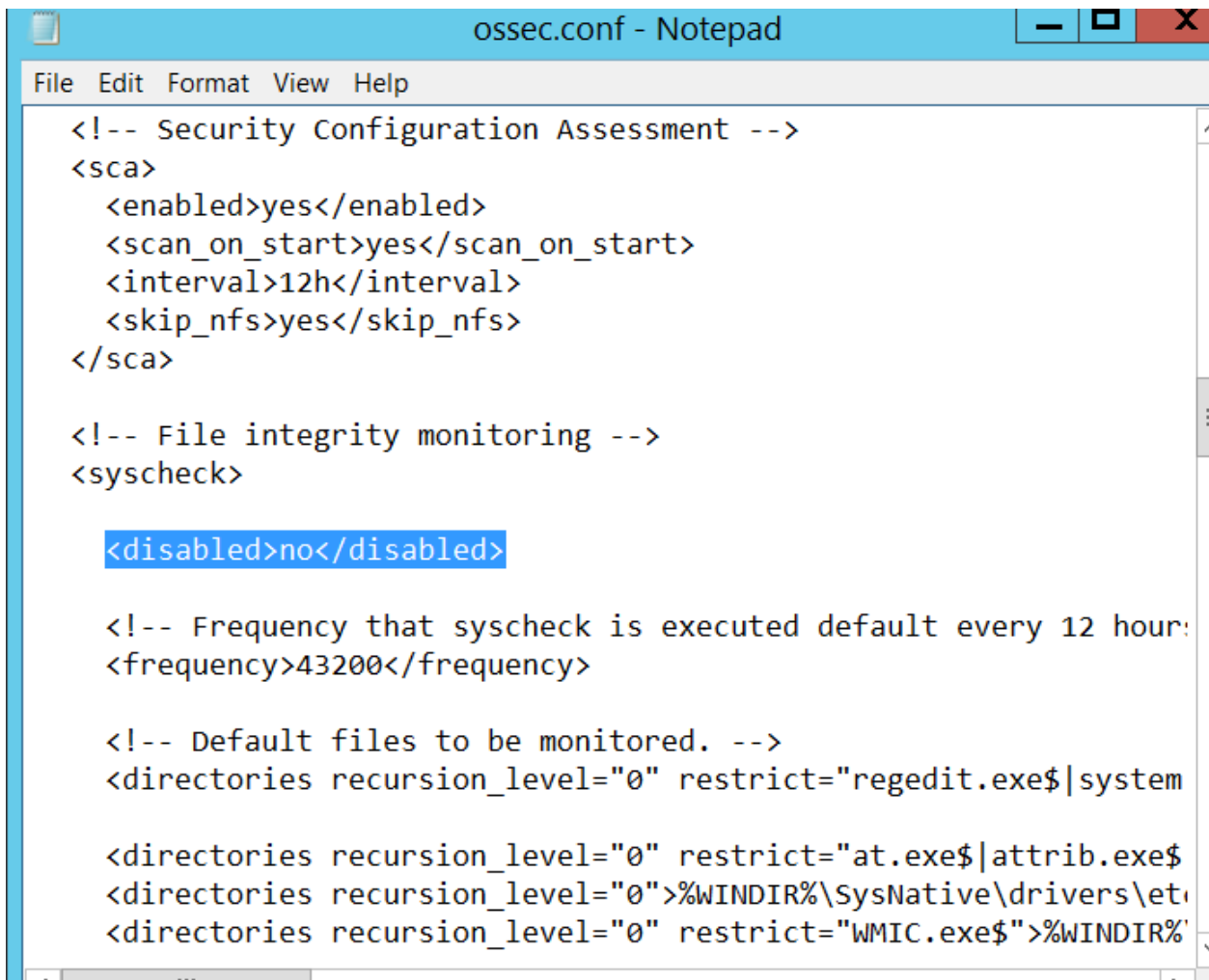
location	/var/ossec/logs/active-responses.log
manager.name	anh-attt
rule.description	active-response/bin/remove-threat.sh removed threat located at /root/eicar.com
rule.firedtimes	1

