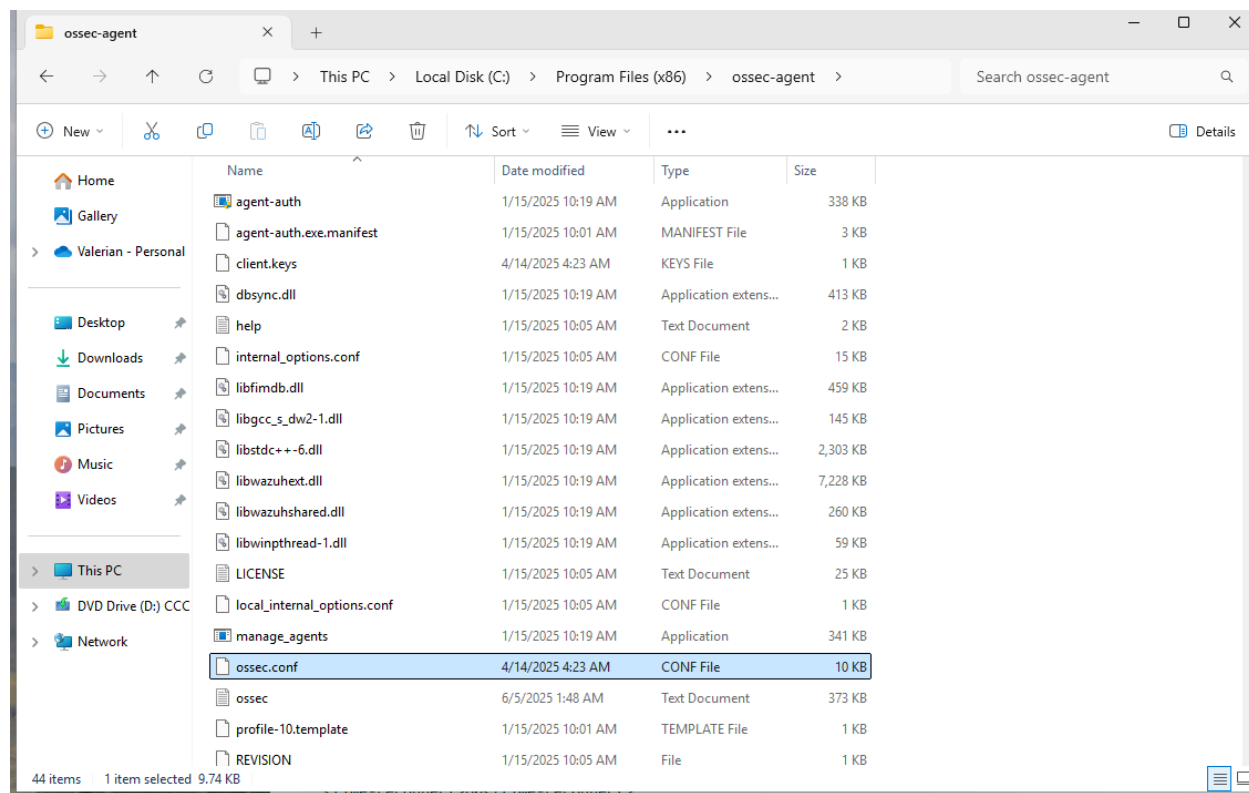
