REPORT TECNICO

“Monitora” Splunk

Redatto da: *Nicolò Calì Cybersecurity Student*

Data: 09/02/2026

Oggetto: *esplorazione della funzionalità "Monitora" di Splunk*

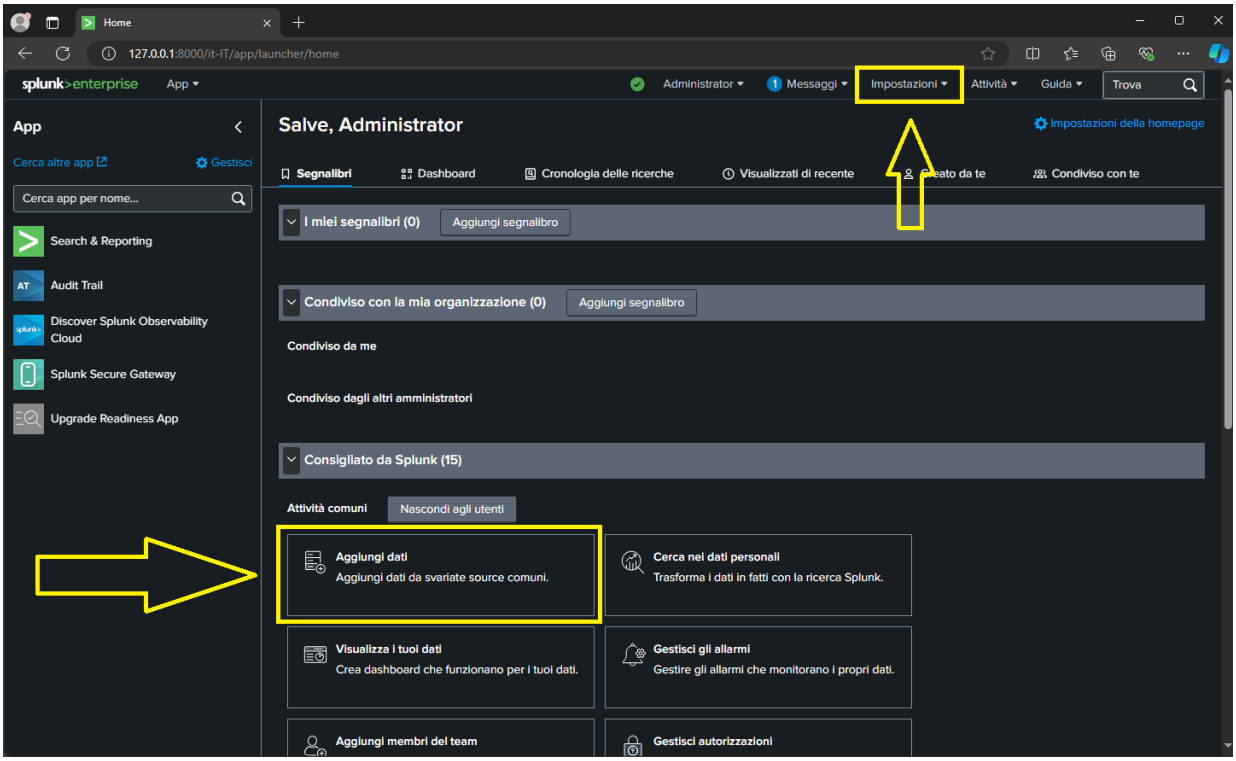
1. Introduzione

Il presente documento ha lo scopo di illustrare la procedura di configurazione della funzionalità "Monitora" all'interno della piattaforma **SIEM Splunk**.

L'obiettivo dell'attività è predisporre l'ambiente per l'acquisizione e l'indicizzazione in tempo reale di flussi di dati (**log**) provenienti dalla macchina locale, verificando il corretto funzionamento del meccanismo di **ingestion** dei dati.

