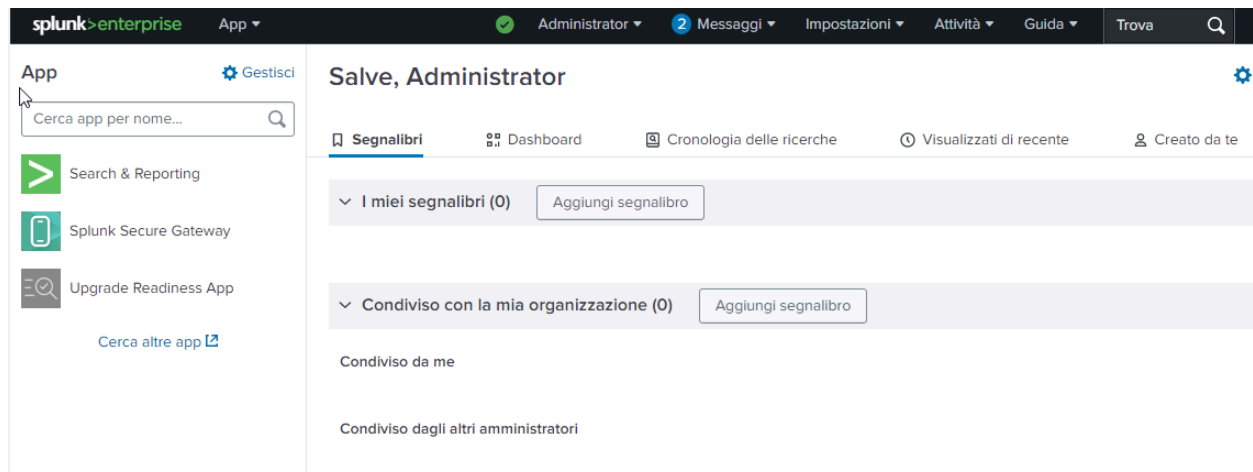


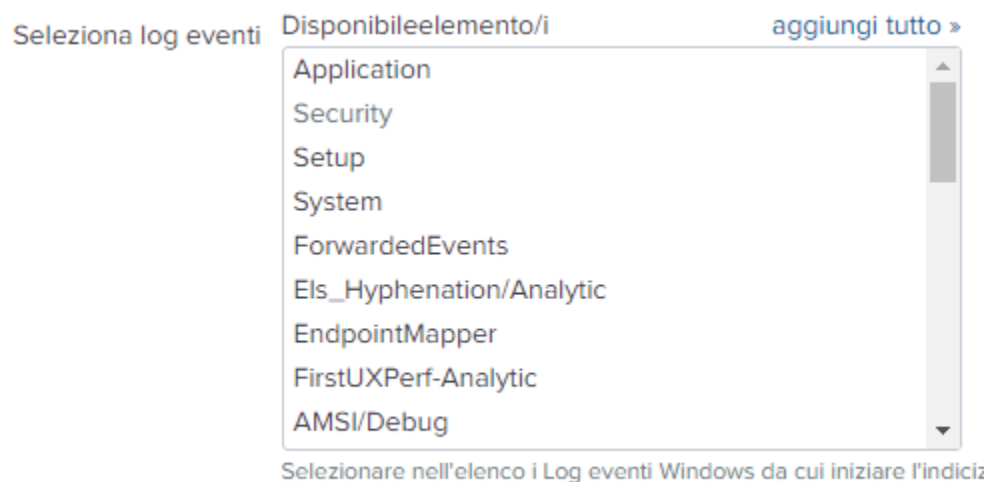
SPLUNK ENTERPRISE & SPLUNK UNIVERSAL FORWARDER

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 nostro caso `source="WinEventLog:*" host="desktop-9k1o4bt"` ci verranno mostrati solo eventi filtrati da quella query.

The screenshot displays the Splunk search results interface. At the top, a search bar contains the query `source="WinEventLog:*" host="desktop-9k1o4bt"`. Below the search bar, a status bar indicates "124.075 di 124.075 eventi corrispondenti" and "Nessun campionamento degli eventi". The interface includes tabs for "Eventi (124.075)", "Pattern", "Statistiche", and "Visualizzazione". A timeline view is selected, showing a zoomed-in view of the events. The main table displays a list of events, with the first event highlighted. The event details show the following information:

Id	Ora	Evento
>	02/12/24 18:47:04,000	12/02/2024 06:47:04 PM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-9K104BT Mostra tutte le 27 righe host = DESKTOP-9K104BT source = WinEventLog:Security
>	02/12/24 18:47:04,000	12/02/2024 06:47:04 PM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-9K104BT Mostra tutte le 27 righe host = DESKTOP-9K104BT source = WinEventLog:Security

The left sidebar shows the "CAMPI SELEZIONATI" (Selected Fields) and "CAMPI INTERESSANTI" (Interesting Fields) sections. The "CAMPI SELEZIONATI" section includes fields like `host`, `source`, `ComputerName`, `Dominio_account`, `EventCode`, `EventType`, `ID_accesso`, `ID_processo`, `ID_sicurezza`, `index`, and `Keywords`. The "CAMPI INTERESSANTI" section includes fields like `host`, `source`, `ComputerName`, `Dominio_account`, `EventCode`, `EventType`, `ID_accesso`, `ID_processo`, `ID_sicurezza`, `index`, and `Keywords`.

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 richiedono comunque una corretta e attenta configurazione e gli addetti al suo utilizzo devono essere continuamente aggiornati.