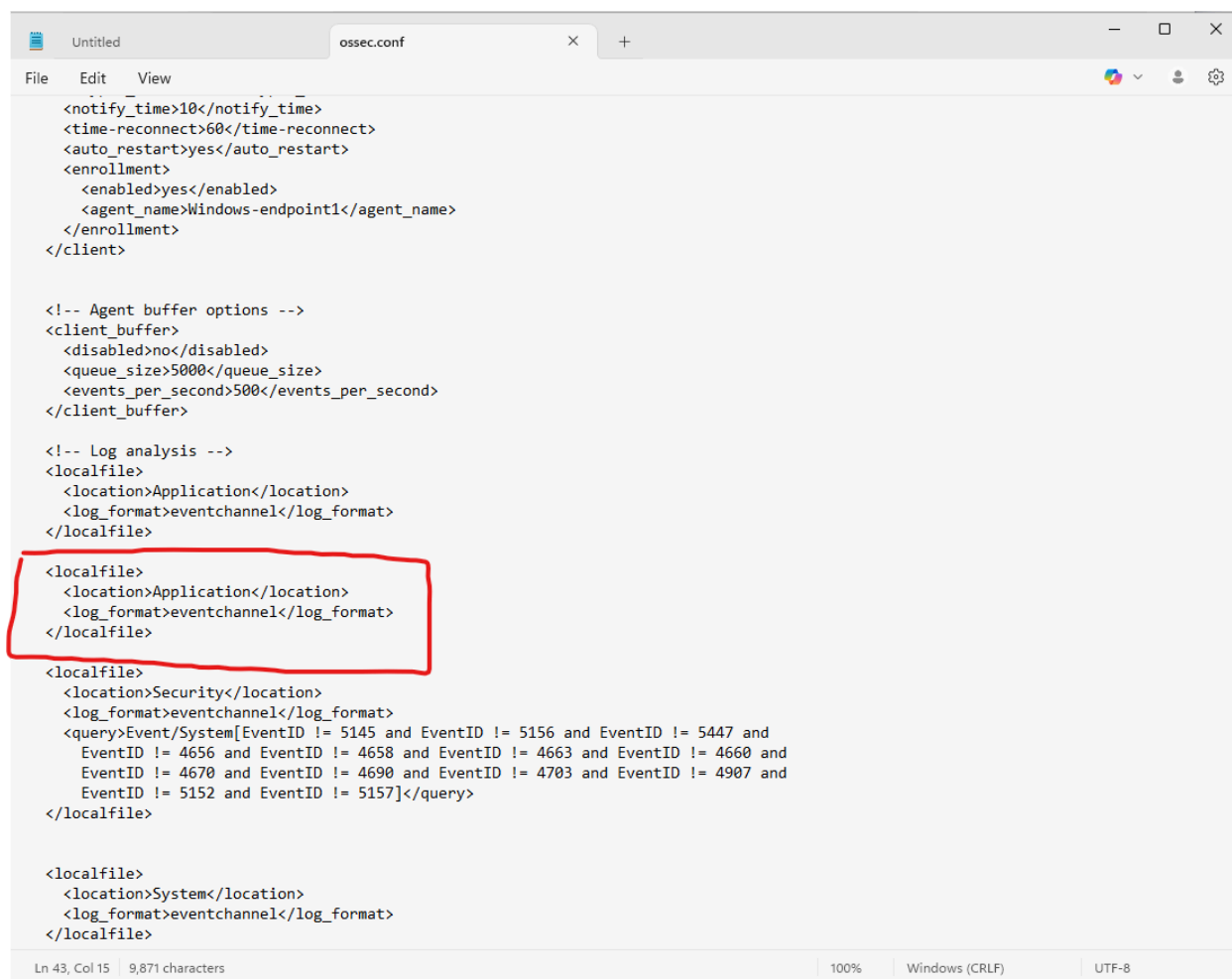


