S10L1

EPICODE

Cyber Security & Ethical Hacking
Esercizio

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.

L'obiettivo di questo esercizio è **configurare la modalità "Monitora"** in **Splunk** e dimostrarne il funzionamento attraverso degli screenshot. Splunk offre diverse funzionalità, ma in questo caso, ci concentriamo sulla capacità di monitorare dati in tempo reale. Questo processo ci permette di raccogliere e analizzare log da diverse fonti, come ad esempio i log degli eventi di Windows.

La prima fase consiste nell'accedere alla schermata principale di **Splunk** e selezionare l'opzione

Aggiungi dati

Questa è la porta d'accesso per iniziare a importare qualsiasi tipo di dato nella piattaforma.

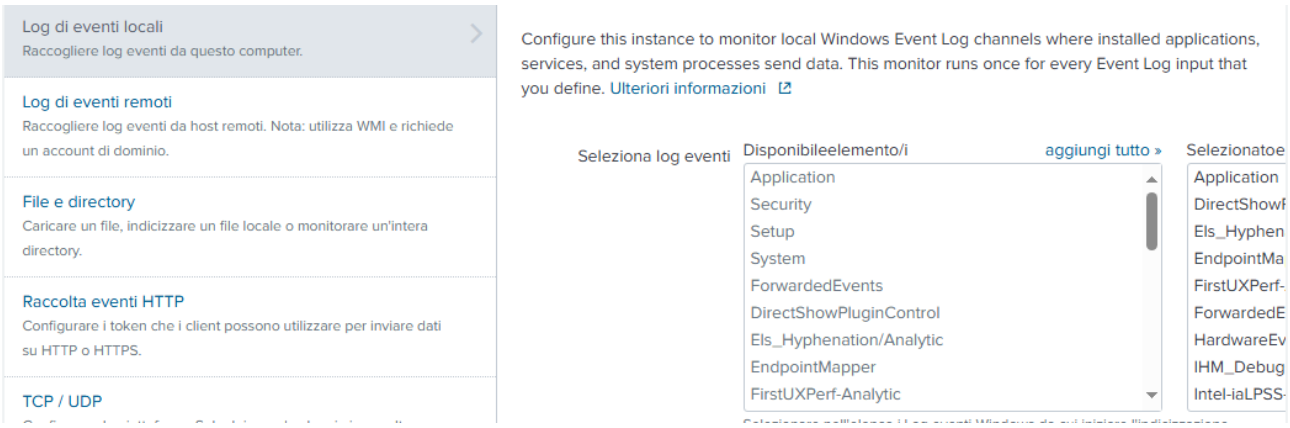
Una volta nella schermata di aggiunta dati, si presentano diverse opzioni. Scegliamo

Monitora

Questa modalità è ideale per l'acquisizione continua di dati da file, porte o script, rendendola perfetta per il monitoraggio in tempo reale.

Successivamente, il sistema ci chiede di specificare la fonte dei dati da monitorare. Abbiamo selezionato

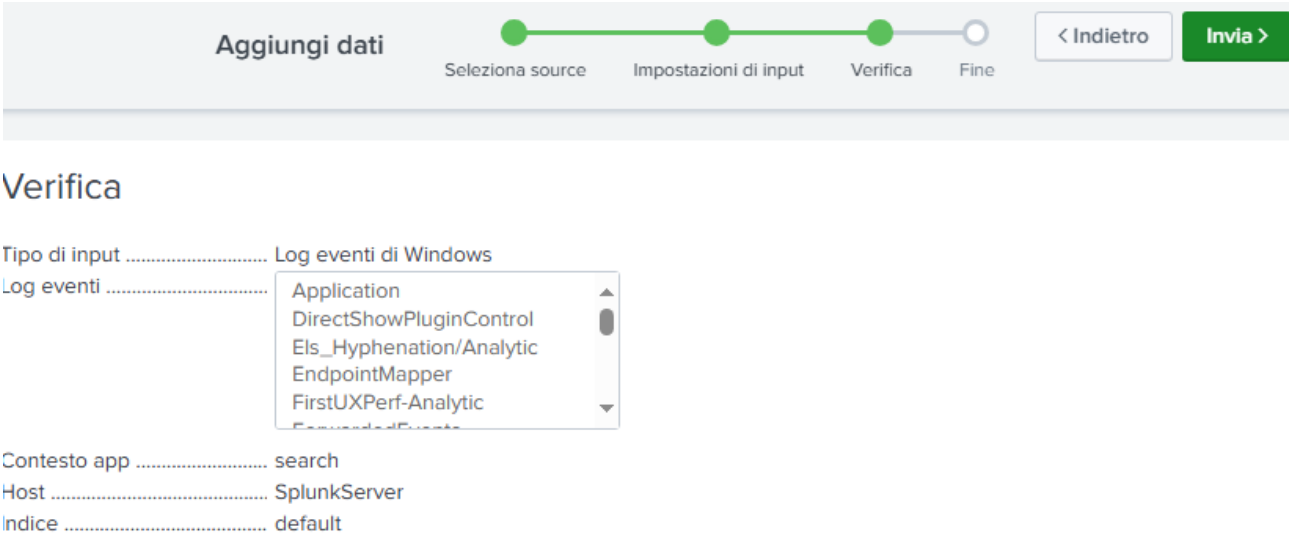
"Log di eventi locali" per raccogliere i log degli eventi di Windows del computer. Per questo esercizio, abbiamo scelto di aggiungere tutti i log disponibili (Application, Security, Setup, System) per una dimostrazione completa.

