

Step 1 – Install Sysmon:

Run this command in elevated powershell in the folder where the exe and xml files are:

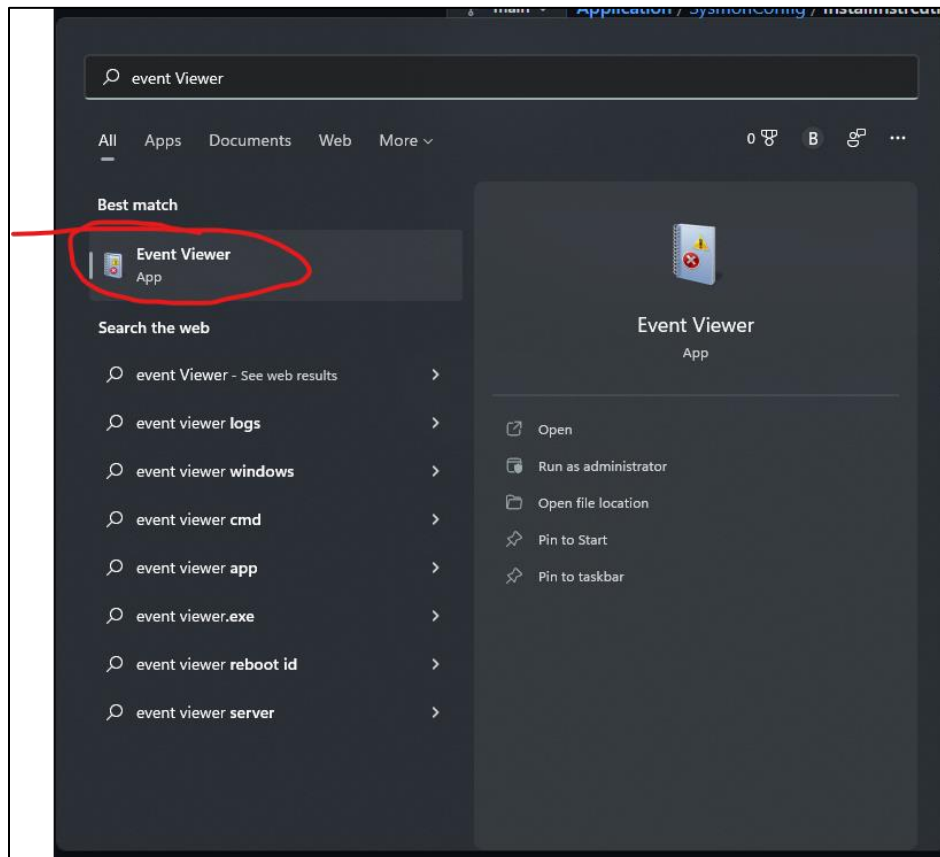
```
sysmon.exe -accepteula -i IncludeAllExcludeCommon.xml
```

```
PS C:\Users\Bryan\Desktop\sysmon> sysmon.exe -accepteula -i IncludeAllExcludeCommon.xml

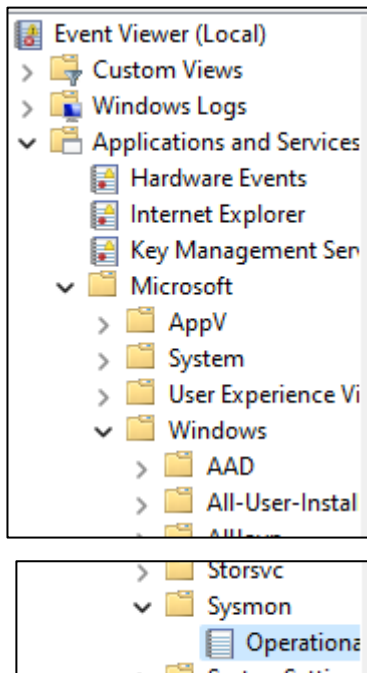
System Monitor v13.32 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2022 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.60
Sysmon schema version: 4.81
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
PS C:\Users\Bryan\Desktop\sysmon> |
```

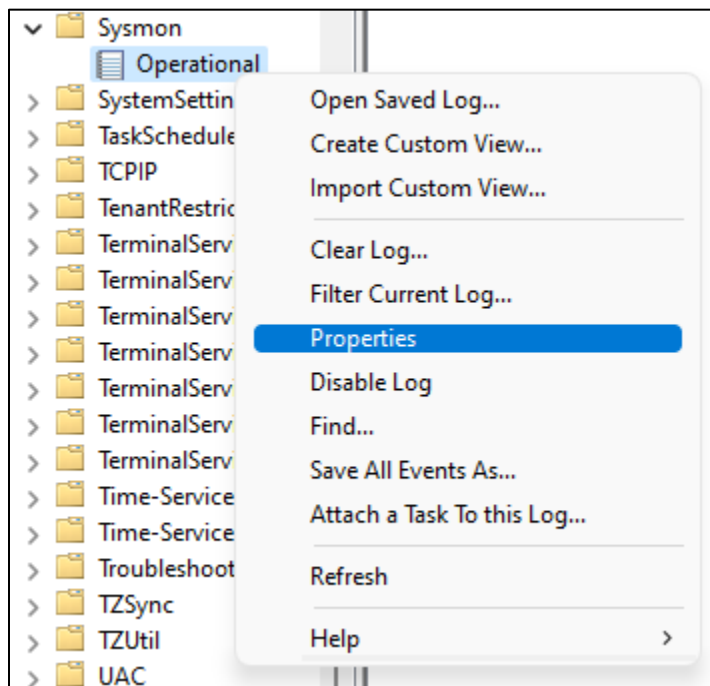
Once installed and started, open Windows Event Viewer