"C:\Program Files (x86)\ossec-agent\ossec.conf"





```
<notify_time>10</notify_time>
<time-reconnect>60</time-reconnect>
<auto_restart>yes</auto_restart>
<enrollment>
  <enabled>yes</enabled>
  <agent_name>Windows-endpoint1</agent_name>
</enrollment>
</client>

<!-- Agent buffer options -->
<client_buffer>
  <disabled>no</disabled>
  <queue_size>5000</queue_size>
  <events_per_second>500</events_per_second>
</client_buffer>

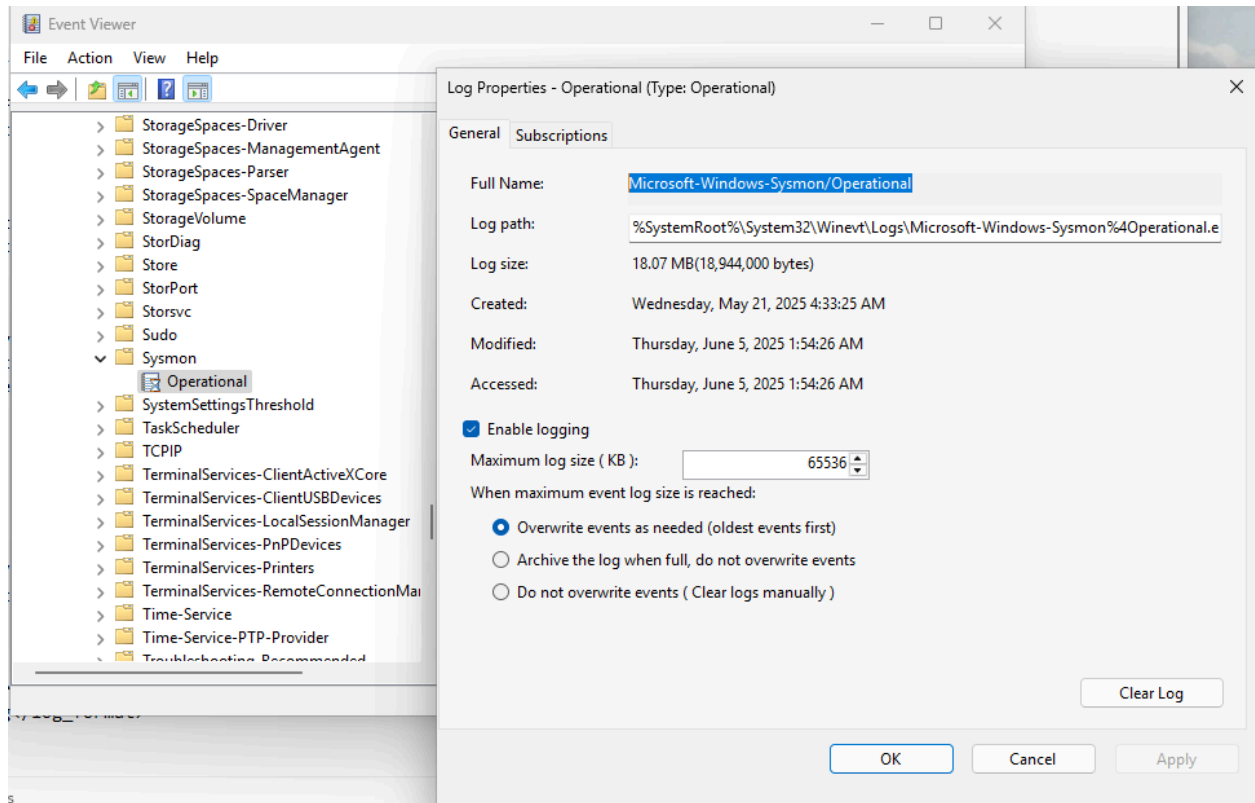
<!-- Log analysis -->
<localfile>
  <location>Application</location>
  <log_format>eventchannel</log_format>
</localfile>

<localfile>
