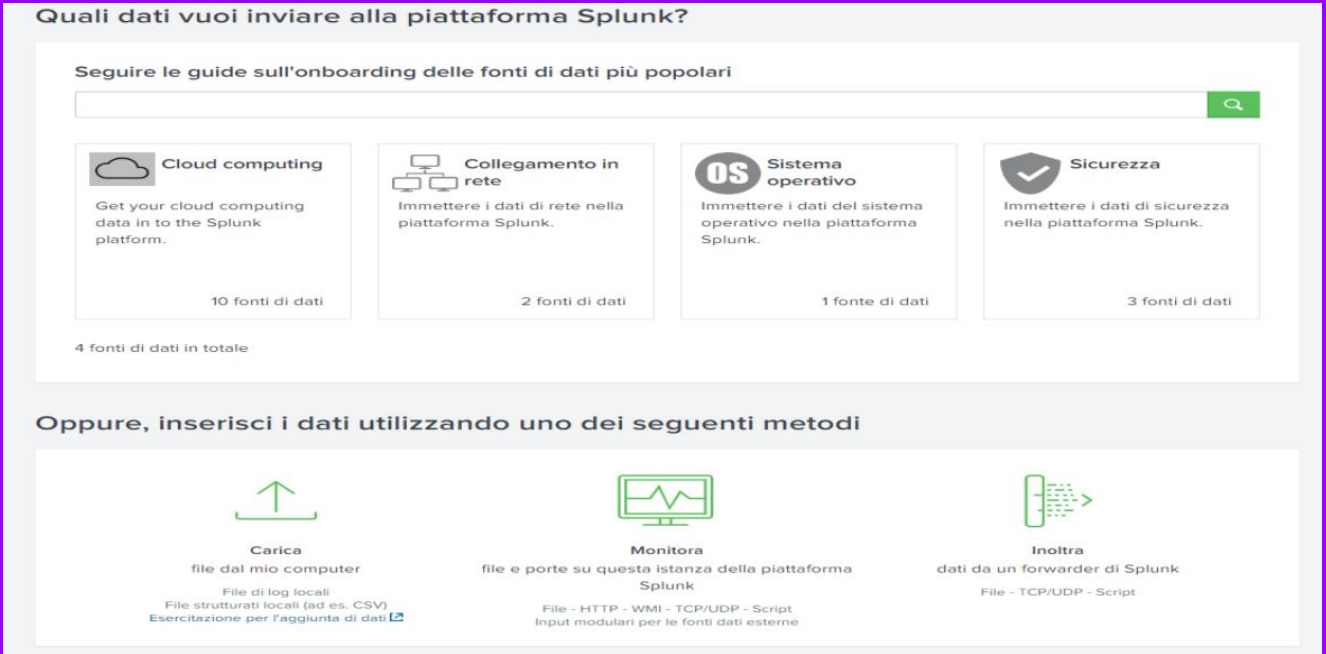
MONITORA SPLUNK

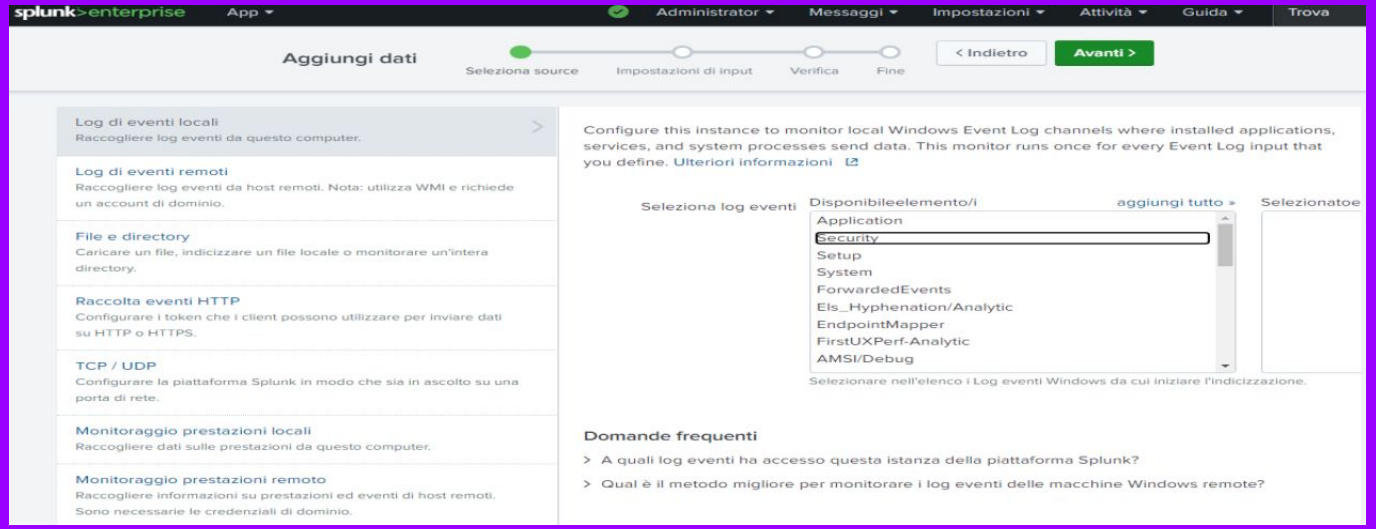
Esercizio di oggi: Configurazione della Modalità Monitora in Splunk

Abbiamo esplorato diverse funzionalità offerte da Splunk. Oggi ci concentreremo sulla modalità "Monitora". Il compito di oggi consiste nel configurare la modalità Monitora in Splunk e realizzare degli screenshot che confermino l'avvenuta configurazione.

