PRATICA S10L1

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

Passaggio 1: Monitoraggio dei dati in Splunk

Mi trovo nella schermata iniziale per l'onboarding dei dati su Splunk Enterprise. In alto compare un messaggio di avviso:

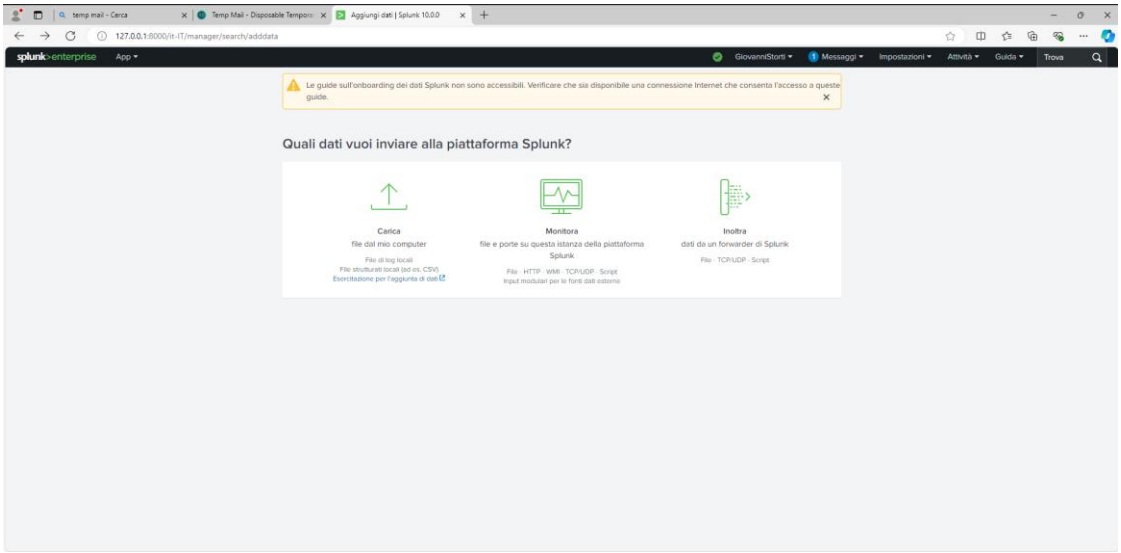
La piattaforma mi chiede: **"Quali dati vuoi inviare alla piattaforma Splunk?"**

Tra le tre opzioni disponibili, scelgo **Monitora**, perché voglio configurare il monitoraggio continuo di una sorgente dati, come un'applicazione locale o un servizio cloud.

L'opzione è descritta così:

"Monitora i dati da una piattaforma locale o da un servizio cloud."

Clicco su **"Monitora i dati"** per iniziare la configurazione del monitoraggio.



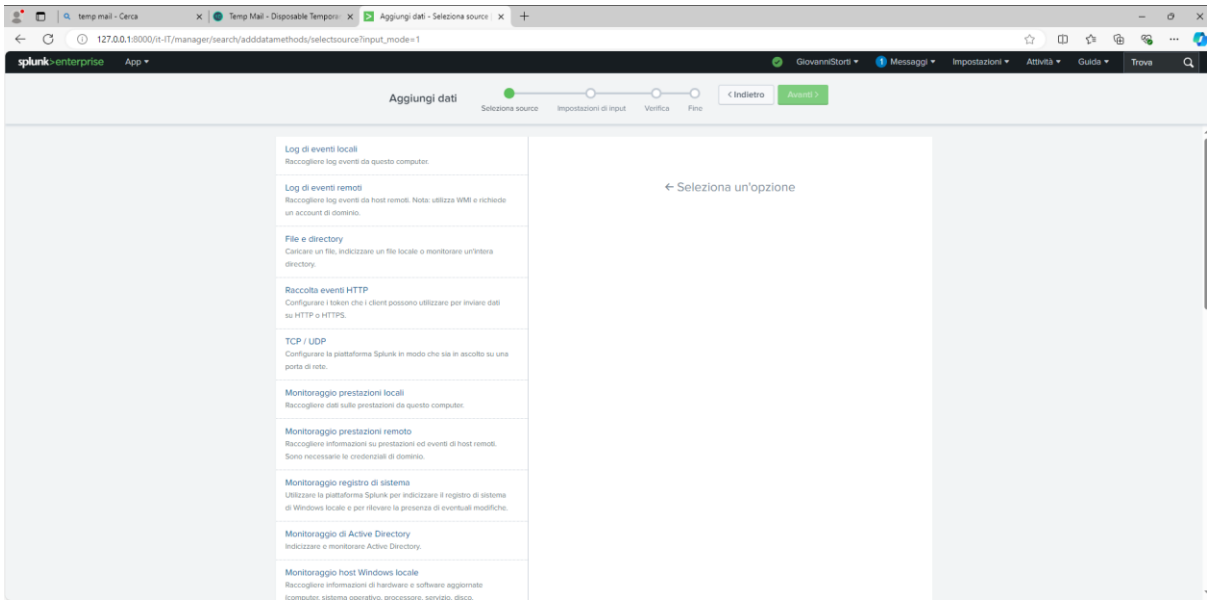
Passaggio 2: Selezione dell'origine dati da monitorare