  <location>Application</location>
  <log_format>eventchannel</log_format>
</localfile>

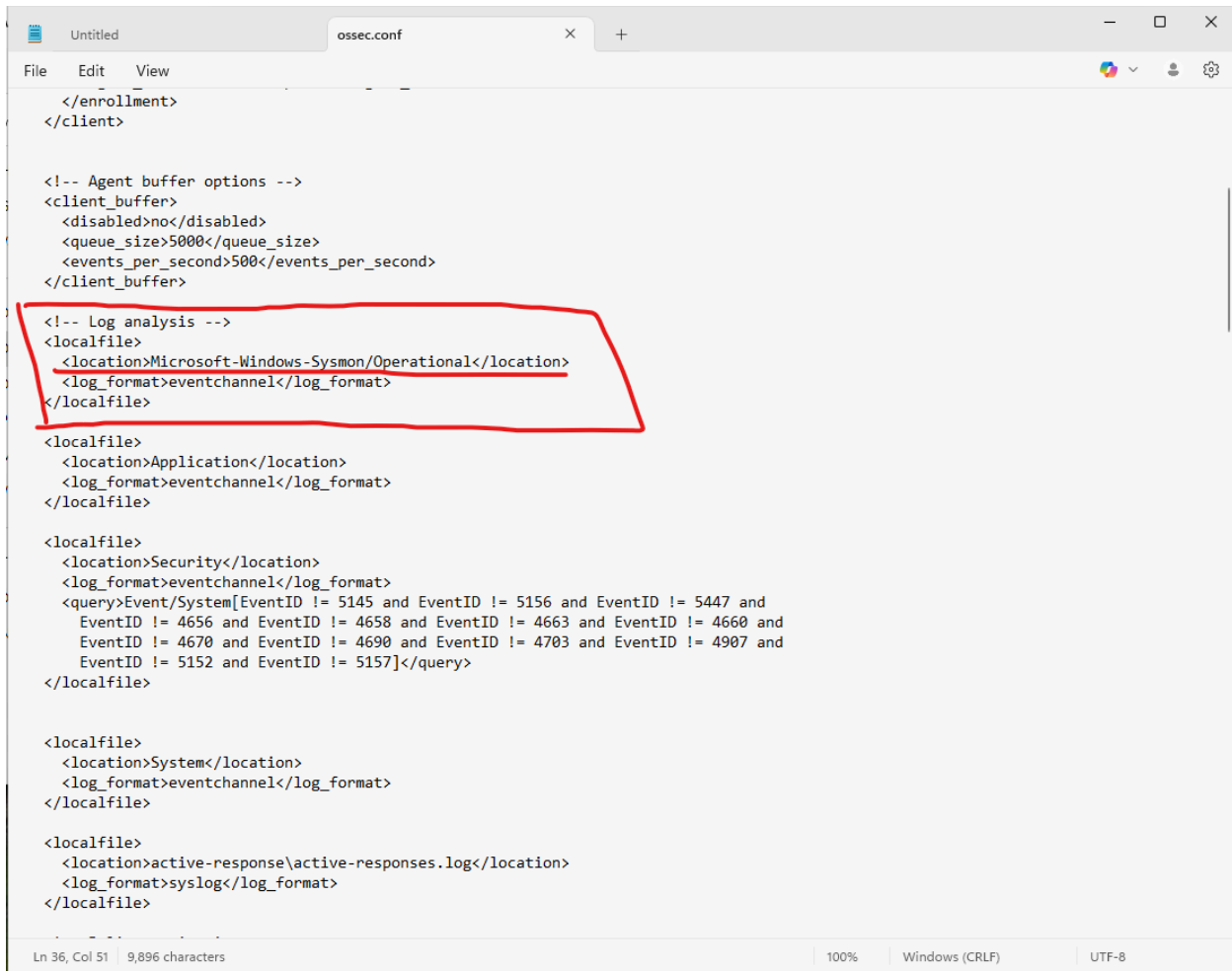
<localfile>
  <location>Security</location>
  <log_format>eventchannel</log_format>
  <query>Event/System[EventID != 5145 and EventID != 5156 and EventID != 5447 and
    EventID != 4656 and EventID != 4658 and EventID != 4663 and EventID != 4660 and
    EventID != 4670 and EventID != 4690 and EventID != 4703 and EventID != 4907 and
    EventID != 5152 and EventID != 5157]</query>
</localfile>

<localfile>
  <location>System</location>
  <log_format>eventchannel</log_format>
</localfile>
```