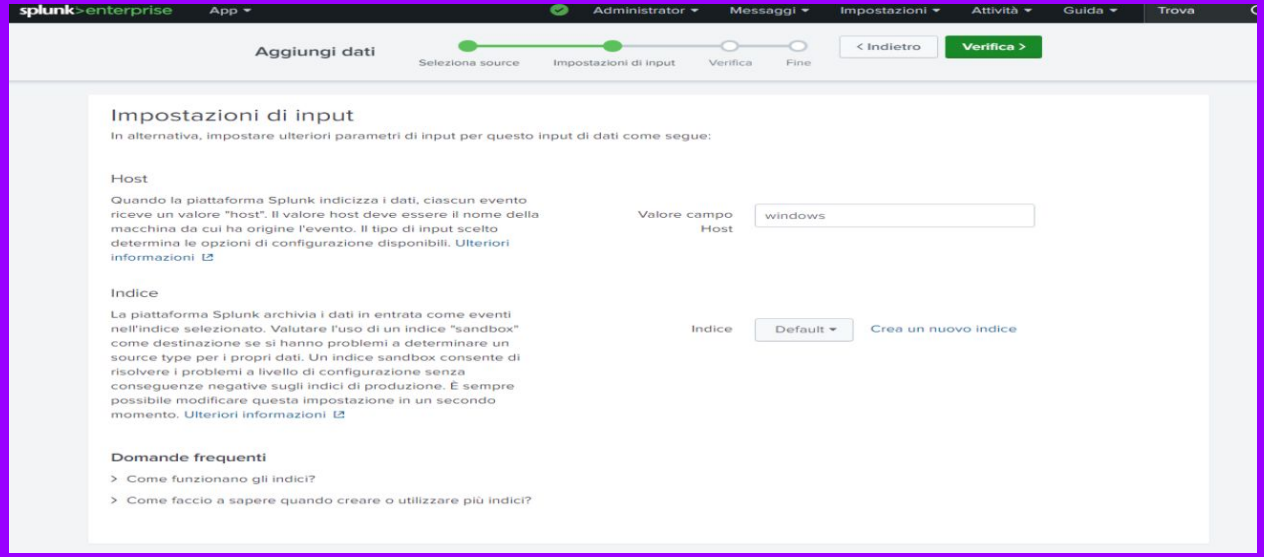
In breve: Lo studente dovrà configurare la modalità Monitora in Splunk e realizzare degli screenshot che mostrino l'esecuzione.



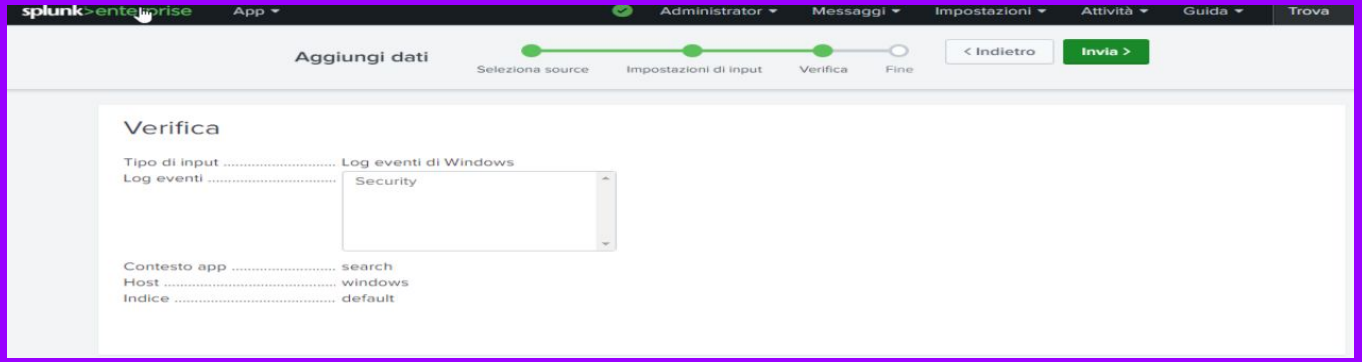
una volta effettuato l'accesso su splunk, andiamo nella sezione aggiungi dati e successivamente su monitora



