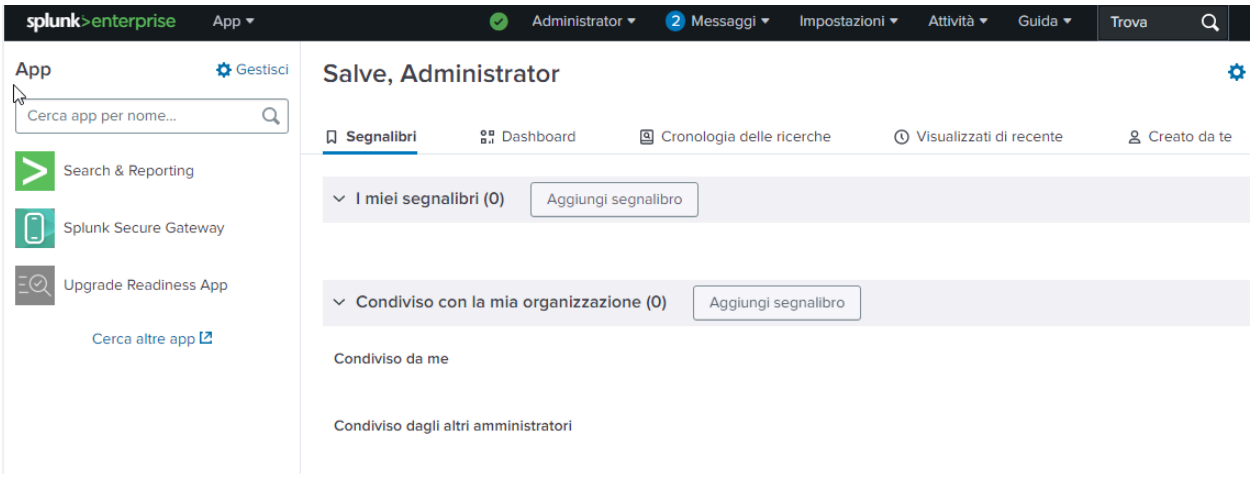
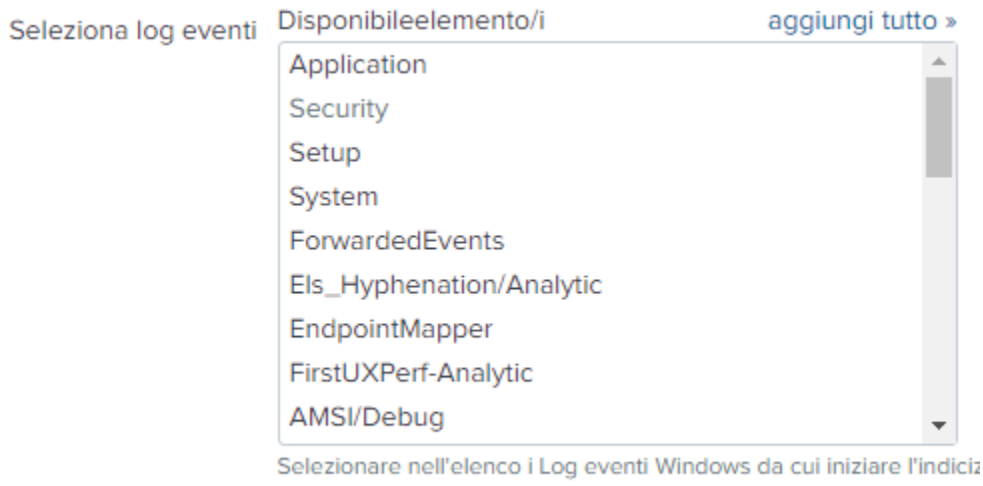
SPLUNK ENTERPRISE & SPLUNK UNIVERSAL FORWARDER

In questo esercizio andremo a configurare SPLUNK ENTERPRISE su macchina Windows Server 2022 e lo metteremo in comunicazione con SPLUNK FORWARDER su macchina Windows 10 Pro. Questo ci permetterà di poter monitorare e analizzare i log del dispositivo.