2. Configurazione dell'ambiente

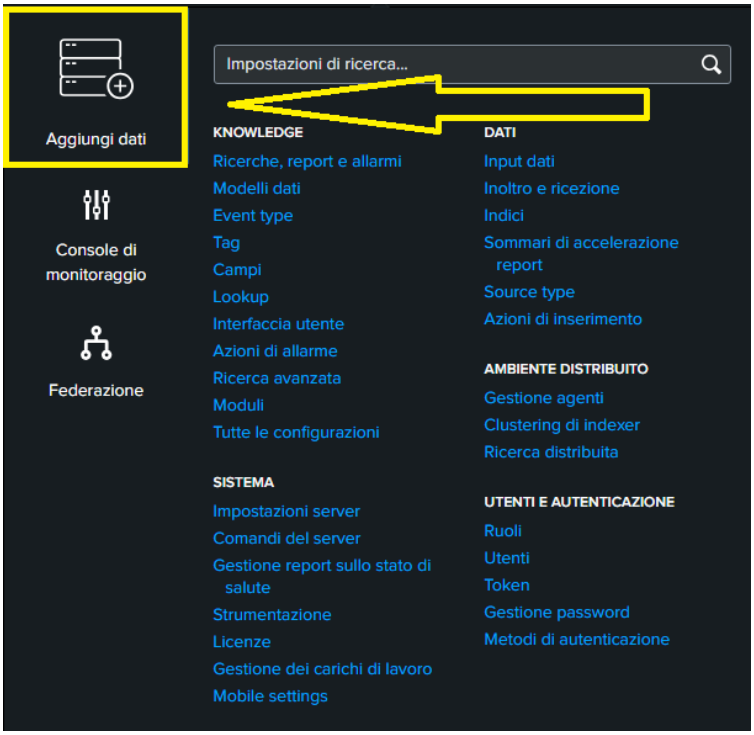
L'esercitazione è stata condotta su una workstation dotata di sistema operativo **Windows 10**. Il software utilizzato è **Splunk Enterprise**, installato localmente e configurato con le impostazioni di default. L'interazione con la piattaforma avviene tramite l'interfaccia web accessibile via browser attraverso il seguente **URL** e **Porta**:



Per accedere alla funzionalità "Monitora" cliccando su "Aggiungi dati" nella pagina principale di Splunk Web.

In alternativa è possibile anche accedervi da:

Impostazioni → Aggiungi dati

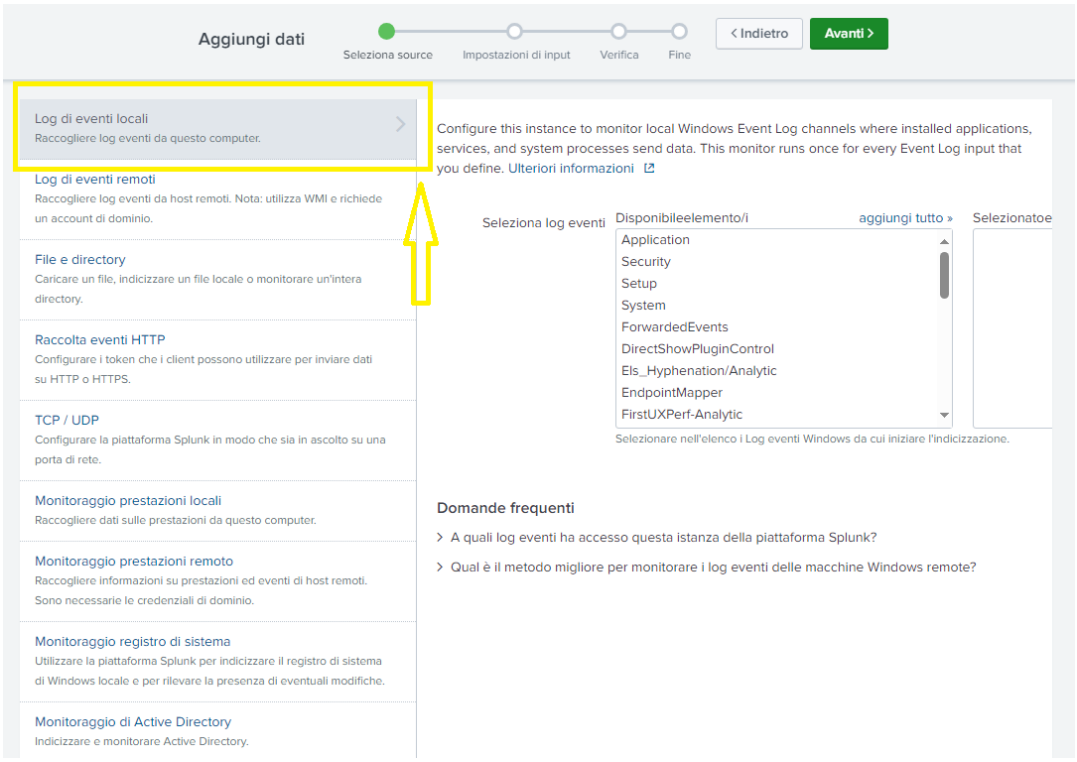


Nella pagina successiva potremo selezionare la modalità “Monitora” come mostrato nella figura in basso.

