**Winlogbeats**

*Download winlog beat and move to the folder:*

*Using Powershell as Administrotor run the following commands:*

cd 'C:\Program Files\Winlogbeat'

*If you get any error about restrictions apply the below command*

Set-ExecutionPolicy unrestricted

*Install as service*

.\install-service-winlogbeat.ps1

*To test if we are getting any logs manually*

.\winlogbeat.exe test config -c .\winlogbeat.yml -e