Configurazione della Data Ingestion in Tempo Reale su Splunk

1. Introduzione e Obiettivi

L'obiettivo di questa sessione di laboratorio è stato il passaggio da un approccio statico (il semplice caricamento di file) a un approccio dinamico e continuo: la **Modalità Monitor**. A differenza dell'upload manuale, la funzione "Monitor" di Splunk permette di sorvegliare file, directory, porte di rete o script in tempo reale.

In questo scenario, il mio compito è configurare un input di dati che osservi attivamente i log di sistema (o un'altra fonte dati presente nella macchina virtuale) e indicizzarli non appena vengono scritti. Questo è il cuore del funzionamento di un SIEM (Security Information and Event Management).

2. Ambiente e Strumenti Utilizzati

Per l'esecuzione dell'esercizio ho utilizzato i seguenti strumenti:

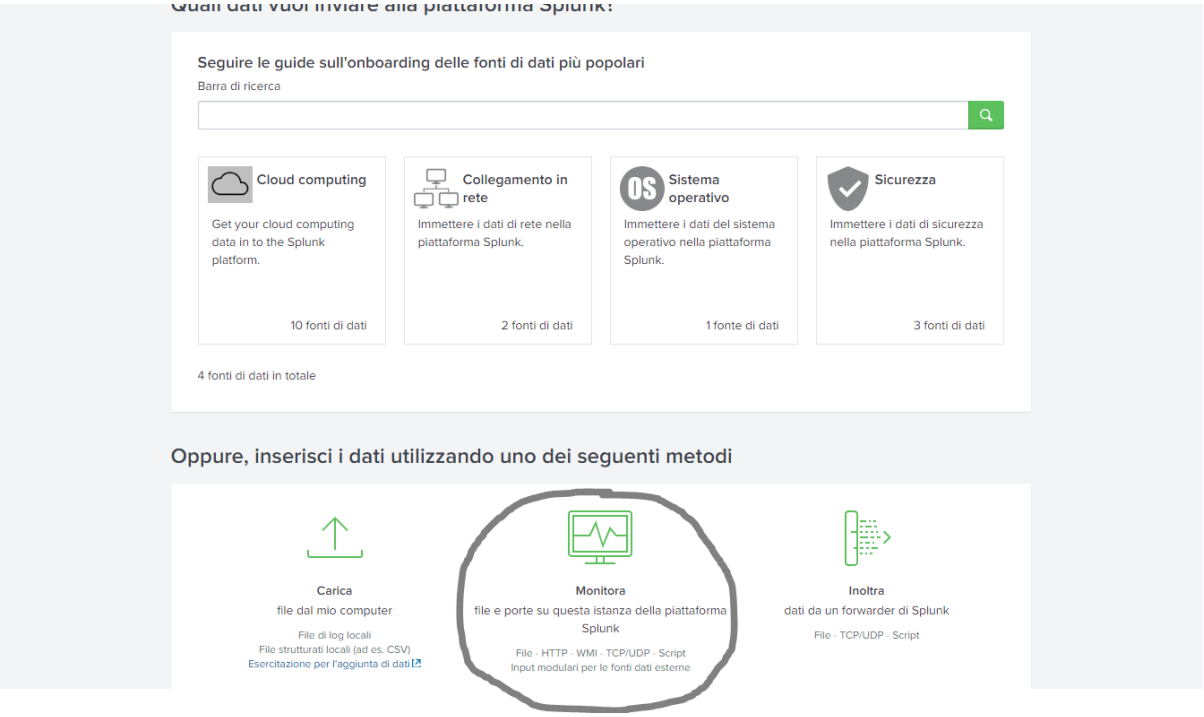
- **Virtualizzazione:** Oracle VirtualBox.
- **Sistema Operativo Guest:** Windows, dove risiede l'istanza Splunk.
- **Software Target:** Splunk Enterprise (versione Web accessibile via browser su porta 8000).
- **Browser:** Edge per l'interazione con la GUI di Splunk.

3.Configurazione

Accesso alla Sezione "Add Data"

Ho iniziato loggandomi nell'interfaccia web di Splunk. Dalla dashboard principale, ho navigato verso le impostazioni per l'aggiunta dei dati.

Ho cliccato sull'icona **Monitora** (Monitor) per iniziare la configurazione di un input locale.



