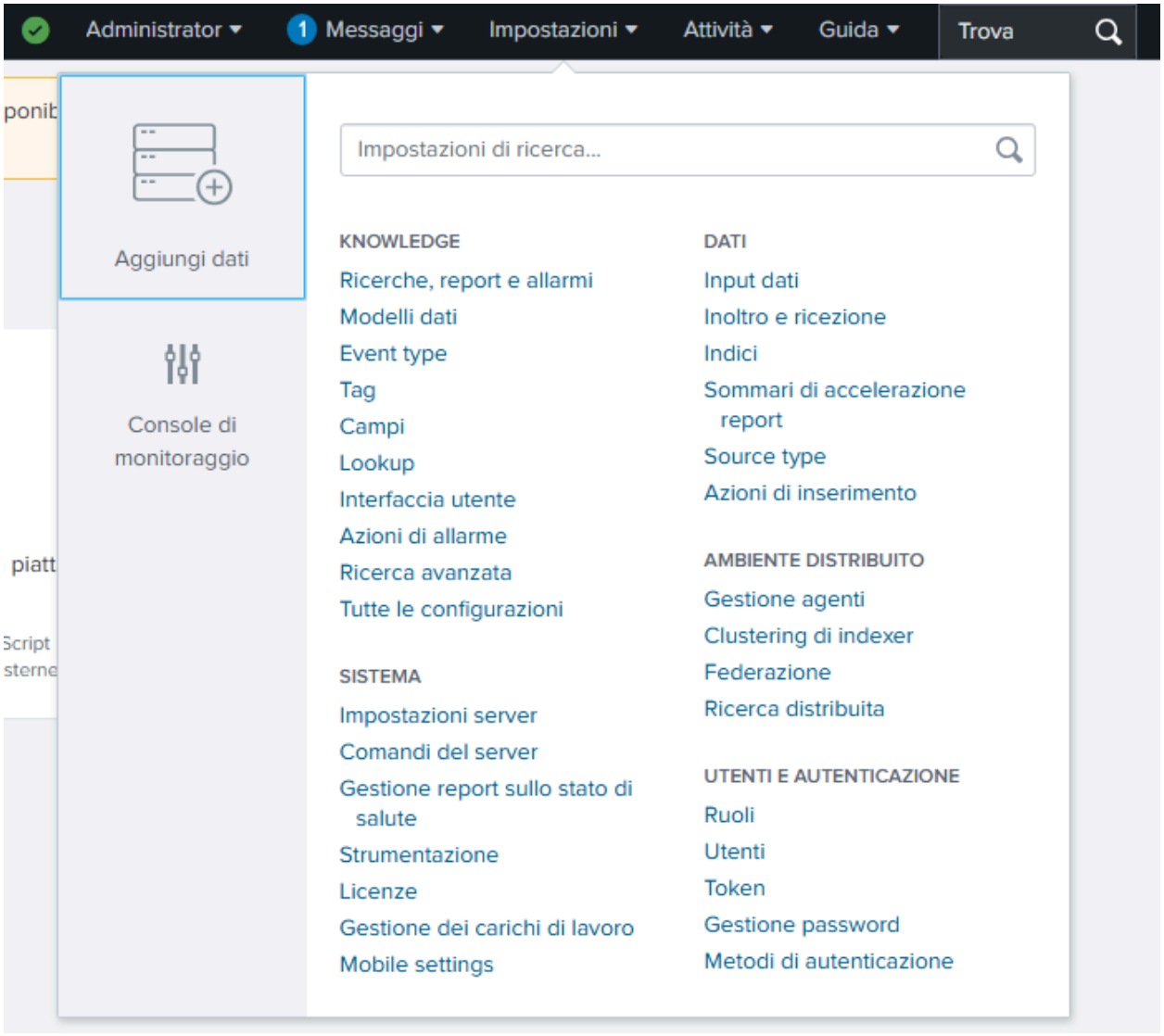
ESERCIZIO S10 L1

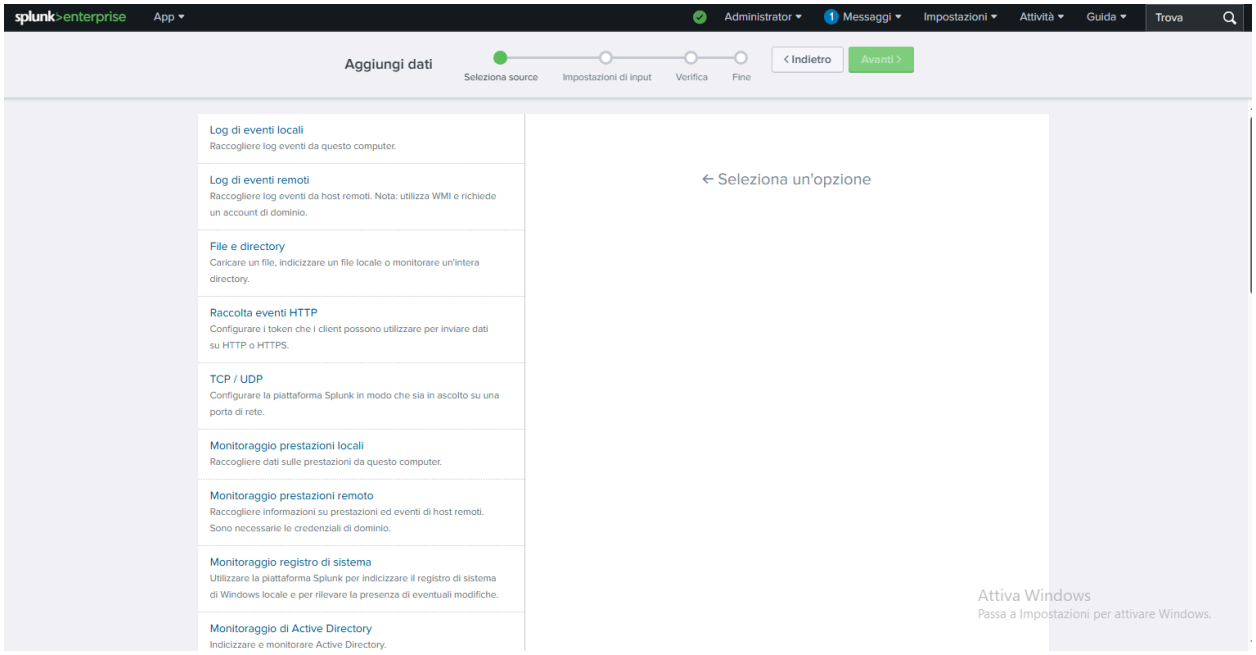
SVOLGIMENTO

Navigo innanzitutto nella sezione **Impostazioni**, poi clicco su **Aggiungi dati**