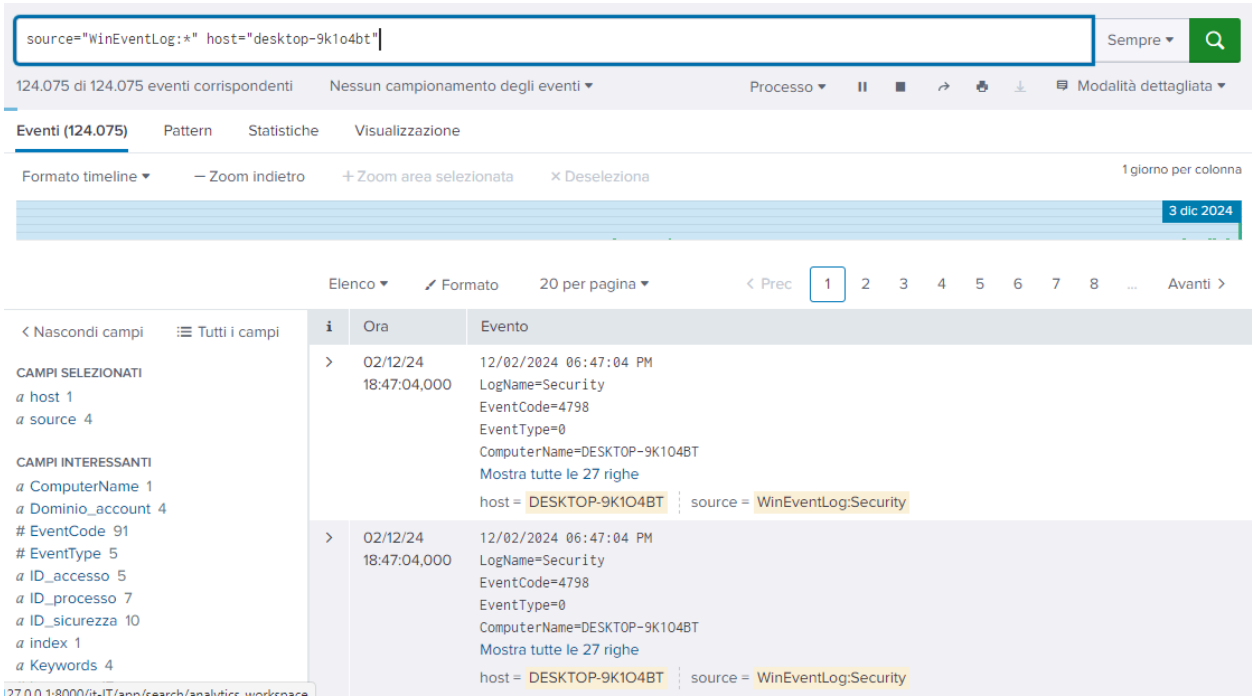


Una volta installati e configurati ci rechiamo su **aggiungi dati** e **monitora** ci apparirà una finestra dove possiamo scegliere che tipo di log monitorare, nel nostro caso scegliamo **LOG DI EVENTI LOCALI**

Ora andiamo a selezionare **la tipologia di LOG** che vogliamo vedere ed analizzare, nel nostro caso andiamo a selezionare **Security**



Nella schermata successiva avremo un elenco ordinato dei LOG di Sicurezza del dispositivo, inoltre possiamo notare che con la query inserita nel nostra caso source=”WinEventLog:*” ci verranno mostrati solo eventi filtrati da quella query.



L’importanza di utilizzare un software come SPLUNK (Siem) è quella di rendere più efficiente e rapida l’analisi e il monitoring degli eventi, questo perché un SIEM ci permette di avere una visione centralizzata di tutti gli eventi di sicurezza di un'azienda, nonostante questa sua semplicità di gestione dei dati però software come Splunk o altro richiedere comunque una corretta e attenta configurazione e gli addetti al suo utilizzo devono essere continuamente aggiornati.