After that you'll need to make a configuration to the ossec file to figure out a specific event that you want to capture. In this case we'll be finding Mimikatz activity on this windows machine. By copying the localfile from above and pasting it. you'll see that there is a location and format within the localfile block. The location file is what wazuh will be retrieving the information from and you'll want to change that to Sysmon as the configuration completed before will find Mimikatz activity.



To replace the location with sysmon, you'll need to go into the event viewer to find sysmon operational like the image above.



```
</enrollment>
</client>

<!-- Agent buffer options -->
<client_buffer>
  <disabled>no</disabled>
  <queue_size>5000</queue_size>
  <events_per_second>500</events_per_second>
</client_buffer>

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

<localfile>
  <location>Application</location>
  <log_format>eventchannel</log_format>
</localfile>

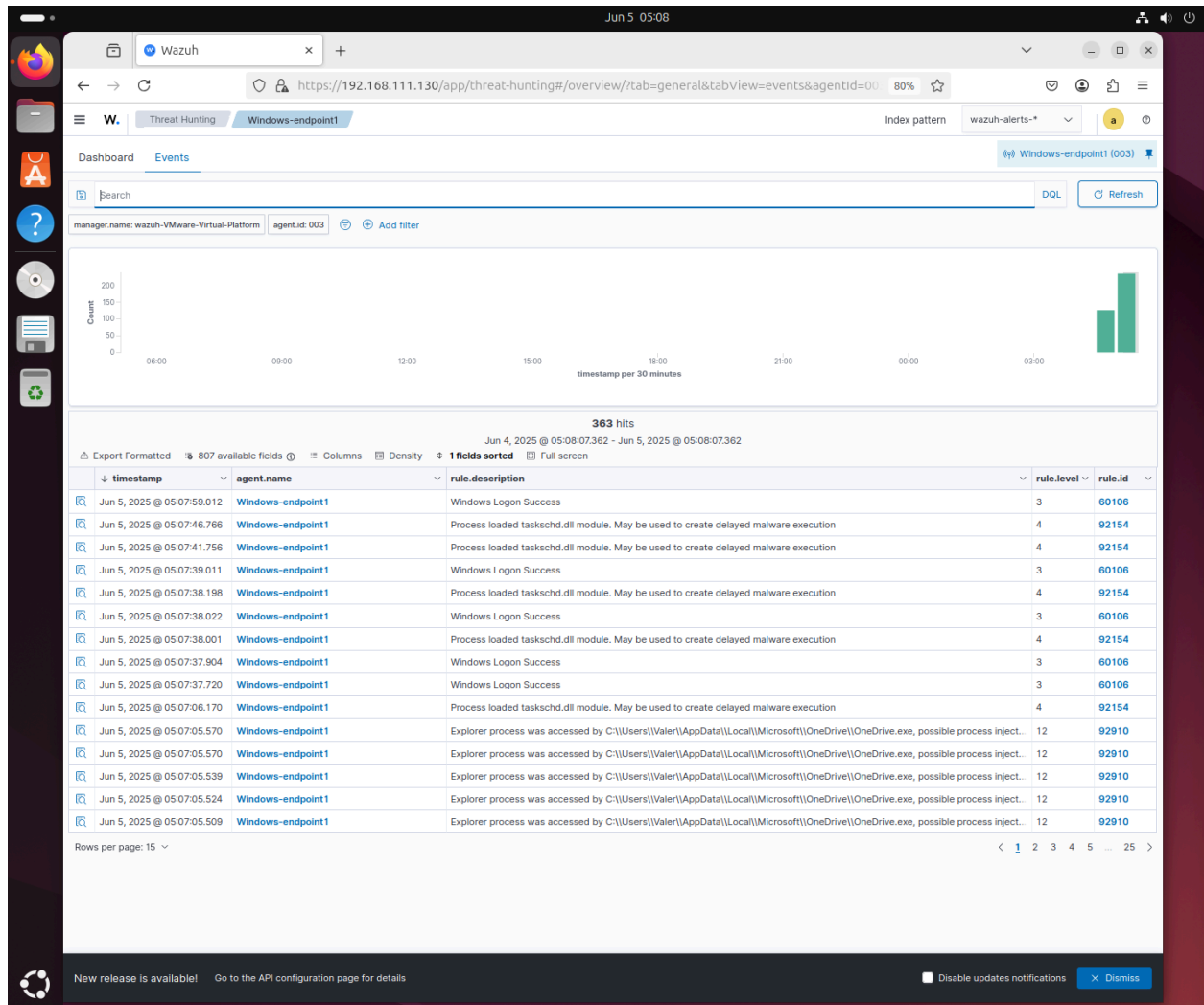
<localfile>
  <location>Security</location>
  <log_format>eventchannel</log_format>
  <query>Event/System[EventID != 5145 and EventID != 5156 and EventID != 5447 and
    EventID != 4656 and EventID != 4658 and EventID != 4663 and EventID != 4660 and
    EventID != 4670 and EventID != 4690 and EventID != 4703 and EventID != 4907 and
    EventID != 5152 and EventID != 5157]</query>
</localfile>

<localfile>
  <location>System</location>
  <log_format>eventchannel</log_format>
</localfile>

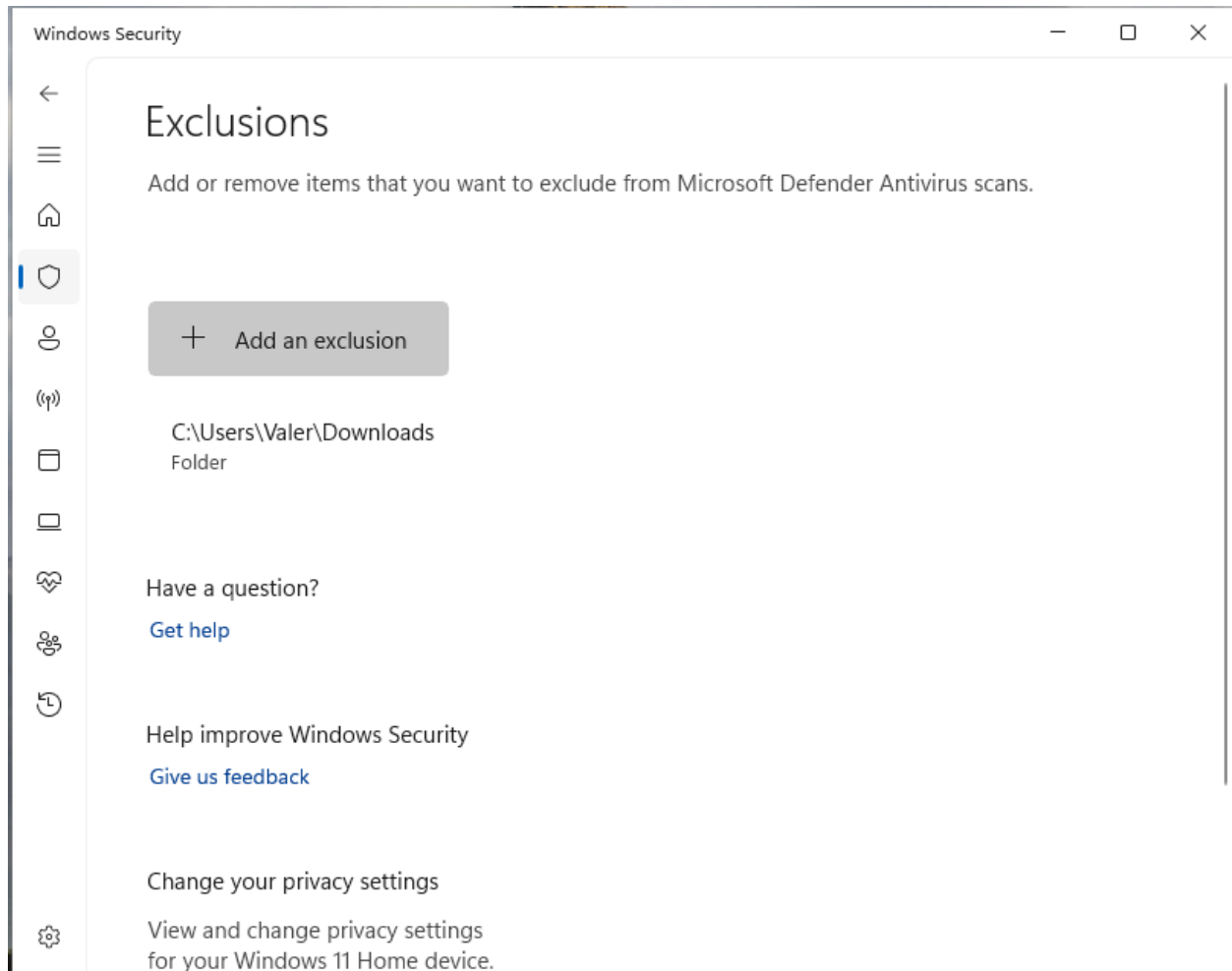
<localfile>
  <location>active-response\active-responses.log</location>
  <log_format>syslog</log_format>
</localfile>
```

