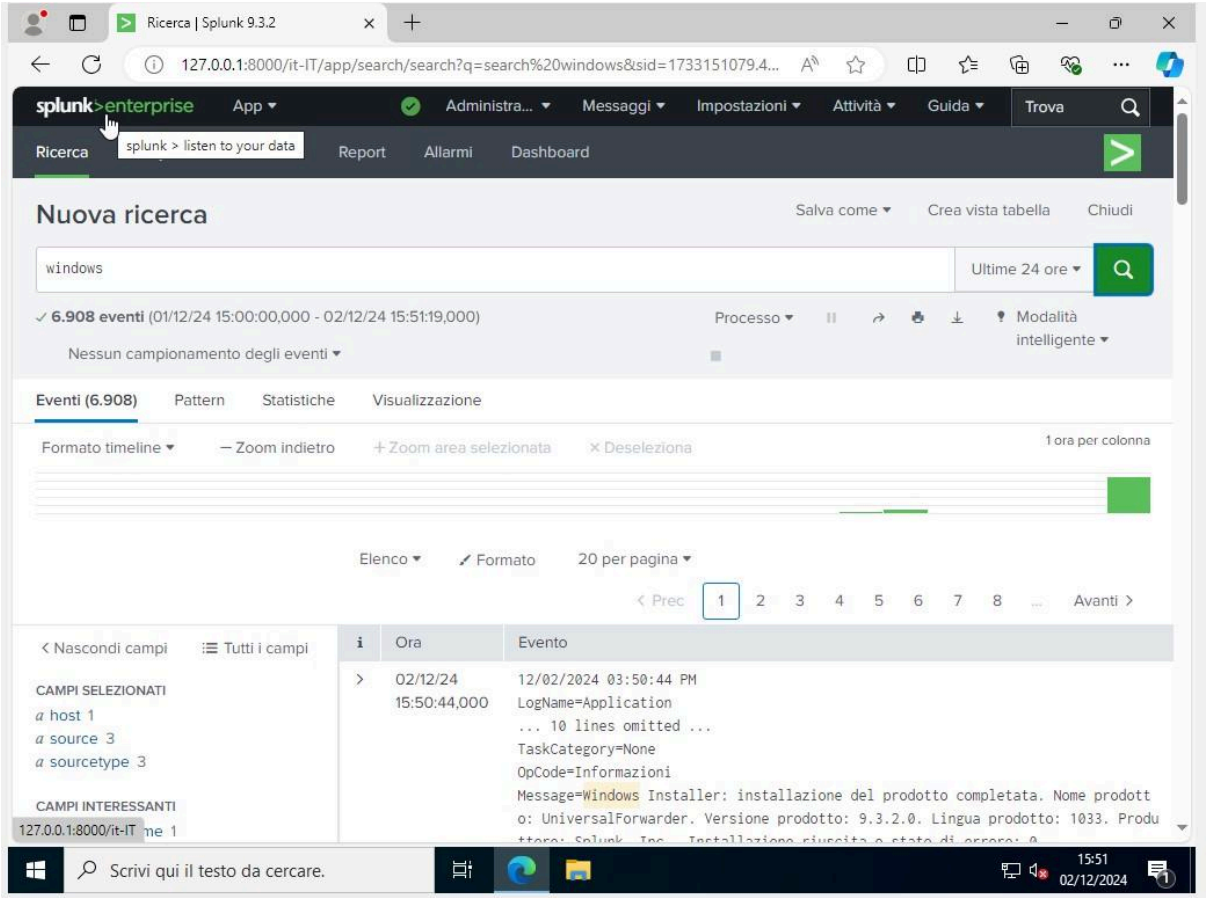
SPLUNK

Splunk è una piattaforma software che si concentra sull'analisi dei dati in tempo reale, con un'attenzione particolare alla gestione e monitoraggio dei log e dei dati di macchina. È utilizzato principalmente da professionisti IT, esperti di sicurezza e team operativi per raccogliere, indicizzare e analizzare enormi volumi di dati non strutturati provenienti da una varietà di fonti. Splunk è ampiamente usato in ambiti come il monitoraggio delle prestazioni, la gestione degli incidenti di sicurezza e l'analisi dei dati aziendali.



L’obiettivo dell’esercizio di oggi era configurare SPLUNK in modalità monitoring.