- In previous part, we have installed FortiSIEM Windows Agent and we were able to see `security logs` and `powershell logs` in the analytics tab.
- now we will enrich the logs collected from the windows agent
- previously we defined the template and selected `Security` and `Windows Powershell` in `ADMIN` tab (inside `Windows Agent Monitor Template`) and some other options like `UEBA` and `Change` of the configuration like `Insatalled Software Change` and `Removable Drive`
- Now, we need to collect some extra logs from `Sysmon` internal module that you can install from `Microsoft` (its very important and mandatory by many regulations)
  - to achieve this we need to add new `Event` log `Type` (choose `Other` as option) - this is inside `Windows Agent Monitor Template`
    - before we come to this step (this is the last step we need to apply), we need to check the operation of the `Agent`, make sure it's working fine.
- To check the operation of Agent
  - go to `ADMIN` > `Health > Agent Health` - make sure that `Agent Status` is `Running Active`
  - also you need to check `Collector Health` - make sure it's `Normal`
  - also check `ANALYTICS` tab to make sure we are getting windows security logs

Steps for enabling the sysmon for any windows PC

```
1/ Download sysmon executables from Microsoft:
https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

2/ Download latest sysmon config xml
https://github.com/SwiftOnSecurity/sysmon-
config/blob/master/sysmonconfig-export.xml

3/ Tune sysmon config xml to fit your environment and be able to
accomplish your use cases

        Example1:  Create exception rules to exclude benign software:
<NetworkConnect onmatch="exclude">

═══════════════════════════════════════════════════════════════════
═══════════════════

        <Image condition="end
```

```
with">AppData\Local\Microsoft\Teams\current\Teams.exe</Image> <!—— Microsoft: Teams——>

        Example2:  monitor all ports over 1024 use: <NetworkConnect onmatch="include">

═══════════════════════════════════════════════════════════════════════
        <DestinationPort name="AllPorts" condition="begin with">1024</DestinationPort>
        <DestinationPort name="AllPorts" condition="end with">65535</DestinationPort>

4/ Sysmon Installation & Configuration

fresh install/config:  Sysmon64.exe -accepteula -i sysmonconfig-export.xml
just config update:    Sysmon64.exe -c sysmonconfig-export.xml
check config:          Sysmon64.exe -c

5/ Validate Sysmon logs on Windows devices: EventViewer > Applications and Service Logs > Microsoft > Windows > Sysmon > Operational

6/  Update Windows Agent Monitor Template to include Sysmon logs
```

- [Sysmon](Sysmon - Sysinternals | Microsoft Learn) event ID is very useful for establishing or developing very complex use cases to detect malicious behavior in windows PC
  - for e.g., some of the use cases is checking the process created from the actual right directory for example not from temporary directory, it will check the parent of the process
  - this kind of `Sysmon` `internals` can help design complex use cases

- after this command `Sysmon64.exe -accepteula -i sysmonconfig-export.xml` if you want to verify if its's installed or not, you need to check `Services` and check its status as `Running`

- final step is to "Update Windows Agent Monitor Template to include Sysmon logs"
  - go to `FortiSIEM` > `ADMIN` > `Windows Agent > Event > Type (choose Other), Event name` and save, now it will appear in Event column

Note

- to get `Event name` , go to `EventViewer > Applications and Service Logs > Microsoft > Windows > Sysmon > Operational` and right click on it and choose `Create Custom View > Filter` , copy value of `Event logs`
- now click on `Apply` in `Host to Template Associations`
- now go back to `ANALYTICS` and search for the event
  - note that normally, `Sysmon` logs will not come until you restart the `FortiSIEM` agent or you reboot your PC where you installed the `Sysmon`

Note:

- to know if its coming from the `Sysmon` or normal security log, check the `Event Type`
- e.g.,
  - `Win-Security-4624` - Normal Event Type
  - `Win-Sysmon-1-Create-Process` - Sysmon Event type
    - through this we are able to design our complex use cases using this kind of detailed logs
    - it will give us the name of the image, the process ID, FileVersion, Hashes, CammandLine used to launch the process, Image itself (like powershell.exe)
      - through this we can design a rule to check for some bad IOCs - this level of details is not available with normal windows security logs
- Sysmon available under `Sysinternals` , that allow you to dig further into your Windows logs and catch bad behaviour