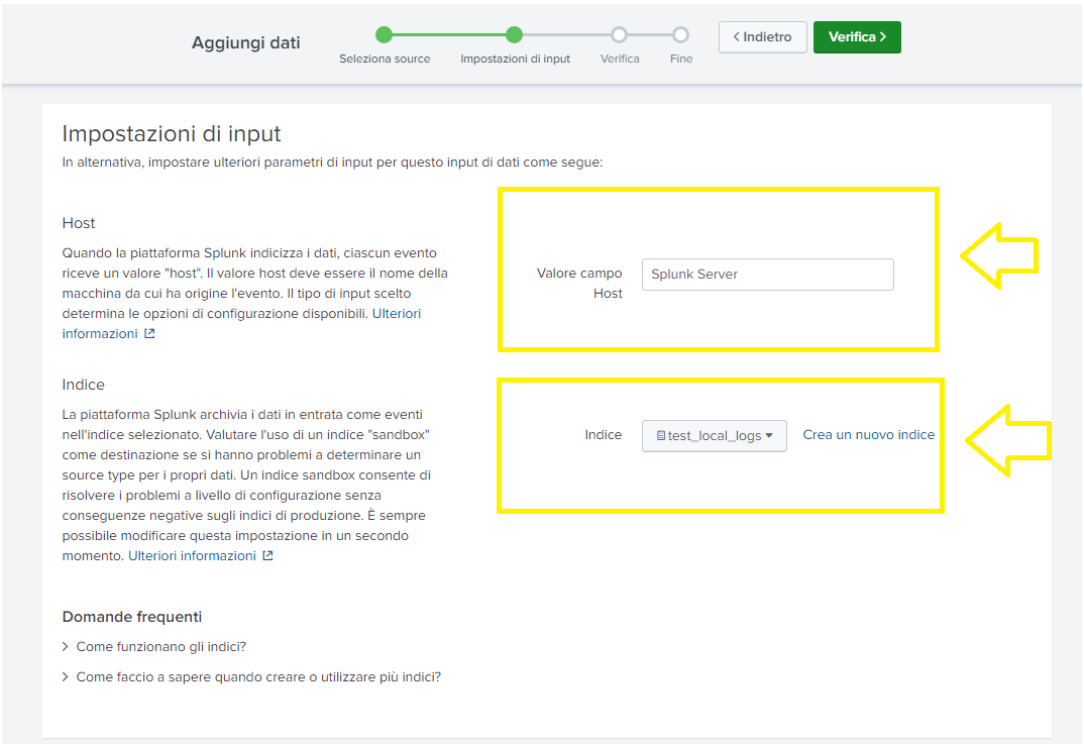
Adesso non ci resta altro che configurare i principali dettagli di questa funzionalità per poi avviarla.

Per prima cosa selezioniamo la source (Nel mio caso scelgo Log di eventi locali) e successivamente assicuriamoci di aggiungere i **Log Eventi** che ci interessano, nel mio caso andrò ad inserire:

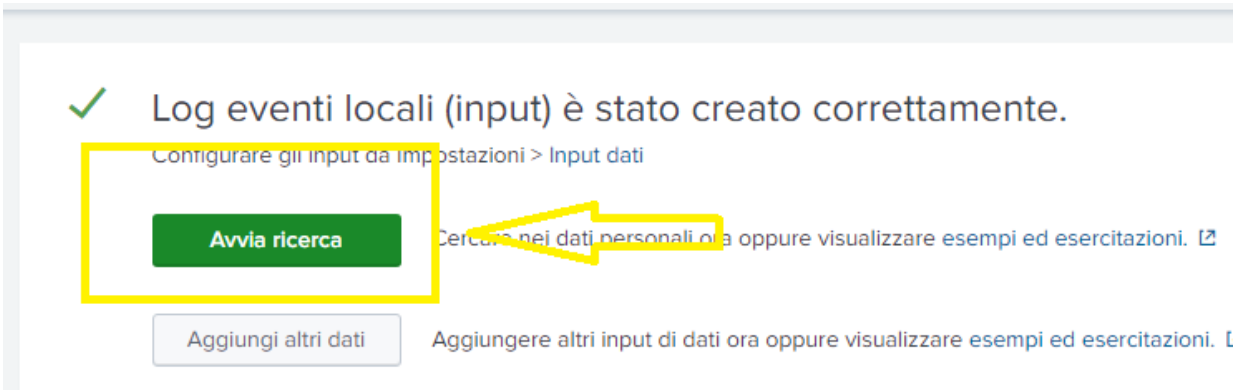
- **Application**
- **Security**
- **System**



A seguire nelle impostazioni di input andrò a cambiare il Valore campo **Host** in “Splunk Server” e l’**Indice** in “test_local_logs”.