Dopo aver scelto di monitorare i dati, Splunk mi porta alla sezione **"Aggiungi dati"**, dove inizia il processo guidato. In alto vedo una barra di avanzamento con quattro step: **Seleziona origine dati → Imposta → Rivedi → Completa** Attualmente sono sul primo step: **Seleziona origine dati**.

A sinistra ho un elenco di possibili sorgenti da cui posso raccogliere i dati. Le opzioni includono:

- **Log di eventi locali** – per monitorare gli eventi generati dal sistema operativo.
- **Log di eventi remoti** – utile se voglio raccogliere eventi da altri host.
- **File e directory** – per monitorare file di log o cartelle specifiche.
- **Raccolta dati HTTP** – se voglio ricevere dati tramite richieste HTTP.
- **TCP/UDP** – per flussi di dati in tempo reale via rete.
- **Monitoraggio protezione avanzata** – per eventi legati alla sicurezza.
- **Registro di sistema** – per monitorare modifiche e accessi al registro.
- **Active Directory** – se voglio tenere traccia delle attività su AD.
- **File di sistema** – per controllare file critici del sistema.

Al momento non ho ancora selezionato nulla, quindi sulla destra compare solo il messaggio **"Seleziona un'opzione"**.

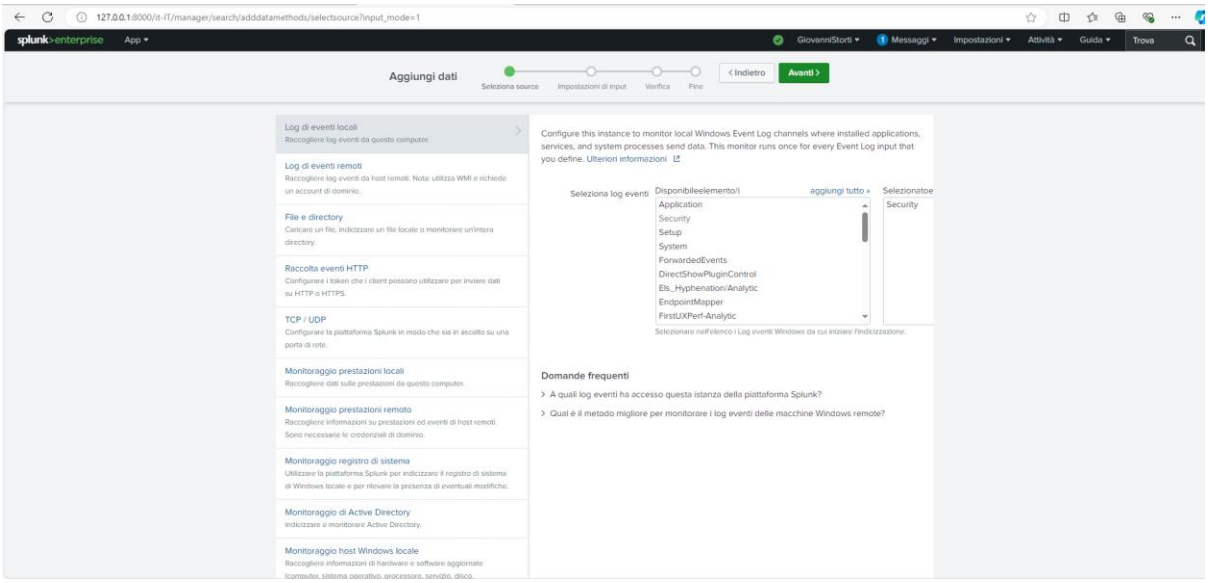


Passaggio 3: Configurazione del monitoraggio dei log di sicurezza locali

Dopo aver selezionato “Monitora i dati”, Splunk mi ha portato alla schermata **“Aggiungi dati”**, dove posso scegliere l’origine da monitorare. Ho selezionato **“Log di eventi locali”** perché voglio tenere traccia degli eventi di sicurezza generati dal sistema operativo.

