Wazuh + Sysmon

create a sysconfig.xml file and save it o windows machine

```
<Sysmon schemaversion="3.30">
 <HashAlgorithms>md5</HashAlgorithms>
 <EventFiltering>
 <!--SYSMON EVENT ID 1 : PROCESS CREATION-->
 <ProcessCreate onmatch="include">
 <Image condition="contains">powershell.exe</Image>
 </ProcessCreate>
 <!--SYSMON EVENT ID 2 : FILE CREATION TIME RETROACTIVELY CHA
NGED IN THE FILESYSTEM-->
 <FileCreateTime onmatch="include"></FileCreateTime>
 <!--SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED-->
 <NetworkConnect onmatch="include"></NetworkConnect>
 <!--SYSMON EVENT ID 4 : RESERVED FOR SYSMON STATUS MESSAGES,
THIS LINE IS INCLUDED FOR DOCUMENTATION PURPOSES ONLY-->
 <!--SYSMON EVENT ID 5 : PROCESS ENDED-->
 <ProcessTerminate onmatch="include"></ProcessTerminate>
 <!--SYSMON EVENT ID 6 : DRIVER LOADED INTO KERNEL-->
 <DriverLoad onmatch="include"></DriverLoad>
 <!--SYSMON EVENT ID 7 : DLL (IMAGE) LOADED BY PROCESS-->
 <ImageLoad onmatch="include"></ImageLoad>
 <!--SYSMON EVENT ID 8 : REMOTE THREAD CREATED-->
 <CreateRemoteThread onmatch="include"></CreateRemoteThread>
 <!--SYSMON EVENT ID 9 : RAW DISK ACCESS-->
 <RawAccessRead onmatch="include"></RawAccessRead>
 <!--SYSMON EVENT ID 10 : INTER-PROCESS ACCESS-->
 <ProcessAccess onmatch="include"></ProcessAccess>
 <!--SYSMON EVENT ID 11 : FILE CREATED-->
 <FileCreate onmatch="include"></FileCreate>
 <!--SYSMON EVENT ID 12 & 13 & 14 : REGISTRY MODIFICATION-->
 <RegistryEvent onmatch="include"></RegistryEvent>
```

```
 <!--SYSMON EVENT ID 15 : ALTERNATE DATA STREAM CREATED-->
 <FileCreateStreamHash onmatch="include"></FileCreateStreamHa
sh>
 <PipeEvent onmatch="include"></PipeEvent>
 </EventFiltering>
</Sysmon>
```