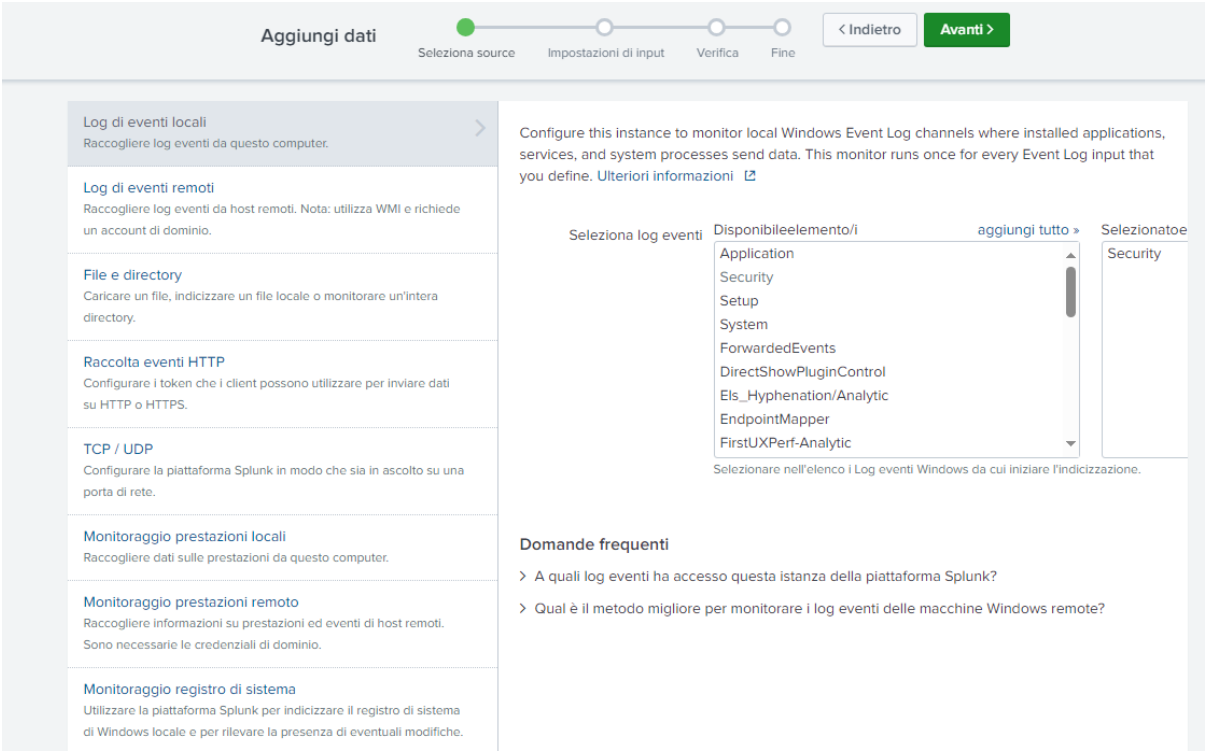
Selezione dei "Local Event Logs" (Log Eventi Locali)

Una volta all'interno del menu di configurazione, invece di selezionare file specifici, ho diretto la mia attenzione alla colonna di sinistra. Qui ho individuato e selezionato la voce Log di eventi locali.

Questa opzione è fondamentale in ambienti Windows perché permette a Splunk di interfacciarsi direttamente con il registro degli eventi di sistema (Event Viewer) senza dover puntare a file .evtx statici.

Azione:

1. Nel menu a sinistra, ho cliccato su **Log di eventi locali**.
2. Nella lista che è apparsa al centro (Available Logs), ho selezionato le tipologie di eventi che desideravo monitorare. Per questo esercizio, ho spuntato:
    a. **Security** (per i tentativi di accesso e audit)
3. Ho verificato che la raccolta fosse impostata per iniziare immediatamente.