## 2. Kịch bản tải malware ở máy Agent Windows Server

- Ở máy Agent Windows Server

### B1: Vào tệp ossec.conf

Tìm khối `<syscheck>`: đảm bảo nó được đặt `<disabled>no</disabled>`



```
ossec.conf - Notepad
File Edit Format View Help

<!-- 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

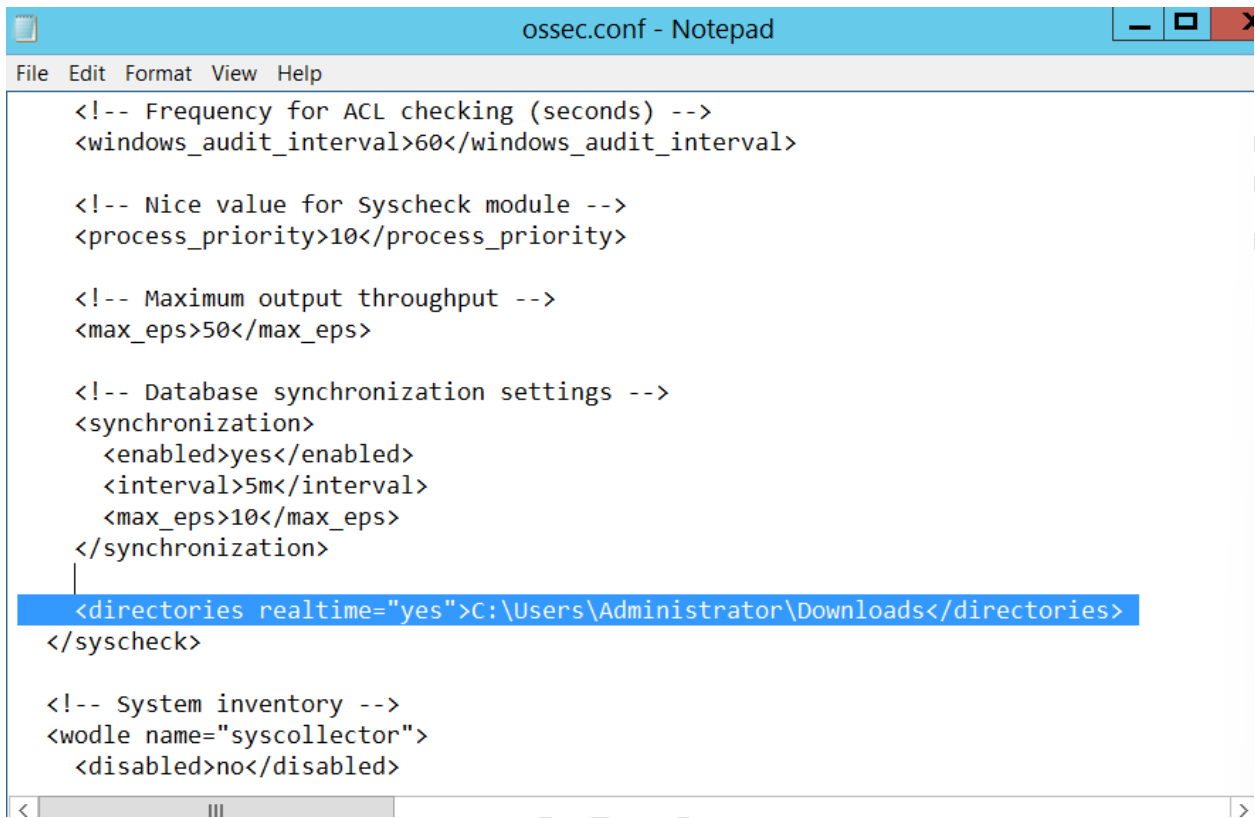
  <directories recursion_level="0" restrict="at.exe$|attrib.exe$
  <directories recursion_level="0">%WINDIR%\SysNative\drivers\etc
  <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%
```

⇒ Điều này cho phép module Wazuh FIM giám sát các thay đổi thư mục

Thêm script trong khối <syscheck> để định cấu hình 1 thư mục để được theo dõi theo thời gian thực realtime.