Nella lista delle categorie disponibili, ho scelto **Security**, che include eventi come accessi, modifiche ai permessi, tentativi di autenticazione e altre attività sensibili. Questa scelta è fondamentale per analizzare comportamenti sospetti o per fare auditing su utenti e processi.

Una volta selezionata la categoria Security, posso procedere con la configurazione dettagliata, come il tipo di eventi da includere, eventuali filtri, e la frequenza di raccolta.



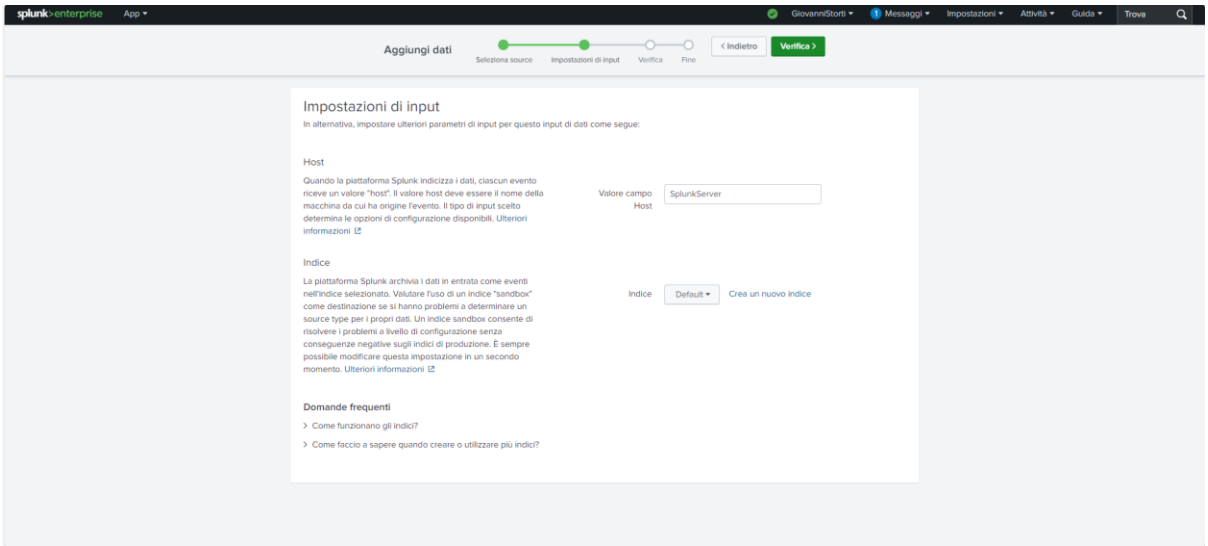
Passaggio 4: Impostazioni di input – configurazione base

Dopo aver selezionato la categoria **Security** nei log di eventi locali, Splunk mi porta alla schermata **“Impostazioni di input”**. Qui posso definire alcune proprietà fondamentali per il flusso dei dati.

Nella sezione **Host**, Splunk mi permette di assegnare un valore personalizzato al campo host, utile per identificare la provenienza degli eventi. Il campo è precompilato con **“Risposte”**, ma decido di **lasciare tutto invariato**, perché per ora va bene così.

Nella sezione **Indice**, è selezionato l’indice **Default**. Anche qui, non creo un nuovo indice: **Lascio l’impostazione predefinita**, così i dati verranno inseriti nell’indice standard di Splunk.

In basso ci sono alcune domande frequenti, ma in questa fase non mi servono. Procedo direttamente al prossimo step.