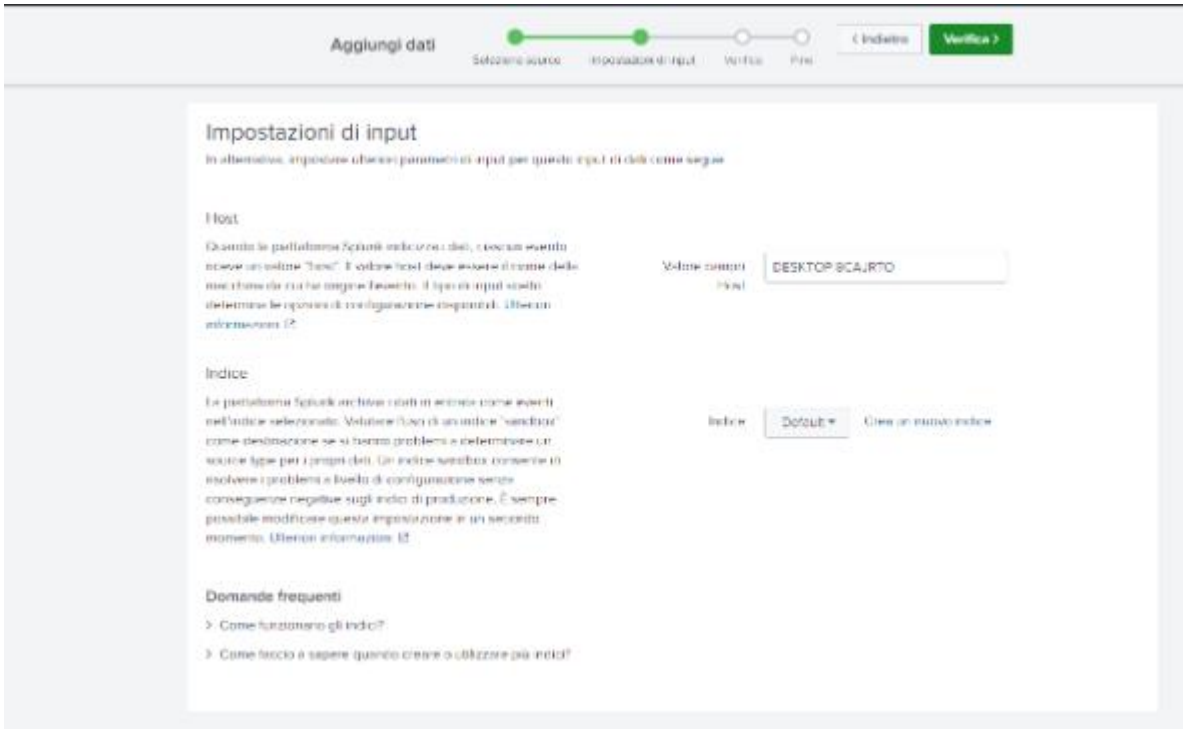


Configurazione delle Impostazioni di Input (Input Settings)

Dopo aver selezionato la sorgente sono arrivato alla schermata di configurazione dei metadati. Questo passaggio è cruciale per etichettare correttamente i dati prima che entrino nel database di Splunk.

Come si vede nello screenshot sottostante, ho configurato i seguenti parametri:

1. **Host:** Il sistema ha precompilato il campo con il valore DESKTOP-8CAJRTO. Ho confermato questa impostazione, poiché permette di identificare univocamente che i log provengono da questa specifica macchina virtuale.
2. **Indice:** Ho mantenuto l'impostazione su Default. In Splunk, l'indice di default corrisponde all'indice **main**. Sebbene in produzione si tenda a creare indici separati (es. windows_logs), per questo laboratorio l'indice principale è la destinazione corretta.

