# 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

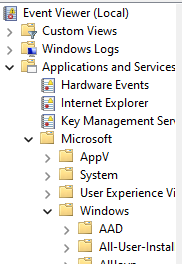
Text

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidenceOnce installed and started, open Windows Event Viewer

Navigate to Applications and Services > Microsoft > Windows > Sysmon



Right-click Operational and select properties

Graphical user interface, application

Description automatically generated

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

Graphical user interface, text, application, email

Description automatically generated

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.



# 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.