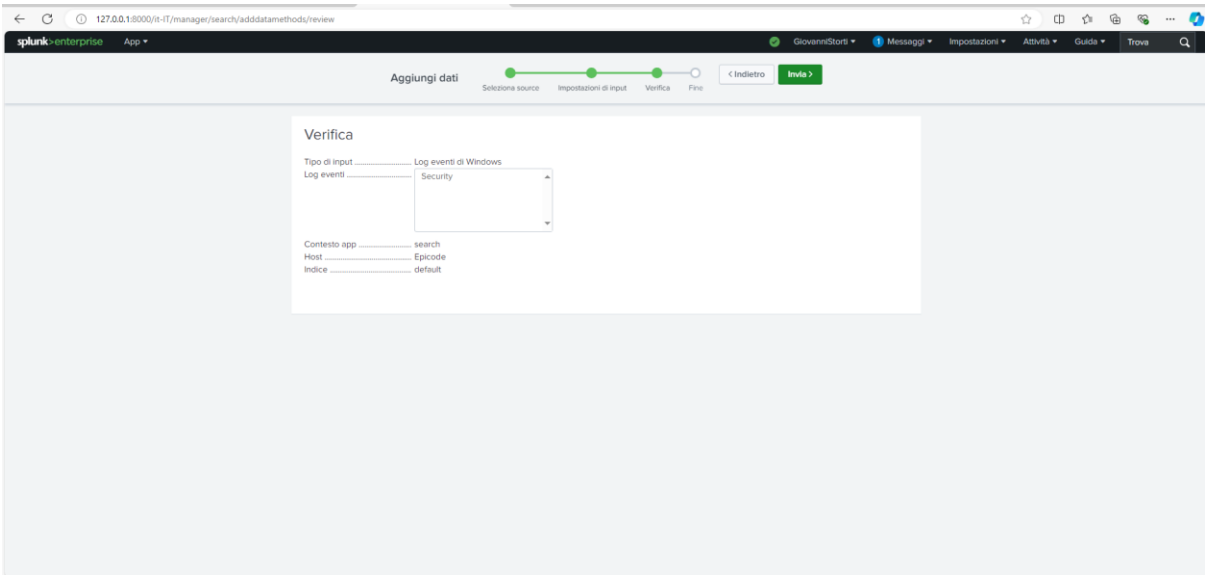
Passaggio 5: Revisione della configurazione

Sono arrivato alla fase di **“Rivedi”** nel processo di aggiunta dati su Splunk. Qui posso verificare che tutte le impostazioni siano corrette prima di completare.

Ecco il riepilogo della configurazione:

- **Tipo di input**: Log eventi di Windows
- **Categoria selezionata**: Security
- **Contesto app**: search
- **Indice**: main

Ho controllato tutto e confermo che le impostazioni sono quelle desiderate. Non ho apportato modifiche, quindi procedo cliccando su **“Completa”** per iniziare la raccolta dei dati.



Passaggio 6: Completamento dell'aggiunta dati e avvio della ricerca

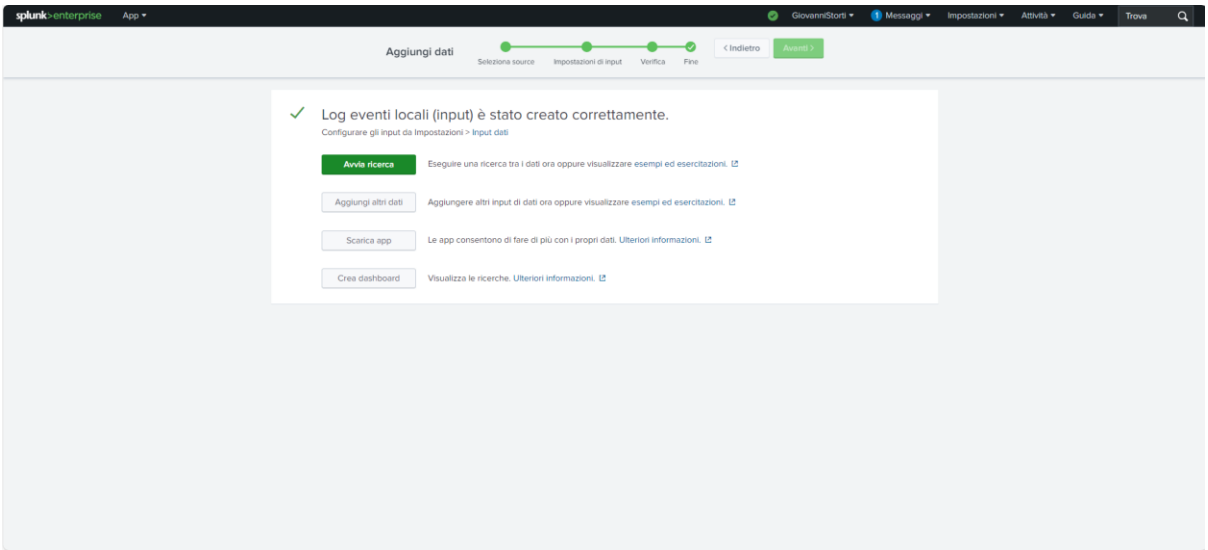
Dopo aver verificato tutte le impostazioni nella fase di revisione, Splunk mi conferma che l'input dei **log eventi locali – Security** è stato creato correttamente. Compare un messaggio con il simbolo di spunta verde:

"✓ Log eventi locali (input) è stato creato correttamente. Configura gli input che hai impostato in questo host."