Ln 36, Col 51 | 9,896 characters | 100% | Windows (CRLF) | UTF-8

And replace it like above and save.

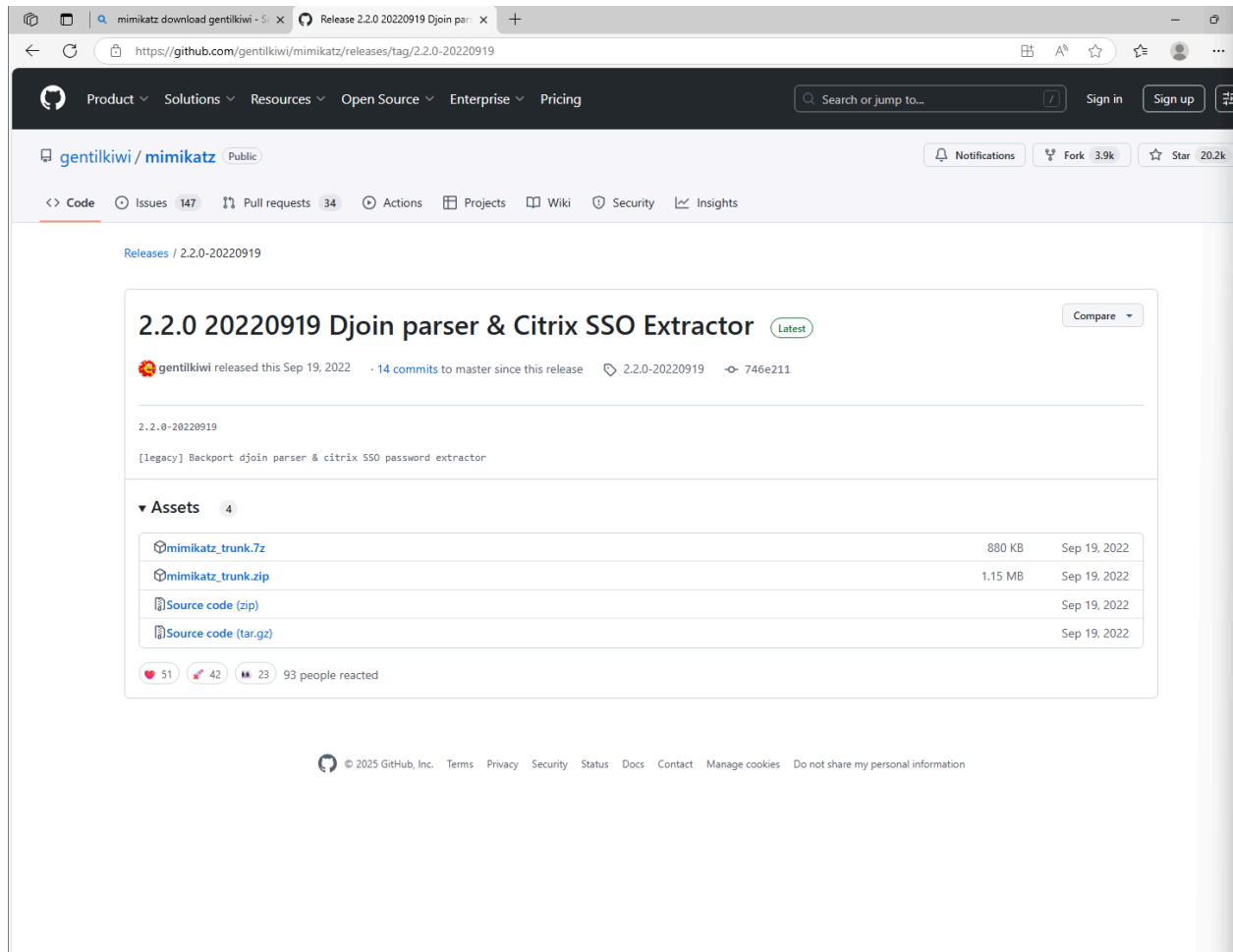


Go on the wazuh manager and go to threat hunting and the windows endpoint, in the search you can filter for sysmon by typing "sysmon" and you'll get all potentially malicious activity detected by sysmon.



Next back to the windows endpoint you'll want to install mimikatz on this operating machine. First you can turn off all windows security for the easy way or go to virus and protecting settings, scroll down till you see exclusions and add the downloads folder to the exclusions list like the image above to only isolate the downloads folder.

This is because windows defender will get a hit when you install mimikatz as it is well known and prevent you from downloading it.



Go to gentilkiwi github for mimikatz and find the latest release which should be the image above. You'll want to download the zip file or any file you'll want, I ain't gonna stop you except your browser so keep that file even when your browser security is screaming at you not to. Next up zip it and go to the administrator on the power shell as you'll be doing the big no no.

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

```
PS C:\WINDOWS\system32> cd C:\Users\Valer\Downloads\mimikatz_trunk\x64
