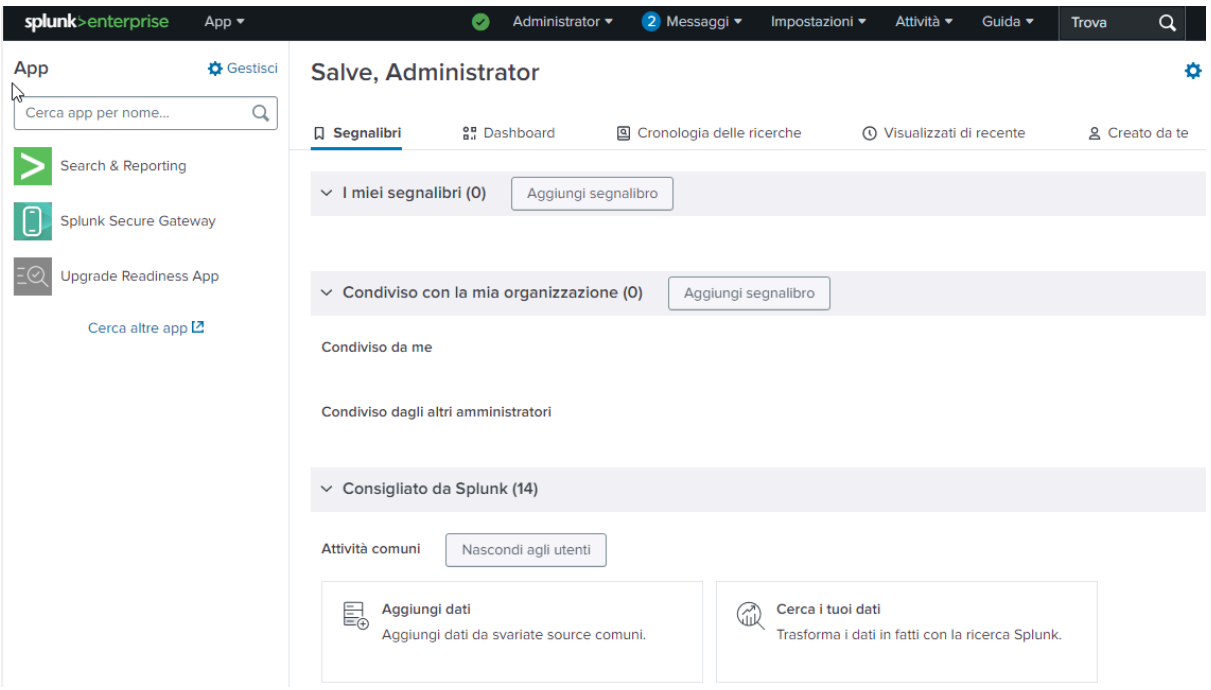
SPLUNK ENTERPRISE

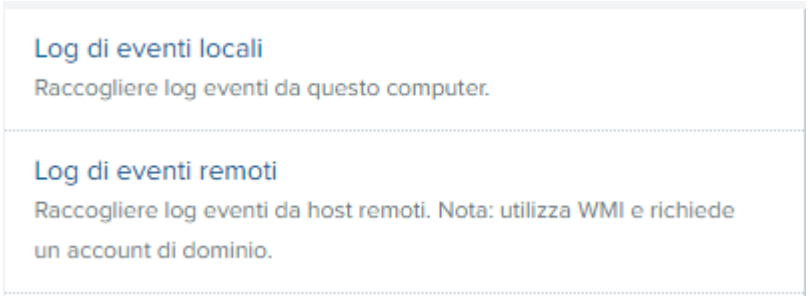
L'obbiettivo di oggi è configurare il servizio monitoraggio sul **SIEM "Splunk"**

SIEM: Software utilizzato per monitorare ed analizzare i dati provenienti da una rete.
Viene utilizzato per rilevare, prevenire e rispondere a potenziali minacce alla sicurezza informatica.