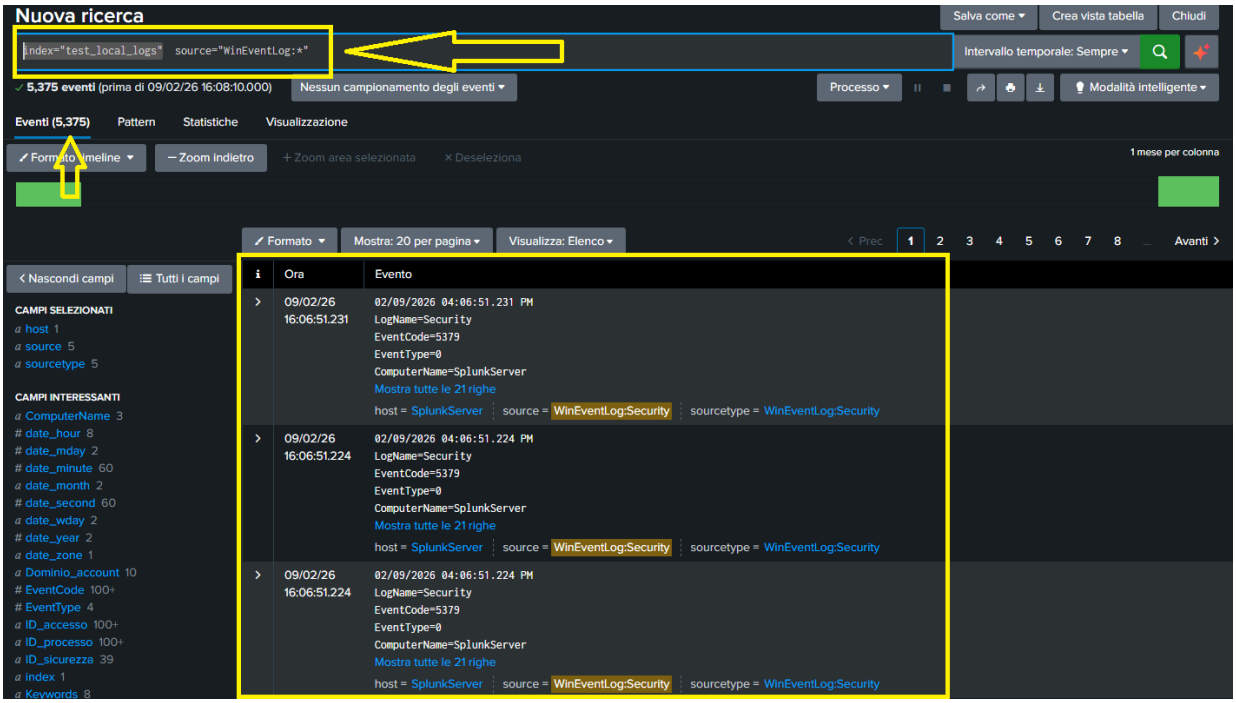


Clicchiamo su Avvia ricerca ed avremo terminato con la configurazione di questo SIEM.



3. Esecuzione

Al termine della configurazione, abbiamo effettuato una verifica per confermare l'effettiva acquisizione dei dati. Utilizzando la stringa di ricerca **`index="test_local_logs" source="WinEventLog:*"`**, abbiamo interrogato la piattaforma per visualizzare tutti i log di sistema in ingresso su quello specifico **index** che avevamo precedentemente creato durante la configurazione.



Come mostrato nella figura, Splunk ha iniziato a indicizzare correttamente gli eventi (**5.375 rilevazioni**), confermando che la modalità "Monitora" è attiva e funzionante sulla macchina Windows 10.

5. Conclusione e Considerazioni

In questo laboratorio abbiamo configurato **Splunk** per monitorare in tempo reale un PC Windows 10.

Abbiamo impostato la raccolta dei log principali (Applicazione, Sicurezza e Sistema) inviandoli correttamente all'indice specifico '**test_local_logs**'. Il test finale è stato un successo: abbiamo rilevato oltre 5.000 eventi, confermando che il sistema funziona.

Questo è il primo passo per la sicurezza: ora che abbiamo una visione centrale di ciò che accade nel computer, siamo pronti per creare grafici di controllo, impostare allarmi e cercare attivamente eventuali minacce.