download sysmon

https://technet.microsoft.com/en-us/sysinternals/sysmon

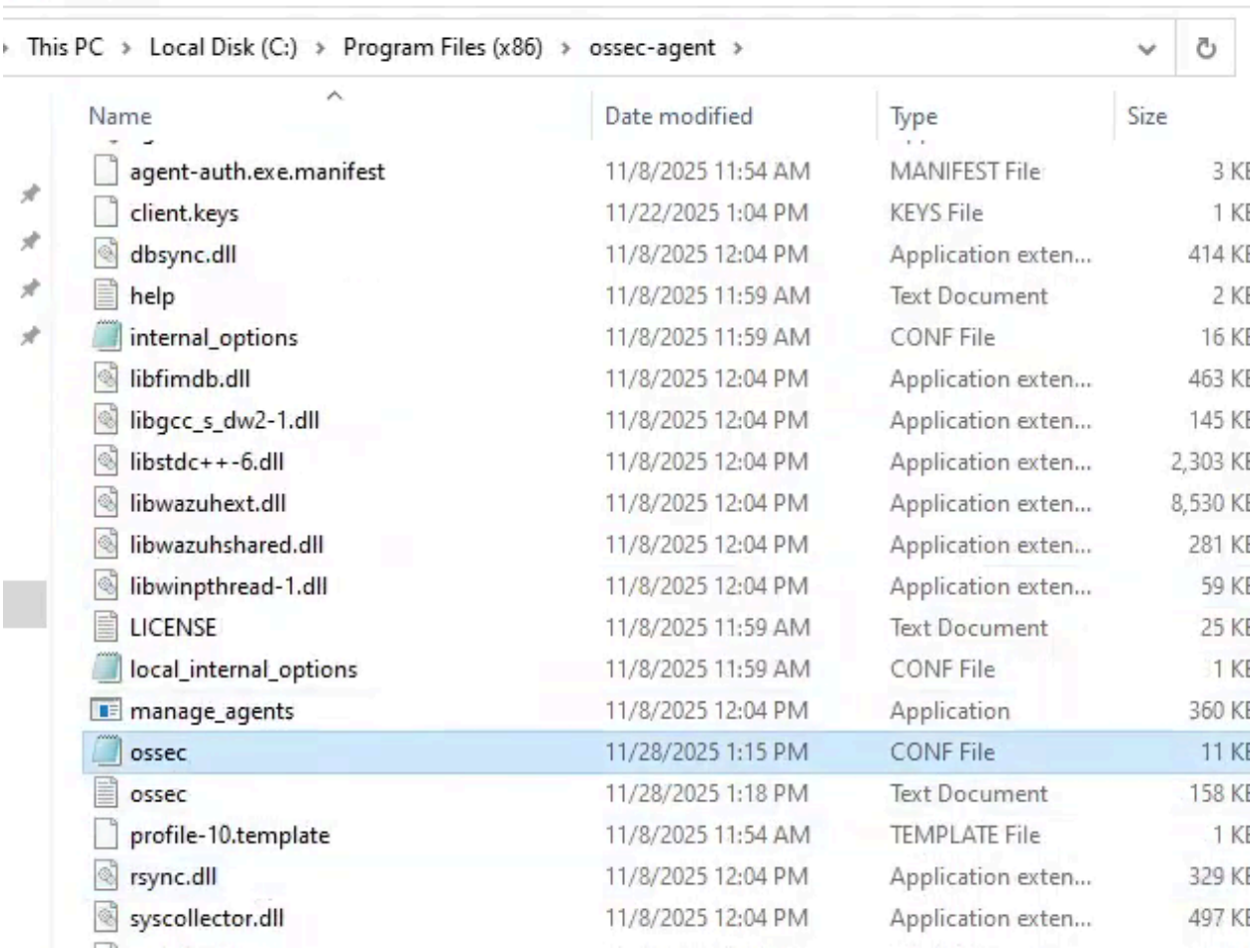
execute on powershell

```
Sysmon64.exe -accepteula -i sysconfig.xml
```

Configure Wazuh agent to monitor Sysmon events

on wazuh agent installatio (generally c:\Program Filex86), open ossec.conf and add to file

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


This PC › Local Disk (C:) › Program Files (x86) › ossec-agent ›
Name
Date modified
Type
Size
agent-auth.exe.manifest 11/8/2025 11:54 AM MANIFEST File 3 KB
client.keys 11/22/2025 1:04 PM KEYS File 1 KB
dbsync.dll 11/8/2025 12:04 PM Application exten... 414 KB
help 11/8/2025 11:59 AM Text Document 2 KB
internal_options 11/8/2025 11:59 AM CONF File 16 KB
libfimdb.dll 11/8/2025 12:04 PM Application exten... 463 KB
libgcc_s_dw2-1.dll 11/8/2025 12:04 PM Application exten... 145 KB
libstdc++-6.dll 11/8/2025 12:04 PM Application exten... 2,303 KB
libwazuhext.dll 11/8/2025 12:04 PM Application exten... 8,530 KB
libwazuhshared.dll 11/8/2025 12:04 PM Application exten... 281 KB
libwinpthread-1.dll 11/8/2025 12:04 PM Application exten... 59 KB
LICENSE 11/8/2025 11:59 AM Text Document 25 KB
local_internal_options 11/8/2025 11:59 AM CONF File 1 KB
manage_agents 11/8/2025 12:04 PM Application 360 KB
ossec 11/28/2025 1:15 PM CONF File 11 KB
ossec 11/28/2025 1:18 PM Text Document 158 KB
profile-10.template 11/8/2025 11:54 AM TEMPLATE File 1 KB
rsync.dll 11/8/2025 12:04 PM Application exten... 329 KB
syscollector.dll 11/8/2025 12:04 PM Application exten... 497 KB

```
  <!-- Active response -->
  <active-response>
    <disabled>no</disabled>
    <ca_store>wpk_root.pem</ca_store>
    <ca_verification>yes</ca_verification>
  </active-response>

  <!-- Choose between plain or json format (or both) for interna
  <logging>
    <log_format>plain</log_format>
  </logging>

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

</ossec_config>

<!-- END of Default Configuration. -->
```