Trong TH này, định cấu hình Wazuh để giám sát thư mục :

```
<directories realtime="yes">C:\Users\Administrator\Downloads</directories>
```



```
<!-- Frequency for ACL checking (seconds) -->
<windows_audit_interval>60</windows_audit_interval>

<!-- Nice value for Syscheck module -->
<process_priority>10</process_priority>

<!-- Maximum output throughput -->
<max_eps>50</max_eps>

<!-- Database synchronization settings -->
<synchronization>
  <enabled>yes</enabled>
  <interval>5m</interval>
  <max_eps>10</max_eps>
</synchronization>

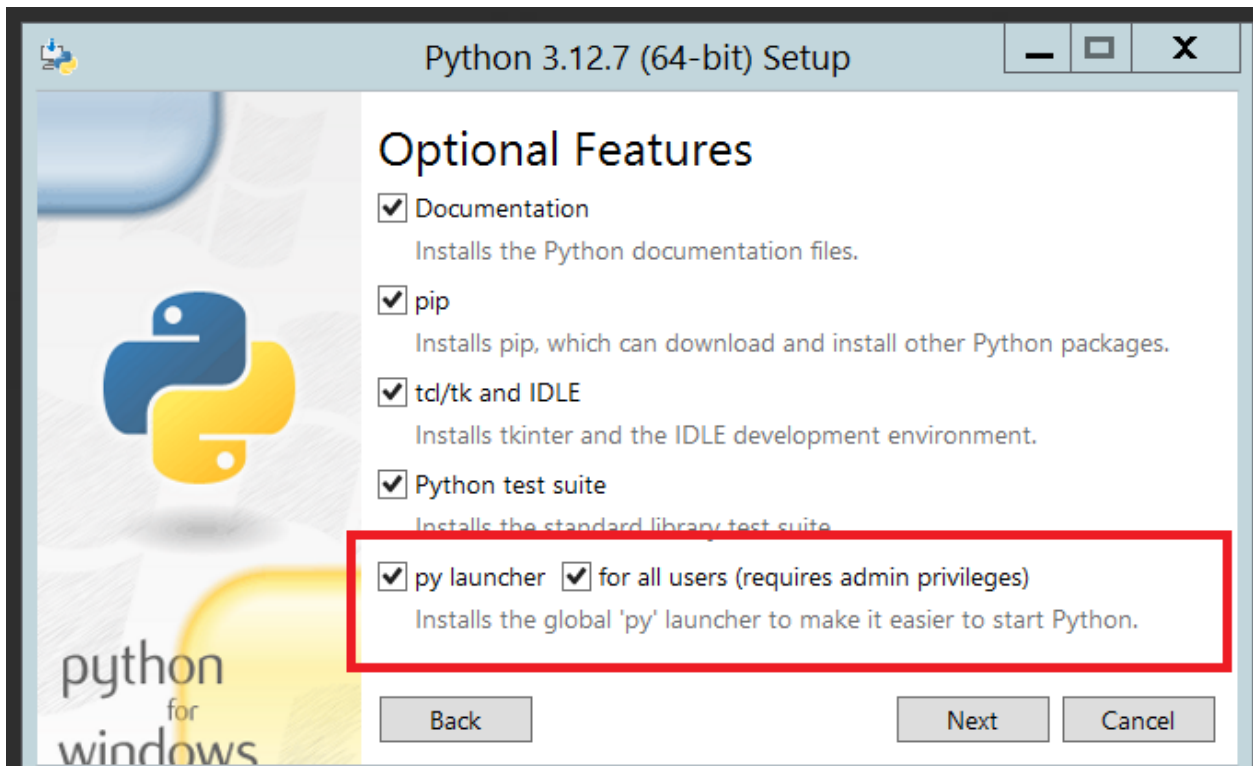
<directories realtime="yes">C:\Users\Administrator\Downloads</directories>
</syscheck>

<!-- System inventory -->
<wodle name="syscollector">
  <disabled>no</disabled>
```