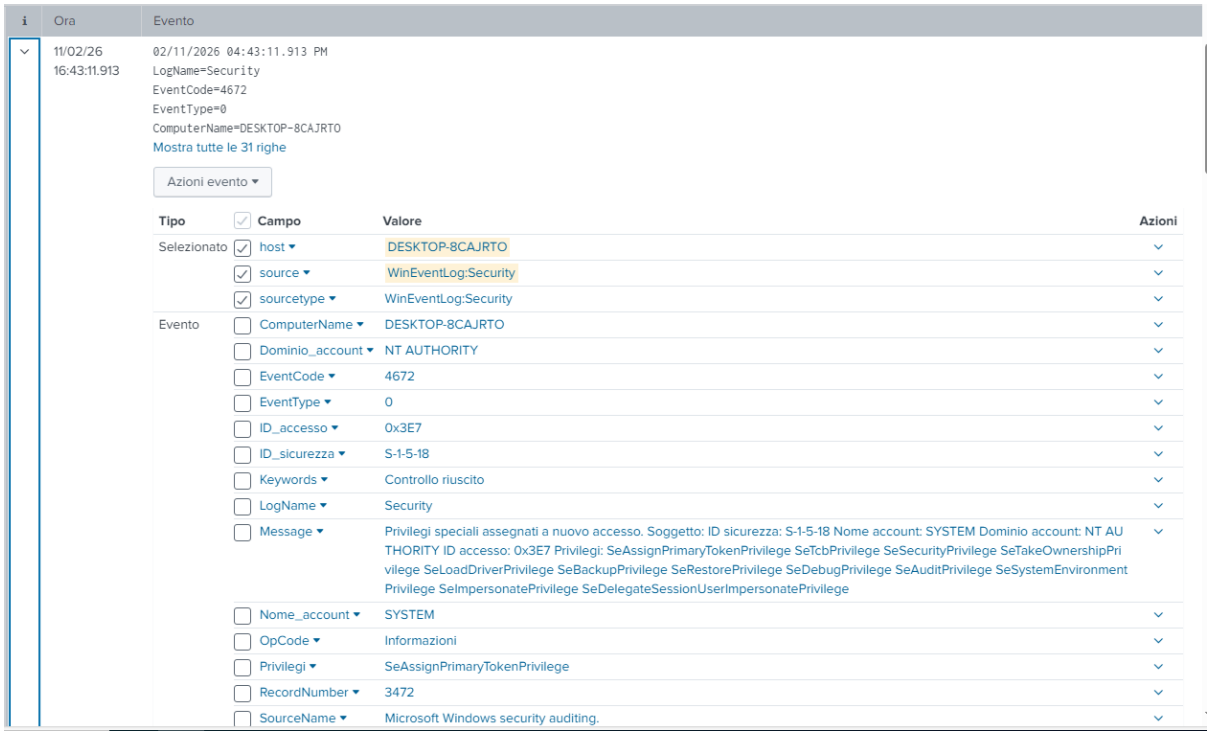


Una volta verificate queste impostazioni, ho cliccato su **Verifica** e successivamente ho confermato l'operazione per avviare immediatamente l'ingestione.

Verifica e Analisi dei Log in Tempo Reale

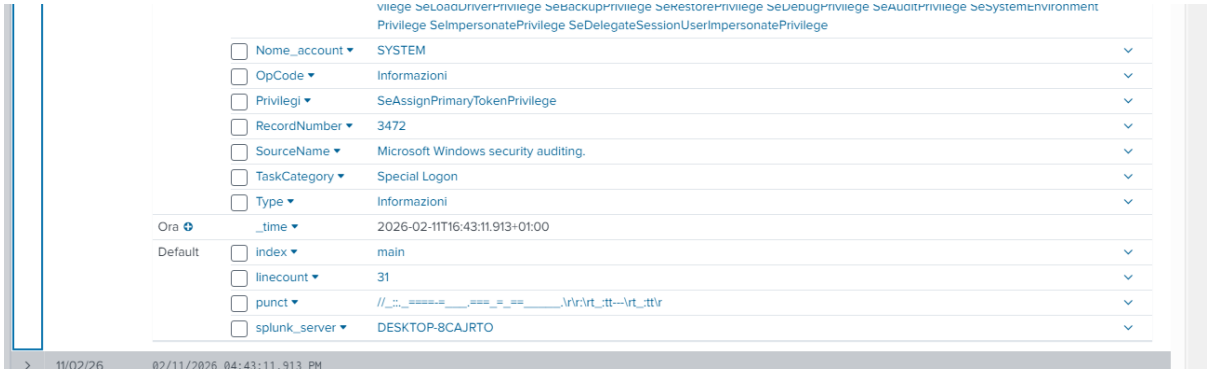
Per confermare il successo dell'operazione, ho cliccato su **Avvia ricerca**. L'obiettivo era verificare non solo la presenza dei dati, ma la qualità del "parsing" (ovvero come Splunk legge e separa i campi).

L'esito è stato positivo. Splunk ha iniziato a mostrare eventi in tempo reale. Ho analizzato nel dettaglio un evento specifico catturato durante la sessione, come mostrato nelle immagini seguenti.



Dallo screenshot si evince che Splunk ha indicizzato correttamente un evento critico di sicurezza:

- **Timestamp:** 02/11/2026 04:43:11 PM (Orario della VM).
- **SourceType:** WinEventLog:Security. Questo conferma che stiamo leggendo il registro di Sicurezza di Windows.
- **Event Code 4672:** Ho espanso i dettagli dell'evento e notato il codice 4672. Questo codice corrisponde a **"Special privileges assigned to new logon"**.
- **Account:** L'utente coinvolto è SYSTEM (NT AUTHORITY), il che indica un'operazione interna di alto livello del sistema operativo.



ho potuto verificare i metadati tecnici aggiuntivi:

- **index = main:** Conferma che la configurazione della Fase 3 è stata applicata correttamente.
- **Campi Estratti:** Sulla colonna di sinistra (la "Field Sidebar"), Splunk ha estratto automaticamente campi utili come ComputerName, EventCode, Privileges e OpCode. Questo dimostra che la modalità "Monitora" non si limita a copiare il testo, ma lo struttura rendendolo pronto per le query di analisi.

5. Conclusione

L'esercizio si è concluso con successo.

1. Ho configurato un input di tipo **"Log di eventi locali"** per monitorare Security.
2. Ho verificato che i dati fluiscono nell'indice main con l'host corretto (DESKTOP-8CAJRTO).
3. Ho dimostrato la capacità di Splunk di interpretare eventi complessi (come l'EventCode 4672) in tempo reale, fornendo visibilità immediata sulle operazioni privilegiate del sistema operativo.

Questa configurazione rappresenta la base per qualsiasi attività di monitoraggio SIEM in ambiente Windows.