restart wazuh agent

on server manager go to /vat/ossec/etc/rules/local_rules.xml and add

```
<group name="sysmon,">
 <rule id="255000" level="12">
 <if_group>sysmon_event1</if_group>
 <field name="sysmon.image">\powershell.exe||\.ps1||\.ps2</fi
eld>
 <description>Sysmon - Event 1: Bad exe: $(sysmon.image)</des
cription>
 <group>sysmon_event1,powershell_execution,</group>
 </rule>
</group>
```

Open

local_rules.xml

local_rules.xml
/var/ossec/etc/rules

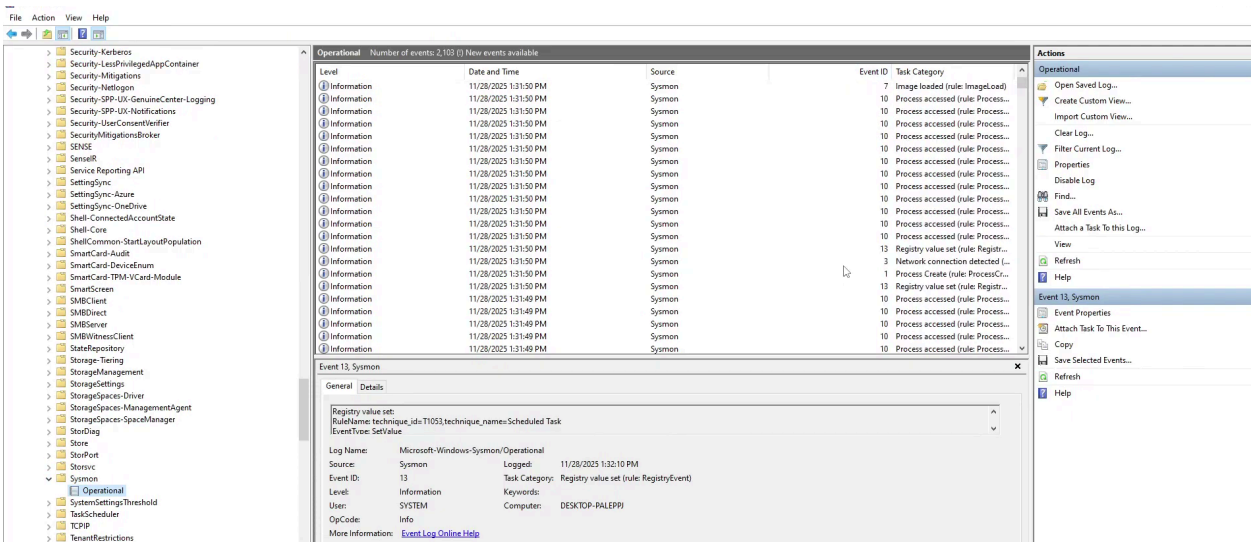
ossec.conf

```
  </rule>

  <rule id="108003" level="12">
    <if_sid>108000</if_sid>
    <field name="YARA.file_not_deleted">\.</field>
    <description>Active response unable to delete malicious file "$(YARA.file_not_deleted)"</description>
  </rule>
</group>

<group name="sysmon,">
 <rule id="255000" level="12">
 <if_group>sysmon_event1</if_group>
 <field name="sysmon.image">\\powershell.exe|\\.ps1|\\.ps2</field>
 <description>Sysmon - Event 1: Bad exe: $(sysmon.image)</description>
 <group>sysmon_event1,powershell_execution,</group>
 </rule>
</group>
```

restart service wazuh-manager and agent

you can check it on windows machine

Event Viewer → App and Services Logs→ Microsoft → Windows → Sysmon → Operactional



on wazuh dashboard

Active (chosse the agent) → Threath Hunting → Events