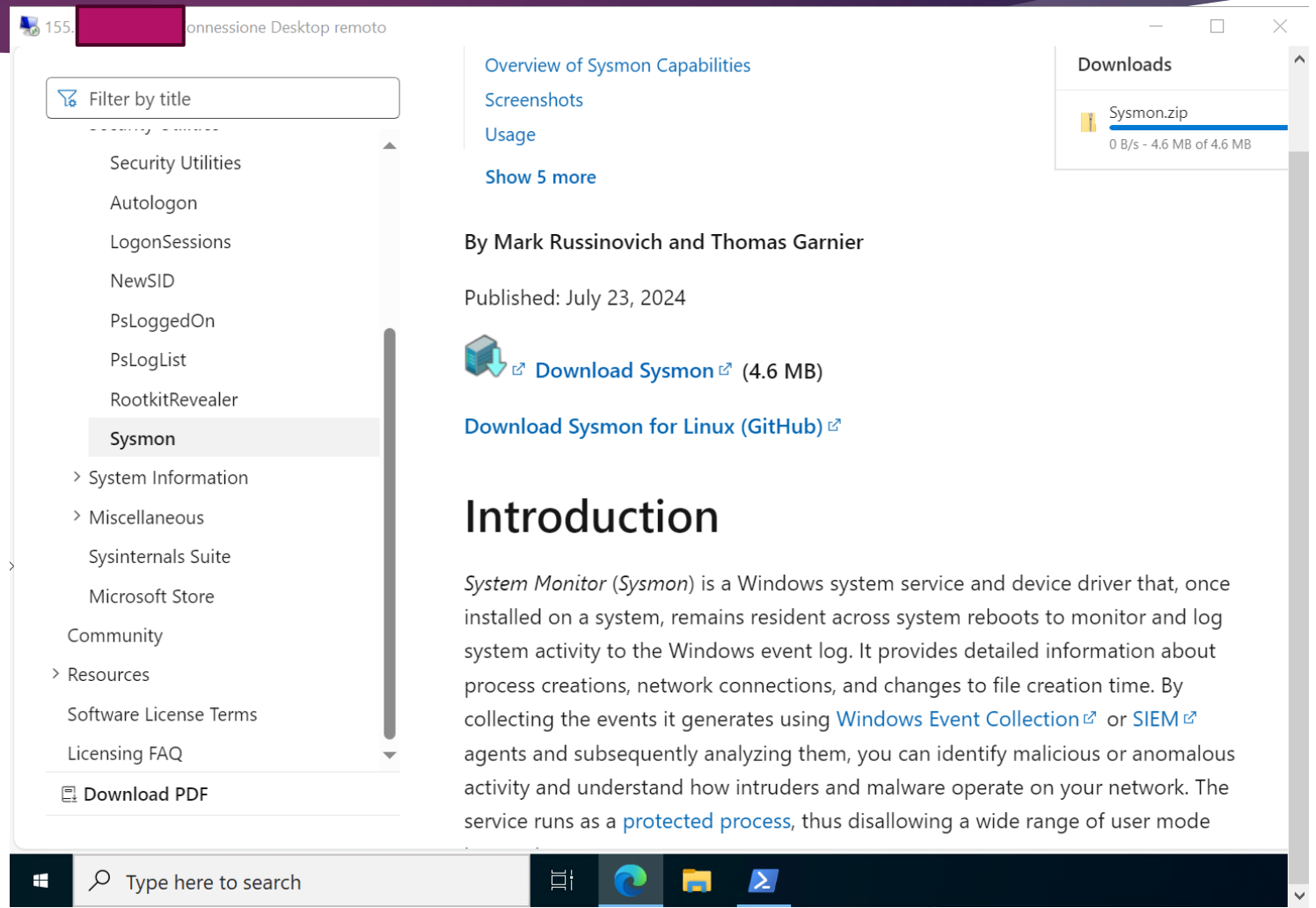
Day 9 – Sysmon Setup

Obiettivi

- **Installare Sysmon su Windows Server**
- **Confermare della raccolta dei dati**