A questo punto, scelgo di **cliccare su "Avvia Ricerca"** per iniziare subito ad analizzare i dati appena acquisiti. Splunk mi porta direttamente nell'interfaccia di ricerca, dove posso eseguire query e visualizzare gli eventi di sicurezza raccolti.

Questo mi permette di:

- Verificare che i dati stiano arrivando correttamente
- Esplorare i log per identificare attività rilevanti
- Iniziare a costruire visualizzazioni o alert personalizzati



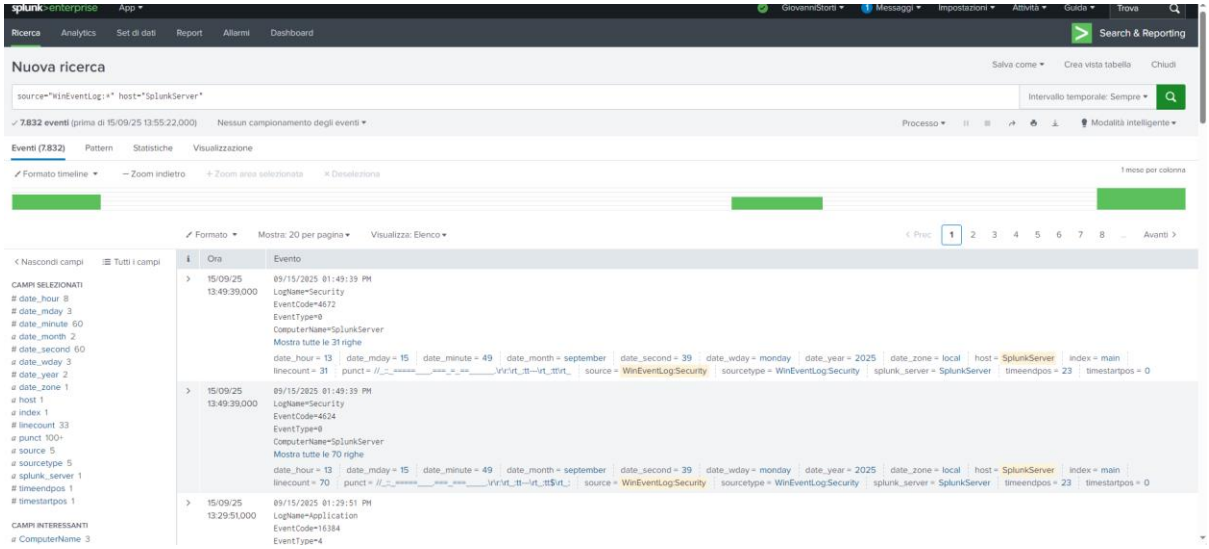
Fase finale: risultati della ricerca

Il programma ha eseguito una ricerca su Splunk utilizzando l'indice **"wineEventlog"** e l'host **"SplunkServer"**. Il risultato? Ho ottenuto **2.922 eventi** relativi ai **log di sistema Windows**, visualizzati in formato tabellare.

Ogni evento è dettagliato con informazioni come:

- **_time** (data e ora dell'evento)
- **EventCode** (codice identificativo, ad esempio 4624)
- **EventType** (tipo di evento, come *wineventlog*)
- **host** e **source** (macchina e origine del log)

Questa ricerca mi conferma che il flusso di dati è attivo e che Splunk sta correttamente raccogliendo e indicizzando i **log di sicurezza** come previsto.



Conclusione dell’esercizio

L’attività di oggi ha permesso di mettere in pratica la configurazione della modalità **Monitora** in Splunk, uno degli strumenti fondamentali per la raccolta e l’analisi continua dei dati. Attraverso la selezione dei log di eventi locali, in particolare quelli di **sicurezza**, lo studente ha seguito l’intero flusso: dalla scelta della sorgente, alla definizione delle impostazioni, fino alla verifica e alla ricerca dei dati acquisiti.

Gli screenshot realizzati documentano ogni fase del processo, dimostrando la corretta configurazione e l’effettiva ricezione degli eventi. Questo esercizio ha consolidato le competenze nell’utilizzo di Splunk per il monitoraggio in tempo reale, aprendo la strada a future analisi più avanzate e alla creazione di dashboard personalizzate.