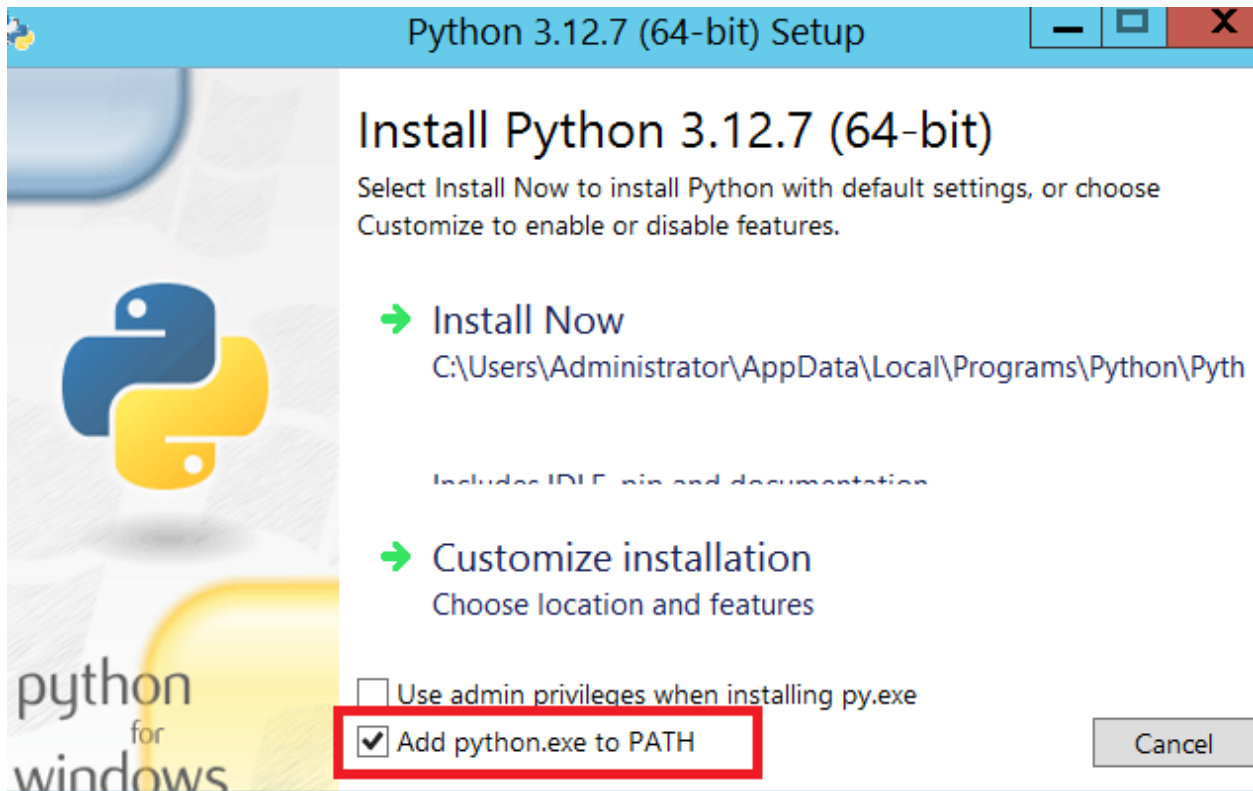
**B2:** Tải xuống trình cài đặt thực thi Python từ [trang web chính thức của Python](#) .

**B3:** Chạy trình cài đặt Python sau khi tải xuống. Đảm bảo kiểm tra các box sau:

- `Install launcher for all users`



- [Add Python 3.X to PATH](#) (Điều này đặt trình thông dịch vào đường dẫn thực thi)



Kiểm tra xem python đã cài thành công chưa

**B4:** Sau khi Python hoàn tất quá trình cài đặt, hãy mở terminal PowerShell dành cho quản trị viên và sử dụng **pip** để cài đặt PyInstaller:

`pip install pyinstaller`

`pyinstaller --version`



```

PS C:\Users\Administrator\Downloads> pip install pyinstaller
Collecting pyinstaller
  Downloading pyinstaller-6.10.0-py3-none-win_amd64.whl.metadata (8.3 kB)
Collecting setuptools>=42.0.0 (from pyinstaller)
  Downloading setuptools-75.1.0-py3-none-any.whl.metadata (6.9 kB)
Collecting altgraph (from pyinstaller)
  Downloading altgraph-0.17.4-py2.py3-none-any.whl.metadata (7.3 kB)
Collecting pyinstaller-hooks-contrib>=2024.8 (from pyinstaller)
  Downloading pyinstaller_hooks_contrib-2024.8-py3-none-any.whl.metadata (16 kB)
Collecting packaging>=22.0 (from pyinstaller)
  Downloading packaging-24.1-py3-none-any.whl.metadata (3.2 kB)
Collecting pefile>=2022.5.30 (from pyinstaller)
  Downloading pefile-2024.8.26-py3-none-any.whl.metadata (1.4 kB)
Collecting pywin32-ctypes>=0.2.1 (from pyinstaller)
  Downloading pywin32_ctypes-0.2.3-py3-none-any.whl.metadata (3.9 kB)
Downloaded pyinstaller-6.10.0-py3-none-win_amd64.whl (1.3 MB)
----- 1.3/1.3 MB 7.6 MB/s eta 0:00:00
Downloaded packaging-24.1-py3-none-any.whl (53 kB)
Downloaded pefile-2024.8.26-py3-none-any.whl (74 kB)
Downloaded pyinstaller_hooks_contrib-2024.8-py3-none-any.whl (322 kB)
Downloaded pywin32_ctypes-0.2.3-py3-none-any.whl (30 kB)
Downloaded setuptools-75.1.0-py3-none-any.whl (1.2 MB)
----- 1.2/1.2 MB 10.5 MB/s eta 0:00:00
Downloaded altgraph-0.17.4-py2.py3-none-any.whl (21 kB)
Installing collected packages: altgraph, setuptools, pywin32-ctypes, pefile, pyinstaller
Successfully installed altgraph-0.17.4 packaging-24.1 pefile-2024.8.26 pyinstaller-6.10.0
PS C:\Users\Administrator\Downloads> pyinstaller --version
6.10.0

```

Ở đây, bạn sử dụng Pyinstaller để chuyển đổi tập lệnh Python phản hồi đang hoạt động thành ứng dụng thực thi có thể chạy trên điểm cuối endpoint Windows.

### **B5: Tạo một tập lệnh active response `remove-threat.py` để xóa tệp khỏi điểm cuối Windows**

Thêm đoạn script này vào file `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")