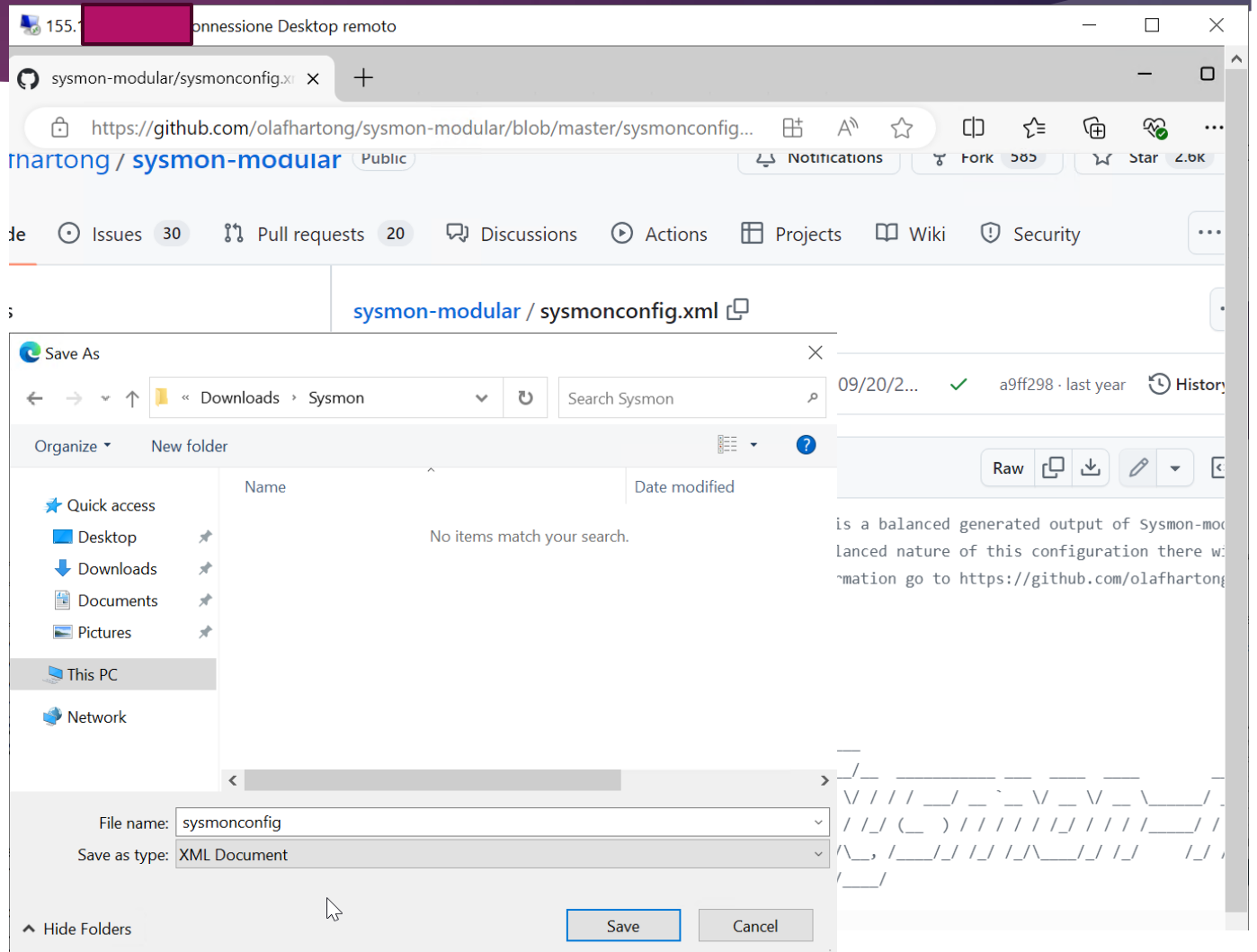
Sysmon Setup

Ci connettiamo da remoto al **Windows Server**, scarichiamo l'ultima versione di **Sysmon** ed estraiamo il contenuto del file scaricato.