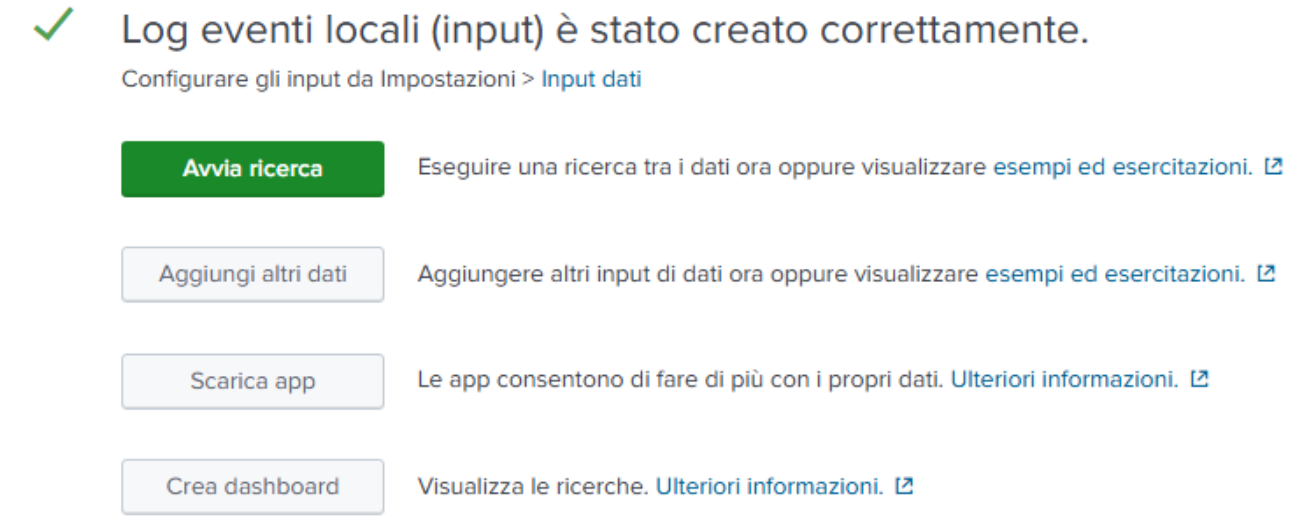


Nella fase di configurazione successiva, abbiamo impostato i parametri di input. Il valore

"Host" è stato lasciato come **SplunkServer** per identificare la macchina di origine dei dati, mentre l'**"Indice"** è stato mantenuto come **default**. Questo indice è il contenitore predefinito dove Splunk archivierà i dati in ingresso.

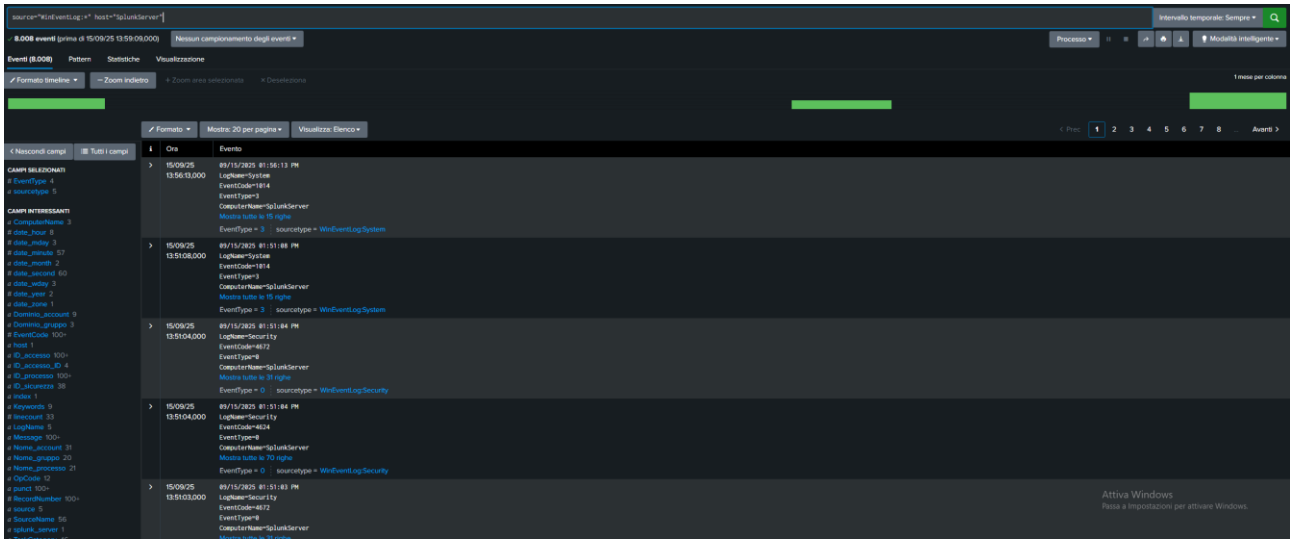
Prima di finalizzare, Splunk mostra un riepilogo delle configurazioni scelte per la verifica. Dopo aver confermato che tutte le impostazioni sono corrette, il processo di configurazione è stato completato con successo. Un messaggio di conferma indica che l'input dei log eventi locali è stato creato.





Infine, abbiamo avviato la ricerca per visualizzare i dati appena acquisiti. Lo screenshot mostra la schermata di **Splunk** con i log degli eventi visualizzati, confermando che la configurazione è stata eseguita correttamente e che il monitoraggio è attivo.

I dati sono ora pronti per essere analizzati, visualizzando informazioni dettagliate come l'ora, il tipo di evento e l'host di provenienza.



L'esito finale della ricerca ha confermato che la configurazione è stata completata correttamente, permettendo di visualizzare i dati in una dashboard intuitiva. Questo processo non solo valida la comprensione delle funzionalità di Splunk, ma sottolinea anche l'importanza di monitorare continuamente i log per mantenere la sicurezza e l'integrità dei sistemi.