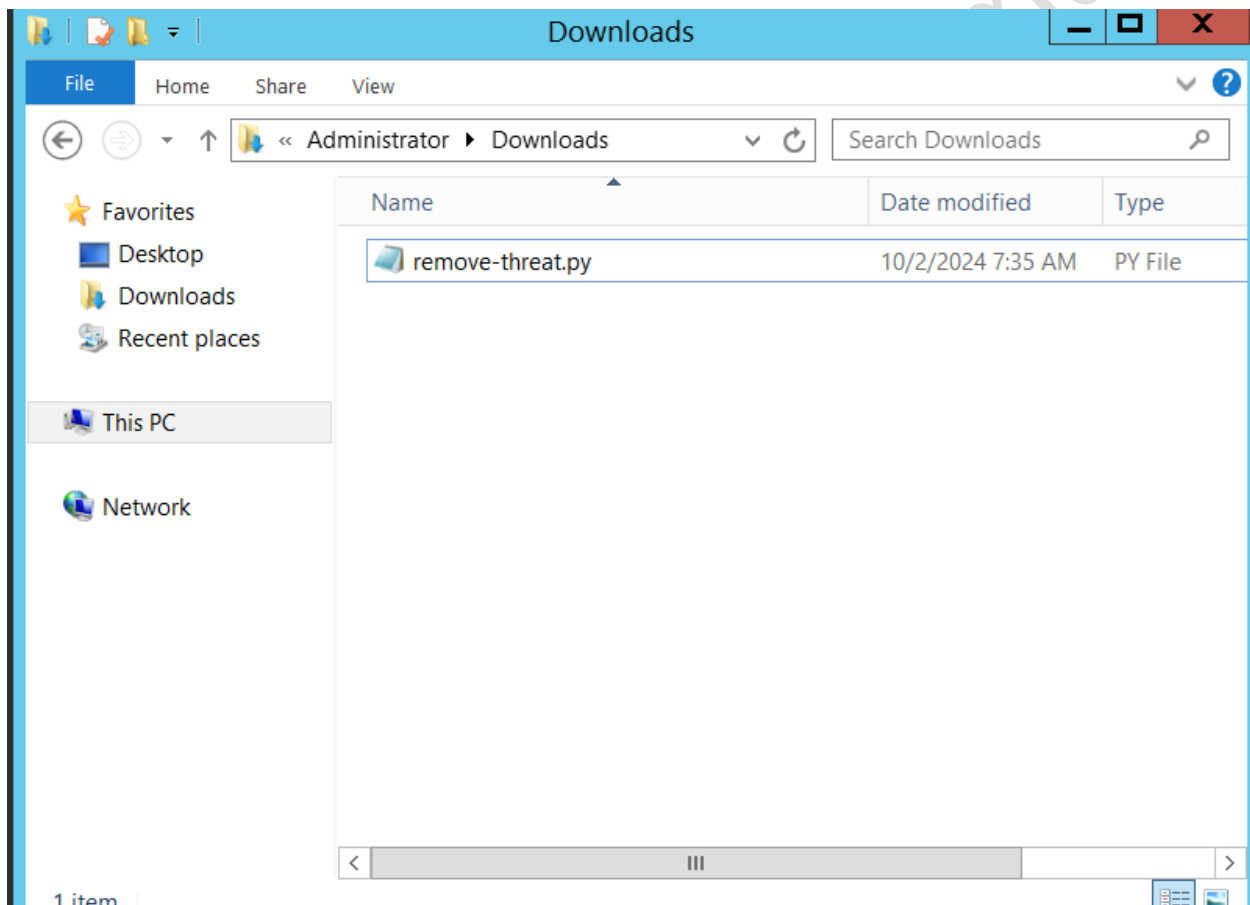
else:
    write_debug_file(argv[0], "Invalid command")
```

```
write_debug_file(argv[0], "Ended")
```

```
sys.exit(OS_SUCCESS)
```

```
if __name__ == "__main__":
```

```
    main(sys.argv)
```

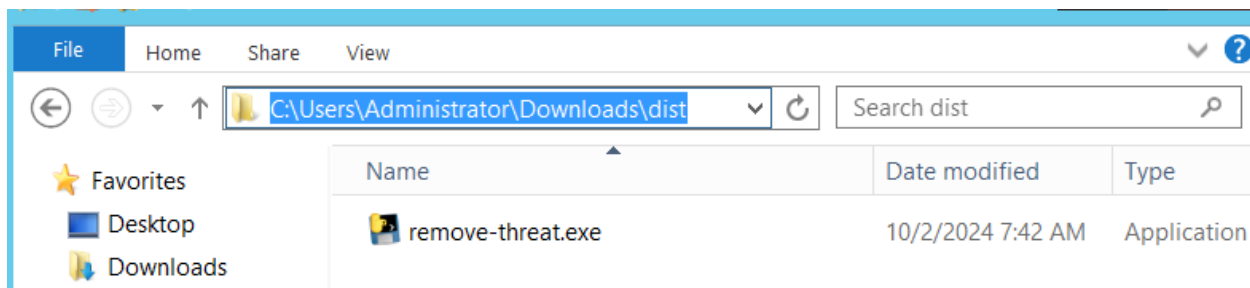


**B6: Chuyển đổi tập lệnh Python phản hồi đang hoạt động `remove-threat.py` thành ứng dụng thực thi Windows. Chạy lệnh PowerShell sau với tư cách quản trị viên để tạo tập thực thi:**

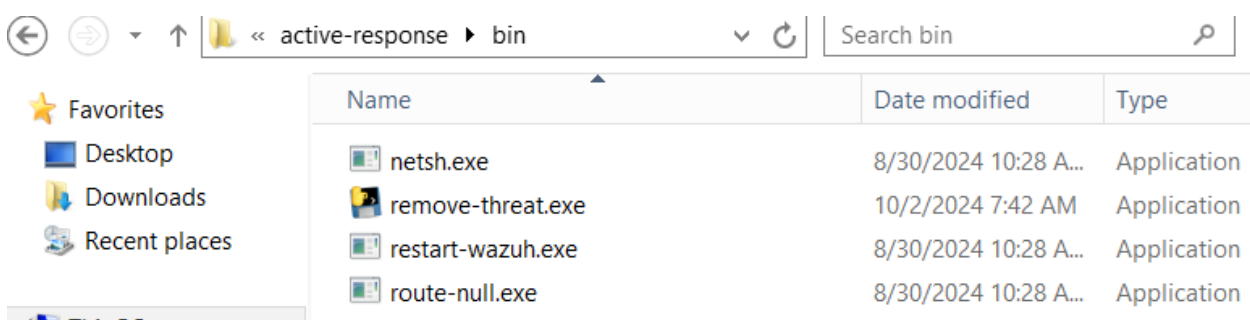
```
> pyinstaller -F \path_to_remove-threat.py
```