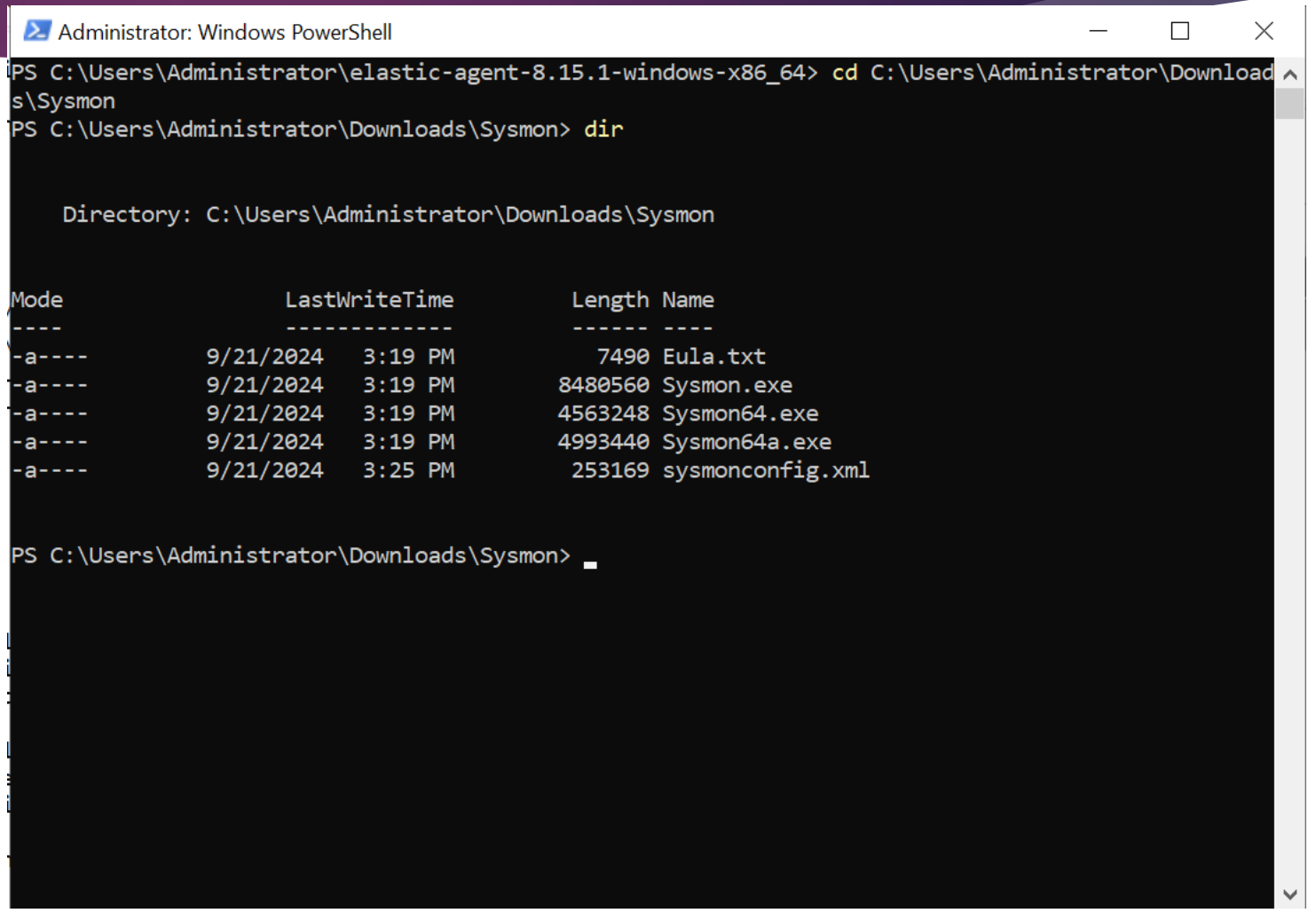
Sysmon Setup

Ora scarichiamo il file di configurazione 'sysmon configuration olaf', uno dei più utilizzati. Clicchiamo su 'Raw' e lo salviamo nella cartella di **Sysmon**.



