Monitora Splunk
S10L1

Traccia:

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.

1) Obiettivo

L'obiettivo dell'esercizio è configurare Splunk Enterprise in modalità "Monitor" per raccogliere e analizzare in tempo reale i log di sistema (Windows Event Logs) dalla macchina locale.

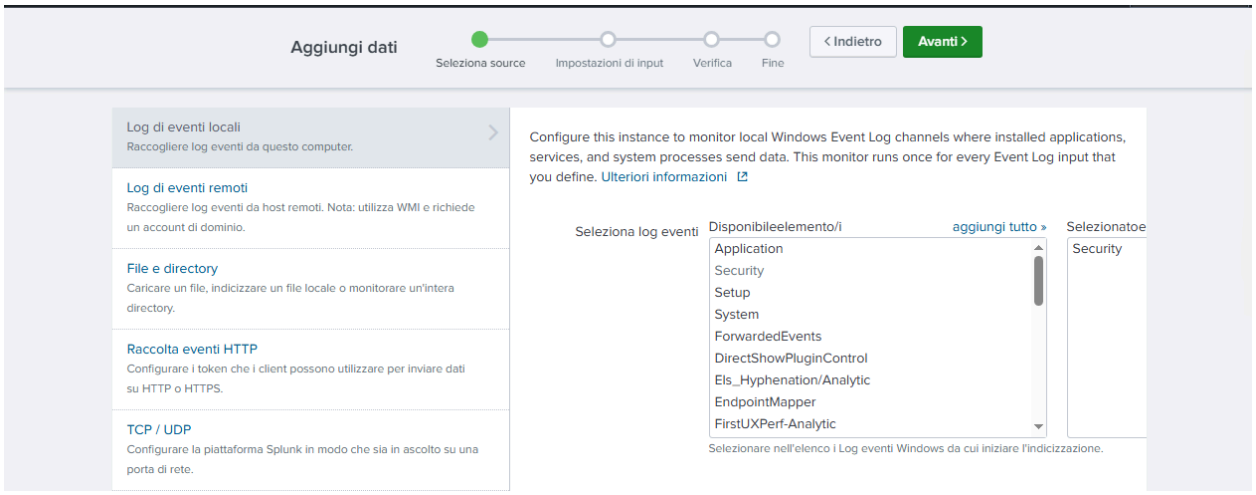
2) Procedura di configurazione

Passo 1: selezione della sorgente dati

Dalla home di Splunk, ho selezionato "Aggiungi dati" e successivamente la modalità **monitor**.

Nella sezione "Log di eventi locali" (Local Event Logs), ho selezionato la tipologia di log da monitorare.

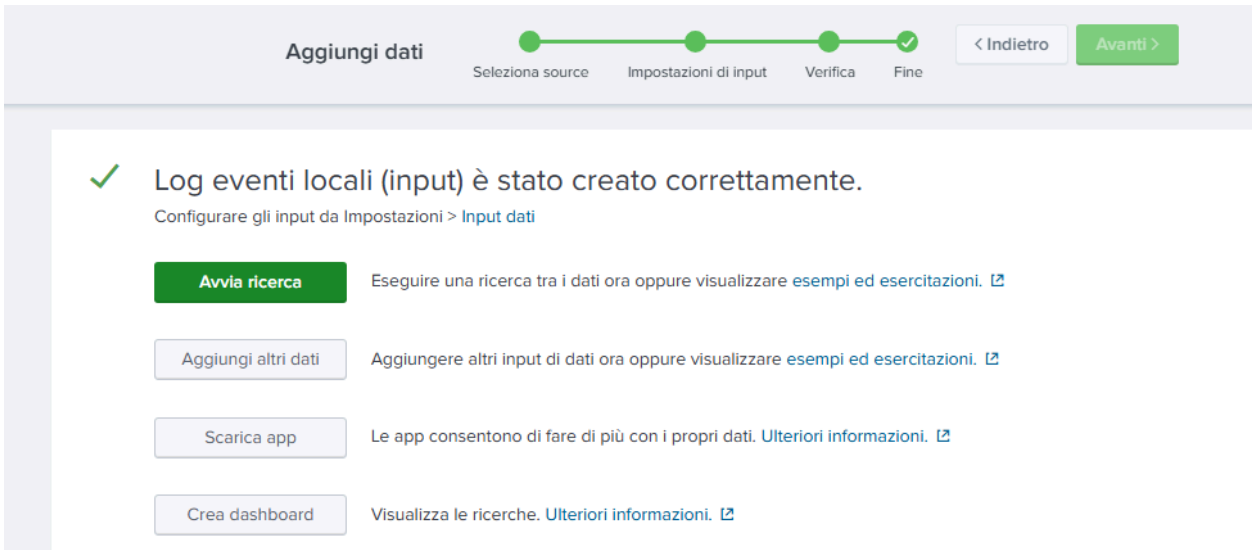
Come mostrato nello screenshot sottostante, ho scelto di monitorare il canale **security** per analizzare gli eventi relativi alla sicurezza del sistema.