```
PS C:\Users\Administrator\Downloads> pyinstaller -F C:\Users\Administrator\Downloads\remove-threat.py
```

Lưu ý đường dẫn nơi `pyinstaller` tạo ra `remove-threat.exe`



**B7:** Di chuyển tập tin thực thi `remove-threat.exe` vào thư mục `C:\Program Files (x86)\ossec-agent\active-response\bin`



**B8:** Khởi động lại tác nhân Wazuh để áp dụng các thay đổi. Chạy lệnh PowerShell sau với tư cách quản trị viên:

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

- Ở máy Wazuh Server

Thực hiện các bước sau trên Wazuh Server để cấu hình tích hợp VirusTotal. Các bước này cũng kích hoạt và kích hoạt tập lệnh phản hồi hoạt động bất cứ khi nào phát hiện tệp đáng ngờ.

**B1:** Thêm cấu hình sau vào `/var/ossec/etc/ossec.conf` tệp trên máy chủ Wazuh để kích hoạt tích hợp VirusTotal.



Thay thế `<YOUR_VIRUS_TOTAL_API_KEY>` bằng [khóa API VirusTotal](#) của chính mình . Điều này cho phép kích hoạt truy vấn VirusTotal bất cứ khi nào bất kỳ quy tắc nào trong nhóm `syscheck` FIM được kích hoạt:

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

**B2: Thêm các khối sau vào tệp `/var/ossec/etc/ossec.conf` máy chủ Wazuh.**

Điều này cho phép phản hồi chủ động và kích hoạt tệp `remove-threat.exe` thực thi khi truy vấn VirusTotal trả về kết quả khớp dương tính với các mối đe dọa:

```
<ossec_config>
  <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>
</ossec_config>
```

```
#VirusTotal for Agent Windows Server
<ossec_config>
  <integration>
    <name>virustotal</name>
    <api_key>7948aa22354fe9532c6b2d185392c672a5749c13e46fa715376c1fba02ee8938</api_key> <!-- Re>
    <group>syscheck</group>
    <alert_format>json</alert_format>
  </integration>
</ossec_config>

<ossec_config>
  <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>
</ossec_config>
```

**B3:** Thêm các quy tắc sau vào tệp `/var/ossec/etc/rules/local_rules.xml` máy chủ Wazuh để cảnh báo về kết quả active response.