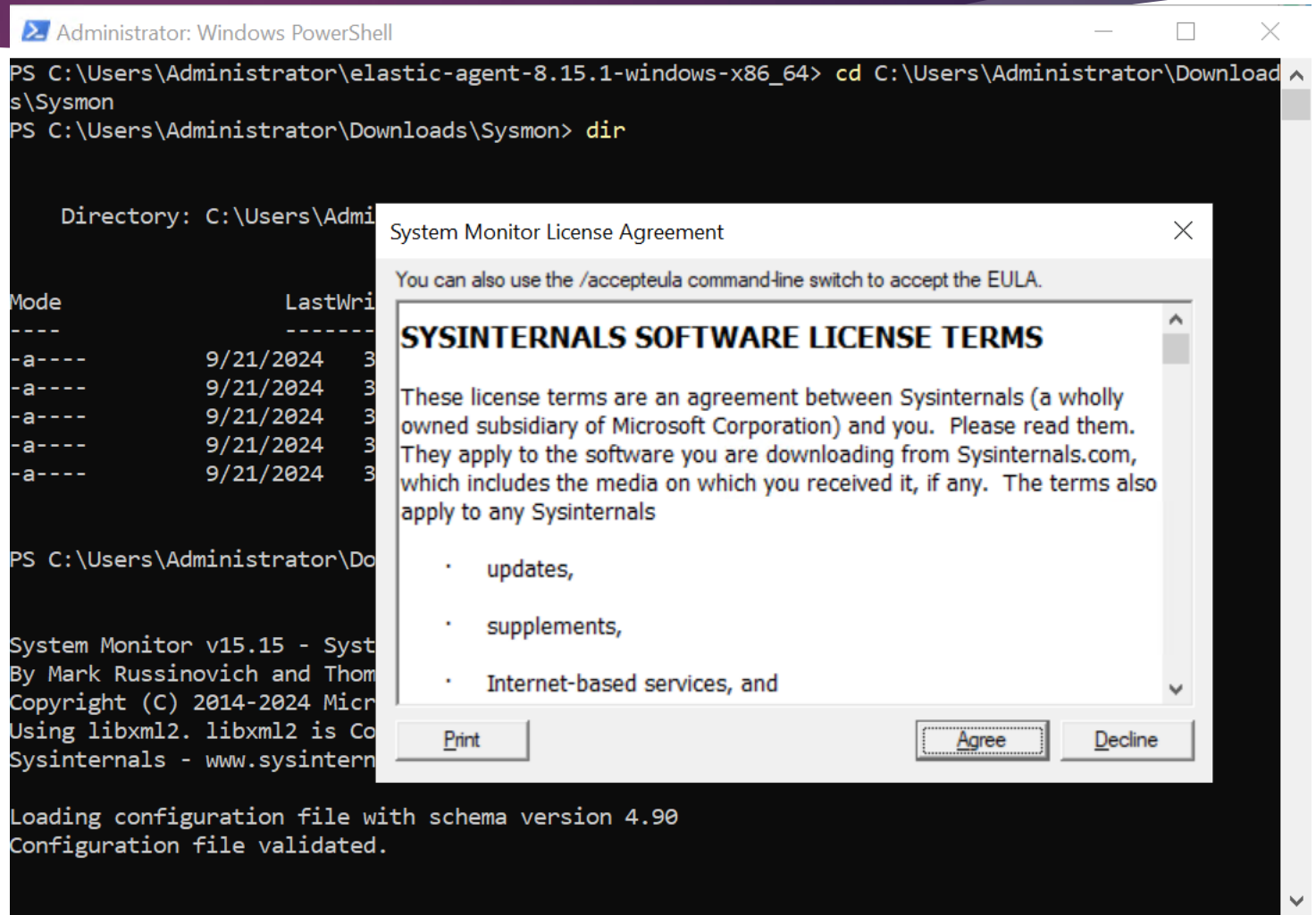
Sysmon Setup

Apriamo **Powershell** come Administrator, effettuiamo un ‘cd’ nel path della cartella **Sysmon.**