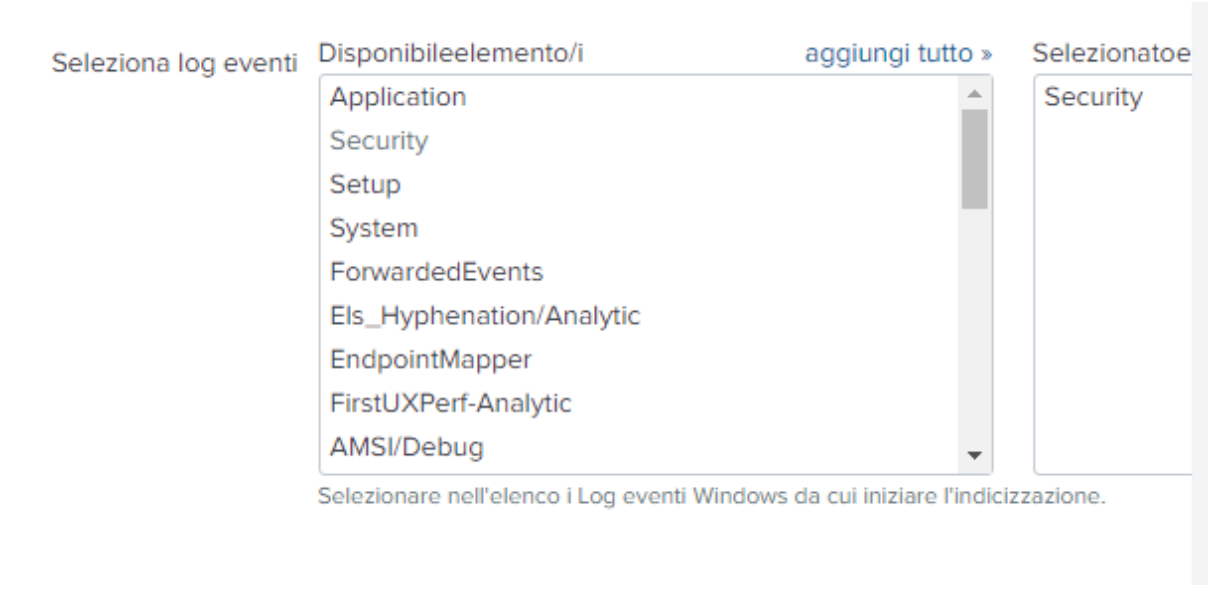


Dopo aver installato il SIEM andiamo a configurarlo per monitorare un dispositivo WIN10.
Selezioniamo la voce "**aggiungi dati**" e subito dopo "**monitora**"

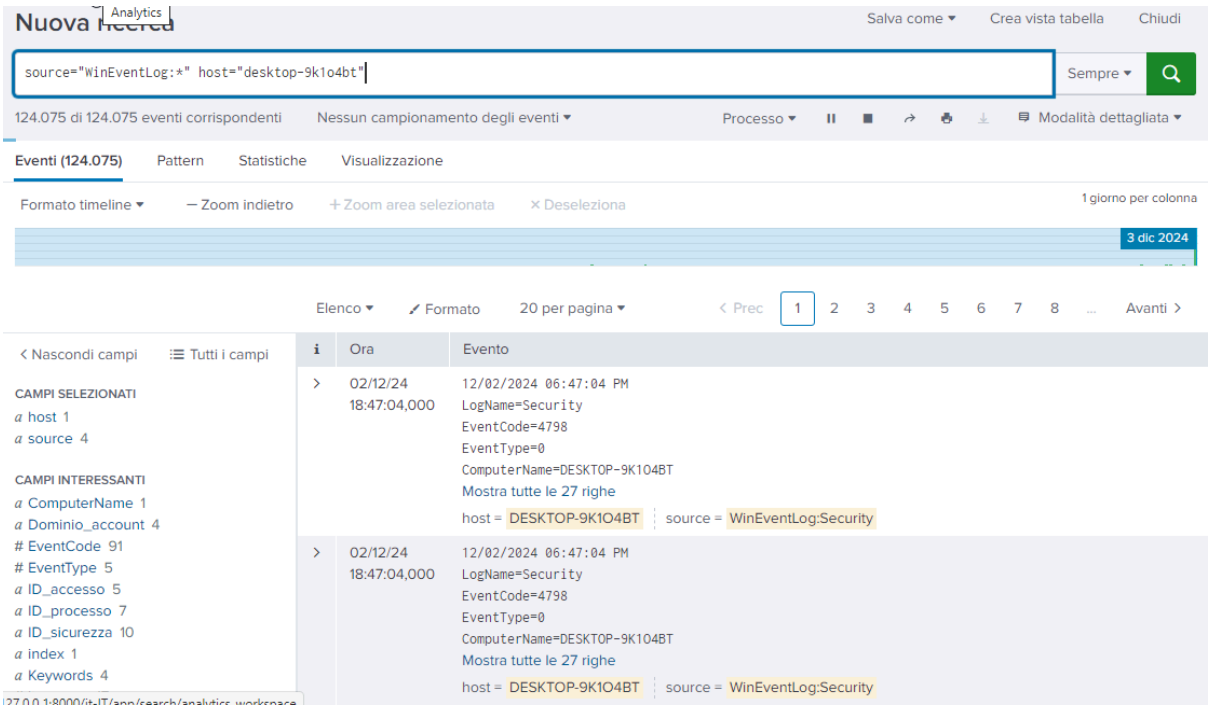
Si aprirà una schermata e si andrà subito a scegliere **“Log di eventi locali** “



Adesso si sceglie cosa monitorare, in questo caso analizzeremo i LOG di sicurezza



Questa è la schermata che mostra tutti i log del dispositivo che ha effettuato



CONSIDERAZIONI:

Un aspetto chiave del SIEM è la sua capacità di offrire una visione centralizzata delle attività di sicurezza di un'organizzazione. Senza un sistema simile, i team di sicurezza potrebbero trovarsi a dover analizzare log e eventi da una miriade di fonti separate, rendendo difficile individuare anomalie o correlare eventi che potrebbero indicare un attacco in corso.

Il SIEM richiede una attenta configurazione ed il personale va continuamente aggiornato su possibili attacchi o nuovi aggiornamenti.
Questo software ha anche delle procedure di automatizzazione, potrebbe subito analizzare e comunicare una minaccia senza la supervisione umana