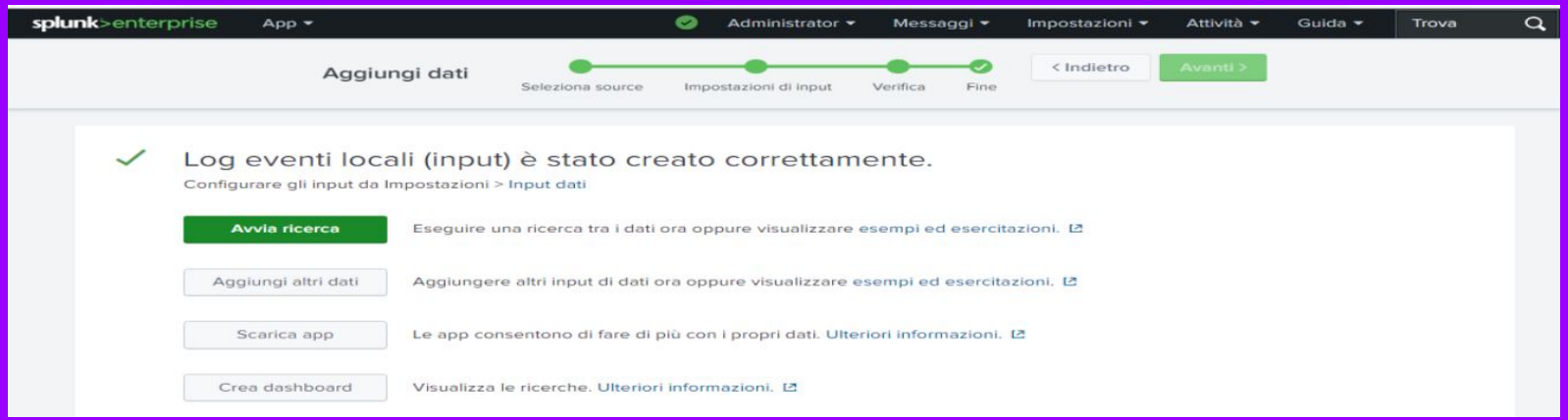
clicchiamo su log di eventi locali, selezioniamo security e successivamente su avanti



controlliamo le impostazioni di imput e clicchiamo su verifica



arrivati a questa schermata clicchiamo su invia



una volta creato il log di eventi locali correttamente avviamo la ricerca

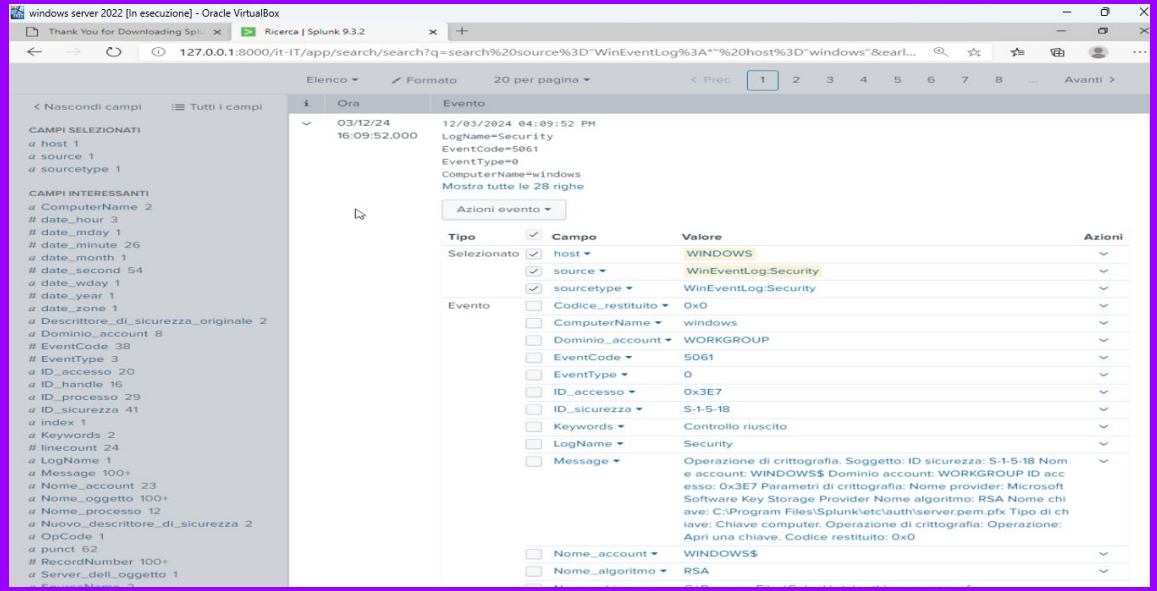
Questa schermata ci dice che:

● Stiamo analizzando i log di sicurezza di Windows (WinEventLog:Security) provenienti da un host specifico (windows).

● Tutti gli eventi trovati appartengono al registro di sicurezza di Windows, il che è comune quando si monitora la sicurezza di un sistema Windows.

● Abbiamo 1245 eventi totali che corrispondono ai criteri di ricerca.

● I campi selezionati e interessanti offrono un'ampia gamma di informazioni utili per l'analisi della sicurezza, come l'ora e la data dell'evento, il nome del computer, e dettagli dell'account.



Questa schermata mostra come Splunk può essere utilizzato per analizzare grandi quantità di dati di log di sicurezza di Windows. Utilizzando i campi selezionati e interessanti, possiamo eseguire query avanzate per ottenere insight significativi sui nostri dati di sicurezza.