Passo 2: impostazione dell'input

Durante la configurazione, ho personalizzato il nome dell'**host** per identificare univocamente la macchina sorgente.

Al termine della procedura guidata, Splunk ha confermato la corretta creazione dell'input dati.

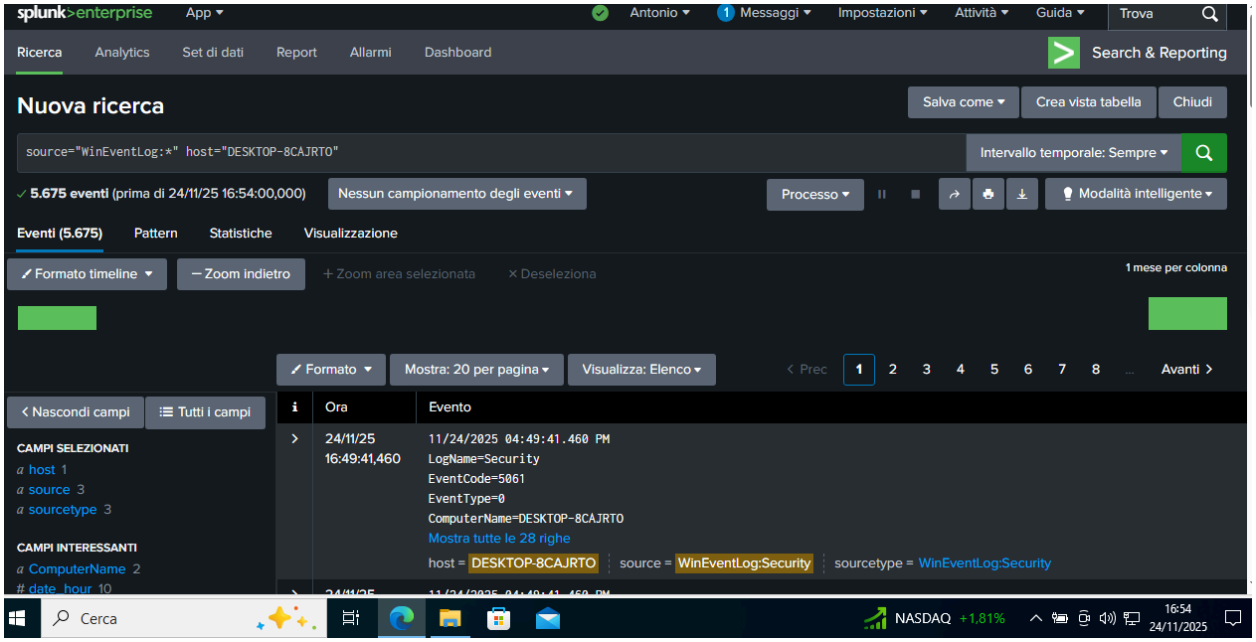


3) Verifica e risultati

Per confermare che la configurazione fosse operativa, ho avviato una ricerca sui dati indicizzati.

Analisi dei risultati:

- **Source:** `WinEventLog:Security`
- **Host:** `DESKTOP-8CAJRTO`
- **Esito:** la ricerca ha restituito **5.675 eventi**, confermando che Splunk sta ricevendo e indicizzando i dati in tempo reale.



4) Conclusione

La configurazione della modalità Monitor è avvenuta con successo, il sistema è ora attivo e sta collezionando i log di sicurezza locali, permettendo future analisi di security monitoring e incident response.