```
<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>
```

```
#For Agent Windows Server
<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.virus
  </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.fil
  </rule>
</group>
```

**B4: Khởi động lại trình quản lý Wazuh để áp dụng các thay đổi cấu hình:**

```
systemctl restart wazuh-manager.service
```

- **Mô phỏng tấn công:**

**B1: Thực hiện theo các bước sau để tạm thời tắt tính năng bảo vệ chống vi-rút Microsoft Defender theo thời gian thực trong Windows Security:**

- Nhấp vào menu **Start** và nhập để tìm kiếm ứng dụng đó. **Windows Security**
- Chọn **Windows Security app** từ kết quả, đi tới **Virus & threat protection** và trong phần **Virus & threat protection settings**, chọn **Manage settings** .
- Tắt tính năng **Real-time protection**.

**B2: Tải tập [EICAR test](#) xuống `C:\Users\<USER_NAME>\Downloads` thư mục trên điểm cuối Windows.**

```
> Invoke-WebRequest -Uri https://secure.eicar.org/eicar.com.txt -OutFile eicar.txt
> cp .\eicar.txt C:\Users\<USER_NAME>\Downloads
```

```
PS C:\Users\Administrator> Invoke-WebRequest -Uri https://secure.eicar.org/eicar.com.txt -OutFile eicar.txt
PS C:\Users\Administrator> cp .\eicar.txt C:\Users\Administrator\Downloads
```

Nếu báo lỗi này:

```
PS C:\Users\Administrator> Invoke-WebRequest -Uri https://secure.eicar.org/eicar.com.txt -OutFile eicar.txt
Invoke-WebRequest : The request was aborted: Could not create SSL/TLS secure channel.
At line:1 char:1
+ Invoke-WebRequest -Uri https://secure.eicar.org/eicar.com.txt -OutFile eicar.txt
+ ~~~~~
+ CategoryInfo          : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebExc
eption
+ FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand
```

Lỗi này là do PowerShell không thể thiết lập kết nối SSL/TLS an toàn với máy chủ. Điều này thường xảy ra khi phiên bản TLS mặc định của hệ thống không tương thích với yêu cầu bảo mật của máy chủ đích. thì ta có thể fix như sau:

1. Mở PowerShell với quyền Administrator:

- Nhấn **Start**, gõ **PowerShell**.
- Nhấp chuột phải vào **Windows PowerShell** và chọn **Run as administrator**.

2. Chạy lệnh sau để thiết lập TLS 1.2:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

Hoặc

`[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12 -bor [Net.SecurityProtocolType]::Tls11 -bor [Net.SecurityProtocolType]::Tls` (Nếu muốn hỗ trợ cả các phiên bản TLS khác (như TLS 1.1 hoặc TLS 1.0), có thể kết hợp chúng bằng cách sử dụng toán tử `-bor`)

```
PS C:\Users\Administrator> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
PS C:\Users\Administrator> Invoke-WebRequest -Uri https://secure.eicar.org/eicar.com.txt -OutFile eicar.txt
PS C:\Users\Administrator> cp .\eicar.txt C:\Users\Administrator\Downloads
PS C:\Users\Administrator>
```

Thao tác này kích hoạt truy vấn VirusTotal và tạo cảnh báo. Ngoài ra, tập lệnh active response sẽ tự động xóa tệp.

**Kết quả:** Vào Wazuh Server để xem cảnh báo

		timestamp per 30 minutes		
Time	rule.description		rule.level	rule.id
> May 1, 2024 @ 23:12:10.563	VirusTotal: Alert - c:\users\thecotilking\downloads\eicar.txt - 64 engines detected this file		12	87105
> May 1, 2024 @ 23:09:06.173	active-response/bin/remove-threat.exe removed threat located at c:\users\thecotilking\downloads\eicar.txt		12	100092
> May 1, 2024 @ 23:07:53.995	File deleted.		7	553
> May 1, 2024 @ 23:07:39.655	VirusTotal: Alert - c:\users\thecotilking\downloads\eicar.txt - 64 engines detected this file		12	87105
> May 1, 2024 @ 23:05:21.518	File added to the system.		5	554

- Có 64 công cụ đã phát hiện ra file này là độc hại.
- File đã bị xóa ngay sau khi được tải xuống.

ngocanhnguyen99.xyz@gmail.com