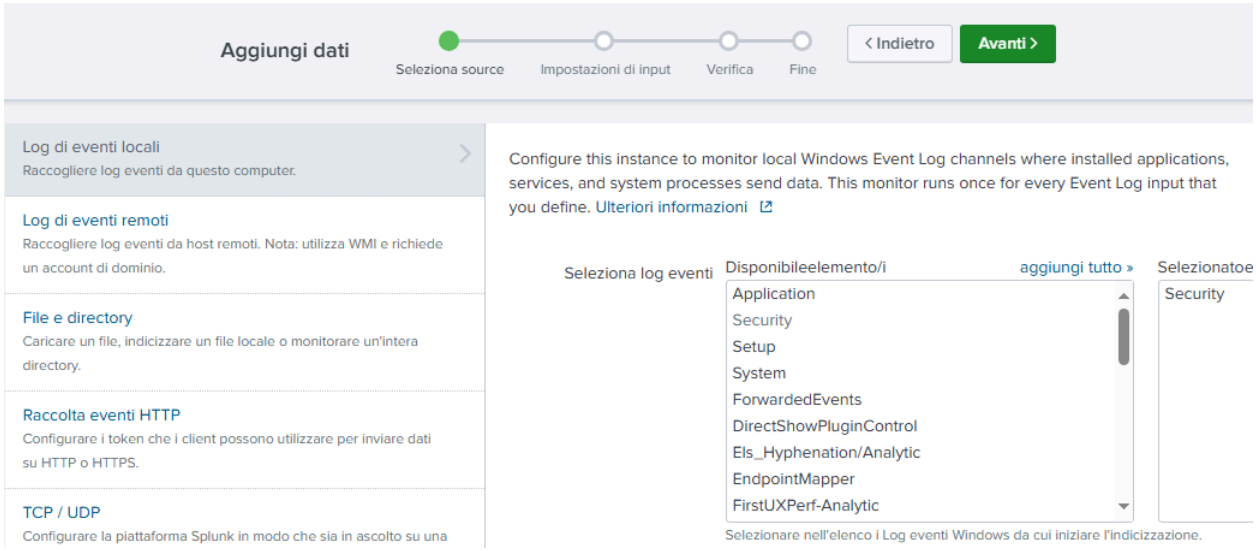


Come richiesto dalla traccia questa volta selezioniamo l'azione **Monitora** :

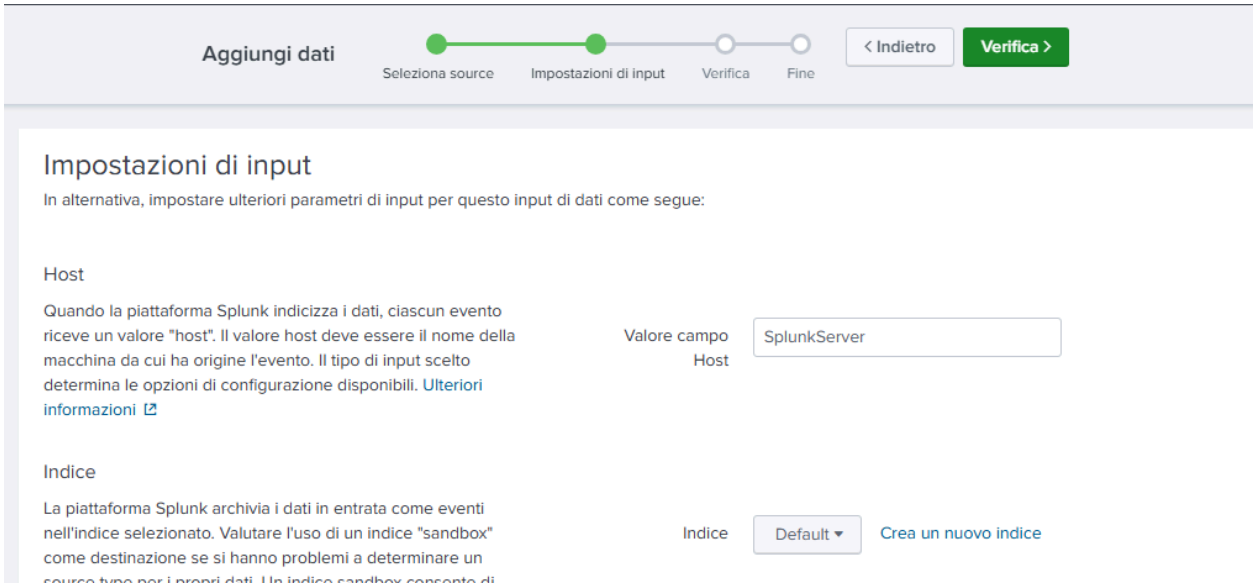
Seleziono a questo punto la prima sezione : **Log di eventi locali**