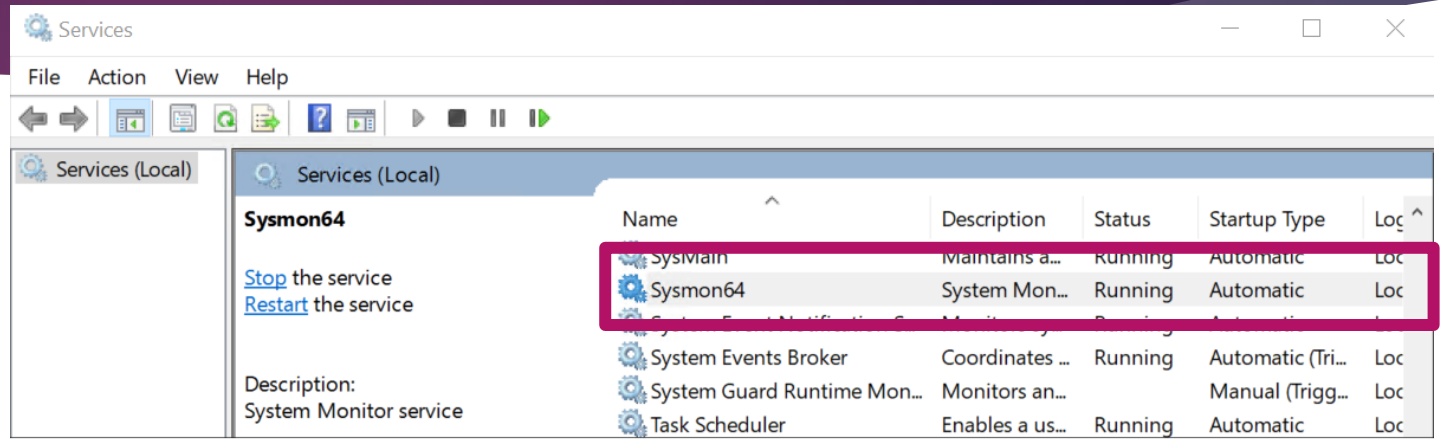
Sysmon Setup

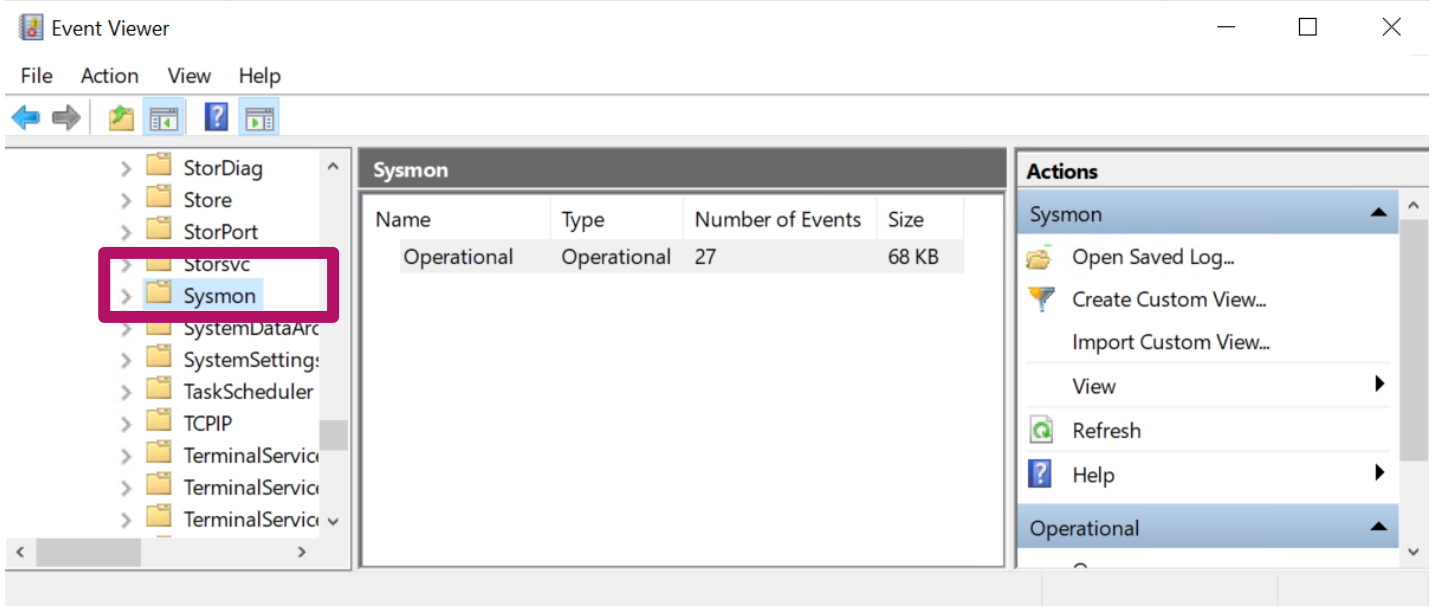
Procediamo con l'installazione di **Sysmon** da **Powershell.**



Sysmon Setup

Una volta installato **Sysmon**, vedremo il servizio attivato tra quelli di Windows, e i log generati saranno visibili su 'Event Viewer' in Application and Services Logs/Microsoft/Windows.





Dal file Operational possiamo visualizzare i primi eventi e, consultando la documentazione di **Sysmon**, comprenderne il significato. Qui possiamo confermare che gli eventi vengono generati.