PS C:\Users\Valer\Downloads\mimikatz_trunk\x64> ls
```

Directory: C:\Users\Valer\Downloads\mimikatz_trunk\x64

Mode	LastWriteTime	Length	Name
-a----	6/5/2025 2:19 AM	37208	mimidrv.sys
-a----	6/5/2025 2:19 AM	1355264	mimikatz.exe
-a----	6/5/2025 2:19 AM	37376	mimilib.dll
-a----	6/5/2025 2:19 AM	10752	mimispool.dll

```
PS C:\Users\Valer\Downloads\mimikatz_trunk\x64> .\mimikatz.exe
```

```
.#####.  mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /** Benjamin DELPY `gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > https://pingcastle.com / https://mysmartlogon.com **/

mimikatz #
```

Now run the mimikatz file, I'm going to hope you have some understanding on linux but the end result should be what you have above.

```
root@wazuh-VMware-Virtual-Platform: /var/ossec/etc

<!--
Wazuh - Manager - Default configuration for ubuntu 24.04
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>yes</logall>
    <logall json>yes</logall json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
    <update_check>yes</update_check>
  </global>

"ossec.conf" 374L, 10317B 12,5 Top
```


Note to self finish and complete this so that it shows the configuration how to get wazuh to detect mimikatz even if they change the name of the program through looking at it's ID.