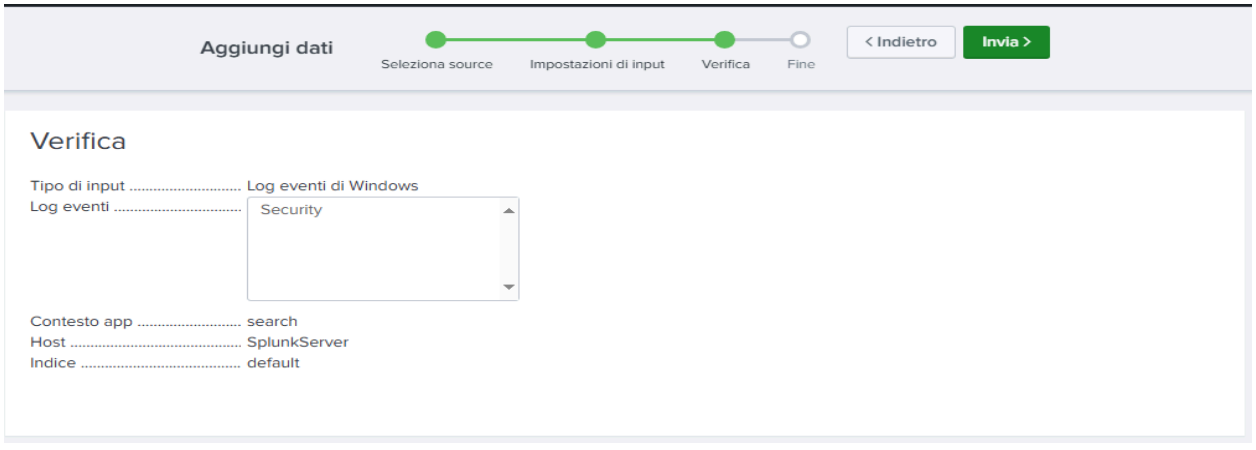
Ora, scelgo le impostazioni desiderate, in questo caso seleziono **Security**