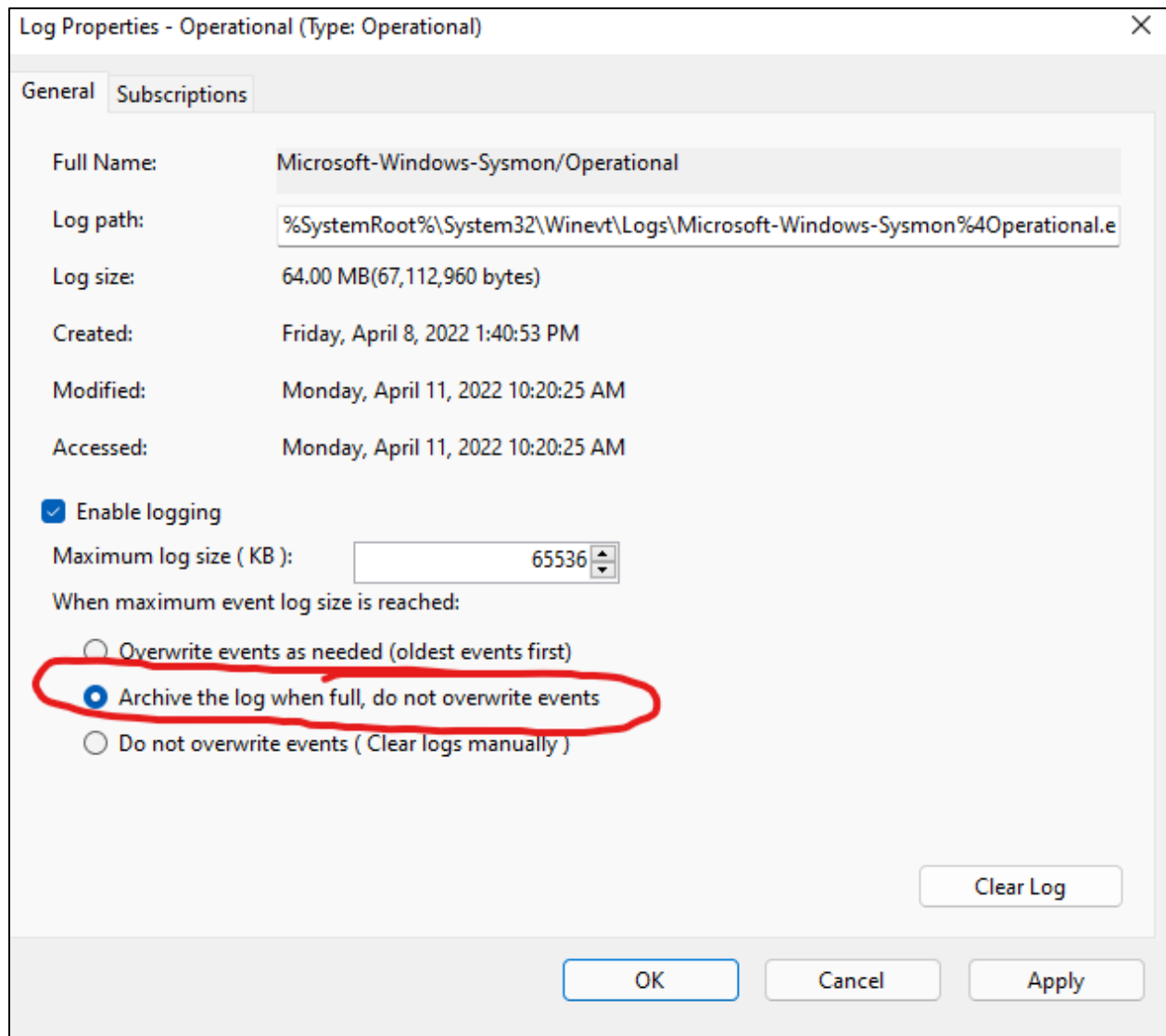
Navigate to Applications and Services > Microsoft > Windows > Sysmon



Right-click Operational and select properties



Change default logging to “Archive the log when full, do not overwrite events”



Select 'OK' and close the events viewer

Step 2 – Train machine:

Train the model using the command 'python RAD.py'. This will take in all Sysmon archive files and run them through the application. Note – The application automatically deletes the files after analyzing them. To avoid this, use the '-s' option.

```
python .\RAD.py -s
```

Step 3 – Generate a prediction:

Once the model is trained using as many log files as wanted, generate a prediction of which events are anomalies by running the application with the '-p' option.

```
python .\RAD.py -p
```