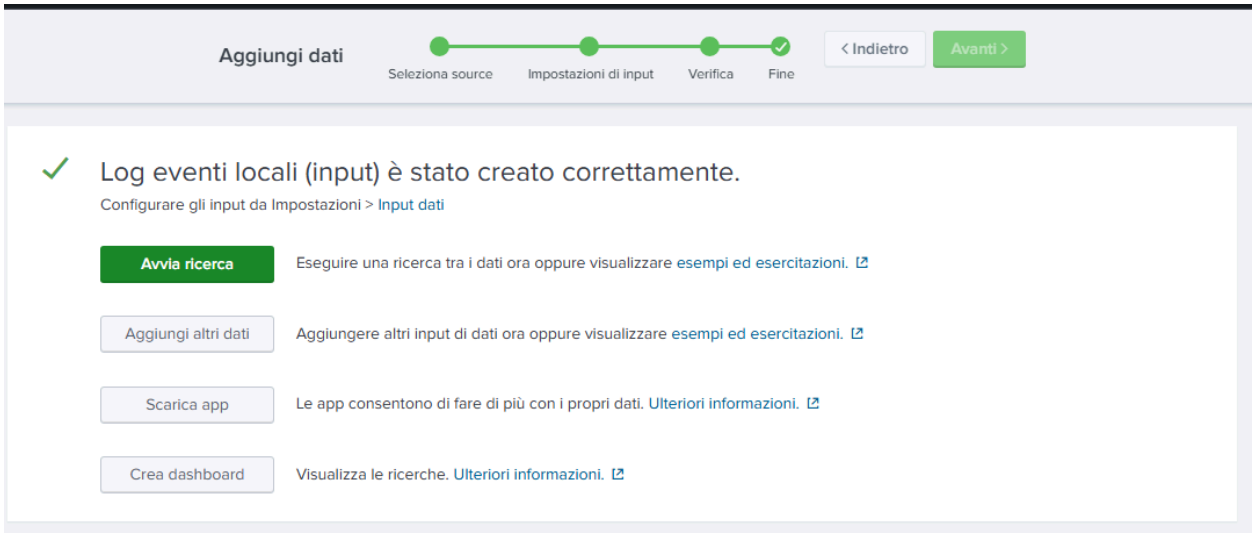
Clicco su **Avanti**



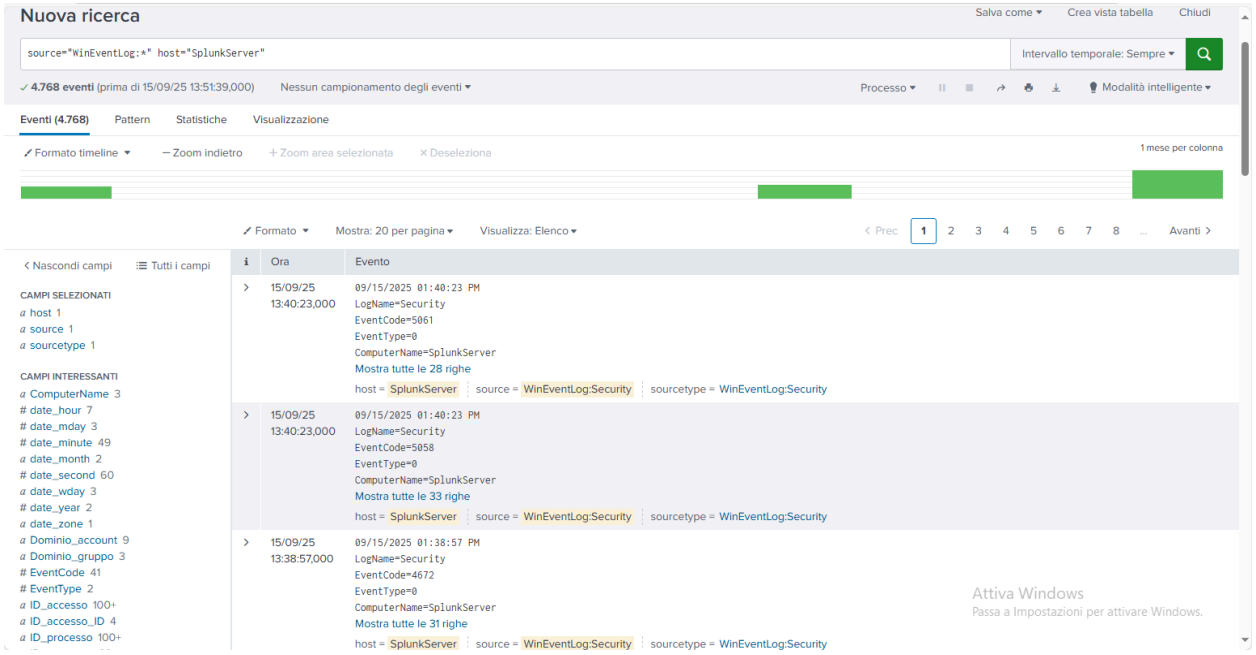
Seleziono **Verifica**



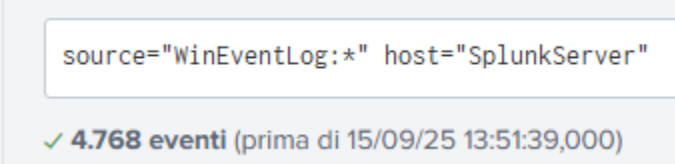
Seleziono Invio e successivamente **Avvia Ricerca**



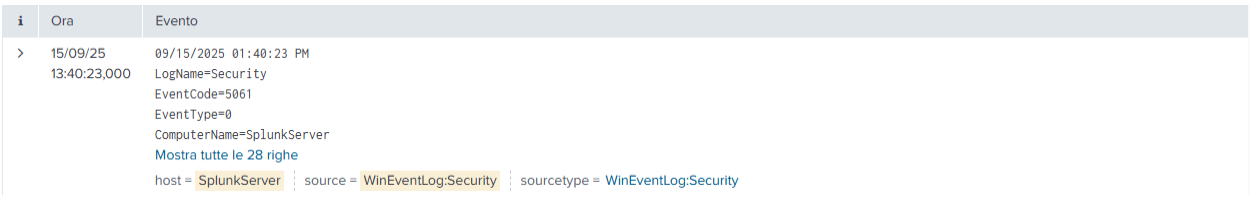
Ecco la schermata di risultato :



La presenza degli eventi log dimostrano il corretto funzionamento del procedimento con Splunk della sezione **Monitora.** Sono presenti di fatto **4.768 eventi.**



Questo è un esempio di evento dove viene mostrata data, ora e caratteristiche.
Host >>> Source >>> Sourcetype



Possiamo cliccare su **Mostra tutte le 28 righe** dove è possibile visualizzare più dettagli dell'evento.